Ιωάννης Μαυρίδης

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράμματα και Βοηθήματα
www.kallipos.gr

HEALLINK
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

ΙΩΑΝΝΗΣ ΜΑΥΡΙΔΗΣ
Αναπληρωτής Καθηγητής

Ασφάλεια Πληροφοριών στο Διαδίκτυο

Ασφάλεια Πληροφοριών στο Διαδίκτυο

Συγγραφή

Ιωάννης Μαυρίδης

Κριτικός αναγνώστης

Αντώνιος Γουγλίδης

Συντελεστές έκδοσης

Τεχνική Επεξεργασία: Σταύρος Σαλονικιάς, Νικόλαος Τσίγγανος

ISBN: 978-960-603-193-9

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ
Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

www.kallipos.gr

Πίνακας περιεχομένων

Πίνακας συντομεύσεων-ακρωνύμια

3DES	Triple-DES
ACL	Access control list
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AS	Autonomous System
CA	Certificate Authority
CBC	Cipher Block Chaining
CERT	Computer Emergency Response Team
CFB	Cipher FeedBack Mode
CRC	Cyclic Redundancy Check
CRHF	Collision-resistant hash functions
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
DES	Data Encryption Standard
DMZ	De-Militarized Zone
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECB	Electronic Codebook
ENISA	European Union for Network and Information Security
GRC	Governance – Risk – Compliance
HTTP	Hyper-Text Transfer Protocol
ICC	International Color Consortium
ICG	Inverse Congruence Generator
ICMP	Internet Control Messaging Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IoT	Internet of Things
ISMS	Information Security Management System
ISO	International Organization for Standardization
IV	Initialization Vector
JDBC	Java Database Connectivity
JRE	Java Runtime Environment
JSP	Java Server Pages
LAN	Local Area Network
LCG	Linear Congruence Generator
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MD5	Message-Digest algorithm 5
MDC	Message Detection Code
MSB	Most Significant Bit
MTA	Mail Transfer Agents
MUA	Mail User Agents
NAT/PAT	Network/Port Address Translation
NIC	Network Interface Controller
OFB	Output FeedBack Mode
OSI	Open Systems Interconnection Model
OUI	Organizationally Unique Identifier
OWHF	One-way hash functions
PAN	Personal Area Network
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
PoC	Point of Contact

QoS	Quality of Service
RA	Registration Authority
RFC	Request For Comments
RTS/CTS	Ready to Send / Clear to Send
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TERENA	Trans-European Research and Education Networking Association
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WSN	Wireless Sensor Network
WWW	World Wide Web
ΒΙΑ	Business impact analysis
ΔτΙ	Διαδίκτυο των Πραγμάτων
IP	Internet Protocol
ΠΣ	Πληροφοριακό Σύστημα
ΣΔΒΔ	Σύστημα Διαχείρισης Βάσεων Δεδομένων
ΥΔΗ	Υποδομή Δημοσίου Κλειδιού

Κεφάλαιο 1. Βασικές έννοιες και ζητήματα ασφάλειας

Σύνοψη
Η ασφάλεια των δεδομένων, καθώς αυτά μεταδίδονται μέσω των διαφόρων δικτύων υπολογιστών, αποτελεί κρίσιμο παράγοντα για την ανάπτυξη ηλεκτρονικών υπηρεσιών και την επιτυχή ενσωμάτωση των δικτυακών υποδομών στην καθημερινότητα των πολιτών. Όμως, το πρόβλημα της ασφάλειας πληροφοριών είναι σύνθετο. Έτσι, παρόλη την ανάπτυξη αποτελεσματικών τεχνικών και μηχανισμών προστασίας των μεταδιδόμενων δεδομένων, η ασφάλεια των διαδικτυακών εφαρμογών έρχεται να προσθέσει ακόμη μεγαλύτερη πολυπλοκότητα. Στο εισαγωγικό αυτό κεφάλαιο παρουσιάζονται οι βασικές έννοιες και ορισμοί της ασφάλειας πληροφοριών, προκειμένου να διευκολύνουν τη συζήτηση και την παρουσίαση των θεμάτων που πραγματεύονται τα επόμενα κεφάλαια του βιβλίου αυτού.

Προαπαιτούμενη γνώση
Για τη μελέτη του κεφαλαίου δεν απαιτούνται ειδικές γνώσεις.

1.1 Εισαγωγή

Όπως συμβαίνει γενικότερα στην πληροφορική, η πρωτότυπη ορολογία παράγεται με αγγλικούς συνήθως όρους. Έτσι, προσπαθώντας κανείς να αποδώσει στα αγγλικά τον ελληνικό όρο «ασφάλεια», μπορεί να συναντήσει αρκετές δυσκολίες στο να βρει διαφορές μεταξύ των όρων: secrecy, security, safety, insurance, assurance, dependability.

Η Ασφάλεια Πληροφοριών (Information Security) αποσκοπεί στην προστασία των πληροφοριών και των πόρων ενός πληροφοριακού συστήματος γενικότερα, από πιθανές ζημιές που μπορεί να προκαλέσουν μείωση της αξίας τους. Επιπλέον, αποσκοπεί στην παροχή αξιόπιστων πληροφοριών, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες όταν τις χρειάζονται. Μια πιο πρακτική θεώρηση της ασφάλειας πληροφοριών, με πολλές αναφορές στην καθημερινότητά μας, είναι ως μια διαδικασία που αποτελείται από τρία διακριτά βήματα:

Εικόνα 1.1 *Τα τρία (3) στάδια της ασφάλειας πληροφοριών.*

- **Πρόληψη** είναι η διαδικασία κατά την οποία λαμβάνονται μέτρα προστασίας για την αποφυγή συνεπειών από μη επιθυμητές ενέργειες.
- **Ανίχνευση** είναι η διαδικασία εντοπισμού ενεργειών και αναζήτησης γεγονότων και προσώπων που προκάλεσαν τις ενέργειες αυτές, καθώς και τις όποιες συνέπειές τους.
- **Αντίδραση** είναι η διαδικασία αποκατάστασης των πόρων που υπέστησαν ζημιά και αντιμετώπισης των επιθέσεων που βρίσκονται σε εξέλιξη.

Τα παραπάνω βήματα είναι κοινά σε διαφορετικά πεδία εφαρμογής, που είναι γνωστά από την καθημερινότητα. Για παράδειγμα, για την προστασία ενός εταιρικού χώρου, οι παραπάνω φάσεις θα μεταφράζονταν στις ενέργειες που αναφέρονται στον ακόλουθο Πίνακα 1.1:

ΠΡΟΛΗΨΗ	ΑΝΙΧΝΕΥΣΗ	ΑΝΤΙΔΡΑΣΗ
Προσθήκη κλειδαριάς	Απουσία εξοπλισμού	Κλήση αστυνομίας
Χτίσιμο φράκτη	Χρήση κλειστού κυκλώματος τηλεόρασης (CCTV)	Χρήση ασφαλιστικής κάλυψης
Κάγκελα στα παράθυρα	Σύστημα συναγερμού	Σύμβαση με εταιρεία φύλαξης

Πίνακας 1.1 *Ενέργειες για προστασία ενός εταιρικού χώρου.*

Στο χώρο των Τεχνολογιών Πληροφορίας και Επικοινωνιών (ΤΠΕ), τα πράγματα δεν είναι πολύ διαφορετικά. Για παράδειγμα, στο σύστημα ηλεκτρονικής βιβλιοθήκης ενός πανεπιστημίου, τα παραπάνω βήματα θα αφορούσαν ενέργειες ανάλογες αυτών που εμφανίζονται στον Πίνακα 1.2:

ΠΡΟΛΗΨΗ	ΑΝΙΧΝΕΥΣΗ	ΑΝΤΙΔΡΑΣΗ
Έλεγχος για κρυπτογραφημένη μετάδοση ευαίσθητων δεδομένων σύνδεσης στο υποσύστημα δανεισμού.	Εντοπισμός «περίεργων» εγγραφών στο υποσύστημα δανεισμού.	Αμφισβήτηση δανεισμών και αλλαγή διαπιστευτηρίων σύνδεσης (username και password).

Πίνακας 1.2 *Ενέργειες για προστασία ενός συστήματος ηλεκτρονικής βιβλιοθήκης.*

Αν και το παραπάνω παράδειγμα πιθανώς να είναι για τους περισσότερους οικείο, χρησιμοποιήθηκαν δύο όροι που είναι χρήσιμο να εξηγηθούν. Ο όρος ΤΠΕ και ο όρος Πληροφορία:

- **ΤΠΕ**: Οι τεχνολογίες αυτές προέκυψαν από τη σύγκλιση της πληροφορικής και των τηλεπικοινωνιών και πραγματεύονται μεθόδους και τεχνικές αποτελεσματικής αποθήκευσης, επεξεργασίας και μετάδοσης δεδομένων που κωδικοποιούν πληροφορίες.

- **Πληροφορία**: Σύμφωνα με το λεξικό Merriam-Webster, είναι η γνώση που επικοινωνείται ή λαμβάνεται.

Επίσης, όπως συμβαίνει και στο παράδειγμα της ηλεκτρονικής βιβλιοθήκης, στόχος της ασφάλειας είναι η προστασία των πληροφοριών. Γενικεύοντας το παράδειγμα, μπορούμε να πούμε ότι στους στόχους της ασφάλειας στις ΤΠΕ είναι:

- **Προστασία Υπολογιστικών Συστημάτων (Computer Security)**: Διαφύλαξη υπολογιστικών πόρων συστήματος από μη εξουσιοδοτημένη χρήση και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά την επεξεργασία και αποθήκευσή τους.

- **Προστασία Επικοινωνιών (Communication Security)**: Διαφύλαξη δικτυακών πόρων και προστασία δεδομένων από ακούσια ή σκόπιμη αποκάλυψη ή τροποποίηση ή διαγραφή κατά τη μετάδοσή τους μέσω δικτύων υπολογιστών.

Η διαφύλαξη των πόρων και η προστασία των δεδομένων δεν ορίζεται αόριστα, αλλά στην βάση των τριών (3) θεμελιωδών ιδιοτήτων της Ασφάλειας Πληροφοριών, που είναι:

- **Εμπιστευτικότητα (Confidentiality)**: αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη αποκάλυψή (ανάγνωση) της.

- **Ακεραιότητα (Integrity)**: αφορά την προστασία της πληροφορίας από μη εξουσιοδοτημένη μεταβολή (τροποποίηση ή διαγραφή) της.

- **Διαθεσιμότητα (Availability)**: αφορά τη διαφύλαξη της εξουσιοδοτημένης πρόσβασης (είτε για αποκάλυψη είτε για μεταβολή) στην πληροφορία, χωρίς εμπόδια ή καθυστέρηση.

Εκτός από τις παραπάνω βασικές ιδιότητες, η ασφάλεια στις ΤΠΕ συσχετίζεται με την επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών:

- **Αναγνώριση (Identification)**: αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας (π.χ. πελάτη) στο σύστημα (π.χ. εξυπηρετητή).

- **Αυθεντικοποίηση (Authentication)**: αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα.

- **Εξουσιοδότηση (Authorization)**: αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα, στη βάση των δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.

- **Αδυναμία αποποίησης (Non-Repudiation)**: αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα.

Η ασφάλεια αποτελεί (ή τουλάχιστον θα έπρεπε να αποτελεί) ένα σημαντικό μέλημα για κάθε έργο ΤΠΕ. Για να μπορέσουμε να κατανοήσουμε καλύτερα τα θέματα ασφάλειας που προκύπτουν στο σχεδιασμό, την υλοποίηση και τη συντήρηση πληροφοριακών συστημάτων, είναι βασικό να χρησιμοποιούνται σωστά οι σχετικοί βασικοί ορισμοί.

1.2 Βασικοί Ορισμοί Ασφάλειας

Για τη διευκόλυνση της παρουσίασης και συζήτησης των ζητημάτων ασφάλειας στις ΤΠΕ, είναι απαραίτητη η κατανόηση και χρήση ορισμένων βασικών όρων, οι οποίοι είναι ορίζονται στη συνέχεια:

- **Αγαθό (asset)** είναι κάθε αντικείμενο (όπως υπολογιστικός ή δικτυακός πόρος, δεδομένα) το οποίο έχει αξία (value) για τον ιδιοκτήτη (owner) του και για αυτό το λόγο πρέπει να προστατευτεί από πιθανή μείωση της αξίας του.

- Για να χρησιμοποιηθεί ένα αγαθό από ένα χρήστη (user), θα πρέπει προηγουμένως να πραγματοποιηθεί η εκχώρηση (grant) του προνομίου / δικαιώματος (privilege) πρόσβασης (access) σε αυτό. Η διαδικασία εκχώρησης ενός δικαιώματος πρόσβασης γίνεται είτε από τον ιδιοκτήτη του αντικειμένου είτε από άλλον χρήστη με δικαίωμα παραχώρησης (controller) είτε από το διαχειριστή του συστήματος.

- Ένα αγαθό μπορεί να εκτίθεται σε ένα **κίνδυνο (danger)**. Ο κίνδυνος αντιπροσωπεύει την αιτία για να περιοριστεί η αξία του αγαθού. Ο περιορισμός της αξίας του αγαθού ονομάζεται **ζημιά (harm).**

- Μια κατάσταση, όπου υπάρχει το ενδεχόμενο πρόκλησης απωλειών ή ζημιών, όπως υποκλοπή (interception) αγαθού, μεταβολή (modification) αγαθού, πλαστογραφία (fabrication) αγαθού ή διακοπή (interruption) της κανονικής λειτουργίας του συστήματος, αποτελεί μια **απειλή (threat)** για το σύστημα. Οι απειλές μπορούν να κατηγοριοποιηθούν ως εξής:

    - **Φυσικές απειλές**, είναι αυτές που προκύπτουν από τη φύση των συστημάτων ή από το περιβάλλον μέσα στο οποίο αναπτύσσονται και λειτουργούν.

- **Εκούσιες απειλές**, είναι αυτές που προκύπτουν από εσκεμμένες κακόβουλες ενέργειες των χρηστών.

- **Ακούσιες απειλές**, είναι αυτές που προκύπτουν από λανθασμένες (ακούσιες) ενέργειες των χρηστών.

- Οι ζημίες προκαλούνται μετά από **επιθέσεις (attack)**. Μια επίθεση προκαλείται ως αποτέλεσμα της εκμετάλλευσης μιας ή περισσότερων ευπαθειών του συστήματος. Μια **ευπάθεια (vulnerability)** μπορεί να αφορά μια αδυναμία στις ρυθμίσεις ή τη διαχείριση του συστήματος ή ένα ευάλωτο σημείο σε ένα υποσύστημα ασφάλειας. Ορισμένες κατηγορίες και χαρακτηριστικά παραδείγματα ευπαθειών είναι:

    - **Ανθρώπινες Ευπάθειες (Human)**: αποτελούν την κρισιμότερη κατηγορία για την ασφάλεια ενός Πληροφοριακού Συστήματος (ΠΣ) και μπορεί να προκαλέσουν τις χειρότερες επιπτώσεις, καθώς προέρχονται εκ των έσω (insiders), δηλαδή από νόμιμους χρήστες που γνωρίζουν καλά το σύστημα και τους μηχανισμούς ασφάλειας.

    - **Ευπάθειες Υλικού και Λογισμικού**: αφορούν προβληματική κατασκευή, καθώς και λανθασμένες ρυθμίσεις και δυσλειτουργίες του υλικού (hardware) και του λογισμικού (software).

    - **Ευπάθειες Μέσων (Media):** αφορούν προβληματικές διαδικασίες διαχείρισης που μπορεί να οδηγήσουν σε κλοπή ή καταστροφή μαγνητικών, οπτικών ή έντυπων μέσων αποθήκευσης δεδομένων.

    - **Ευπάθειες Επικοινωνιών (Communications)**: αφορούν κατασκευαστικές αδυναμίες, λανθασμένες ρυθμίσεις, καθώς και δυσλειτουργίες των δικτυακών συνδέσεων.

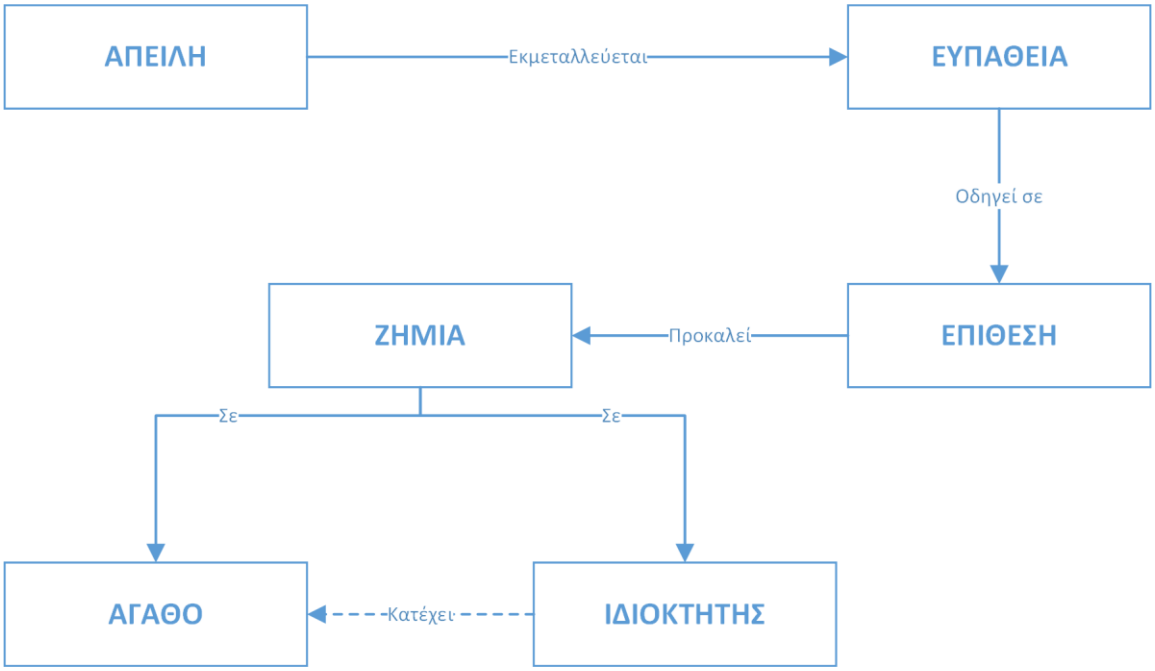
    - **Φυσικές Ευπάθειες (Physical)**: αφορούν το φυσικό χώρο όπου αναπτύσσονται και λειτουργούν τα συστήματα (π.χ. datacenters).

    - **Εκ φύσεως Ευπάθειες (Natural)**: αφορούν φυσικά φαινόμενα (π.χ. φυσικές καταστροφές), περιβαλλοντικές εξαρτήσεις κ.ά.

- Οι **επιπτώσεις (impacts)** που μπορεί να προκαλέσει μια επιτυχημένη επίθεση, αφορούν κυρίως τη μείωση της αξίας των αγαθών ή/και τη πρόκληση προσωρινής δυσλειτουργίας ή διακοπής της λειτουργίας του συστήματος.

Η αντιμετώπιση των απειλών επιτυγχάνεται με μέτρα προστασίας (controls) ή **αντίμετρα (countermeasures)**, τα οποία συνίστανται σε προληπτικά κυρίως μέτρα (π.χ. πράξη, συσκευή, διαδικασία ή μέθοδος) τεχνικής και διαχειριστικής φύσης που αποσκοπούν στη μείωση ή εξάλειψη των γνωστών ευπαθειών του συστήματος. Η απόκτηση και εφαρμογή των μέτρων προστασίας συνεπάγεται ένα πρόσθετο **κόστος (cost)** λειτουργίας του οικείου οργανισμού.

Ορισμένες από τους παραπάνω βασικές έννοιες συσχετίζονται, όπως παρουσιάζεται στην επόμενη Εικόνα 1.2:



Εικόνα 1.2 *Συσχέτιση βασικών εννοιών.*

Σύμφωνα με τα παραπάνω, μπορούμε να ορίσουμε ως γενικότερο στόχο της ασφάλειας πληροφοριών τον καθορισμό μιας επιθυμητής ισορροπίας (συνήθως στη βάση μιας εμπεριστατωμένης μελέτης) μεταξύ του κόστους των μέτρων προστασίας και της ζημιάς που ενδέχεται να υποστούν τα αγαθά του οργανισμού σε πιθανές περιπτώσεις επιτυχών επιθέσεων.

1.3 Ζητήματα Ασφάλειας στο Διαδίκτυο

Ένα δίκτυο αποτελείται από ένα σύνολο διασυνδεδεμένων υπολογιστικών κόμβων οι οποίοι έχουν τη δυνατότητα να ανταλλάσσουν μεταξύ τους πληροφορίες, καθώς και τους συνδέσμους μέσω των οποίων διακινούνται οι πληροφορίες αυτές. Ένα δίκτυο υλοποιείται με σκοπό να παρέχει στους χρήστες του τη δυνατότητα να αποκτήσουν δυνατότητα διαμοιρασμένης πρόσβασης σε δεδομένα, λογισμικό, συσκευές κ.ά.

Η διασύνδεση δύο ή περισσότερων, πιθανότατα ανομοιογενών δικτύων, με σκοπό τη μεταξύ τους επικοινωνία και τη συνολική λειτουργία τους ως ένα λογικό δίκτυο, υλοποιεί το Διαδίκτυο (Internet). Το Διαδίκτυο σχεδιάστηκε αρχικά για το υπουργείο άμυνας των ΗΠΑ (δεκαετία του 1960), έχοντας ως σκοπό τη δημιουργία ενός δικτύου μεταγωγής πακέτων που θα μπορεί να λειτουργεί ακόμη και σε περίπτωση ύπαρξης κατεστραμμένων κόμβων ή συνδέσεων, υποστηρίζοντας πολλές εναλλακτικές διαδρομές. Από τότε, μεσολάβησε η λειτουργία του ARPANET που τη διασύνδεση ακαδημαϊκών ιδρυμάτων. Σήμερα, το Διαδίκτυο έχει καταφέρει να αποτελέσει ένα παγκόσμιο και χαμηλού κόστους ομοιογενές μέσο για τη διακίνηση πληροφοριών και την παροχή υπηρεσιών, στις οποίες περιλαμβάνονται και εφαρμογές που παρέχουν διακίνηση ευαίσθητων δεδομένων, όπως τραπεζικές συναλλαγές, ηλεκτρονικό εμπόριο και εφαρμογές τηλεϊατρικής, για τις οποίες η ασφάλεια πληροφοριών αποτελεί μείζον ζήτημα.

Κατά τη σχεδίαση του Διαδικτύου, μέχρι και την έκδοση 4 του πρωτοκόλλου IP (Internet Protocol version 4), η ασφάλεια δεν αποτελούσε ένα από τα χαρακτηριστικά που λήφθηκαν υπόψη κατά το σχεδιασμό του, καθώς βασικός στόχος ήταν η ανθεκτική λειτουργικότητά του και η ευκολία πρόσβασης σε αυτό. Ως αποτέλεσμα, δεν υπήρξαν εγγενείς μηχανισμοί προστασίας των επικοινωνιών, ενώ ούτε ακόμη υπάρχει ένας γενικός μηχανισμός για την επιβολή μιας πολιτικής ελέγχου προσπέλασης, καθώς και ρυθμίσεων διαμόρφωσης. Έτσι, σε κάθε υλοποίηση με το πρωτόκολλο IPv4, οι μηχανισμοί ασφάλειας θα πρέπει να εφαρμόζονται ως ένα επιπρόσθετο συστατικό. Στην αδυναμία διαμόρφωσης μιας ενιαίας πολιτικής ασφάλειας και διαχείρισης, συμβάλλει και η ετερογένεια των διασυνδεδεμένων δικτύων, καθώς και η φύση της υπόστασης του Διαδικτύου που θα πρέπει να μην εξαρτά τη λειτουργία του από ένα ή περισσότερα κέντρα διαχείρισης και ελέγχου.

Μερικά από τα βασικά ζητήματα ασφάλειας του Διαδικτύου, αφορούν την αντιμετώπιση επιθέσεων, όπως:

- **Πλαστοπροσωπία (masquerading)**: Συμβαίνει όταν ένας μη εξουσιοδοτημένος χρήστης προσπαθεί μέσω αντιποίησης ταυτότητας να ξεγελάσει το σύστημα ελέγχου πρόσβασης και να χρησιμοποιήσει πόρους του συστήματος ως να ήταν κάποιος άλλος νόμιμα εξουσιοδοτημένος χρήστης.

- **Παθητική παρακολούθηση (passive tapping)**: Συμβαίνει όταν ο επιτιθέμενος αποκτά πρόσβαση στη διακίνηση δεδομένων και τα καταγράφει, π.χ. με σκοπό τη μετέπειτα ανάλυσή τους.

- **Ενεργή παρακολούθηση (active tapping)**: Συμβαίνει όταν ο επιτιθέμενος αποκτά πρόσβαση στη διακίνηση δεδομένων και είτε τα τροποποιεί είτε εισάγει δικά του πλαστά δεδομένα.

- **Αποποίηση (repudiation)**: Συμβαίνει όταν μια νόμιμα εξουσιοδοτημένη οντότητα αποποιείται τη συμμετοχή της σε μια ενέργεια (π.χ. αποστολή ενός μηνύματος) στο σύστημα.

- **Άρνηση Εξυπηρέτησης (denial of service)**: Συμβαίνει όταν ο επιτιθέμενος προκαλεί υπερβολική κατανάλωση ή δέσμευση πόρων προκειμένου να παρεμποδίσει την ομαλή λειτουργία συστήματος.

- **Επανεκπομπή μηνυμάτων (replay)**: Συμβαίνει όταν ο επιτιθέμενος συνδυάζει παθητική παρακολούθηση με καταγραφή μηνυμάτων και μεταγενέστερη επανεκπομπή (playback) τους (π.χ. κρυπτογραφημένα συνθηματικά).

- **Ανάλυση επικοινωνίας (traffic analysis)**: Πρόκειται για μορφή παθητικής παρακολούθησης (ακόμη και κρυπτογραφημένων δεδομένων), με σκοπό την ανάλυση της κυκλοφορίας / διακίνησης δεδομένων και την έμμεση εξαγωγή συμπερασμάτων που μπορεί να οδηγήσει σε χρήσιμες αποκαλύψεις για επόμενη επίθεση.

- **Κακόβουλο λογισμικό (viruses, Trojan horses, worms)**: Λογισμικό του οποίου ο επιτιθέμενος επιδιώκει την εκτέλεση από νόμιμα εξουσιοδοτημένες οντότητες με σκοπό την εξαπόλυση πρόσθετων επιμέρους επιθέσεων.

Η αντιμετώπιση των παραπάνω ζητημάτων αποτελεί απαραίτητη προϋπόθεση για την ανάπτυξη των διαφόρων υπηρεσιών Διαδικτύου και την αποδοχή τους από τους τελικούς χρήστες, όπως για παράδειγμα η ανάπτυξη του ηλεκτρονικού εμπορίου και γενικότερα του ηλεκτρονικού επιχειρείν. Σε διαφορετική περίπτωση, είναι πιθανόν να προκληθούν συνέπειες, όπως:

- **Αποκάλυψη πληροφοριών**: Προκαλείται από την απώλεια της εμπιστευτικότητας της πληροφορίας και έχει ως αποτέλεσμα την αποκάλυψη μέρους ή του συνόλου της διαβαθμισμένης ή ευαίσθητης πληροφορίας που τηρείται σε ένα Π.Σ.

- **Αλλοίωση πληροφοριών:** Προκαλείται από την απώλεια της ακεραιότητας της πληροφορίας που προκύπτει από τη μη εξουσιοδοτημένη εισαγωγή, τροποποίηση ή διαγραφή τμήματος ή του συνόλου της πληροφορίας που τηρείται σε ένα Π.Σ.

- **Άρνηση Εξυπηρέτησης**: Στις διαδικτυακές υπηρεσίες η άρνηση εξυπηρέτησης που παρουσιάζεται είτε ως ολική αδυναμία εξυπηρέτησης είτε ως αλλοίωση των ποιοτικών στοιχείων της (όπως ο χρόνος απόκρισης) προκαλεί την απώλεια της διαθεσιμότητας του συστήματος στους νόμιμους χρήστες του. Όταν ένα σύστημα ή μια υπηρεσία είναι μη διαθέσιμη, προκαλείται αύξηση του κόστους λειτουργίας, που παρουσιάζεται ως άμεση

απώλεια κερδών από την αδυναμία χρήσης της υπηρεσίας ή ως έμμεση απώλεια από προσφυγή των χρηστών σε ανταγωνιστικές υπηρεσίες.

- **Δυσφήμηση**: Το Διαδίκτυο αποτελεί ένα ιδιαίτερα ανταγωνιστικό περιβάλλον, όπου η φήμη μιας υπηρεσίας αποτελεί ένα από τα βασικά κριτήρια επιλογής της. Τα συμβάντα (αν)ασφαλείας σε αυτό το νέο μέσο κοινοποιούνται γρήγορα και προκαλούν αρνητική φήμη (δυσφήμηση) και απώλεια δυνητικών ή παρόντων χρηστών.

- **Κόστος**: Ήδη αναφέρθηκε πώς προκύπτει το κόστος στην περίπτωση της άρνησης εξυπηρέτησης. Επιπροσθέτως, όμως, κάθε συνέπεια ενός συμβάντος ασφάλειας συμμετέχει στην αύξηση του κόστους είτε μέσω της δυσφήμησης είτε μέσω των ενεργειών για την αποκατάσταση της ζημιάς και την εφαρμογή αντιμέτρων, είτε μέσω ποινών που μπορεί να επιβληθούν από αρχές, όπως τα δικαστήρια.

Οι συνέπειες που αναφέρονται παραπάνω είναι αρκετές για να καταδείξουν τη σημασία της Ασφάλειας Πληροφοριών στο Διαδίκτυο. Η αποφυγή των συνεπειών προϋποθέτει την κατανόηση και υλοποίηση μεθοδολογιών και τεχνολογιών που μπορούν να διασφαλίσουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών.

1.4 Διάρθρωση του Εγχειριδίου

Αφού ορίστηκαν αρκετές από τις βασικές έννοιες που είναι απαραίτητες για την εισαγωγή στην Ασφάλεια Πληροφοριών στο Διαδίκτυο, ακολουθεί το Κεφάλαιο 2 όπου γίνεται μια επισκόπηση των τεχνολογιών δικτύων στις οποίες βασίζει τη λειτουργία του το Διαδίκτυο.

Στο επόμενο Κεφάλαιο 3, παρουσιάζονται κλασσικές τεχνολογίες ασφάλειας στην περίμετρο των δικτύων, όπως τα τείχη προστασίας (firewalls) και τα συστήματα ανίχνευσης εισβολών (IDS), ενώ γίνεται μια σύντομη παρουσίαση των ζητημάτων ασφάλειας των ασύρματων δικτύων.

Ένας κυρίαρχος τομέας υπηρεσιών στο Διαδίκτυο, είναι αυτός των διαδικτυακών εφαρμογών (Web applications). Στα Κεφάλαια 4 και 5, εξετάζονται οι εφαρμογές αυτές ως προς την αρχιτεκτονική τους, τα θέματα ασφάλειας που αντιμετωπίζουν, καθώς και ως προς το βέλτιστο τρόπο ανάπτυξης και χρήσης τους.

Η κρυπτογραφία αποτελεί τη βασική τεχνική διασφάλισης της εμπιστευτικότητας των δεδομένων, όταν αυτά μεταδίδονται μέσω των δικτυακών συνδέσεων, ενσύρματων και ασύρματων. Στο κεφάλαιο 6, εξετάζονται βασικές αρχές της κρυπτογραφίας και της στεγανογραφίας. Ακόμη, γίνεται παρουσίαση βασικών και προαπαιτούμενων εννοιών από τη θεωρία πληροφοριών, ώστε στο κεφάλαιο 7 να γίνει αναφορά σε διαδεδομένα σύγχρονα κρυπτογραφικά κρυπτοσυστήματα και αλγορίθμους, καθώς και σε ζητήματα ανθεκτικότητάς τους με την εφαρμογή κρυπταναλυτικών τεχνικών.

Στη συνέχεια, το Κεφάλαιο 8 ασχολείται με την ακεραιότητα μηνυμάτων και τις συναρτήσεις κατακερματισμού, εξετάζοντας επιπλέον ζητήματα αυθεντικότητας προέλευσης και μηνυμάτων, ενώ στο Κεφάλαιο 9 επιχειρείται η αξιοποίηση των παραπάνω κρυπτογραφικών τεχνικών για τη δημιουργία ψηφιακών υπογραφών και την αντιμετώπιση του προβλήματος πιστοποιημένης αντιστοίχισης δημόσιου κλειδιού και της ταυτότητας του κατόχου του με τη χρήση ψηφιακών πιστοποιητικών και τη διαχείρισή τους στο πλαίσιο υποδομών δημοσίου κλειδιού (PKI).

Το Κεφάλαιο 10, αξιοποιεί τις γνώσεις των προηγούμενων κεφαλαίων για να παρουσιάσει τον τρόπο ασφαλούς μετάδοσης δεδομένων μέσω ανασφαλών δημοσίων δικτύων δεδομένων με την εγκατάσταση και λειτουργία εικονικών ιδιωτικών δικτύων (VPN) με διάφορους τρόπους λειτουργίας.

Στο Κεφάλαιο 11, γίνεται μια εκτενής αναφορά σε ζητήματα, πρότυπα και καλές πρακτικές διαχείρισης της ασφάλειας, ιδιαίτερα σε ότι αφορά δικτυακά περιβάλλοντα και υπηρεσίες.

Η κατάλληλη καταγραφή και απόκριση σε συμβάντα (αν)ασφάλειας, σε συνδυασμό με την αξιοποίηση τεχνικών ηλεκτρονικής εγκληματολογίας (digital forensics) για μια εις βάθος διερεύνηση του κάθε συμβάντος, με σκοπό τη συλλογή και επεξεργασία πληροφοριών που θα οδηγήσουν στον εντοπισμό των απαραίτητων πειστηρίων, τα οποία θα βοηθήσουν στην πλήρη διαλεύκανση και την ανίχνευση όλων των παραγόντων μιας επίθεσης (ταυτότητα επιτιθέμενου, ζημία που δημιουργήθηκε, συνολικός αντίκτυπος της επίθεσης, κ.ά.), παρουσιάζονται στο Κεφάλαιο 12.

Τέλος, στο Κεφάλαιο 13, γίνεται περιγραφή των ζητημάτων ιδιωτικότητας και των τρόπων αντιμετώπισης περιστατικών επιθέσεων που πραγματοποιούνται με τη χρήση ηλεκτρονικών μορφών επικοινωνίας και των φαινομένων ηλεκτρονικού εγκλήματος που απασχολούν την παγκόσμια κοινότητα.

Βιβλιογραφία

Πάγκαλου Γ., Μαυρίδη Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ. (2004). Ασφάλεια Πληροφοριακών Συστημάτων. Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Κριτήρια Αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Οι τρείς θεμελιώδεις ιδιότητες της ασφάλειας είναι:
α) Η ακεραιότητα, η ιδιωτικότητα και η διασφάλιση.
β) Η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα.
γ) Η εμπιστευτικότητα, η διαχειρισιμότητα και η μη-απάρνηση.
δ) Τα αγαθά, οι απειλές και οι ευπάθειες.

2. Ένα αγαθό:
α) Έχει αξία.
β) Έχει ευπάθειες.
γ) Είναι ασφαλές.
δ) Είναι υπολογιστικός πόρος.

3. Τα αντίμετρα:
α) Εφαρμόζονται μόνο μετά από μια επιτυχημένη επίθεση.
β) Εφαρμόζονται μόνο μετά από μια αποτυχημένη επίθεση.
γ) Είναι αντίποινα προς τον επιτιθέμενο.
δ) Στοχεύουν στη μείωση των ευπαθειών.

4. Το ακρωνύμιο ΤΠΕ:
α) Σημαίνει: τεχνολογίες πληροφορικής και επικοινωνιών.
β) Σημαίνει: τεχνολογίες πληροφορίας και επικοινωνιών.
γ) Σημαίνει: τεχνικές πληροφορίας και επικοινωνιών.
δ) Σημαίνει: τεχνολογίες πληροφορικής και επικοινωνιών.

5. Μία επίθεση εκμεταλλεύεται:
α) Ένα αντίμετρο.
β) Μια ευπάθεια.
γ) Έναν κίνδυνο.
δ) Κανένα από τα παραπάνω.

6. Οι απειλές:
α) Δημιουργούνται πάντα από εκούσιες ενέργειες.
β) Εκμεταλλεύονται ευπάθειες.
γ) Οδηγούν πάντα σε ζημιά.
δ) Δε μπορούν να αντιμετωπιστούν.

7. Ο όρος ασφάλεια στις ΤΠΕ μεταφράζει τον όρο:
α) Security.
β) Assurance.
γ) Insurance.
δ) Police.

8. Η αποκάλυψη πληροφοριών στοχεύει στην παραβίαση της:
α) Εμπιστευτικότητας.
β) Ακεραιότητας.
γ) Διαθεσιμότητας.
δ) Αυθεντικότητας

9. Η άρνηση-εξυπηρέτησης στοχεύει στην παραβίαση της:
α) Εμπιστευτικότητας.
β) Ακεραιότητας.
γ) Διαθεσιμότητας.
δ) Αυθεντικότητας

10. Η αλλοίωση πληροφοριών στοχεύει στην παραβίαση της:
α) Εμπιστευτικότητας.
β) Ακεραιότητας.
γ) Διαθεσιμότητας.
δ) Αυθεντικότητας

Κεφάλαιο 2. Δίκτυα και Διαδίκτυο

Σύνοψη
Σκοπός του κεφαλαίου είναι η εισαγωγή σε βασικές έννοιες δικτύωσης και σχετικών τεχνολογιών, καθώς και η αναφορά σε επιθέσεις ασφαλείας κατά επίπεδο μελέτης των δικτύων υπολογιστών. Στόχος είναι η διαμόρφωση της απαραίτητης θεωρητικής θεμελίωσης για τα δίκτυα υπολογιστών και το διαδίκτυο, έτσι ώστε να διευκολύνεται στη συνέχεια η κατανόηση των εννοιών που θα αναλυθούν στα επόμενα κεφάλαια του παρόντος βιβλίου.

Προαπαιτούμενη γνώση
Για την παρακολούθηση του κεφαλαίου απαιτούνται απλές γνώσεις δικτύων υπολογιστών.

2.1 Εισαγωγή

Στα σημερινά πληροφοριακά συστήματα, πολύ σπάνια θα συναντήσουμε αυτόνομα υπολογιστικά συστήματα, δηλαδή συστήματα που λειτουργούν απομονωμένα και χωρίς να επικοινωνούν με άλλα. Συνήθως, συναντούμε ομάδες συστημάτων οι οποίες διασυνδέονται με σκοπό π.χ. τη συνεργατική επεξεργασία ή το διαμοιρασμό πληροφοριών. Μια διασυνδεδεμένη ομάδα υπολογιστικών συστημάτων ονομάζεται δίκτυο. Τα βασικά συστατικά ενός δικτύου υπολογιστών είναι:

- Υπολογιστικές συσκευές (υπολογιστές, εκτυπωτές, δρομολογητές κλπ.) ως κόμβοι.
- Γραμμές μεταφοράς δεδομένων μεταξύ των κόμβων.
- Λογισμικό και πρωτόκολλα δικτύωσης.

Τα δίκτυα υπολογιστών αποτελούν πλέον αναπόσπαστο κομμάτι της καθημερινής δραστηριότητας. Σκοπός του κεφαλαίου αυτού δεν είναι η εμβάθυνση σε θέματα δικτύων υπολογιστών, αλλά η παρουσίαση των βασικών στοιχείων και πρωτοκόλλων που απαρτίζουν το Διαδίκτυο (Internet), καθώς και η παρουσίαση νέων τάσεων και τεχνολογιών, έτσι ώστε στη συνέχεια να είναι δυνατή η μελέτη θεμάτων ασφάλειας πληροφοριών στο Διαδίκτυο.

Ο πιο συχνός διαχωρισμός των δικτύων γίνεται με βάση της διασποράς των συστημάτων στο χώρο, καθώς και του ιδιαίτερου ρόλου που καλούνται να επιτελέσουν. Έτσι, μπορούμε να διακρίνουμε τις παρακάτω κατηγορίες δικτύων υπολογιστών:

- Δίκτυα Τοπικής Περιοχής (Local Area Networks - LAN).
- Δίκτυα Ευρείας Περιοχής (Wide Area Networks - WAN).
- Μητροπολιτικά Δίκτυα (Metropolitan Area Networks - MAN).
- Δίκτυα Προσωπικής Περιοχής (Personal Area Networks - PAN).

2.1.1 Δίκτυα Τοπικής Περιοχής

Η πιο απλή μορφή δικτύου, που συναντάμε καθημερινά, είναι τα δίκτυα υπολογιστών τα οποία βρίσκονται σε έναν ενιαίο διαχειριστικά χώρο, όπως τα οικιακά δίκτυα ή τα δίκτυα σε μικρές ή μεσαίες επιχειρήσεις. Τα βασικά συστατικά των δικτύων αυτών είναι υπολογιστές και διακομιστές, μεταγωγείς, ασύρματα σημεία πρόσβασης και συνήθως ένας δρομολογητής που αναλαμβάνει τη διασύνδεσή τους με απομακρυσμένα δίκτυα. Η διασύνδεση των στοιχείων αυτών γίνεται με συνδέσμους υψηλής διαμεταγωγικής ικανότητας, όπως καλώδια UTP ή οπτικές ίνες.

2.1.2 Δίκτυα Ευρείας Περιοχής

Τα δίκτυα ευρείας περιοχής, συνήθως, αποτελούνται από διασυνδεδεμένα τοπικά δίκτυα, τα οποία βρίσκονται διασπαρμένα σε μια μεγάλη γεωγραφική περιοχή. Η σύνδεση των δικτύων αυτών μεταξύ τους γίνεται συνήθως

με μη-ιδιόκτητες, χαμηλότερης διαμεταγωγικής ικανότητας γραμμές, που ανήκουν σε κάποιο πάροχο υπηρεσιών δικτύωσης. Οι γραμμές αυτές παρουσιάζουν συνήθως υψηλό κόστος, κάτι που αποτελεί περιοριστικό παράγοντα για την ανάπτυξή τους.

2.1.3 Μητροπολιτικά Δίκτυα

Ένα μητροπολιτικό δίκτυο αποτελείται από ένα σύνολο δικτύων στα στενά πλαίσια της γεωγραφικής έκτασης κτιρίων ενός οργανισμού (campus) ή μιας κοινότητας (π.χ. ενός δήμου). Συνήθως, η γεωγραφική διασπορά δεν είναι μεγάλη και η διασύνδεση των τοπικών δικτύων γίνεται με ιδιωτικές ασύρματες ή ενσύρματες ζεύξεις.

2.1.4 Δίκτυα Προσωπικής Περιοχής

Η ανάπτυξη των σύγχρονων προσωπικών ψηφιακών βοηθών (personal assistant), δηλαδή φορητών υπολογιστικών συσκευών με δυνατότητες δικτύωσης (π.χ. smartphones, smart watches κλπ.), έχουν οδηγήσει στον ορισμό μιας νέας κατηγορίας δικτύων που εκτείνονται γύρω από το πρόσωπο, το οποίο και ακολουθούν καθώς κινείται. Στα δίκτυα προσωπικής περιοχής, οι συμμετέχουσες συσκευές διασυνδέονται με χαμηλής ισχύος ασύρματες ζεύξεις (π.χ. Bluetooth).

2.2 Διαστρωμάτωση

Ένα δίκτυο αποτελείται από ένα πλήθος κόμβων, οι οποίοι πρέπει να μπορούν να επικοινωνούν μεταξύ τους. Όπως στην ανθρώπινη επικοινωνία, για να μπορέσουν δυο άνθρωποι να συνεννοηθούν, πρέπει να μιλούν την ίδια γλώσσα και να ακολουθούν συγκεκριμένους κανόνες επικοινωνίας, έτσι και στην επικοινωνία μεταξύ των κόμβων ενός δικτύου υπολογιστών, πρέπει να ακολουθούνται συγκεκριμένοι κανόνες που καθορίζονται από τα πρωτόκολλα επικοινωνίας.

Για την διευκόλυνση της μελέτης ενός δικτύου και την καλύτερη σχεδίασή του, μπορούμε να οργανώσουμε τα πρωτόκολλα επικοινωνίας σε επίπεδα. Έτσι, με τη χρήση των πρωτοκόλλων του κάθε επιπέδου επιτελούνται συγκεκριμένες λειτουργίες, με σκοπό να παρέχονται επιμέρους υπηρεσίες στο αμέσως επόμενο επίπεδο.

Το πιο γνωστό μοντέλο οργάνωσης πρωτοκόλλων επικοινωνίας είναι το Μοντέλο Διεπαφής Ανοικτών Συστημάτων (Open Systems Interconnection Model – OSI Model) ISO/IEC 7498-1, το οποίο διαμορφώθηκε από το Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization) με την τελευταία αναθεώρησή του το 1994. Το μοντέλο αυτό περιγράφει επτά (7) επίπεδα οργάνωσης πρωτοκόλλων και η πληρότητά του το αναγάγει σε μοντέλο αναφοράς (Reference Model).

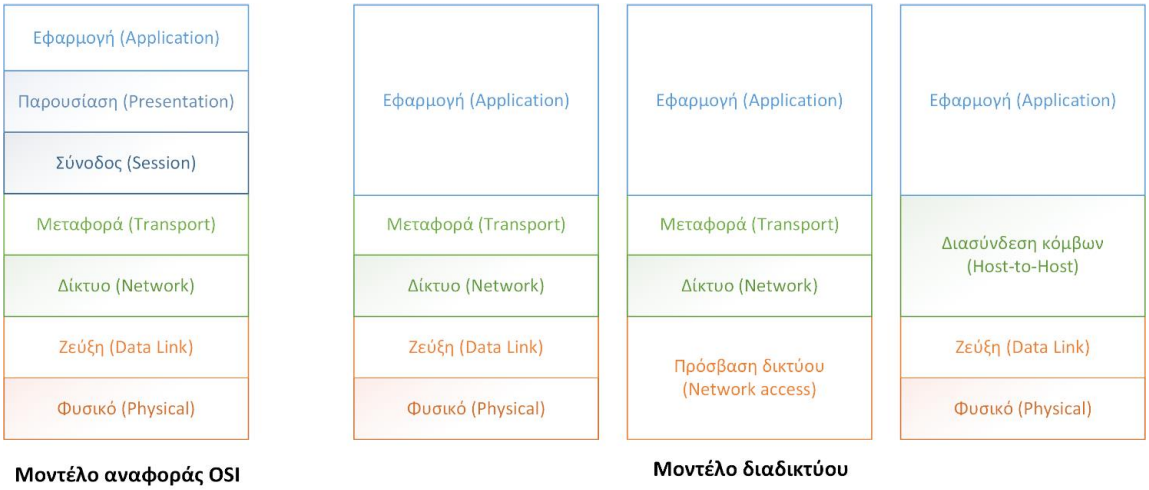
Τα πρωτόκολλα των σύγχρονων TCP/IP δικτύων ακολουθούν το Μοντέλο αναφοράς του Διαδικτύου (Internet Model), το οποίο διακρίνει λιγότερα επίπεδα από το Μοντέλο OSI, όπως φαίνεται στην εικόνα 2.1. Συγκεκριμένα, στη διεθνή βιβλιογραφία αναφέρονται από 3 ως 5 επίπεδα στις διάφορες εκδοχές του Μοντέλου του Διαδικτύου, με συνηθέστερο αυτό των τεσσάρων (4) επιπέδων, τα οποία είναι:

- Το επίπεδο **εφαρμογής**, που περιλαμβάνει πρωτόκολλα που καθορίζουν την επικοινωνία μεταξύ των εφαρμογών λογισμικού.

- Το επίπεδο **μεταφοράς**, που περιλαμβάνει πρωτόκολλα που καθορίζουν την από άκρο σε άκρο (end-to-end) επικοινωνία μεταξύ διεργασιών δυο κόμβων.

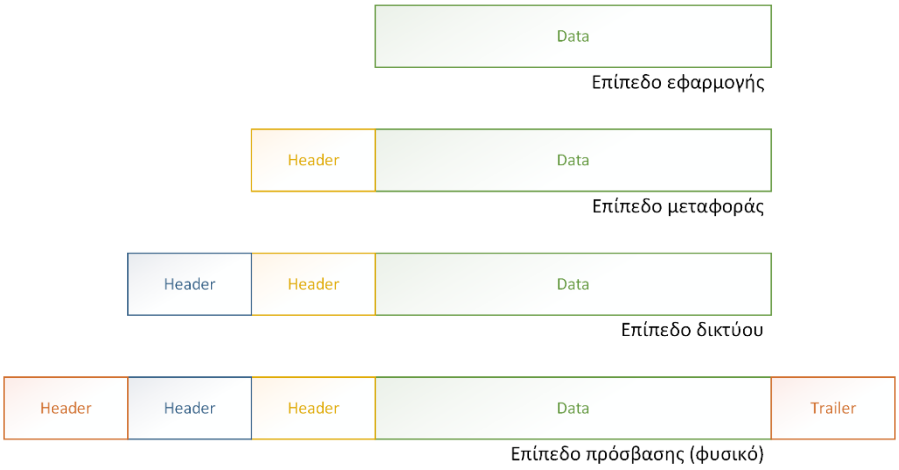
- Το επίπεδο **δικτύου**, που περιλαμβάνει πρωτόκολλα που καθορίζουν τη διευθυνσιοδότηση των κόμβων, με τη χρήση του ιεραρχικού σχήματος διευθύνσεων IP, αλλά και τη δρομολόγηση και προώθηση πακέτων (packets) μεταξύ δικτύων.

- Το επίπεδο **πρόσβασης δικτύου**, που περιλαμβάνει πρωτόκολλα που καθορίζουν την πρόσβαση στο φυσικό μέσο και τη διακίνηση πλαισίων (frames) σε ένα σύνδεσμο.



Εικόνα 2.1 *Τα μοντέλα αναφοράς OSI και Διαδικτύου (3 εκδοχές).*

Σύμφωνα με το μοντέλο αναφοράς, όταν ένας κόμβος αποστέλλει πληροφορία, η πληροφορία αυτή μεταφέρεται μεταξύ των επιπέδων. Η πληροφορία που προέρχεται από το ανώτερο επίπεδο, ενθυλακώνεται κατάλληλα έτσι ώστε να αποσταλεί στο αμέσως κατώτερο. Η ενθυλάκωση αυτή γίνεται με την προσθήκη κεφαλίδας, έτσι ώστε τα πρωτόκολλα του αντίστοιχου επιπέδου στη μεριά του παραλήπτη να μπορούν να χειριστούν κατάλληλα την πληροφορία αυτή.



Εικόνα 2.2 *Ενθυλάκωση πληροφορίας.*

Κατά τη λήψη των δεδομένων, ακολουθείται η αντίστροφη διαδικασία. Οι κεφαλίδες σε κάθε επίπεδο αφαιρούνται έτσι ώστε να προωθηθεί η πληροφορία με την κατάλληλη κεφαλίδα στο ανώτερο επίπεδο.

Στη συνέχεια, θα εξεταστούν τα τέσσερα επίπεδα του Μοντέλου του Διαδικτύου και θα παρατεθούν τα βασικά πρωτόκολλα κάθε επιπέδου, η γνώση των οποίων είναι σημαντική για τη συνέχεια.

2.3 Το Επίπεδο Πρόσβασης Δικτύου

Το επίπεδο πρόσβασης δικτύου (ή επίπεδο ζεύξης) και τα πρωτόκολλα που υλοποιούνται σε αυτό, ασχολούνται με τη μεταφορά πλαισίων (frames) από άκρο σε άκρο μιας ζεύξης και ελέγχουν ενέργειες, όπως η πρόσβαση στο μέσο (medium access), η ανίχνευση σφαλμάτων (error detection), η διόρθωση σφαλμάτων (error correction), η αναμετάδοση (retransmission) και ο έλεγχος ροής (flow control).

Κάθε κόμβος αποκτά πρόσβαση στο φυσικό μέσο με τη χρήση κατάλληλων διεπαφών, γνωστών ως Network Interface Cards (NIC). Κάθε τέτοια διεπαφή έχει μια μοναδική διεύθυνση πρόσβασης στο μέσο (Media Access Control address), γνωστή ως διεύθυνση MAC (MAC address) με μήκος 48 bit.

Η διεύθυνση MAC είναι μοναδική. Η μοναδικότητά της προκύπτει από την επίπεδη δομή της και συγκεκριμένα:

- Τα πρώτα 24 bit αποτελούν το μοναδικό αναγνωριστικό οργανισμού (Organizationally Unique Identifier – OUI) και προσδιορίζουν τον κατασκευαστή του υλικού. Κάποιος κατασκευαστής μπορεί να χρησιμοποιεί έναν ή περισσότερους τέτοιους αριθμούς για το υλικό που παράγει.

- Τα επόμενα 24 bit είναι το αναγνωριστικό της διεπαφής (Network Interface Controller – NIC) και είναι μοναδικά για κάθε υλικό ενός συγκεκριμένου OUI.

Η MAC address που αποτελείται μόνο από 1 (FF:FF:FF:FF:FF:FF), ονομάζεται broadcast address (διεύθυνση εκπομπής) και έχει ως προορισμό κάθε συνδεδεμένο κόμβο.

2.3.1 Πρόσβαση στο μέσο

Μια μη αποδεκτή κατάσταση σε ότι αφορά την πρόσβαση στο φυσικό μέσο είναι η σύγκρουση πλαισίων. Σε κάθε χρονική στιγμή, επιτρέπεται η κυκλοφορία ενός μόνο πλαισίου σε κάθε collision domain. Όταν διαπιστωθεί πως κυκλοφορούν περισσότερα του ενός πλαίσια, δηλαδή δυο τουλάχιστον κόμβοι μεταδίδουν ταυτόχρονα, τα πλαίσια συγκρούονται και κατά συνέπεια απορρίπτονται.

Σε ένα παραδοσιακό δίκτυο όπου όλοι οι κόμβοι διασυνδέονται σε ένα συγκεντρωτή (hub), το σύνολο του δικτύου αποτελεί ένα collision domain. Έτσι, πρέπει να χρησιμοποιούνται κατάλληλα πρωτόκολλα, τα οποία θα διασφαλίζουν την απρόσκοπτη πρόσβαση στο μέσο ενός κόμβου κάθε φορά και θα ρυθμίζουν τις επανεκπομπές. Τέτοια πρωτόκολλα είναι το ALOHA, το Slotted ALOHA και το CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

Σήμερα, η ευρεία χρήση των μεταγωγέων (switches) και η υποστήριξη full duplex επικοινωνίας έχει εξαλείψει την ανάγκη χρήσης των πρωτοκόλλων αυτών, καθώς κάθε κόμβος απαρτίζει ένα collision domain με κάθε διεπαφή του switch, ενώ το σύνολο των διασυνδεδεμένων κόμβων αποτελεί το broadcast domain. Παρόλα αυτά, για λόγους συμβατότητας, η μορφή των πλαισίων δεν έχει αλλάξει, ενώ διατηρείται το πρωτόκολλο CSMA/CD.

Το πρόβλημα παραμένει στα ασύρματα δίκτυα, όπου το μέσο είναι κοινό για όλους τους κόμβους, καθώς τα πλαίσια μεταδίδονται μέσω του αέρα. Το δεύτερο πρόβλημα, σχετίζεται με το γεγονός ότι στον αέρα μια σύγκρουση δεν είναι δυνατό να ανιχνευθεί. Έτσι, πλέον, στόχος δεν είναι η ανίχνευση συγκρούσεων, όπως επιδιώκεται με τη χρήση του πρωτοκόλλου CSMA/CD, αλλά η αποφυγή συγκρούσεων με τη χρήση μηχανισμών που υλοποιούν πρωτόκολλα όπως τα CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) και RTS/CTS (Ready to Send / Clear to Send), των οποίων μια αναλυτική παρουσίαση δεν εμπίπτει στο παρόν εγχειρίδιο.

2.3.2 Ανίχνευση και διόρθωση σφαλμάτων

Ένα σημαντικό πρόβλημα στο επίπεδο ζεύξης είναι οι αλλοιώσεις που μπορεί να προκύψουν κατά τη μεταφορά των πλαισίων μέσω των γραμμών επικοινωνίας. Για την ανίχνευση των αλλοιώσεων αυτών, χρησιμοποιούνται τεχνικές ανίχνευσης όπως:

- Έλεγχος ισοτιμίας.
- Κυκλικός έλεγχος πλεονασμού (CRC).

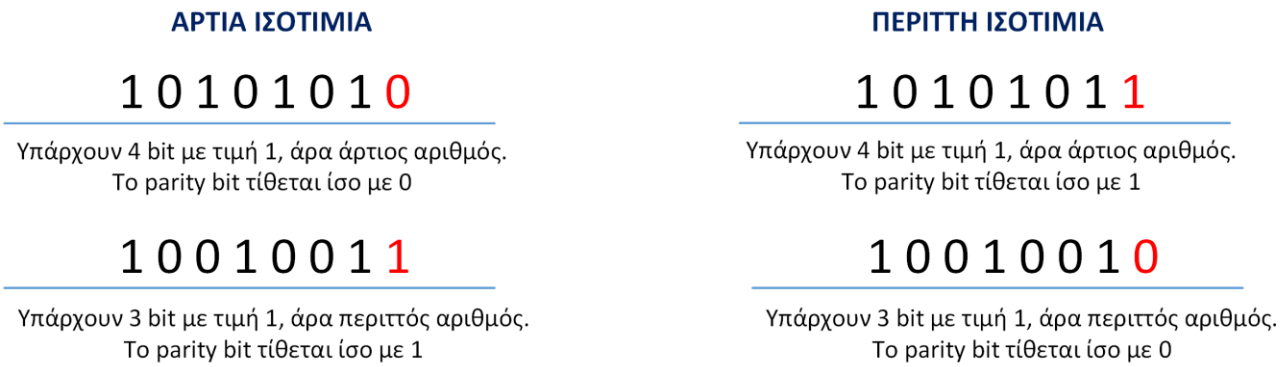
2.3.2.1 Έλεγχος ισοτιμίας

Ο πιο απλός έλεγχος για ανίχνευση αλλοιώσεων κατά τη μετάδοση της πληροφορίας που λαμβάνει ο δέκτης, είναι ο έλεγχος ισοτιμίας. Στον έλεγχο αυτό, τα δεδομένα χωρίζονται σε τμήματα των n - 1 bit. Για κάθε τέτοιο

τμήμα, προστίθεται ένα επιπλέον bit, το bit ισοτιμίας (parity bit). Η τιμή του bit αυτού τίθεται από τον αποστολέα έτσι ώστε:

- Ο συνολικός αριθμός των 1 στο τμήμα των n bit να είναι άρτιος, αν χρησιμοποιηθεί άρτια ισοτιμία.
- Ο συνολικός αριθμός των 1 στο τμήμα των n bit να είναι περιττός, αν χρησιμοποιηθεί περιττή ισοτιμία.

Στην εικόνα 2.3 φαίνονται οι περιπτώσεις άρτιας και περιττής ισοτιμίας για ένα τμήμα δεδομένων 8 bit (1 Byte).



Εικόνα 2.3 *Καθορισμός bit ισοτιμίας.*

Όταν ο παραλήπτης λάβει το τμήμα των n bit, γνωρίζοντας φυσικά την ισοτιμία που έχει συμφωνηθεί να χρησιμοποιείται, μπορεί να αντιληφθεί αν ένα bit έχει αλλοιωθεί, όπως φαίνεται στην εικόνα 2.4.

Εικόνα 2.4 *Χρήση της ισοτιμίας στο δέκτη.*

Ο έλεγχος ισοτιμίας με ένα (1) parity bit, μπορεί να ανιχνεύσει αλλοιώσεις σε περιττό αριθμό bit, χωρίς να μπορεί να αντιληφθεί ποια bit έχουν αλλοιωθεί. Όμως, αν αλλοιωθεί άρτιος αριθμός bit, ο δέκτης δεν θα είναι σε θέση να αντιληφθεί το σφάλμα. Για τη δυνατότητα ανίχνευσης περισσότερων λαθών και με εντοπισμό του κάθε λάθους, μπορούν να χρησιμοποιηθούν δισδιάστατες ισοτιμίες, όπου υπάρχουν bit ισοτιμίας γραμμής, καθώς και bit ισοτιμίας στήλης, όπως φαίνεται στην Εικόνα 2.5.

0	0	0	1	1	1	0	1
1	0	0	0	0	1	1	0
0	1	1	1	1	0	1	1
0	1	0	0	1	0	0	1
0	1	1	1	0	1	1	1
1	1	0	0	1	0	1	0
1	1	1	0	0	0	0	1
1	1	0	1	0	0	0	1

Εικόνα 2.5 *Δυσδιάστατος έλεγχος άρτιας ισοτιμίας.*

2.3.2.2 Κυκλικός Έλεγχος Πλεονασμού

Ο κυκλικός έλεγχος πλεονασμού (Cyclic Redundancy Check – CRC) βασίζεται στην αριθμητική modulo-2 και έχει τη δυνατότητα να εντοπίζει λάθη σε μια δέσμη μεταδιδόμενων bit. Στο τέλος μιας τέτοιας δέσμης, δηλαδή μιας ακολουθίας από k bit, ο αποστολέας θα προσαρτήσει μια πρόσθετη ακολουθία από r bit και θα μεταδώσει τελικά ένα μήνυμα μήκους k+r bit. Η ακολουθία των πρόσθετων r bit είναι γνωστή ως Frame Check Sequence (FCS).

Πριν την αποστολή, ο αποστολέας και ο παραλήπτης προκαθορίζουν ένα μοτίβο, δηλαδή μια ακολουθία από r + 1 bit, γνωστό και ως generator (G), του οποίου το πιο σημαντικό bit (Most Significant Bit - MSB) έχει πάντα τιμή το 1. Ο αποστολέας, στη συνέχεια, διαμορφώνει το FCS έτσι ώστε η διαίρεση modulo-2 της ακολουθίας k+r προς το G να δίνει υπόλοιπο 0. Ο παραλήπτης επαναλαμβάνει τη διαίρεση modulo-2 και αν το υπόλοιπο είναι μηδέν (0), τότε επιβεβαιώνει ότι η αρχική δέσμη δεν έχει αλλοιωθεί κατά τη μετάδοσή της.

2.3.3 Δημιουργία κύκλων

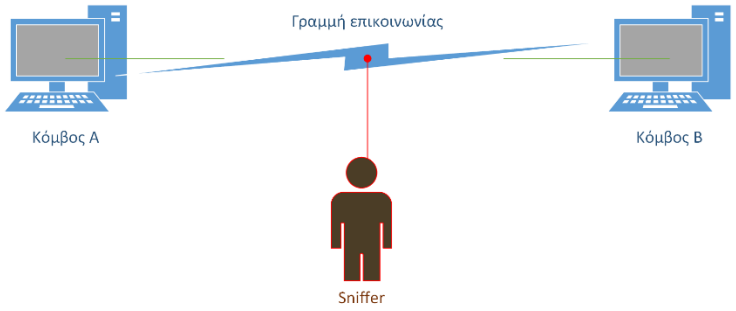
Η δημιουργία κύκλων σε ένα δίκτυο προκύπτει όταν ένας κόμβος προορισμού είναι προσβάσιμος από διαφορετικά μονοπάτια. Σε μια τέτοια περίπτωση, τα πλαίσια εκπομπής (broadcast) ταξιδεύουν συνεχώς στο δίκτυο. Για την αντιμετώπιση του φαινομένου αυτού, έχει εισαχθεί το πρωτόκολλο STP (Spanning Tree Protocol), το οποίο με κάθε νέα σύνδεση δημιουργεί εκ νέου ένα δέντρο επικάλυψης (spanning tree) με κόμβους-γράφου τους κόμβους του δικτύου.

2.3.4 Επιθέσεις επιπέδου ζεύξης

Στη συνέχεια, θα παρουσιαστούν σύντομα οι βασικές επιθέσεις στο επίπεδο ζεύξης.

2.3.4.1 Sniffing

Ως sniffing ορίζεται η προσπάθεια να υποκλέψει (με παθητική παρακολούθηση) μια τρίτη, ως προς μια επικοινωνία, οντότητα πληροφορίες που δεν προορίζονται για αυτή. Για να το καταφέρει αυτό, αρκεί να αποκτήσει πρόσβαση στο μέσο μέσω του οποίου διακινείται η πληροφορία. Αυτό μπορεί να συμβεί είτε όταν το μέσο είναι διαμοιραζόμενο και αποτελεί ένα ενιαίο collision domain (δίκτυα όπου χρησιμοποιείται hub ή ασύρματα δίκτυα), είτε όταν η οντότητα καταφέρει να αντιγράφει όλη την πληροφορία που διακινείται σε μια συγκεκριμένη διεπαφή (π.χ. port mirroring).

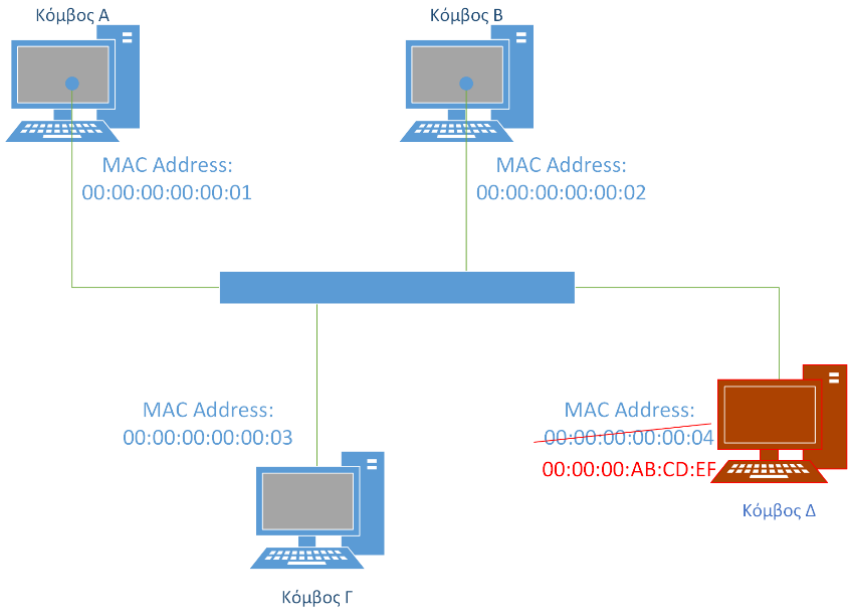


Εικόνα 2.6 *Sniffing*.

Για την αντιμετώπιση της επίθεσης sniffing, θα πρέπει είτε να ελέγχεται η πρόσβαση στο μέσο, π.χ. με αυθεντικοποίηση των συμμετεχόντων (με χρήση πρωτοκόλλων, όπως το 802.11x), είτε να παρέχεται προστασία της εμπιστευτικότητας της διακινούμενης πληροφορίας, π.χ. με χρήση κρυπτογραφικών τεχνικών, οι οποίες θα παρουσιαστούν σε επόμενα κεφάλαια.

2.3.4.2 MAC Spoofing

Όπως αναφέρθηκε νωρίτερα, κάθε διεπαφή που συνδέεται με το φυσικό μέσο μετάδοσης, αναγνωρίζεται μοναδικά (διευθυνσιοδοτείται) από μια διεύθυνση ελέγχου πρόσβασης στο μέσο (media access control), γνωστή ως MAC address, που είναι μοναδική και έχει αποδοθεί στο υλικό από τον κατασκευαστή του. Κάποιος επιτιθέμενος, μπορεί δυνητικά να παρεμβληθεί σε μια επικοινωνία με διαφορετική διεύθυνση MAC από την πραγματική της διεπαφής που χρησιμοποιεί, με σκοπό να υποκλέψει frames που προορίζονται για άλλο παραλήπτη ή ακόμη για να μην είναι δυνατός ο εντοπισμός της προέλευσης των πλαισίων που ο ίδιος αποστέλλει.



Εικόνα 2.7 *MAC Spoofing*.

Η διαδικασία που απαιτείται για την επίθεση MAC spoofing, είναι μάλλον απλή και εύκολη να υλοποιηθεί με τη βοήθεια προϊόντων λογισμικού, που κυκλοφορούν ευρέως στο Διαδίκτυο. Ως αντίμετρο, μεταξύ άλλων, θα πρέπει να χρησιμοποιούνται διεπαφές δικτύου (NIC) στις οποίες να μην είναι δυνατή η αλλαγή της διεύθυνσης που έχει αποδώσει ο κατασκευαστής τους.

2.4 Το Επίπεδο Δικτύου

Το επίπεδο δικτύου είναι αυτό στο οποίο λαμβάνει χώρα η προώθηση των πακέτων δεδομένων (δεδομενογραμμάτων – datagrams) μεταξύ των δικτύων, στη βάση των κανόνων δρομολόγησης (routing). Στο επίπεδο αυτό, υπάρχουν πρωτόκολλα δρομολόγησης, πρωτόκολλα ελέγχου, καθώς και το βασικό πρωτόκολλο που καθορίζει την προώθηση και διευθυνσιοδότηση, το Internet Protocol (IP). Σήμερα, στο μεγαλύτερο μέρος του Internet χρησιμοποιείται παραδοσιακά η έκδοση 4 του πρωτοκόλλου (IPv4). Λόγω των περιορισμών της, όμως, υπάρχει η ανάγκη αντικατάστασής της από την πιο πρόσφατη έκδοση 6 (IPv6).

Αυτό που είναι σημαντικό να τονιστεί, είναι πως το πρωτόκολλο IPv4 σχεδιάστηκε χωρίς να ληφθεί υπόψιν η ασφάλεια των πληροφοριών. Στα σημερινά δίκτυα IPv4, η ασφάλεια υλοποιείται ως ένα επιπρόσθετο χαρακτηριστικό, ενώ κάτι τέτοιο δεν ισχύει στα νεότερα δίκτυα IPv6.

Σε αυτή την ενότητα, θα γίνει μια ανασκόπηση του πρωτοκόλλου IP, κυρίως σε ότι αφορά τη διευθυνσιοδότηση, έτσι ώστε να διευκολυνθεί η άνετη κατανόηση των επόμενων κεφαλαίων.

2.4.1 IPv4

Η τέταρτη έκδοση του πρωτοκόλλου IP είναι αυτή που χρησιμοποιείται τις τελευταίες δεκαετίες. Στην έκδοση αυτή, κάθε διεύθυνση αποτελείται από 32 bit, τα οποία μπορούν να χωριστούν σε τέσσερις ομάδες, των οκτώ (8) bit (1 Byte). Ένα τμήμα αυτών των 32 bit προσδιορίζει το δίκτυο (τμήμα δικτύου) και το υπόλοιπο προσδιορίζει μοναδικά την κάθε υπολογιστική συσκευή (τμήμα κόμβων). Για ευκολία απομνημόνευσης, καθώς ο άνθρωπος είναι εξοικειωμένος με το δεκαδικό σύστημα αρίθμησης, μια διεύθυνση IP μπορεί να γραφεί ως μια ακολουθία από τέσσερις δεκαδικούς αριθμούς (που προκύπτουν από τα τέσσερα Byte της διεύθυνσης), που ξεχωρίζουν μεταξύ τους με χρήση της τελείας.

Αρχικά, καθορίστηκαν τρεις (3) κλάσεις διευθύνσεων, ως εξής:

- Η κλάση A περιλαμβάνει τις διευθύνσεις 1.0.0.0 – 126.255.255.255. Το τμήμα δικτύου αποτελούν τα 8 πρώτα (MSB) bit και τα υπόλοιπα το τμήμα κόμβων (host).
- Η κλάση B περιλαμβάνει τις διευθύνσεις 128.0.0.0 – 191.255.255.255. Το τμήμα δικτύου αποτελούν τα 16 πρώτα bit και τα υπόλοιπα το τμήμα κόμβων.
- Η κλάση C περιλαμβάνει τις διευθύνσεις 192.0.0.0 – 223.255.255.255. Το τμήμα δικτύου αποτελούν τα 24 πρώτα bit και τα υπόλοιπα το τμήμα κόμβων.
- Η κλάση D περιλαμβάνει τις διευθύνσεις 224.0.0.0 – 239.255.255.255 και χρησιμοποιείται για πολυεκπομπή (multicast).

Οι διευθύνσεις (240.0.0.0 – 254.255.255.255) χρησιμοποιούνται για ερευνητικούς σκοπούς, ενώ οι διευθύνσεις 127.0.0.0 – 127.255.255.255 δεν χρησιμοποιούνται, καθώς είναι δεσμευμένες για loopback και διαγνωστικούς σκοπούς.

Αρχικά, για τη διευθυνσιοδότηση κάθε δικτύου αποδίδονταν ένα ολόκληρο δίκτυο διευθύνσεων. Δηλαδή, αποδίδονταν 2^{24} διευθύνσεις για δίκτυο κλάσης A, 2^{16} διευθύνσεις για δίκτυο κλάσης B και 256 διευθύνσεις για δίκτυο κλάσης C. Όπως είναι λογικό, με μια τέτοια χρήση, οι διαθέσιμες διευθύνσεις δικτύων πολύ σύντομα θα είχαν εξαντληθεί, αφού θα είχαν αποδοθεί προς χρήση σε οργανισμούς ή εταιρίες που μπορεί θεωρητικά να δέσμευαν 2^{24} διευθύνσεις ακόμη και αν είχαν να διευθυνσιοδοτήσουν ελάχιστους κόμβους.

Τη λύση στην ταχύτατη εξάντληση των διευθύνσεων κλήθηκαν να δώσουν οι τεχνικές: subnetting και Network/Port Address Translation (NAT/PAT).

2.4.1.1 Subnetting

Μπορούμε να δημιουργήσουμε μικρότερα υποδίκτυα, απλά μειώνοντας τα bit του τμήματος κόμβων (Host). Άρα, για παράδειγμα, σε ένα δίκτυο κλάσης A, η IP διεύθυνση κανονικά θα έπρεπε να είναι όπως φαίνεται στην Εικόνα 2.8:

Εικόνα 2.8 *Μορφή διεύθυνσης για δίκτυο κλάσης Α.*

Όμως, δημιουργώντας ένα νέο τμήμα, με δέσμευση των πρώτων 16 από τα 24 bit του τμήματος κόμβων, έχουμε τη διαμόρφωση της διεύθυνσης όπως φαίνεται στην Εικόνα 2.9:

Εικόνα 2.9 *Μορφή διεύθυνσης με τμήμα υποδικτύου.*

Έτσι, μια διεύθυνση δεν καθορίζεται πλέον από την κλάση στην οποία ανήκει, αλλά από το σύνολο των bit δικτύου και υποδικτύου. Έτσι ένα υποδίκτυο ορίζεται ως: **<Διεύθυνση_Υποδικτύου>/<Πλήθος Subnet bit>**

Σημειώνεται, ότι στην αναπαράσταση μιας διεύθυνσης υποδικτύου το σύνολο των bit του τμήματος κόμβων (στο εξής θα αναφέρονται και ως host bit) λαμβάνει την τιμή 0. Έτσι, η διεύθυνση 15.6.0.0/16 είναι ένα παράδειγμα μιας διεύθυνσης υποδικτύου. Η αναγραφή του αριθμού 16, που προσδιορίζει τα bit υποδικτύου (στο εξής θα αναφέρονται και ως subnet bit), είναι απαραίτητη, καθώς αν έλειπε τότε η διεύθυνση 15.6.0.0 θα ερμηνευόταν ως μια κανονική διεύθυνση κλάσης Α.

Η διεύθυνση στην οποία όλα τα host bit έχουν την τιμή 1, είναι η διεύθυνση (ευρείας) εκπομπής (broadcast). Ένα τέτοιο παράδειγμα είναι η διεύθυνση 15.6.255.255.

Το πλήθος των subnet bit καθορίζεται ανάλογα από τις εκάστοτε ανάγκες. Αν σε ένα δίκτυο, για παράδειγμα, υπάρχει η ανάγκη για 25 κόμβους, τότε βρίσκουμε την πιο κοντινή δύναμη του 2, δηλαδή $2^5=32$, που να τους καλύπτει. Άρα, απαιτούμε 5 bit για το τμήμα κόμβων (host bit). Οπότε, το μέγεθος του τμήματος υποδικτύου (subnet bit) θα αποτελείται από 32 – 5 = 27 bit. Ένα τέτοιο παράδειγμα, είναι η διεύθυνση 195.251.209.128/27.

2.4.1.2 Μετάφραση διεύθυνσης

Ακόμη και με την εκχώρηση subnets και όχι δικτύων, ο διαθέσιμος χώρος διευθύνσεων του πρωτοκόλλου IPv4 είναι ιδιαίτερα περιορισμένος. Πολλές φορές, όμως, υπάρχουν περιπτώσεις δικτύων όπου οι κόμβοι δεν απαιτείται να είναι προσπελάσιμοι από εξωτερικά δίκτυα.

Για τέτοιου είδους δίκτυα, υπάρχουν τρεις ομάδες διευθύνσεων, οι οποίες μπορούν να επαναχρησιμοποιηθούν σε πολλά διαφορετικά δίκτυα. Αυτό μπορεί να συμβαίνει, καθώς δεν παραβιάζεται ο κανόνας της μοναδικής διεύθυνσης ανά host σε όλο το Διαδίκτυο, γιατί ακριβώς τα πακέτα με διεύθυνση αποστολέα ή προορισμού μια από αυτές τις διευθύνσεις δεν προωθούνται προς το υπόλοιπο Διαδίκτυο (Internet). Οι τρεις αυτές ομάδες διευθύνσεων ονομάζονται ιδιωτικές (private) και ορίζονται από τις ακόλουθες διευθύνσεις υποδικτύων:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Πώς όμως μπορούν οι κόμβοι (hosts) να επικοινωνούν αφού τα πακέτα με τέτοιες διευθύνσεις δεν προωθούνται προς το υπόλοιπο Internet; Η λύση ονομάζεται μετάφραση διεύθυνσης (address translation) και λειτουργεί ως εξής:

- Στο δίκτυο ενός οργανισμού εκχωρείται μια ή και περισσότερες πραγματικές διευθύνσεις IP (δημόσιες, δηλαδή διευθύνσεις για πακέτα που προωθούνται στο υπόλοιπο εξωτερικό Διαδίκτυο).

- Όταν πρόκειται να αποσταλεί ένα πακέτο στο υπόλοιπο Διαδίκτυο, ο δρομολογητής αντικαθιστά την ιδιωτική (private) διεύθυνση αποστολέα στην κεφαλίδα του πακέτου με μια από τις δημόσιες IP του δικτύου του οργανισμού και καταχωρεί σε ένα πίνακα τη συσχέτιση αυτή.

- Όταν παραληφθεί ένα πακέτο από το Διαδίκτυο, με αντίστροφο τρόπο, η δημόσια IP προορισμού στην κεφαλίδα του πακέτου, αντικαθίσταται με την συσχετιζόμενη ιδιωτική διεύθυνση του εσωτερικού κόμβου.

Η μέθοδος αυτή ονομάζεται Network Address Translation (NAT). Αντίστοιχα, αν ένας εσωτερικός κόμβος με ιδιωτική διεύθυνση IP πρέπει να παρέχει υπηρεσίες προς το υπόλοιπο Διαδίκτυο, τότε δημιουργείται στο δρομολογητή μια κατάλληλη συσχέτιση, έτσι ώστε πακέτα προς την υπηρεσία που παρέχει ο εξυπηρετητής αυτός (host) να μεταφράζονται κατάλληλα και να προωθούνται σε αυτόν. Η μέθοδος αυτή λειτουργεί στο επίπεδο μεταφοράς και ονομάζεται Port Address Translation (PAT).

2.4.1.3 Επίθεση IP Spoofing

Μια διεύθυνση IP είναι μοναδική για κάθε κόμβο που συμμετέχει σε ένα δίκτυο. Είτε το δίκτυο αυτό είναι ένα ιδιωτικό δίκτυο, είτε είναι ένα δημόσιο δίκτυο, όπως το Internet. Η διεύθυνση IP, επομένως, αποτελεί ένα μοναδικό αναγνωριστικό του κόμβου και κάθε αποστολέας γνωρίζει τη διεύθυνση IP του παραλήπτη των δεδομένων που αποστέλλει ή της προέλευσης των δεδομένων που παραλαμβάνει.

Η επίθεση IP Spoofing πραγματοποιείται τροποποιώντας τη διεύθυνση IP της προέλευσης (source address). Έτσι, ο επιτιθέμενος μπορεί να προσποιηθεί (masquerade) πως είναι ένας έμπιστος κόμβος και με τον τρόπο αυτό να εδραιώσει μια επικοινωνία.

Οι συνέπειες, καθώς και τρόποι αντιμετώπισης της επίθεσης IP spoofing θα εξεταστούν στο επόμενο κεφάλαιο.

2.4.2 IPv6

Παρά τη χρήση των τεχνικών subnetting και NAT/PAT στο διαδίκτυο με πρωτόκολλο IPv4, ο διαθέσιμος χώρος διευθύνσεων παρέμεινε αισθητά περιορισμένος. Ακόμη και αν είχαμε στη διάθεσή μας το σύνολο των διαθέσιμων διευθύνσεων, αυτές θα ήταν μόλις 2^{32}= 4.294.967.296 (λίγο πάνω από 4 δισεκατομμύρια), που έχει αποδειχθεί ότι είναι πολύ λίγες σε σχέση με τις τρέχουσες ανάγκες. Για παράδειγμα, είναι απαγορευτικές για σκέψεις υλοποίησης τεχνολογιών όπως το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT).

Επιπλέον, ήδη με τις περιορισμένες εφαρμογές του παραδοσιακού Διαδικτύου, οι διαθέσιμες διευθύνσεις έχουν οριστικά τελειώσει, καθώς το τελευταίο υποδίκτυο έχει ήδη εκχωρηθεί. Το πρόβλημα είχε γίνει γνωστό αρκετά χρόνια πριν και ήδη από το 1992 ο οργανισμός IETF (Internet Engineering Task Force) ζήτησε προδιαγραφές για ένα IP πρωτόκολλο νέας γενιάς (Internet Protocol next generation - IPng). Το πρώτο RFC (RFC 1752) που περιέγραφε το νέο αυτό πρωτόκολλο δημοσιεύτηκε το 1995. Η τελική μορφή του νέου πρωτοκόλλου, που ονομάστηκε τελικά IPv6, περιγράφεται στο RFC 2460 που δημοσιεύτηκε το 1998.

Στο πρωτόκολλο IPv6, κάθε διεύθυνση αποτελείται από 128 bit. Η αύξηση στον αριθμό των bit οδηγεί σε ένα συνολικό χώρο 2^{128}=340.282.366.920.938.463.463.374.607.431.768.211.456 διευθύνσεων. Με το τεράστιο αυτό νούμερο (λίγο πάνω από 340 undecillionths ή ενδεκάκις εκατομμύρια) λέγεται (με τόνο υπερβολής, φυσικά) ότι θα μπορούσε κανείς να διευθυνσιοδοτήσει κάθε κόκκο άμμου που υπάρχει στον πλανήτη!

Πέρα από τον μεγάλο πλήθος διευθύνσεων που παρέχει, κάτι που καθιστά τη λύση του NAT μη απαραίτητη πλέον, το πρωτόκολλο IPv6 παρουσιάζει αρκετές ακόμη βελτιώσεις, σε τομείς όπως:

- Εγγενή υποστήριξη του IPsec: Το πρωτόκολλο IPsec, το οποίο θα εξεταστεί σε επόμενο κεφάλαιο, παρέχει υπηρεσίες αυθεντικοποίησης και εμπιστευτικότητας δεδομένων στο επίπεδο του δικτύου. Στο πρωτόκολλο IPv6, το IPsec συμπεριλαμβάνεται, ενώ η χρήση του είναι προαιρετική.

- Διαφορετική κεφαλίδα: Η κεφαλίδα στο IPv6 είναι διπλάσια από την κεφαλίδα του IPv4, κυρίως λόγω του μεγάλου μήκους των διευθύνσεων. Παρόλα αυτά, η μορφοποίησή της έχει απλοποιηθεί σημαντικά, επιταχύνοντας την επεξεργασία της σημαντικά. Έτσι, τα optional headers τοποθετούνται μεταξύ της κεφαλίδας δικτύου και της κεφαλίδας μεταφοράς, ώστε να μην απαιτείται η επεξεργασία τους από τους ενδιάμεσους δρομολογητές.

- Τεράστιο χώρο διευθύνσεων: Το πλήθος των συνολικά διαθέσιμων διευθύνσεων είναι 2^{128}.

- Υποστήριξη stateless και statefull διαμόρφωσης διευθύνσεων IP: Υπάρχει η δυνατότητα αυτόματης εκχώρησης διεύθυνσης IP, χωρίς τη μεσολάβηση ενεργειών του χρήστη ή του διαχειριστή.

- Κατακερματισμό από τον αποστολέα μόνο: Στο πρωτόκολλο IPv6 δεν υπάρχει η δυνατότητα κατάτμησης πακέτων σε ενδιάμεσους κόμβους.

- Υποστήριξη διαχείρισης προτεραιοτήτων: Η ποιότητα υπηρεσίας (Quality of Service – QoS) είναι μια βασική απαίτηση στα σύγχρονα δίκτυα. Συνήθως, επιτυγχάνεται με την παροχή εξυπηρέτησης διαφορετικής προτεραιότητας, ανάλογα με τον τύπο των πακέτων (π.χ. τα πακέτα φωνής αποκτούν μεγαλύτερη προτεραιότητα από τα πακέτα που μεταφέρουν δεδομένα). Επιπλέον, στο πρωτόκολλο IPv6 παρέχεται αισθητή βελτίωση του τρόπου διαχείρισης των προτεραιοτήτων.

- Υποστήριξη κινητικότητας: Στο πρωτόκολλο IPv6 παρέχεται εγγενώς η δυνατότητα υποστήριξης κινητικότητας (mobility).

Η αναπαράσταση των διευθύνσεων IPv6 γίνεται με τη χρήση δεκαεξαδικών αριθμών, σε 8 τετράδες, χωρισμένες με άνω-κάτω τελεία (:) και ακολουθούμενες μετά από μια πλάγια κάθετο (**/**) και το μήκος προθέματος (prefix length) σε δεκαδική μορφή. Η έννοια του prefix στο IPv6 αντικαθιστά αυτή του subnet στο IPv4.

Στη δεκαεξαδική αναπαράσταση μιας IPv6 διεύθυνσης, μια σειρά μηδενικών (bit με τιμή 0) μπορεί να παραληφθεί αν:

- πρόκειται για leading zeroes μιας τετράδας
- απαρτίζει μια σειρά από τετράδες, αλλά για μια μόνο φορά.

Σχετικά παράδειγμα ισοδύναμων αναπαραστάσεων σε πλήρη παράθεση δεκαεξαδικών και με συντομευμένη μορφή λόγω των μηδενικών:

- fe80:0000:0000:cd4f:0aff:0000:0000:4afc/64 ↔ fe80::cd4f:0aff:0:0:4afc/64
- fe80:0000:0000:cd4f:0aff:0000:0000:4afc/64 ↔ fe80:0:0:cd4f:0aff:0:0:4afc/64
- 0000:0000:0000:0000:0000:0000:0000:0001/64 ↔ 0:0:0:0:0:0:0:1
- 0000:0000:0000:0000:0000:0000:0000:0001/64 ↔ ::1

Στο πρωτόκολλο IPv6 δεν προβλέπεται η broadcast διεύθυνση. Οι IPv6 διευθύνσεις διακρίνονται ως εξής:

- **Unicast**: Διευθύνσεις που αποδίδονται σε ένα μόνο host.

- **Multicast**: Διευθύνσεις που αντιστοιχούν σε περισσότερους από ένα host. Πακέτα προς παραλήπτες με τέτοιες διευθύνσεις παραδίδονται σε όλους τους host τους οποίους διευθυνσιοδοτούν.

- **Anycast**: Διευθύνσεις που αντιστοιχούν σε περισσότερους από ένα host. Πακέτα προς παραλήπτες με τέτοιες διευθύνσεις παραδίδονται σε ένα μόνο από τους host τους οποίους διευθυνσιοδοτούν.

Οι unicast διευθύνσεις διακρίνονται σε κατηγορίες, οι βασικότερες εκ των οποίων είναι:

- **Global**: Αντιστοιχούν μόλις στο 1/8 του συνόλου των διευθύνσεων και είναι αντίστοιχες με τις δημόσιες διευθύνσεις IPv4 (public addresses), δηλαδή διευθυνσιοδοτούν κόμβους προσβάσιμους από το υπόλοιπο Διαδίκτυο.

    - Διακρίνονται από το πρόθεμα (prefix): 2000::/3 (001)

    - Περιλαμβάνουν τις διευθύνσεις από 2000:: έως 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

  Ένα παράδειγμα global διεύθυνσης είναι η διεύθυνση 2000:db8::1234.

- **Unique Local (Site-Local)**: Είναι αντίστοιχες των ιδιωτικών διευθύνσεων του IPv4: 10.0.0.0/8, 172.16.0.0/12 και 192.168.0.0/16. Οι διευθύνσεις αυτές χρησιμοποιούνται σε τοπικά d;iktya IR (intranets), όταν δεν υπάρχει επιθυμία προώθησης πακέτων από τους εσωτερικούς δρομολογητές προς το υπόλοιπο Internet. Τα πρώτα 48 bit είναι σταθερά, ενώ τα επόμενα 16 συνήθως χρησιμοποιούνται για να προσδιορίσουν το υποδίκτυο.

    - Διακρίνονται από το prefix: FC00::/7 (1111 110)

- **Link-Local**: Είναι αντίστοιχες των διευθύνσεων του IPv4: 169.254.0.0/16. Οι διευθύνσεις αυτές αποδίδονται σε κάθε διεπαφή και χρησιμοποιούνται για την επικοινωνία κόμβων που διασυνδέονται μέσω ενός κοινού μέσου, έτσι ώστε να λειτουργήσουν πρωτόκολλα, όπως το network discovery. Αποδίδονται αυτόματα και, συνήθως, τα τελευταία 64 bit είναι ο προσδιοριστής EUI-64 (Extender Unique Identifier), που προκύπτει από τα 48 bit της φυσικής διεύθυνσης (MAC address) της δικτυακής διεπαφής (NIC), όπως προβλέπεται από το RFC 4291.

    - Διακρίνονται από το prefix: FE80::/10 (1111 1110 10)

- **Special**: Στις ειδικές διευθύνσεις περιλαμβάνονται η απροσδιόριστη (unspecified) και η διεύθυνση που είναι αντίστοιχη του localhost στο IPv4:

    - Unspecified: ::/128 (αντίστοιχη της 0.0.0.0 του IPv4)

    - Localhost: ::1/128 (αντίστοιχη της 127.0.0.1 του IPv4)

- **Transition**: Ειδικές διευθύνσεις που χρησιμοποιούνται σε σενάρια παράλληλης λειτουργίας ή μετατροπής μεταξύ του IPv6 και του IPv4.

2.4.3 Δρομολόγηση

Με τον όρο δρομολόγηση (routing), αναφερόμαστε στο σχεδιασμό των διαδρομών κίνησης των πακέτων, καθώς και στη δημιουργία των σχετικών πινάκων δρομολόγησης, στη βάση των οποίων οι δρομολογητές θα

μπορούν να παίρνουν αποφάσεις προώθησης μέσω της κατάλληλης διεπαφής. Η δρομολόγηση μπορεί να είναι στατική ή δυναμική.

Η στατική δρομολόγηση προϋποθέτει το σχεδιασμό των πινάκων δρομολόγησης «με το χέρι» (manually). Σε κάθε δρομολογητή δημιουργούνται από το διαχειριστή πίνακες στους οποίους αναφέρεται για κάθε δίκτυο προορισμού η διεπαφή εξόδου ή η διεύθυνση IP της διεπαφής του άμεσα διασυνδεδεμένου κόμβου. Για τα άγνωστα (υπόλοιπα) δίκτυα που δεν καθορίζονται σαφώς, ακολουθείται η ίδια λογική, με τη διεπαφή ή διεύθυνση εξόδου να ονομάζεται αυτή τη φορά προεπιλεγμένη πύλη (default gateway).

Η δυναμική δρομολόγηση βασίζεται στην αυτοματοποιημένη δημιουργία των πινάκων δρομολόγησης από τα πρωτόκολλά δρομολόγησης, τα οποία αποφασίζουν για τη βέλτιστη διαδρομή αξιοποιώντας συγκεκριμένα κριτήρια. Ενδεικτικά, αναφέρονται τα πρωτόκολλα RIP, EIGRP και OSPF. Τα πρωτόκολλα αυτά ανήκουν στην κατηγορία των πρωτοκόλλων IGP (Interior Gateway Protocols), τα οποία χρησιμοποιούνται για τον καθορισμό των πινάκων δρομολόγησης μέσα σε ένα αυτόνομο σύστημα (Autonomous System – AS). Αντιστοίχως, υπάρχουν τα πρωτόκολλα EGP (Exterior gateway Protocol), που αφορούν τη δρομολόγηση μεταξύ διαφορετικών αυτόνομων συστημάτων, με πιο σύνηθες το πρωτόκολλο BGP.

2.4.4 ICMP

Το Internet Control Messaging Protocol (ICMP) είναι ένα πρωτόκολλο ελέγχου που χρησιμοποιείται από το πρωτόκολλο IP με σκοπό τη μεταφορά μηνυμάτων ελέγχου, λαθών και πληροφοριών κατάστασης. Το ICMP χρησιμοποιείται από το IPv4 και σε νεότερη μορφή του (ICMP6) από το IPv6. Υλοποιείται με μικρού μεγέθους μηνύματα που προσδιορίζονται με συγκεκριμένο κωδικό τύπου (type). Η πιο συχνή χρήση του ICMP είναι το μήνυμα αιτήματος echo request (ICMP type 8), το οποίο απαντάται με μήνυμα απόκρισης ICMP echo reply (type 0) από τον απέναντι host εφόσον υπάρχει και επιθυμεί να κάνει αισθητή την παρουσία του.

Τα μηνύματα ICMP, συνήθως, επιτρέπεται να κινούνται ελεύθερα. Θα πρέπει να σημειωθεί, όμως, ότι ένα ICMP πακέτο περιέχει και ένα προαιρετικό πεδίο Data. Το payload που μπορεί να εισαχθεί από έναν επιτιθέμενο στο πεδίο αυτό, μπορεί να αποτελέσει ένα μέσο αποστολής κακόβουλου κώδικα στον υπολογιστή-στόχο.

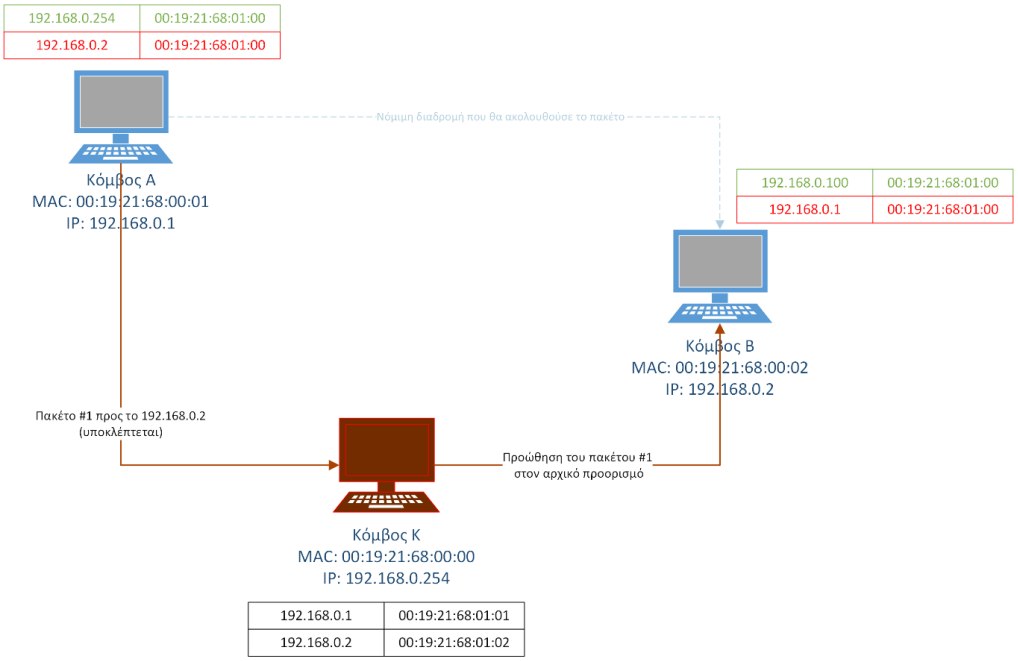
Τέλος, η χρήση του ICMP είναι πολύ συχνή σε επιθέσεις άρνησης εξυπηρέτησης (Denial of Service - DoS). Η επίθεση υλοποιείται με τη μαζική αποστολή πακέτων, τα οποία ο υπολογιστής-στόχος καλείται να απαντήσει. Όμως στην προσπάθεια αυτή παρασύρεται σε εξάντληση των πόρων του, με αποτέλεσμα να μην εξυπηρετούνται κατόπιν τα νόμιμα αιτήματα.

2.4.5 ARP

Αναφέρθηκε, νωρίτερα, πως κάθε επίπεδο του Μοντέλου του Διαδικτύου παρέχει υπηρεσίες στο αμέσως επόμενο, ενθυλακώνοντας την πληροφορία που λαμβάνει από το αμέσως προηγούμενο. Άρα, όταν ένα πακέτο πρέπει να ταξιδέψει από τον κόμβο Α στον κόμβο Β (έχοντας ως διεύθυνση προέλευσης την IP διεύθυνση του κόμβου Α και ως διεύθυνση προορισμού την IP διεύθυνση του κόμβου Β) θα ενθυλακωθεί σε πλαίσια με διεύθυνση προέλευσης τη διεύθυνση MAC της διεπαφής (NIC) του κόμβου Α και διεύθυνση προορισμού τη διεύθυνση MAC της διεπαφής του κόμβου Β.

Από τα παραπάνω, προκύπτει πως θα πρέπει να υπάρχει μια αντιστοίχιση μεταξύ των IP διευθύνσεων των κόμβων και των διευθύνσεων MAC των διεπαφών τους. Για να δημιουργηθεί κα να τηρηθεί η αντιστοίχιση αυτή, ενημερώνονται πίνακες στους οποίους μια διεύθυνση IP αντιστοιχίζεται με μια διεύθυνση MAC. Οι πίνακες αυτοί ονομάζονται πίνακες ARP και το πρωτόκολλο που καθορίζει τον τρόπο δημιουργίας και διαχείρισής τους ονομάζεται Address Resolution Protocol (ARP). Το πρωτόκολλο ARP περιγράφεται στο RFC 826.

Κάθε κόμβος τηρεί ένα πίνακα ARP όπου εκεί βρίσκονται οι αντιστοιχίες φυσικών διευθύνσεων (MAC) και διευθύνσεων δικτύου (IP). Άρα αν ένας επιτιθέμενος αποκτήσει πρόσβαση στον πίνακα αυτό δυο κόμβων που επικοινωνούν, μπορεί να τους αναγκάσει να διοχετεύουν όλη την πληροφορία μέσω του επιτιθέμενου, όπως φαίνεται στην Εικόνα 2.10.



Εικόνα 2.10 *ARP Poisoning.*

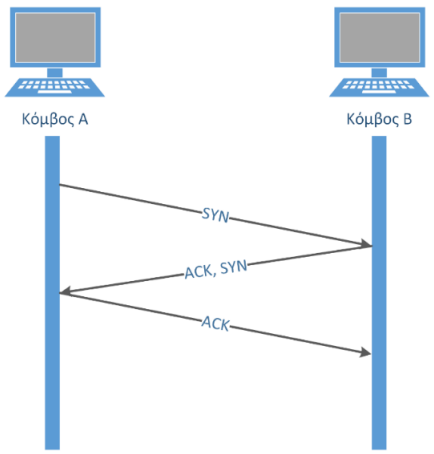
2.5 Το επίπεδο Μεταφοράς

Στο επίπεδο δικτύου, λαμβάνεται μέριμνα για τη διασύνδεση δυο κόμβων δικτύου, έστω Α και Β. Το επόμενο επίπεδο, το επίπεδο μεταφοράς, υλοποιείται από πρωτόκολλα τα οποία αναλαμβάνουν την επικοινωνία μεταξύ δυο εργασιών των κόμβων Α και Β, μέσω μιας διαδικασίας πολύπλεξης – αποπολύπλεξης με χρήση των 65535 διαθέσιμων θυρών. Συγκεκριμένα, κάθε διεργασία χρησιμοποιεί μια θύρα για να δημιουργήσει μια σύνδεση και να στείλει ή να λάβει δεδομένα. Ο συνδυασμός διεύθυνσης IP και αριθμού πόρτας (port) ονομάζεται socket.

Στο επίπεδο μεταφοράς συναντάμε δυο βασικά πρωτόκολλα. Το User Datagram Protocol (UDP) και το Transport Control Protocol (TCP). Στη συνέχεια, θα παρατεθεί μια σύντομη περιγραφή τους.

2.5.1 Το πρωτόκολλο TCP

Το πρωτόκολλο TCP, που περιγράφεται στο RFC793, είναι ένα προσανατολισμένο στη σύνδεση (connection oriented) πρωτόκολλο, δηλαδή απαιτείται αρχικά η εδραίωση μιας σύνδεσης μετά από μια διαδικασία τρίδρομης χειραψίας (three-way handshake), όπως φαίνεται στην εικόνα 2.11.



Εικόνα 2.11 *Three-way handshake.*

Αρχικά, ο κόμβος Α αρχικοποιεί τη σύνδεση, αποστέλλοντας ένα segment με ενεργοποιημένο (set) το flag SYN του TCP header. Ο κόμβος Β λαμβάνει το segment και απαντά με ένα δικό του segment, όπου έχει ενεργοποιημένα τα flags SYN και ACK. Ο κόμβος Α επιβεβαιώνει, απαντώντας με τη σειρά του με ένα segment, που έχει ενεργοποιημένο το flag ACK.

Η διαδικασία τρίδρομης χειραψίας αποτελεί μια ευπάθεια του TCP πρωτοκόλλου, καθώς μπορεί να χρησιμοποιηθεί από μια κακόβουλη οντότητα για την υλοποίηση μιας επίθεσης πλημμύρας (SYN flood attack). Στην επίθεση αυτή, ο εισβολέας αρχικοποιεί συνεχώς συνδέσεις (στέλνοντας segments με το SYN flag ενεργοποιημένο) χωρίς ποτέ να τις ολοκληρώνει. Έτσι δεσμεύονται συνεχώς πόροι ως την τελική εξάντληση (οπότε η επίθεση αναβαθμίζεται σε τύπου DoS) των διαθέσιμων πόρων.

Το πρωτόκολλο IP είναι πρωτόκολλο βέλτιστης προσπάθειας (best effort). Αυτό σημαίνει, πως δεν εγγυάται ούτε την παράδοση ενός πακέτου, ούτε τον έλεγχο συμφόρησης στο δίκτυο. Το πρωτόκολλο TCP, αντιθέτως, παρέχει:

- Αξιόπιστη μεταφορά δεδομένων (reliable data transfer), μέσω της υλοποίησης μηχανισμών ανίχνευσης λαθών και επαναμετάδοσης.

- Έλεγχο ροής. Το πρωτόκολλο TCP χρησιμοποιεί ενταμιευτές (buffers), όπου αποθηκεύει τα ληφθέντα δεδομένα μέχρι να τα διοχετεύσει στην εφαρμογή-παραλήπτη. Αν η ροή διοχέτευσης (τροφοδοσίας) είναι ταχύτερη από το ρυθμό επεξεργασίας (κατανάλωσής) τους από την εφαρμογή, υπάρχει το ενδεχόμενο υπερχείλισης του ενταμιευτή και απώλειας δεδομένων. Το πρωτόκολλο TCP μπορεί και καθορίζει ένα «παράθυρο» (window) λήψης συγκεκριμένου μεγέθους έτσι ώστε ο ρυθμός της να μην οδηγήσει σε υπερχείλιση του buffer του αποδέκτη.

- Έλεγχο συμφόρησης (congestion control). Το πρωτόκολλο TCP έχει τη δυνατότητα να ανιχνεύει συμφόρηση στο δίκτυο και να προσαρμόζει ανάλογα το ρυθμό μετάδοσης. Έχουν προταθεί διάφοροι μηχανισμοί ελέγχου συμφόρησης, όπως η διακύμανση του χρόνου RTT, η αργή εκκίνηση, η γρήγορη επαναμετάδοση, κ.ά., των οποίων η περιγραφή δεν εμπίπτει στο πλαίσιο του παρόντος βιβλίου.

2.5.2 Το πρωτόκολλο UDP

Το πρωτόκολλο UDP, που περιγράφεται από το RFC 7683, είναι, σε αντίθεση με το TCP, ένα πρωτόκολλο ασυνδεσμικής (connectionless) μεταφοράς. Αυτό σημαίνει ότι δεν απαιτείται η εδραίωση σύνδεσης πριν την αποστολή δεδομένων, ενώ δεν παρέχεται κάποιος μηχανισμός αξιόπιστης μεταφοράς ή ελέγχου ροής. Το πρωτόκολλο UDP είναι ουσιαστικά ένα best effort πρωτόκολλο με μοναδικό (προαιρετικό) έλεγχο το άθροισμα ελέγχου.

Θα μπορούσε να ισχυριστεί κανείς, ότι δεν υπάρχει ανάγκη χρήσης του πρωτοκόλλου UDP όταν το TCP παρέχει όλους αυτούς τους μηχανισμούς. Παρόλα αυτά, το πρωτόκολλο UDP χρησιμοποιείται σε περιπτώσεις όπου:

- Υλοποιούνται εφαρμογές πραγματικού χρόνου, όπου οι επαναμεταδόσεις δεν είναι επιθυμητές.

- Δεν απαιτείται αξιόπιστη μετάδοση.

- Απαιτείται γρήγορη μετάδοση ή πολυεκπομπή δεδομένων.

- Η εφαρμογή στο ανώτερο επίπεδο (εφαρμογής) υλοποιεί η ίδια τους απαραίτητους μηχανισμούς αξιόπιστης επικοινωνίας.

Γενικά, το UDP βρίσκει εφαρμογή σε περιπτώσεις εφαρμογών που είναι ανελαστικές στο χρόνο, ενώ το TCP σε περιπτώσεις εφαρμογών που είναι ανελαστικές στην ακριβή (χωρίς λάθη ή ελλείψεις) μετάδοση των δεδομένων.

2.6. Το επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής είναι αυτό στο οποίο, για παράδειγμα, εκτελούνται οι διαδικτυακές εφαρμογές που χρησιμοποιούμε καθημερινά. Υπηρεσίες, όπως ο παγκόσμιος ιστός, η ηλεκτρονική αλληλογραφία, η ονοματοδοσία και πολλές ακόμη άλλες, χρησιμοποιούν για τη λειτουργία τους πρωτόκολλα του επιπέδου εφαρμογής.

Στο επίπεδο εφαρμογής, ιδιαίτερο ρόλο επιτελεί ο ανθρώπινος παράγοντας, είτε με το ρόλο του κατασκευαστή είτε με το ρόλο του χρήστη. Σε πολλές περιπτώσεις, εντοπίζονται ευπάθειες προερχόμενες από αστοχίες και παραλείψεις κατά την ανάπτυξη των διαδικτυακών εφαρμογών (Web applications), οι οποίες συνήθως διορθώνονται με αναβαθμίσεις (ενημερώσεις) του λογισμικού εφαρμογών ή/και του λογισμικού συστήματος.

Στη συνέχεια, θα αναφερθούμε σε τρία βασικά πρωτόκολλα του επιπέδου εφαρμογής:

- Το DNS, που έχει θεμελιώδη σημασία στον κόσμο του Internet, καθώς αποτελεί τον απαραίτητο «τηλεφωνικό κατάλογό» του.
- Το SMTP, που είναι το βασικό στοιχείο λειτουργίας του e-mail («ταχυδρομείου» στο Internet).
- Το HTTP, το οποίο είναι το πιο συχνά χρησιμοποιούμενο από τις διαδικτυακές εφαρμογές πρωτόκολλο.

2.6.1 Σύστημα ονοματοδοσίας

Κάθε host που συμμετέχει σε ένα δίκτυο IP, όπως για παράδειγμα το Internet, πρέπει να έχει τουλάχιστον μια διεύθυνση IP μέσω της οποίας είναι προσβάσιμος. Άρα, για να επικοινωνήσει κάποιος με ένα δικτυωμένο host θα πρέπει να γνωρίζει τη διεύθυνση IP του τελευταίου. Το παραπάνω, γίνεται εύκολα κατανοητό αν σκεφτεί κανείς πως για κάθε συνδρομητή τηλεφωνίας αντιστοιχεί ένας τουλάχιστον τηλεφωνικός αριθμός τον οποίο πρέπει να γνωρίζει κανείς για να τον καλέσει και να μιλήσει μαζί του.

Μερικά από τα προβλήματα με τους συνδρομητές τηλεφωνίας είναι ότι:

- είναι δύσκολο να θυμόμαστε τους αριθμούς τηλεφώνου,
- ένας χρήστης μπορεί εύκολα να αλλάξει αριθμό τηλεφώνου, οπότε άμεσα πρέπει να μάθουν όλοι οι υπόλοιποι τον καινούργιο αριθμό τηλεφώνου για να μπορούν να επικοινωνήσουν μαζί του.

Τα παραπάνω προβλήματα μπορούν εύκολα να επιλυθούν με τη χρήση ηλεκτρονικών καταλόγων (όπως οι επαφές σε ένα κινητό τηλέφωνο). Έτσι, δεν χρειάζεται πλέον να θυμόμαστε τον αριθμό, τον οποίο έχουμε καταχωρήσει στον κατάλογο, αλλά το όνομα του συνδρομητή.

Αντίστοιχα, στα δίκτυα IP είναι πιο εύκολο να θυμόμαστε ονόματα κόμβων (όπως για παράδειγμα www.uom.gr ή mail.google.com) παρά διευθύνσεις IPv4, όπως 195.251.213.104 ή 173.194.112.86. Πόσο μάλλον όταν πρέπει να αναφερόμαστε σε διευθύνσεις IPv6.

Το σύστημα που έχει αναπτυχθεί με σκοπό να μεταφράζει τα ονόματα, που εύκολα θυμόμαστε, σε διευθύνσεις IP, που αναγνωρίζουν οι δρομολογητές, είναι το DNS (Domain Name Service). Η λειτουργία του DNS περιγράφεται στα RFC 1034 και 1035. Τα βασικά στοιχεία του συστήματος είναι:

- Ο χώρος ονομάτων: Είναι μια ιεραρχική δενδρική δομή.
- Η βάση δεδομένων DNS: Είναι μια ιεραρχική και κατανεμημένη βάση δεδομένων. Οι εγγραφές ομαδοποιούνται σε ζώνες και τα βασικά στοιχεία κάθε εγγραφής είναι:
    - το όνομα,
    - η κλάση της εγγραφής,

- ο τύπος της εγγραφής,
- το περιεχόμενο (συνήθως μια διεύθυνση IP),
- η διάρκεια ζωής.

- Οι διακομιστές ονοματοδοσίας: Είναι οι διακομιστές που παρέχουν την υπηρεσία DNS.

- Οι επιλύτες (resolvers): Οι διεργασίες που εκτελούνται στα συστήματα πελάτες (clients) και είναι υπεύθυνες για το ερώτημα προς τους διακομιστές και τη λήψη των απαντήσεων από αυτούς.

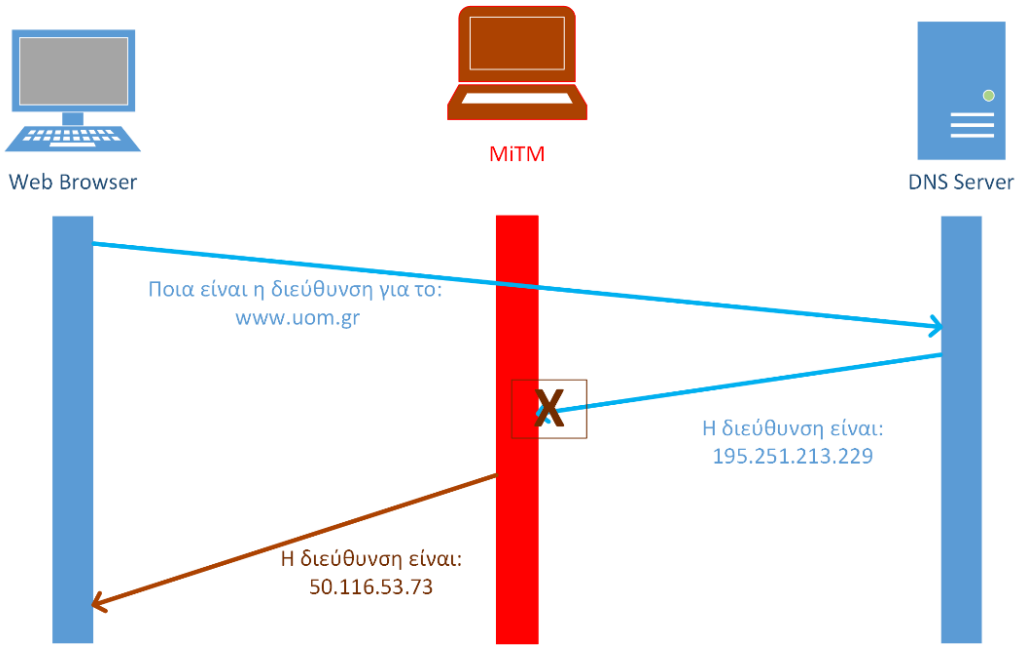
Το σύστημα DNS, υλοποιείται με χρήση κατάλληλων εφαρμογών, όπως το Bind ή το Microsoft DNS Server. Έχουν παρουσιαστεί ευπάθειες στο σύστημα DNS, οι οποίες μπορούν να οδηγήσουν σε επιθέσεις, ορισμένες από τις οποίες περιγράφονται στη συνέχεια (RFC 3833).

2.6.2 Επιθέσεις επιπέδου εφαρμογής

Στη συνέχεια, θα παρουσιαστούν σύντομα ορισμένες βασικές επιθέσεις στο επίπεδο εφαρμογής.

2.6.2.1 Packet Interception

Τα ερωτήματα και οι απαντήσεις σε ένα σύστημα DNS χρησιμοποιούν ένα UDP πακέτο το οποίο μεταδίδεται χωρίς κρυπτογράφηση. Έτσι, μπορεί να πραγματοποιηθεί μια επίθεση ενδιάμεσου (monkey-in-the-middle), κατά την οποία ο ενδιάμεσος αλλοιώνει ένα ερώτημα ή συνηθέστερα μια απάντηση. Με τον τρόπο αυτό, ο resolver μπορεί να οδηγηθεί σε μια διαφορετική τοποθεσία από την επιθυμητή, η οποία ενδέχεται να ελέγχεται από τον επιτιθέμενο.



Εικόνα 2.12 *Επίθεση ενδιάμεσου.*

Η αντιμετώπιση των επιθέσεων αυτών είναι εφικτή με χρήση των Security Extensions του DNS (DNSSEC), όπου, με τη βοήθεια της κρυπτογραφίας, διασφαλίζεται η αυθεντικότητα του κάθε μηνύματος. Ο τρόπος με τον οποίο επιτυγχάνεται κάτι τέτοιο, θα εξεταστεί σε επόμενα κεφάλαια.

2.6.2.2 Betrayal by Trusted Server

Ουσιαστικά, αποτελεί μια επίθεση ενδιάμεσου (man-in-the-middle), με τη διαφορά πως ο ενδιάμεσος είναι ένας κανονικός DNS server, ο οποίος θεωρείται έμπιστος από τον επιλύτη (resolver). Πολλές φορές, κατά την αυτόματη απόδοση παραμέτρων δικτύου σε ένα host, ο χρήστης αποδέχεται (πέρα από τη διεύθυνση IP που του αποδίδεται) και παραμέτρους, όπως οι διακομιστές ονοματοδοσίας (DNS servers). Είναι δυνατό, ένας από τους αποδιδόμενους διακομιστές, για κάποιο λόγο, να υποδεικνύει (μέσω των απαντήσεών του) στον επιλύτη σκόπιμα λανθασμένες τοποθεσίες.

2.6.2.3 Distributed Denial of Service

Μια κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS) έχει ως σκοπό τον κατακλυσμό ενός εξυπηρετητή από πακέτα με συχνότητα μεγαλύτερη από εκείνη με την οποία ο τελευταίος μπορεί να ανταποκριθεί. Τα πακέτα αυτά είναι συνήθως:

- Πακέτα τύπου ICMP.
- Πακέτα ερωτημάτων (queries).

Σε κάθε περίπτωση, η αναχαίτιση επιθέσεων DDoS είναι εφικτή με χρήση κατάλληλου φιλτραρίσματος πακέτων.

2.6.2.4 Cache Poisoning

Το σύστημα DNS έχει ιεραρχική δομή οργάνωσης. Έτσι, ο κάθε επιλύτης (resolver) απευθύνει το ερώτημά του σε ένα DNS διακομιστή (server). Εάν ο server αυτός δεν τηρεί αρχείο ζώνης (μια ζώνη αποτελεί ένα τμήμα του χώρου ονομάτων DNS) για το domain του ερωτήματος, θα πρέπει να απευθύνει το ερώτημα σε ένα server που βρίσκεται υψηλότερα στην ιεραρχία. Όταν τελικά λάβει απάντηση, πέρα από το να την προωθήσει στον επιλύτη, την αποθηκεύει σε μια μνήμη (cache), έτσι ώστε αν ερωτηθεί ξανά στο μέλλον, να μπορεί να απαντήσει άμεσα.

Άρα, λοιπόν, το πρώτο σημείο στο οποίο ένας DNS server αναζητά μια απάντηση, είναι η τοπική μνήμη cache. Αυτή την μνήμη προσπαθεί να εκμεταλλευτεί ένας επιτιθέμενος, όταν εξαπολύει μια επίθεση που στοχεύει στην εισαγωγή πλαστών εγγραφών δεδομένων, έτσι ώστε η απάντηση που θα δοθεί στον επιλύτη, όταν ρωτήσει κάτι που αφορά την παραποιημένη εγγραφή, να είναι παραπλανητική.

Για την επίλυση του παραπάνω προβλήματος, ενδείκνυται η χρήση DNSSEC, έτσι ώστε κάθε απάντηση να συνοδεύεται από την κατάλληλη ψηφιακή υπογραφή (βλ. Κεφάλαιο 8). Μόνον απαντήσεις, οι οποίες υπογράφονται από τον αναμενόμενο server μπορούν να γίνονται αποδεκτές και να εισάγονται κατόπιν στην μνήμη cache.

2.6.3 Το πρωτόκολλο HTTP

Το HTTP είναι το πρωτόκολλο πάνω στο οποίο βασίζεται η λειτουργία του World Wide Web (WWW). Είναι ένα stateless πρωτόκολλο που χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP. Ο όρος stateless αφορά τη λειτουργία του πρωτοκόλλου και συγκεκριμένα ότι χειρίζεται κάθε δοσοληψία (transaction) ξεχωριστά. Έτσι, μια σύνοδος ξεκινά με ένα αίτημα από τον πελάτη προς το διακομιστή και τερματίζεται με την απάντηση από το διακομιστή προς τον πελάτη. Η απάντηση περιλαμβάνει ένα ή περισσότερα αντικείμενα, χωρίς να τηρούνται κάπου πληροφορίες συνόδου.

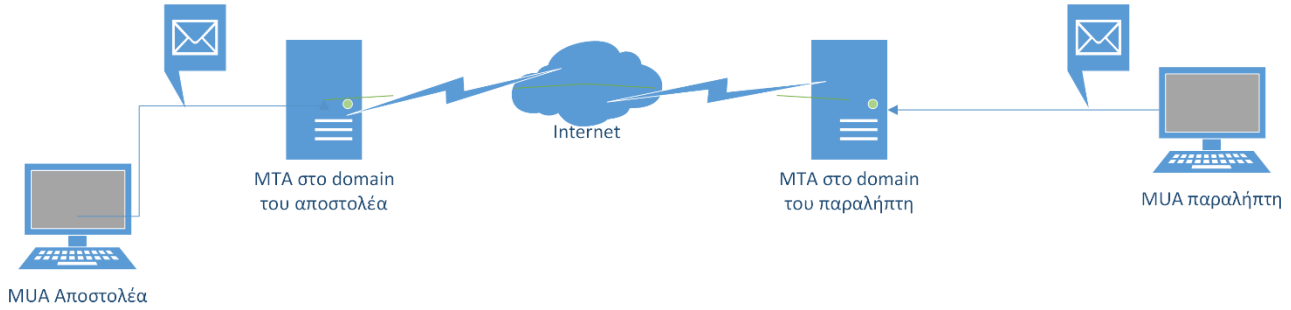
Το ακρωνύμιο HTTP (Hyper-Text Transfer Protocol) είναι συνήθως παραπλανητικό, καθώς με το HTTP μπορούν να μεταφερθούν δεδομένα διαφόρων μορφότυπων (π.χ. ήχος, video, κ.ά.), πέραν του κειμένου. Ένα μήνυμα HTTP αποτελείται από την κεφαλίδα (header), η οποία, στην περίπτωση του αιτήματος περιλαμβάνει τη μέθοδο και τα στοιχεία αιτήματος, ενώ στην περίπτωση της απάντησης περιλαμβάνει την κατάσταση απόκρισης και τα στοιχεία απάντησης. Επίσης, περιλαμβάνεται το σώμα (body), όπου περιέχονται τα δεδομένα που διακινούνται.

Περισσότερες πληροφορίες για τη μορφή των μηνυμάτων και για την ασφάλεια του HTTP πρωτοκόλλου θα παρουσιαστούν στα Κεφάλαια 4 και 5.

2.6.4 Ηλεκτρονική αλληλογραφία

Η ηλεκτρονική αλληλογραφία ή ηλεκτρονικό ταχυδρομείο (e-mail) είναι μια από τις δημοφιλέστερες υπηρεσίες του Internet. Η υπηρεσία αυτή βασίζεται στο πρωτόκολλο SMTP (Simple Mail Transfer Protocol), το οποίο περιγράφεται στο RFC 2821 και είναι ένα από τα παλιότερα πρωτόκολλα του Internet (εμφανίστηκε πολύ πριν το HTTP).

Το SMTP, όπως φανερώνει και το όνομά του, είναι ένα ιδιαίτερα απλό πρωτόκολλο. Το πρωτόκολλο SMTP χρησιμοποιείται για την παράδοση της αλληλογραφίας στους MTA (Mail Transfer Agents), προς τους οποίους αποστέλλουν την αλληλογραφία αυτή οι MUA (Mail User Agents).



Εικόνα 2.13 *Διακίνηση ηλεκτρονικής αλληλογραφίας (e-mail).*

Στην Εικόνα 2.13, ο MUA του πελάτη (π.χ. Mozilla Thunderbird, Microsoft Outlook, κλπ.) επικοινωνεί με τον MTA που εξυπηρετεί το domain του αποστολέα (sender), ο οποίος εκτελεί κατάλληλο λογισμικό (π.χ. Sendmail) και μόλις λάβει το μήνυμα, το προωθεί στον MTA που εξυπηρετεί το domain του παραλήπτη (recipient). Η εύρεση του MTA του παραλήπτη γίνεται με χρήση της υπηρεσίας DNS.

Για την επικοινωνία του MUA του αποστολέα με τον MTA και την παράδοση μηνύματος προς αποστολή, ο MUA χρησιμοποιεί SMTP commands, όπως παρουσιάζονται στην Εικόνα 2.14.

```
File  Edit  View  Search  Terminal  Help
$ telnet mail.[redacted].gr 25
Trying 62.[redacted].201...
Connected to mail.[redacted].gr.
Escape character is '^]'.
220 ESMTP
HELO thisisatest.net
250 ch[redacted].gr
MAIL FROM:<me@thisisatest.net>
250 2.1.0 Ok
RCPT TO:<[redacted]@uom.gr>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Hello,

This is a nice test!

.
250 2.0.0 from MTA(smtp:[127.0.0.1]:10025): 250 2.0.0 Ok: queued as 9FDD330001D1
quit
221 2.0.0 Bye
Connection closed by foreign host.
$
```

Εικόνα 2.14 *Αποστολή μηνύματος e-mail με χρήση του SMTP.*

Στην παραπάνω εικόνα, παρατηρούμε πως συνδεθήκαμε με έναν SMTP server και στείλαμε μήνυμα από την ανύπαρκτη διεύθυνση me@thisisatest.net, το οποίο ο παραλήπτης, στη συνέχεια, παρέλαβε κανονικά, όπως φαίνεται στην Εικόνα 2.15 που ακολουθεί:

Εικόνα 2.15 *Μήνυμα που παραλήφθηκε.*

Στον τομέα της ασφάλειας, το SMTP δεν υλοποιεί κανένα σχετικό μηχανισμό, καθώς κατά το σχεδιασμό του όλοι οι εμπλεκόμενοι για τη διακίνηση της αλληλογραφίας θεωρούνταν έμπιστοι. Έτσι, κάθε MTA δέχεται μηνύματα αλληλογραφίας χωρίς να ελέγχει αν ο αποστολέας είναι υπαρκτός. Αυτή η παραδοχή του συστήματος είναι και ο βασικός λόγος για την άνθηση της ανεπιθύμητης αλληλογραφίας (spam mail). Ακόμη, στις αρχικές υλοποιήσεις, σε έναν MTA μπορούσε να συνδεθεί ο καθένας και να τον χρησιμοποιήσει χωρίς να ελέγχεται η ταυτότητά του (open relay).

Παρατηρούμε ότι η αλληλογραφία μεταφέρεται ως απλό κείμενο (plaintext), δηλαδή χωρίς κρυπτογράφηση. Το SMTP έχει σχεδιαστεί για να μεταφέρει δεδομένα ASCII 7-bit. Σήμερα, μπορούμε να παρατηρήσουμε, ότι μέσω ηλεκτρονικού ταχυδρομείου μεταφέρονται αρχεία εικόνας, ήχου, λογιστικά φύλλα κοκ. Θα αναρωτηθεί κανείς, πώς γίνεται να χρησιμοποιείται για τη μεταφορά δεδομένων διαφόρων μορφότυπων ένα πρωτόκολλο σχεδιασμένο να μεταφέρει ASCII κείμενο; Ο τρόπος με τον οποίο γίνεται αυτό, είναι η μετατροπή όλων των δεδομένων σε μορφή ASCII, κάτι που επιτυγχάνεται με τη χρήση της κωδικοποίησης Base64.

Άρα, μπορούμε να εντοπίσουμε δυο σημαντικά ζητήματα για την ασφάλεια:

- Δεν υπάρχει έλεγχος της ταυτότητας αποστολέα.
- Τα μηνύματα μεταφέρονται ως απλό κείμενο (plaintext).

Για την αντιμετώπιση των παραπάνω ζητημάτων προτείνονται:

- Η χρήση μηχανισμού αυθεντικοποίησης.
- Ο περιορισμός των τερματικών που επιτρέπεται να χρησιμοποιήσουν το server για αποστολή αλληλογραφίας, με χρήση κατάλληλων λιστών πρόσβασης.
- Η χρήση τεχνικών απόκρυψης του περιεχομένου (π.χ. κρυπτογραφίας).

2.7 Συστήματα Διάχυτου Υπολογισμού

Η ανάπτυξη των δικτύων και κυρίως της ασύρματης δικτύωσης, έχει δώσει σάρκα και οστά στο όραμα του Mark Weiser, ο οποίος πρώτος είχε εισάγει τον όρο της απανταχού παρούσας ή διάχυτης υπολογιστικής (ubiquitous / pervasive computing). Με τον όρο αυτό, αναφερόμαστε στη διασπορά διασυνδεδεμένων υπολογιστικών συστημάτων στο φυσικό χώρο, χωρίς αυτά να γίνονται ενοχλητικά ή άμεσα αντιληπτά από τους χρήστες με τους οποίους αλληλεπιδρούν.

Η ανάπτυξη των υποδομών στις επικοινωνίες, έχει δώσει τεράστια ώθηση στο διάχυτο υπολογισμό. Στη συνέχεια, θα παρουσιαστούν εν συντομία τρεις βασικές και πολλές φορές αλληλεπικαλυπτόμενες εφαρμογές του, καθώς η ανάλυση του χώρου δεν είναι αντικείμενο του παρόντος εγχειριδίου.

2.7.1 Προσωπικά δίκτυα

Ένα προσωπικό δίκτυο είναι ένα προσωποκεντρικό δίκτυο, το οποίο προσαρμόζεται στο πλαίσιο (context) με σκοπό να παρέχει υπηρεσίες στο χρήστη. Το προσωπικό δίκτυο δεν περιορίζεται γύρω από ένα άτομο (χρήστη), όπως ένα δίκτυο προσωπικής περιοχής, αλλά προσαρμόζεται στο πλαίσιο και, κάνοντας χρήση τεχνολογιών διασύνδεσης, παρέχει υπηρεσίες προς το χρήστη. Ένα παράδειγμα προσωπικού δικτύου, είναι το δίκτυο στο οποίο συμμετέχει ένα έξυπνο σπίτι (smart home), το οποίο εξυπηρετεί τις προσωπικές ανάγκες ενός χρήστη, ενόσω αυτός μπορεί να βρίσκεται στο χώρο εργασίας του.

Τα προσωπικά δίκτυα αποτελούν ad-hoc δίκτυα, όπου οι συνδέσεις δεν είναι κεντρικά διαχειριζόμενες, αλλά προκύπτουν κατά βούληση μεταξύ των συσκευών. Στα ad-hoc δίκτυα, γενικότερα, ανακύπτει το ζήτημα της αυθεντικοποίησης (authentication) και της εξουσιοδότησης (authorization), καθώς δεν υπάρχει κάποιος κεντρικός συνδεδεμένος πάροχος ταυτοτήτων (identity provider), ούτε κάποιο σημείο απόφασης και εφαρμογής πολιτικών ελέγχου πρόσβασης.

Μια λύση, που εφαρμόζεται συνήθως, είναι το μοντέλο του resurrecting duckling. Κάθε συσκευή (όπως ένα DVD player) θεωρείται ως μια slave συσκευή. Αυτή μπορεί να εντυπωθεί (imprinted) σε μια master συσκευή και να μείνει πιστή σε αυτή, και μόνο σε αυτή, μέχρι να αποδεσμευτεί (ακολουθώντας την όπως τα μικρά παπάκια τη μητέρα πάπια). Με τον τρόπο αυτό, απαιτείται η αυθεντικοποίηση μόνο στη master συσκευή. Οι slave συσκευές μπορούν να εντυπωθούν σε μια διαφορετική master μόνο μετά την αποδέσμευσή τους από την προηγούμενη.

2.7.2 Ασύρματα δίκτυα αισθητήρων

Ένα ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network – WSN) αποτελείται από συσκευές χαμηλής επεξεργαστικής ισχύος, με μικρή κατανάλωση ενέργειας, που φέρουν έναν ή περισσότερους αισθητήρες και υλοποιούν αδόμητα ή δομημένα δίκτυα. Σκοπός τους είναι η εποπτεία αντικειμένων ή η παρακολούθηση και συλλογή δεδομένων.

Στα αδόμητα δίκτυα, οι αισθητήρες είναι περισσότεροι και διασυνδέονται μεταξύ τους, υλοποιώντας αλγόριθμους δρομολόγησης πληροφορίας, συνήθως με βάση τη βέλτιστη διαχείριση ενέργειας. Αντιθέτως, στα δομημένα δίκτυα, οι αισθητήρες, συνήθως, διασυνδέονται σε έναν κεντρικό σταθμό.

Ένα WSN παρουσιάζει ιδιαίτερα ενδιαφέρουσες ερευνητικές προκλήσεις, όσον αφορά την ασφάλεια πληροφοριών, καθώς τα δεδομένα εκπέμπονται μέσω ενός κοινού μέσου (αέρας) και, λόγω των περιορισμών των συσκευών, πρέπει οι μηχανισμοί διασφάλισης της εμπιστευτικότητας και της ακεραιότητας να λαμβάνουν υπόψη τη χαμηλή επεξεργαστική ισχύ και την περιορισμένη παροχή ενέργειας.

2.7.3 Internet of Things

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) αποτελεί μια ολιστική προσέγγιση, η οποία ωθείται από τη συνεχή ανάπτυξη των ασύρματων επικοινωνιών, μέσω της οποίας ένα σύνολο δικτυωμένων αντικειμένων (πραγμάτων) που μας περιβάλλουν θα μπορούν να αναγνωρίζονται μονοσήμαντα και να αλληλεπιδρούν μεταξύ τους. Τέτοια πράγματα (things) μπορούν να είναι οικιακές ηλεκτρικές συσκευές, που ως τώρα δεν συμμετείχαν ως ενεργά στοιχεία ενός δικτύου, αισθητήρες σε φυτά, καροτσάκια σε καταστήματα τροφίμων, κ.ά.

Το Διαδίκτυο των Πραγμάτων (ΔτΠ) βρίσκει εφαρμογή σε σχεδόν κάθε τομέα της ανθρώπινης δραστηριότητας, όπως μεταφορές, υγεία, έξυπνα περιβάλλοντα, προσωπική και κοινωνική ζωή, καινοτόμες υπηρεσίες, κ.ά. Οι βασικές προκλήσεις ασφαλείας που αντιμετωπίζει το ΔτΠ είναι:

- Να παρέχει αντοχή σε επιθέσεις, καθώς θα πρέπει να αποφεύγονται τα μοναδικά σημεία αστοχίας (single points of failure), ενώ το δίκτυο θα πρέπει να μπορεί να ανακάμψει μετά από μια επίθεση (resilience).

- Να παρέχει αυθεντικοποίηση των συμμετεχόντων πραγμάτων, δηλαδή όλες οι οντότητες που συμμετέχουν στο IoT θα πρέπει να μπορούν να αυθεντικοποιούνται.

- Να παρέχει κατάλληλη εξουσιοδότηση, ώστε ο έλεγχος πρόσβασης να επιτρέπει ή όχι την πρόσβαση στη βάση των δικαιωμάτων κάθε συμμετέχουσας οντότητας.

- Να διασφαλίζει την ιδιωτικότητα, καθώς το IoT υπάρχει δυνητικά παντού. Επομένως, θα πρέπει να μην είναι δυνατή η εκμετάλλευσή για την παραβίαση της ιδιωτικότητας των ανθρώπων που συμμετέχουν και περιβάλλονται από αυτό.

Βιβλιογραφία

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. http://doi.org/10.1016/j.comnet.2010.05.010

Convery, S. (2004). Network security architectures. Indianapolis, IN: Cisco Press.

de Vivo, M., de Vivo, G. O., & Isern, G. (1998). Internet Security Attacks at the Basic Levels. SIGOPS Oper. Syst. Rev., 32(2), 4–15. http://doi.org/10.1145/506133.506136

Jacobsson, M., Niemegeers, I., & Groot, S. H. de. (2010). Personal networks: wireless networking for personal devices. Chichester, West Sussex ; Hoboken, NJ: John Wiley.

Kurose, J. F., & Ross, K. W. (2013). Computer networking: a top-down approach (6th ed). Boston: Pearson.

Stajano, F., & Anderson, R. (2002). The Resurrecting Duckling: security issues for ubiquitous computing. Computer, 35(4), 22–26. http://doi.org/10.1109/MC.2002.1012427

Stallings, W. (2014). Data and computer communications (Tenth edition). Boston: Pearson.

Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. http://doi.org/10.1016/j.clsr.2009.11.008

Weiser, M. (1993). Some Computer Science Issues in Ubiquitous Computing. Commun. ACM, 36(7), 75–84. http://doi.org/10.1145/159544.159617

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), 2292–2330. http://doi.org/10.1016/j.comnet.2008.04.002.

Κριτήρια Αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Το μοντέλο OSI:
α) Καθορίζει τα επίπεδα ασφάλειας κάθε επιπέδου.
β) Είναι θεωρητικό πρότυπο αναφοράς.
γ) Καθορίζει 4 επίπεδα.
δ) Καθορίζει 7 επίπεδα.

2. Ο έλεγχος ισοτιμίας:
α) Συγκρίνει το μέγεθος των πλαισίων.
β) Καθορίζει πότε δύο bytes είναι ισότιμα.
γ) Μπορεί να ανιχνεύσει λάθος σε 1 bit.
δ) Λέγεται αλλιώς και CRC.

3. Το Spanning Tree Protocol (STP):
α) Υλοποιείται για την αποφυγή δημιουργίας κύκλων (loops).
β) Υλοποιείται για την δημιουργία κύκλων (loops).
γ) Τοποθετεί τα byte σε δενδρική δομή.
δ) Υλοποιείται μόνο σε hub.

4. Ποια από τα παρακάτω αποτελούν αντίμετρα σε μια επίθεση sniffing:
α) Η χρήση κρυπτογραφίας.
β) Η χρήση aDSL.
γ) Η υλοποίηση του parity bit.
δ) Η χρήση ισχυρών συνθηματικών.

5. Ποια από τις παρακάτω διευθύνσεις ανήκει στο υποδίκτυο 195.251.209.128/29:
α) 195.251.109.126.
β) 195.251.109.129.
γ) 195.251.109.135.
δ) 195.251.109.29.
ε) Όλες οι παραπάνω
στ) Καμία από τις παραπάνω.

6. Ένας δρομολογητής (router):
α) Δρομολογεί πακέτα.
β) Προωθεί πακέτα.
γ) Έχει πάντα μια μόνο διεπαφή (interface)
δ) Λειτουργεί στο επίπεδο εφαρμογής του TCP/IP.

7. Ποια από τα παρακάτω είναι πρωτόκολλα επιπέδου εφαρμογής:
α) CDMA/CD.
β) ALOHA.
γ) TCP.
δ) SMTP.
ε) GRE
στ) HTTP
ζ) UDP
η) DNS
θ) IPv6

8. Μια επίθεση DoS στοχεύει στην παραβίαση της:
α) Εμπιστευτικότητας.
β) Ακεραιότητας.
γ) Διαθεσιμότητας.
δ) Ιδιωτικότητας.

9. Το πρωτόκολλο HTTP είναι πρωτόκολλο:
α) Επιπέδου πρόσβασης δικτύου.
β) Επιπέδου μεταφοράς.
γ) Επιπέδου δικτύου.
δ) Επιπέδου εφαρμογής.

10. Τα προσωπικά δίκτυα:
α) Αποτελούνται μόνο από δίκτυα προσωπικής περιοχής.
β) Εκτείνονται σε πολύ μικρή έκταση.
γ) Δεν επιτρέπουν ad-Hoc συνδέσεις.
δ) Κανένα από τα παραπάνω.

Κεφάλαιο 3. Ασφαλής Διασύνδεση

Σύνοψη
Με βάση τις βασικές αρχές δικτύωσης που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, σε αυτό το κεφάλαιο θα εξεταστούν μέθοδοι εξασφάλισης των ιδιοτήτων της ασφάλειας στην περίμετρο και εντός ενός δικτύου. Αναλυτικότερα, θα γίνει μια σύντομη εισαγωγή στην ανάγκη προστασίας του δικτύου από εξωτερικούς κινδύνους και, στη συνέχεια, θα μελετηθούν δύο βασικά θέματα που πρέπει να λαμβάνονται υπόψη για την προστασία του: η ασφάλεια της περιμέτρου, για την οποία θα παρουσιαστούν τα τείχη προστασίας (firewalls) και τα συστήματα ανίχνευσης εισβολών (IDS), καθώς επίσης η ασφάλεια ασύρματων δικτύων, τα οποία παρουσιάζουν ιδιαίτερη αύξηση χρήσης σε συνδυασμό με την εξέλιξη των φορητών συσκευών (π.χ. smartphones, tablets).

Προαπαιτούμενη γνώση
Για την παρακολούθηση του κεφαλαίου απαιτείται η μελέτη των προηγούμενων Κεφαλαίων 1 και 2.

3.1 Εισαγωγή

Στα δύο προηγούμενα κεφάλαια, συζητήθηκαν βασικά ζητήματα ασφάλειας, καθώς και διάφορα είδη επιθέσεων. Οι επιθέσεις αυτές εκμεταλλεύονται ευπάθειες σχεδιασμού και ρυθμίσεων, ενώ εκπονούνται από επίδοξους εισβολείς οι οποίοι ακολουθούν μια, συνήθως, αναμενόμενη μεθοδολογία. Στόχος του διαχειριστή ασφάλειας ενός δικτύου είναι να αναπτύξει την κατάλληλη αμυντική στρατηγική, έτσι ώστε το δίκτυό του να είναι σε θέση να ανταπεξέρχεται σε τέτοιες επιθέσεις, καθώς και να καταγράφονται όλες οι λεπτομέρειες της διεξαγωγής τους.

Στην πρώτη παράγραφο αυτού του κεφαλαίου, θα αναφερθούν τα πιο γνωστά προφίλ επιτιθέμενων, καθώς και μια ενδεικτική μεθοδολογία επιθέσεων, η οποία συνήθως ακολουθείται. Στη συνέχεια, θα αναφερθούν τα δύο πιο γνωστά αμυντικά μοντέλα: lollipop και onion.

3.1.1 Προφίλ επιτιθέμενων

Οι επιτιθέμενοι δεν έχουν πάντα τα ίδια κίνητρα και τον ίδιο τρόπο δράσης. Οι πιο συνηθισμένες κατηγορίες επιτιθέμενων περιγράφονται στη συνέχεια.

3.1.1.1 Hackers

Οι Hackers διαθέτουν εξειδικευμένες γνώσεις και δεξιότητες στις τεχνολογίες ΤΠΕ και, ανάλογα με τα κίνητρά τους, μπορούν να κατηγοριοποιηθούν σε:

- Black-Hat hackers: Στόχος τους είναι το προσωπικό, συνήθως οικονομικό, όφελος. Αναφέρονται συχνά και με τον όρο crackers.

- White-Hat hackers: Στόχος τους είναι ο εντοπισμός ευπαθειών, με σκοπό την αποκάλυψη και την μείωση ή απαλοιφή τους. Ως εκ τούτου, φροντίζουν να μην προκαλέσουν ζημία σε συστήματα ή δεδομένα, αλλά να κοινοποιήσουν το πρόβλημα στις αρμόδιες αρχές και οργανισμούς για να αντιμετωπιστεί.

- Grey-Hat hackers: Στόχος τους είναι, επίσης, ο εντοπισμός ευπαθειών. Η διαφορά με τους White-Hat hackers έγκειται στο ότι δεν τις αποκαλύπτουν στις αρμόδιες αρχές και οργανισμούς (π.χ. στις κατασκευάστριες εταιρείες), αλλά είτε παίρνουν την κατάσταση στα χέρια τους και αντεπιτίθενται σε τυχόν επιθέσεις που προσπαθούν να εκμεταλλευτούν τις ευπάθειες αυτές, είτε τις κοινοποιούν σε επιλεγμένο κοινό με κίνητρα που δεν περιορίζονται πάντα μέσα στα όρια της νομιμότητας.

3.1.1.2 Script Kiddies

Συνήθως, δεν διαθέτουν εξειδικευμένες γνώσεις, όπως οι hackers, αλλά χρησιμοποιούν έτοιμα εργαλεία (hacking tools), δηλαδή εργαλεία που έχουν κατασκευαστεί από άλλους, για να προκαλέσουν τη μέγιστη δυνατή ζημιά με στόχο τη δυσφήμιση ή απλά για να διασκεδάσουν.

Είναι ιδιαίτερα επικίνδυνοι, καθώς δεν έχουν επίγνωση της κρισιμότητας της κατάστασης και συνήθως, όντας μικροί σε ηλικία και χωρίς να υπολογίζουν τις σχετικές ευθύνες, δεν υπολογίζουν τις συνέπειες για τους ίδιους.

3.1.1.3 Κυβερνο-κατάσκοποι

Σε αντίθεση με τους hackers, στόχος των κυβερνο-κατασκόπων (cyber spies) δεν είναι ο εντοπισμός ευπαθειών σε οποιοδήποτε σύστημα. Οι κατάσκοποι μισθώνονται από τρίτους, με σκοπό να διεισδύσουν σε ένα δίκτυο-στόχο, ώστε να υποκλέψουν συγκεκριμένες πληροφορίες, χωρίς να γίνουν αντιληπτοί από τους διαχειριστές του.

3.1.1.4 Κυβερνο-εγκληματίες

Στόχος των κυβερνο-εγκληματιών (cybercriminals) είναι το προσωπικό τους οικονομικό όφελος, ή η οικονομική καταστροφή του ιδιοκτήτη του δικτύου-στόχου. Ενδεικτικά παραδείγματα επιθέσεων από κυβερνο-εγκληματίες, είναι το spamming, το phishing και διάφορες απάτες με στόχο πάντα το οικονομικό κέρδος.

Μια υποκατηγορία των κυβερνο-εγκληματιών είναι οι κυβερνο-τρομοκράτες (cyberterrorists), οι οποίοι έχουν ως στόχο την τρομοκράτηση με επιθέσεις, όπως αυτή της κατανεμημένης άρνησης εξυπηρέτησης (DDoS) και της περαιτέρω χρήσης των στόχων για προπαγανδιστικούς ή άλλους παράνομους σκοπούς.

3.1.1.5 Insiders

Πολλές επιθέσεις δεν ξεκινούν από επιτιθέμενους εκτός του δικτύου, αλλά από νόμιμους χρήστες που δρουν μέσα από το ίδιο το δίκτυο. Οι εσωτερικοί αυτοί χρήστες είτε ακούσια ή εκούσια αποκαλύπτουν πληροφορίες ή εισάγουν κακόβουλο λογισμικό.

Η μεγάλη ανάπτυξη των ασύρματων δικτύων και η άναρχη υλοποίησή τους, έχει επιτρέψει την εκδήλωση επιθέσεων μέσα από τα δίκτυα ακόμη και από μη νόμιμους χρήστες τους, όπως για παράδειγμα σε περιπτώσεις απρόσκλητων συνδέσεων.

3.1.2 Μεθοδολογία επίθεσης

Οι διαφόρων ειδών επιθέσεις ακολουθούν, συνήθως, μια μεθοδολογία που απαρτίζεται από μια ακολουθία βημάτων, τα οποία σε γενικές γραμμές είναι:

- Αναζήτηση πληροφοριών για το στόχο: Ο επιτιθέμενος προσπαθεί να συλλέξει πληροφορίες για το στόχο, όπως εκδόσεις λειτουργικών συστημάτων, εκδόσεις λογισμικού, τοπολογία δικτύου, διαθέσιμα ασύρματα δίκτυα κ.α., προκειμένου να εντοπίσει πιθανές γνωστές ευπάθειες (π.χ. στη βάση NVD).

- Απόπειρα απόκτησης πρόσβασης: Αφού εντοπιστούν κάποιες ευπάθειες, ο επιτιθέμενος προσπαθεί να τις εκμεταλλευτεί, ώστε να αποκτήσει πρόσβαση στο δίκτυο, κατά προτίμηση με όσο το δυνατόν πιο αυξημένα δικαιώματα.

- Τροποποίηση ρυθμίσεων: Έχοντας αποκτήσει πρόσβαση, ο επιτιθέμενος τροποποιεί όσες ρυθμίσεις μπορεί, έτσι ώστε η πρόσβασή του σε μελλοντικές απόπειρες να είναι πιο εύκολη, τόσο από πλευράς χρόνου και κόπου, όσο και από πλευράς του να διακινδυνεύσει να εντοπιστεί η εισβολή του από τους διαχειριστές του δικτύου.

- Διαγραφή ιχνών: Κάθε φορά που ολοκληρώνει μια εισβολή, ο επιτιθέμενος φροντίζει ώστε να σβήνει τα ίχνη του από το σύστημα.

- Αναζήτηση πρόσθετων πληροφοριών μέσα από το δίκτυο: Ο επιτιθέμενος, έχοντας αποκτήσει πρόσβαση σε έναν κόμβο του δικτύου, προσπαθεί να εντοπίσει ακόμη περισσότερα συστήματα στο δίκτυο, στα οποία στη συνέχεια θα προσπαθήσει να παρεισφρήσει, χρησιμοποιώντας ως προκεχωρημένη θέση την τρέχουσα κατάσταση της εισβολή του.

- Πρόκληση ζημιάς: Στην περίπτωση που το αποφασίσει, είτε επειδή δεν κατάφερε να αποκτήσει τα αυξημένα δικαιώματα που ήθελε, είτε για άλλους λόγους, μπορεί να καταφύγει στην τακτική της πρόκλησης ζημιάς, αποκαλύπτοντας, τροποποιώντας ή διαγράφοντας δεδομένα και ρυθμίσεις του δικτύου.

Στο Κεφάλαιο 5, θα συζητήσουμε μια ανάλογη μεθοδολογία με βήματα που διατρέχονται σε μια τυπική επίθεση με στόχο μια διαδικτυακή εφαρμογή.

3.1.3 Αμυντικά μοντέλα

Όπως έχουμε ήδη αναφέρει, στην ασφάλεια πληροφοριών, πρωταρχικός στόχος είναι η προστασία της εμπιστευτικότητας της ακεραιότητας και της διαθεσιμότητας.

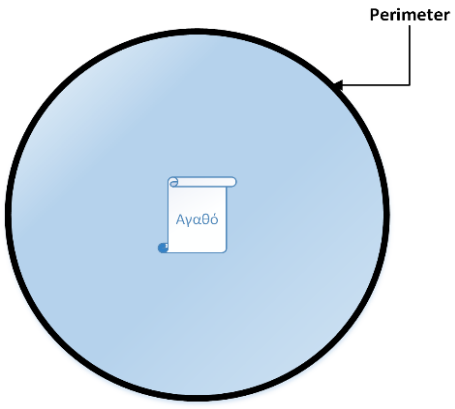
Δύο από τις πλέον δημοφιλείς προσεγγίσεις που ακολουθούνται για την αμυντική προστασία ενός δικτύου είναι γνωστές ως αμυντικά μοντέλα, ως εξής:

- Lollipop model: αφορά τη δημιουργία μιας ισχυρής αμυντικής περιμέτρου, θεωρώντας κάθε αντικείμενο εντός αυτής έμπιστο.

- Onion model: αφορά την υλοποίηση μιας πολυεπίπεδης προσέγγισης, γνωστής ως «defense in-depth».

3.1.3.1 Lollipop model

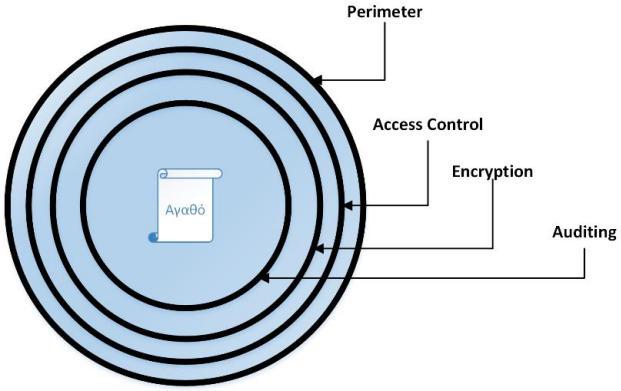
Το μοντέλο Lollipop, περιγράφει τη δημιουργία μιας ισχυρής περιμέτρου, που συνήθως υλοποιείται με συσκευές που ελέγχουν την είσοδο προς και την έξοδο από το εσωτερικό δίκτυο. Στο μοντέλο αυτό, ισχύει η παραδοχή πως η περίμετρος είναι απαραβίαστη. Αν αυτή όμως παραβιαστεί, τα αντικείμενα που βρίσκονται εντός του δικτύου είναι τελείως απροστάτευτα.



Εικόνα 3.1 *Το μοντέλο Lollipop.*

3.1.3.2 Onion model

Το μοντέλο Onion, ή defense in-depth, δεν περιορίζεται στην ασφάλεια περιμέτρου, αλλά υλοποιεί ένα σύνολο αντιμέτρων σε πολλαπλά επίπεδα, όπως έλεγχο πρόσβασης, τεχνικές κρυπτογραφίας, έλεγχο ανίχνευσης εισβολών, προστασία δικτυακών εφαρμογών κ.ά. Η ασφάλεια περιμέτρου αφορά απλά το «εξωτερικό περίβλημα», ενώ αν ο επιτιθέμενος το παραβιάσει θα πρέπει να αντιμετωπίσει όλα τα αντίμετρα που λειτουργούν στα υπόλοιπα επίπεδα προστασίας.



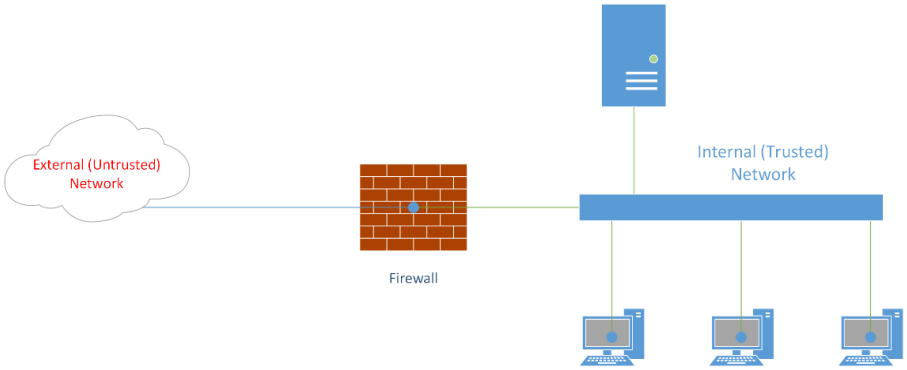
Εικόνα 3.2 *Το μοντέλο Onion.*

3.2 Ασφάλεια Περιμέτρου

Η λέξη «περίμετρος, ίσως να θυμίζει ένα φράκτη, ένα τείχος ή μια ένοπλη στρατιωτική περιπολία. Όταν αναφερόμαστε σε ένα δίκτυο, ως περίμετρο μπορούμε, αντίστοιχα, να θεωρήσουμε κάθε συσκευή, πραγματική ή εικονική, που διαχωρίζει το δίκτυο αναφοράς από όλα τα υπόλοιπα δίκτυα που το περιβάλλουν και, φυσικά, το ίδιο το Διαδίκτυο. Ως δίκτυο αναφοράς, σε σχέση με την περίμετρο, νοείται το εσωτερικό δίκτυο του οποίου τους πόρους επιθυμούμε να προστατεύσουμε. Για την επίτευξη της προστασίας αυτής χρησιμοποιούνται, σε συνδυασμό ή ξεχωριστά, διατάξεις τείχους προστασίας (firewall) και συστημάτων ανίχνευσης εισβολών (IDS).

3.2.1 Τείχος προστασίας

Το τείχος προστασίας (firewall) διαχωρίζει δύο δίκτυα με διαφορετικό βαθμό εμπιστοσύνης, ελέγχοντας την κίνηση δεδομένων μεταξύ τους (από και προς το κάθε δίκτυο).



Εικόνα 3.3 *Τείχος προστασίας.*

Μπορούμε, αρχικά, να διαχωρίσουμε τα τείχη προστασίας σε δύο βασικές κατηγορίες:

- Προσωπικά, τα οποία στοχεύουν στην προστασία ενός κόμβου (host) από εξωτερικές απειλές και συνήθως υλοποιούνται με μια εφαρμογή λογισμικού.

- Δικτυακά, τα οποία χρησιμοποιούνται για την προστασία ολόκληρου δικτύου από εξωτερικές απειλές και, συνήθως, υλοποιούνται από ένα ανεξάρτητο υπολογιστικό σύστημα ή ενσωματώνονται σε έναν περιμετρικό δρομολογητή.

Ο σχεδιασμός μιας διάταξης firewall πρέπει να διέπεται από βασικές αρχές, όπως οι ακόλουθες:

- Όλη η κίνηση μεταξύ των δικτύων πρέπει να διέρχεται μέσα από το firewall.

- Μόνον η κίνηση που καθορίζεται από την πολιτική που εφαρμόζει το firewall, επιτρέπεται να περάσει από αυτό.

- Το firewall πρέπει να είναι απαραβίαστο.

3.2.2 Είδη firewall

Τα τείχη προστασίας (firewalls) ταξινομούνται στις ακόλουθες βασικές κατηγορίες:

- Φιλτράρισμα πακέτων (Packet Filters).
- Πύλες κυκλώματος (Circuit-level Gateways).
- Πύλες εφαρμογών (Application-level Gateways).

3.2.2.1 Packet Filters

Ένα packet filtering firewall είναι η πιο κοινή διάταξη firewall. Εξετάζει κάθε πακέτο που εισέρχεται (ingress filtering) ή εξέρχεται (egress filtering) από αυτό. Η εξέταση περιορίζεται στις κεφαλίδες του επιπέδου δικτύου (IP headers) και του επιπέδου μεταφοράς (TCP/UDP headers) για να εξαχθούν:

- το πρωτόκολλο επικοινωνίας (protocol field),
- η διεύθυνση της προέλευσης (source address),
- η θύρα προέλευσης (source port),
- η διεύθυνση προορισμού (destination address),
- η θύρα προορισμού (destination port).

Οι παραπάνω πληροφορίες εξετάζονται στη βάση ενός συνόλου κανόνων, έτσι ώστε να καθοριστεί αν θα επιτραπεί ή θα απαγορευτεί η διέλευση του πακέτου. Συγκεκριμένα, οι κανόνες υλοποιούν μια λίστα ελέγχου πρόσβασης (access control list – ACL):

#	Src Addr	Src Port	Dst Addr	Dst Port	Proto	Action	Comment
1	192.168.0.0/16	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
2	172.16.0.0/12	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
3	10.0.0.0/8	*	192.168.1.0/24	*	*	permit	Permit outbound traffic
4	any	*	192.168.1.21	80	TCP	permit	Access to web server
5	any	*	192.168.1.31	25	TCP	permit	Access to mail server
6	any	500	192.168.1.2	500	UDP	permit	Access to isakmp
7	any	4500	192.168.1.2	4500	UDP	permit	Access to isakmp-nat
8	any	*	192.168.1.0/24	*	*	deny	Deny all

Πίνακας 3.1 *Λίστα Ελέγχου Πρόσβασης.*

Στον Πίνακα 3.1 παρουσιάζεται μια λίστα η οποία εξετάζει την εισερχόμενη κίνηση και περιλαμβάνει 8 κανόνες, σύμφωνα με τους οποίους:

- Επιτρέπεται η κίνηση από το δίκτυο 192.168.0.0/16 προς το δίκτυο 192.168.1.0/24
- Επιτρέπεται η κίνηση από το δίκτυο 172.16.0.0/12 προς το δίκτυο 192.168.1.0/24
- Επιτρέπεται η κίνηση από το δίκτυο 10.0.0.0/8 προς το δίκτυο 192.168.1.0/24

Οι τρείς αυτοί πρώτοι κανόνες συναντώνται συχνά σε λίστες που ελέγχουν την εισερχόμενη κίνηση που ξεκινά από το Διαδίκτυο και έχει ως προορισμό το εσωτερικό δίκτυο. Πακέτα από τα δίκτυα που αναφέρονται (10.0.0.0/8, 172.16.0.0/16 και 192.168.0.0/16), δεν προωθούνται μεταξύ δρομολογητών του Διαδικτύου. Άρα, η λήψη ενός τέτοιου πακέτου υποδεικνύει την εκδήλωση της επίθεσης τύπου spoofing attack, όπου ο επιτιθέμενος έχει τροποποιήσει τη διεύθυνση προέλευσης με στόχο να θεωρηθούν τα πακέτα ως προερχόμενα από το εσωτερικό δίκτυο.

- Επιτρέπεται η κίνηση από παντού προς τον κόμβο 192.168.1.21 στην θύρα 80, όπου «ακούει» ένας web server.
- Επιτρέπεται η κίνηση από παντού προς τον κόμβο 192.168.1.31 στην θύρα 25, όπου «ακούει» ένας mail server.
- Επιτρέπεται η κίνηση από παντού προς τον κόμβο 192.168.1.2 στην θύρα 500, όπου «ακούει» μια υπηρεσία isakmp (αν η λέξη αυτή σας είναι άγνωστη, κρατήστε τη στη μνήμη σας ως τη μελέτη του Κεφαλαίου 10).
- Επιτρέπεται η κίνηση από παντού προς τον κόμβο 192.168.1.2 στην θύρα 500, όπου «ακούει» μια υπηρεσία isakmp, όταν αυτή λειτουργεί πίσω από NAT.
- Απαγορεύεται η κίνηση από οπουδήποτε προς το δίκτυο 192.168.1.0/24.

Οι παραπάνω κανόνες (4-7) καθορίζουν την κίνηση που επιτρέπεται να διέλθει από τα εξωτερικά δίκτυα προς το εσωτερικό, που προφανώς είναι το 192.168.1.24/0. Κάθε πακέτο ελέγχεται ως προς την ικανοποίηση κάθε κανόνα, ώστε να ληφθεί η απόφαση έγκρισης της διέλευσής του ή όχι. Για να είναι όμως δυνατή η αμφίδρομη επικοινωνία θα πρέπει να καθοριστεί και η εξερχόμενη κίνηση με μια λίστα από κατάλληλους κανόνες.

Η παραπάνω προσέγγιση, όπου πρέπει ρητά να καθοριστούν κανόνες για κάθε είδους εξερχόμενης και εισερχόμενης κίνησης, αποτελεί την υλοποίηση του stateless packet filtering. Όμως, παρουσιάζει τα ακόλουθα προβλήματα:

- Κάθε πακέτο πρέπει να ελέγχεται μέχρι να βρεθεί κανόνας που να ικανοποιείται από το πακέτο αυτό και να ληφθεί η απόφαση για την εφαρμογή της ενέργειας (action) που αναφέρεται στον κανόνα. Αυτός ο τρόπος λειτουργίας σε δίκτυα με συχνή κίνηση και μεγάλο αριθμό πακέτων, μπορεί να προκαλέσει αισθητές καθυστερήσεις στην εξυπηρέτηση της κίνησης αυτής.

- Ο διαχειριστής θα πρέπει να ορίζει κανόνες και για την εισερχόμενη αλλά και για την εξερχόμενη κίνηση, αυξάνοντας έτσι το διαχειριστικό φόρτο.

- Το stateless packet filter είναι επιρρεπές σε επιθέσεις τύπου IP Spoofing (που τη γνωρίσαμε ήδη) και TCP Fragmentation, που υλοποιείται κατακερματίζοντας τα πακέτα σε μικρά τμήματα (fragments) έτσι ώστε το πεδίο κεφαλίδας FLAGS του TCP να μη βρίσκεται στο πρώτο τμήμα αλλά σε ένα από τα υπόλοιπα τμήματα που διέρχονται χωρίς να ελέγχονται από το firewall.

Για την αντιμετώπιση των παραπάνω προβλημάτων, τα packet filters είναι δυνατό να υλοποιηθούν έχοντας την ικανότητα να τηρούν την κατάσταση (state) κάθε σύνδεσης. Όταν ένας κόμβος από το εσωτερικό δίκτυο εκκινεί μια σύνδεση σε έναν άλλο κόμβο εκτός του δικτύου, το firewall καταχωρεί τη σύνδεση αυτή σε ένα πίνακα καταστάσεων (state table). Έτσι, για κάθε νέο εισερχόμενο ή εξερχόμενο από το δίκτυο πακέτο που φτάνει στο firewall:

- Αν το πακέτο αυτό ανήκει σε μια εδραιωμένη (established) σύνδεση επικοινωνίας, η διέλευσή του επιτρέπεται.

- Αν το πακέτο εκκινεί μια νέα σύνδεση (πακέτο τύπου SYN), δημιουργείται νέα εγγραφή στον πίνακα καταστάσεων. Τηρούνται, ακόμη, λίστες πρόσβασης ώστε να καθοριστεί η επιτρεπόμενη κίνηση.

- Αν το πακέτο δεν ανήκει σε μια εδραιωμένη σύνδεση και δεν είναι ένα SYN πακέτο, τότε απορρίπτεται.

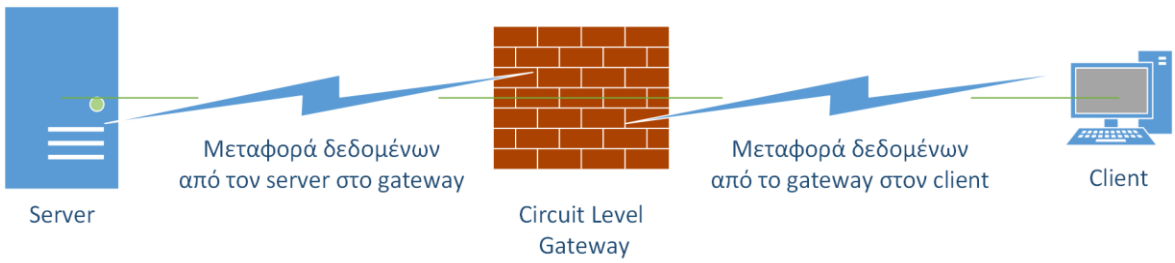
Src Addr	Src Port	Dst Addr	Dst Port	Protocol	State
192.168.1.41	45523	1.1.1.1	80	TCP	ESTABLISHED
192.168.1.47	52214	2.2.2.2	53	UDP	ESTABLISHED

Πίνακας 3.2 *Πίνακας καταστάσεων.*

Όταν η σύνδεση τερματιστεί, η σχετική εγγραφή αφαιρείται από τον πίνακα. Επίσης αφαιρούνται εγγραφές όταν λήξει ο μέγιστος χρόνος μιας αδρανούς σύνδεσης. Ο τύπος του firewall που τηρεί την κατάσταση των συνδέσεων ονομάζεται Stateful.

3.2.2.2 Circuit Level Gateways

Οι πύλες κυκλώματος (circuit gateways) έχουν ως αρχή λειτουργίας την απαγόρευση δημιουργίας απευθείας συνδέσεων μεταξύ ενός κόμβου του προστατευόμενου δικτύου και ενός κόμβου του εξωτερικού δικτύου. Σε αντίθεση δηλαδή με τα packet filters, δεν γίνεται απλά έλεγχος και εδραίωση σύνδεσης μεταξύ των επικοινωνούντων μερών, αλλά δημιουργούνται δύο διαφορετικές συνδέσεις μεταξύ των δύο κόμβων και της πύλης (gateway). Η τελευταία, στη συνέχεια, προωθεί τα segments που λαμβάνει από της μια σύνδεσης στην άλλη.



Εικόνα 3.4 *Πύλη κυκλώματος.*

Όταν ένας πελάτης επιθυμεί να εδραιώσει μια σύνδεση με ένα διακομιστή, η διαδικασία που ακολουθείται είναι:

1. Ο πελάτης ζητάει τη σύνδεση στο gateway.
2. Το gateway ελέγχει αν μια τέτοια σύνδεση επιτρέπεται.
3. Αν επιτρέπεται, τότε η σύνδεση εδραιώνεται.
4. Το gateway προωθεί τα πακέτα, χωρίς να τα αλλοιώνει, από το ένα host στο άλλο.
5. Όταν το gateway δεχτεί σχετικό αίτημα, τερματίζει τις συνδέσεις.

Ένα πρωτόκολλο που χρησιμοποιείται από τις πύλες κυκλωμάτων είναι το SOCKS. Στην υλοποίησή του ορίζονται:

- Ο SOCKS Server, που εκτελείται στο gateway.
- Ο SOCKS Client, που ενσωματώνεται στις εφαρμογές πελάτη, που κάνουν χρήση τροποποιημένων, για την υποστήριξη του SOCKS, πρωτόκολλων.
- Το SOCKS Client Library, που χρησιμοποιείται από τους διακομιστές που προστατεύονται από το firewall.

Όταν ένας πελάτης επιθυμεί να προσπελάσει μια υπηρεσία που προστατεύεται από ένα circuit level gateway, πρώτα εδραιώνει μια TCP σύνδεση με τον SOCKS Server (που ακούει στην πόρτα 1080), ακόμη και αν επιθυμεί, στη συνέχεια, να χρησιμοποιήσει μια υπηρεσία που υλοποιείται με UDP. Ο πελάτης αυθεντικοποιείται και, αν η πρόσβαση επιτραπεί, τότε το firewall προωθεί τα πακέτα για την επικοινωνία μεταξύ των δύο κόμβων.

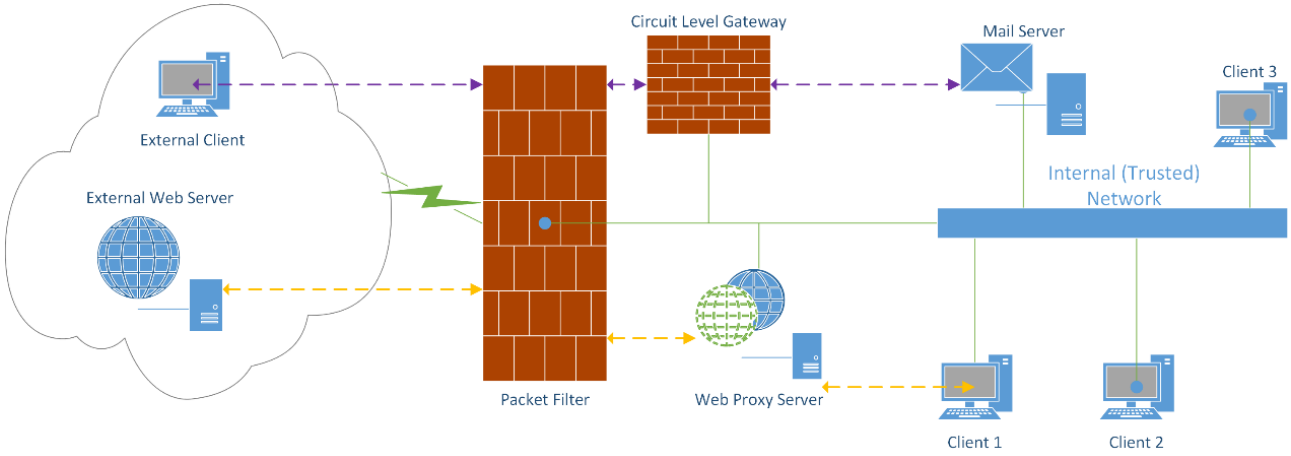
3.2.2.3 Application Level Gateways

Οι πύλες εφαρμογών (application gateways), πιο γνωστές ως proxy servers, υλοποιούνται συνήθως με προϊόντα λογισμικού που εγκαθίστανται σε έναν ή περισσότερους διακομιστές. Οι proxy servers λειτουργούν ως ενδιάμεσοι κόμβοι. Έτσι, όταν ένας πελάτης επιθυμεί, εκ μέρους ενός χρήστη, πρόσβαση σε μια συγκεκριμένη υπηρεσία, αποστέλλει την αίτηση αυτή στον proxy server, ο οποίος στη συνέχεια αυθεντικοποιεί το χρήστη και προωθεί τα πακέτα που λαμβάνει από τον πελάτη στον διακομιστή προορισμού και τις απαντήσεις του τελευταίου στον πρώτο.

Αν και η λειτουργία των proxy servers μοιάζει με αυτή των circuit level gateways, υπάρχουν βασικές διαφορές:

- Οι proxy servers έχουν τη δυνατότητα να εξετάσουν το payload των πακέτων (deep inspection). Με τον τρόπο αυτό, μπορούν να εντοπιστούν ίχνη κακόβουλου λογισμικού ή να γίνει κάποια ενέργεια (π.χ. απαγόρευση πρόσβασης σε συγκεκριμένους ιστότοπους) με βάση τα περιεχόμενα του πακέτου.
- Οι proxy servers εξυπηρετούν συγκεκριμένες υπηρεσίες. Για παράδειγμα, ένας εξειδικευμένος proxy server για υπηρεσίες web δεν μπορεί να χρησιμοποιηθεί για άλλες υπηρεσίες. Ο mail server είναι, επίσης, μια κλασσική περίπτωση proxy server.

Οι τρείς διαφορετικοί τύποι firewall που εξετάστηκαν δεν είναι αμοιβαία αποκλειστικοί, αλλά μπορούν να συνδυαστούν σε ένα δίκτυο, όπως φαίνεται στην Εικόνα 3.5:



Εικόνα 3.5 *Ανάπτυξη firewalls.*

Σύμφωνα με την Εικόνα 3.5, ο πελάτης Client 1 χρησιμοποιεί τον Proxy Server για την πρόσβαση στις υπηρεσίες του εξωτερικού web server. Την ίδια στιγμή, ένας εξωτερικός πελάτης (external client) συνδέεται με τον εσωτερικό mail server μέσω ενός circuit level gateway. Όλες οι επικοινωνίες ελέγχονται από ένα packet filter στο άκρο του δικτύου.

3.2.3 Bastion hosts

Τα bastion hosts είναι κόμβοι (υπολογιστικά συστήματα) που χαρακτηρίζονται κρίσιμοι για τη λειτουργία του δικτύου και για αυτό εκτελούν έμπιστα λειτουργικά συστήματα (Trusted Operating Systems – TOS). Ένα λειτουργικό σύστημα χαρακτηρίζεται έμπιστο αν:

- Δεν περιέχει ελαττώματα.
- Δεν περιέχει γνωστές ευπάθειες.
- Έχει παραμετροποιηθεί με το βέλτιστο τρόπο.
- Η διαχείρισή του είναι η βέλτιστη.

Τα bastion hosts, που χρησιμοποιούνται για την εγκατάσταση λογισμικού που υλοποιεί circuit ή application gateways, θα πρέπει να πληρούν τα ακόλουθα κριτήρια:

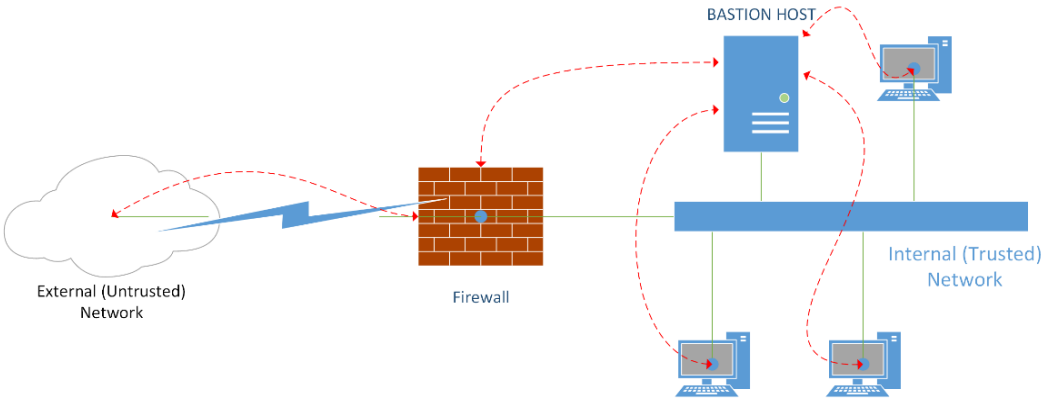
- Κάθε bastion host πρέπει να συνδέεται με τον ελάχιστο απαραίτητο αριθμό κόμβων, έτσι ώστε η διαχείριση να είναι ευκολότερη και μια πιθανή παραβίασή του να επηρεάσει όσο τους λιγότερους κόμβους.
- Θα πρέπει να τηρούνται λεπτομερή αρχεία καταγραφής, έτσι ώστε να είναι δυνατός ο εντοπισμός προβλημάτων και ενεργειών.
- Αν στο bastion host εκτελούνται περισσότεροι από ένας proxies, θα πρέπει η λειτουργία τους να είναι ανεξάρτητη και ο τερματισμός ή η απεγκατάσταση του ενός να μην επηρεάζει τους υπόλοιπους.
- Το λογισμικό των proxies θα πρέπει να είναι απλό, με λίγες γραμμές κώδικα, έτσι ώστε η αποσφαλμάτωσή του να είναι εύκολη.
- Ο αποθηκευτικός χώρος να χρησιμοποιείται για την αποθήκευση των αρχείων παραμέτρων. Η δυνατότητα εγγραφής άλλης πληροφορίας είναι καλό να αποφεύγεται ή να απαγορεύεται, προκειμένου να αποτραπεί πιθανή εγγραφή τμήματος κακόβουλου κώδικα.
- Οι υπηρεσίες που έχουν εγκατασταθεί στο bastion host πρέπει να εκτελούνται από χρήστη με περιορισμένα προνόμια (non-privileged).
- Το bastion host θα πρέπει να μπορεί να αυθεντικοποιεί τους χρήστες που το χρησιμοποιούν σε επίπεδο πρόσβασης δικτύου. Ο κάθε proxy (ως λογισμικό) που εκτελείται σε αυτόν, πιθανώς να αυθεντικοποιεί επιπρόσθετα τους χρήστες σε επίπεδο εφαρμογής.

3.2.4 Τοπολογίες firewall

Αναφέρθηκε προηγουμένως πως είναι δυνατή η ταυτόχρονη εγκατάσταση περισσότερων από έναν τύπο firewall. Ακολουθεί μια σύντομη αναφορά στις συνηθέστερες τοπολογίες που συναντώνται.

3.2.4.1 Single-Homed Bastion Host

Στην τοπολογία Single-Homed Bastion Host, το εσωτερικό δίκτυο συνδέεται με το Διαδίκτυο μέσω ενός packet filter. Εντός του δικτύου υπάρχει ακόμη εγκατεστημένο ένα bastion host, μέσω του οποίου διοχετεύεται όλη η κίνηση πριν τα πακέτα φτάσουν στον προορισμό τους.

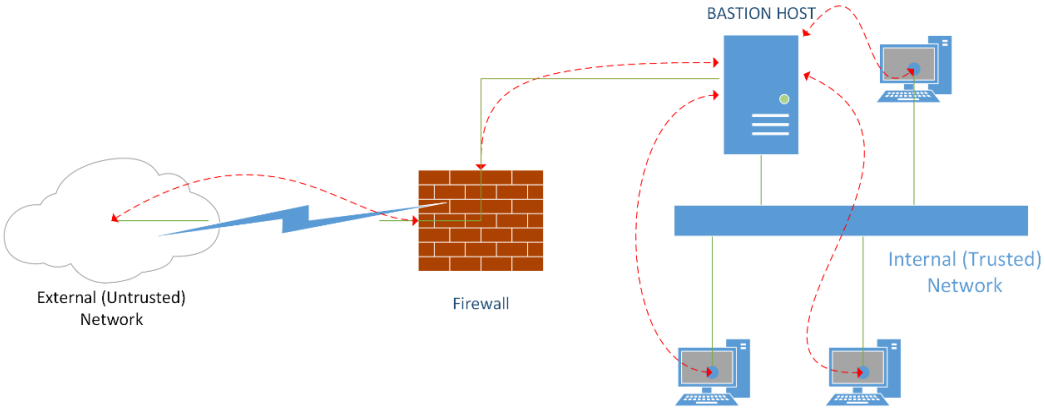


Εικόνα 3.6 *Single-Homed Bastion Host.*

Το μειονέκτημα της υλοποίησης αυτής είναι πως αν ο επιτιθέμενος αποκτήσει πρόσβαση στο packet filter, μπορεί να τροποποιήσει την πολιτική του, έτσι ώστε η κίνηση να μη διοχετεύεται πλέον μέσω του bastion host, αλλά κατευθείαν στους εσωτερικούς hosts.

3.2.4.2 Dual-Homed Bastion Host

Στην τοπολογία Dual-Homed Bastion Host, το packet filter συνδέεται με το εσωτερικό δίκτυο μόνο μέσω του bastion host. Έτσι, δεν είναι πλέον εφικτή η παράκαμψή του.

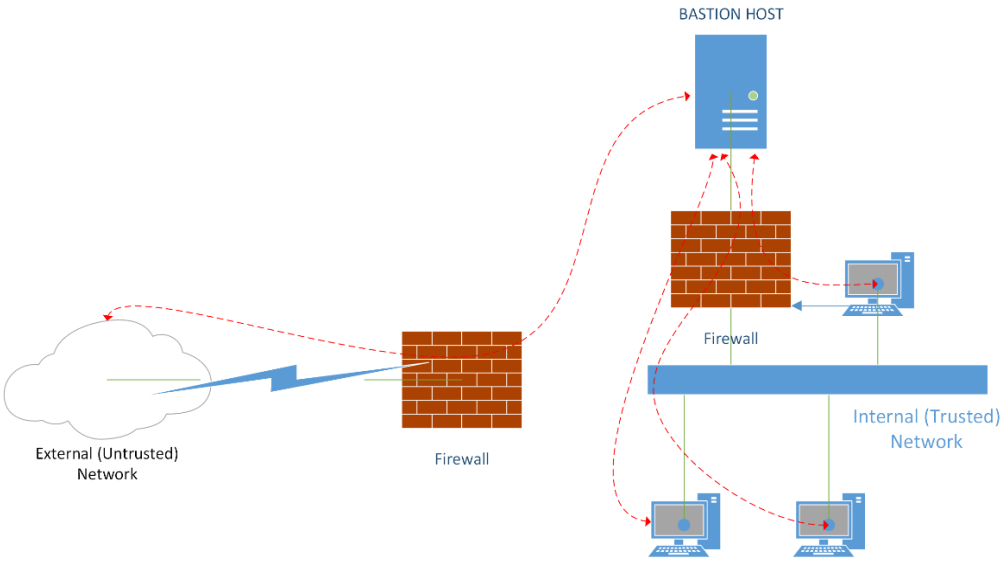


Εικόνα 3.7 *Dual-Homed Bastion Host.*

Στην περίπτωση αυτή, ακόμη και αν ο επιτιθέμενος αποκτήσει πρόσβαση στο packet filter, θα πρέπει επιπροσθέτως να ξεπεράσει το εμπόδιο του bastion host.

3.2.4.3 Screened Subnets

Στην περίπτωση του screened subnet, το bastion host δεν συνδέεται απευθείας με το εσωτερικό δίκτυο, αλλά μέσω ενός δεύτερου packet filter.



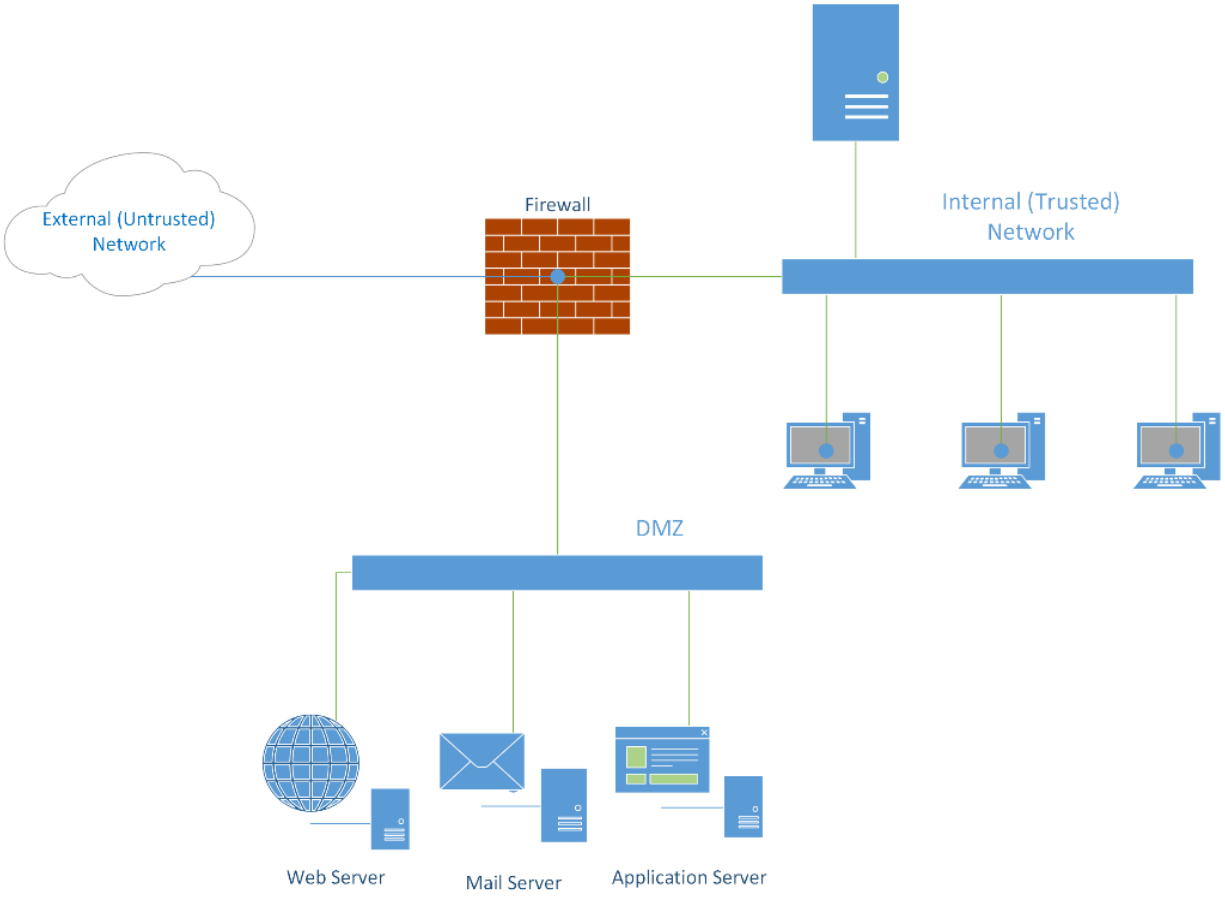
Εικόνα 3.8 *Screened subnet.*

Στην τοπολογία αυτή, το εσωτερικό δίκτυο απομονώνεται τελείως.

3.2.4.4 DMZ

Σε πολλές περιπτώσεις, στο δίκτυο μιας εταιρίας ή ενός οργανισμού, υπάρχουν διακομιστές οι οποίοι φιλοξενούν υπηρεσίες, όπως web services, ηλεκτρονική αλληλογραφία κοκ. Στις υπηρεσίες αυτές συνδέονται χρήστες που βρίσκονται σε μη έμπιστα δίκτυα, όπως το Διαδίκτυο, οπότε οι υπηρεσίες αυτές αποτελούν στόχο διαδικτυακών επιθέσεων.

Για την αποφυγή της απόκτησης πρόσβασης και σε άλλους κόμβους του δικτύου μετά από μια επιτυχημένη επίθεση κατά κάποιας από τις υπηρεσίες, οι διακομιστές που φιλοξενούν τις υπηρεσίες θα πρέπει να τοποθετηθούν σε ένα δεύτερο δίκτυο, το οποίο συνδέεται με το Διαδίκτυο μέσω ενός packet filter και με το εσωτερικό δίκτυο μέσω ενός δεύτερου packet filter. Τα δύο φίλτρα μπορούν να βρίσκονται στην ίδια φυσική υπολογιστική μηχανή, η οποία διαθέτει τρείς διεπαφές: μια συνδεδεμένη με το εσωτερικό δίκτυο, μια συνδεδεμένη με το Internet και μια που συνδέεται με το απομονωμένο δίκτυο των διακομιστών, το οποίο είναι γνωστό ως αποστρατικοποιημένη ζώνη (De-Militarized Zone – DMZ).



Εικόνα 3. 9 *DMZ.*

3.2.5 Ανίχνευση Εισβολών

Η ανίχνευση εισβολών (intrusion detection) στοχεύει στην ανακάλυψη κακόβουλων ενεργειών μέσω της ανάλυσης καταγραφών (auditing) και του εντοπισμού ύποπτης συμπεριφοράς ενός επιτιθέμενου που έχει καταφέρει να αποκτήσει πρόσβαση στο σύστημα. Η αρχή της λειτουργίας της βασίζεται στην υπόθεση πως ο επιτιθέμενος θα συμπεριφερθεί διαφορετικά σε σχέση με ένα νόμιμο χρήστη του συστήματος. Καθώς η ανάλυση των καταγραφών από το διαχειριστή είναι εργασία επίπονη και χρονοβόρα, έχουν αναπτυχθεί συστήματα τα οποία είναι επιφορτισμένα με την ανάλυση αυτή σε πραγματικό χρόνο, τα οποία είναι γνωστά ως Intrusion Detection Systems (IDS).

3.2.5.1 Κατηγορίες IDS

Η ανίχνευση εισβολών μπορεί να λαμβάνει χώρα σε επίπεδο δικτύου ή σε επίπεδο κόμβου. Έτσι, τα αντίστοιχα συστήματα IDS κατηγοριοποιούνται σε:

- Host-based IDS, που υλοποιούνται με λογισμικό εγκατεστημένο στον κόμβο (host), του οποίου την εισερχόμενη και εξερχόμενη κίνηση ελέγχουν.
- Network-Based IDS, που αποτελούνται από dedicated κόμβους, οι οποίοι περιέχουν δικτυακές διεπαφές που έχουν τεθεί σε κατάσταση ασυδοσίας (promiscuous mode) και καταγράφουν και ελέγχουν το σύνολο της κίνησης του δικτύου. Αποτελούνται από:

- Το Network Tap (π.χ. sniffer), το οποίο συνδέεται με κατάλληλη διεπαφή δικτύου (π.χ. port-mirroring switch port) και μπορεί να καταγράφει το σύνολο της κίνησης του δικτύου.

- Το Detection Engine, το οποίο είναι επιφορτισμένο με την ανάλυση των καταγραφών από την κίνηση του δικτύου.

Τα δύο είδη IDS παρουσιάζουν πλεονεκτήματα και μειονεκτήματα, όπως φαίνεται στον Πίνακα 3.3.

Τύπος	**Πλεονεκτήματα**	**Μειονεκτήματα**
Network-based	Απαιτείται μικρός αριθμός επιλεγμένων σημείων στο δίκτυο που ελέγχεται.	Δεν είναι δυνατή η ανάλυση κρυπτογραφημένων δεδομένων.
	Δεν εμπλέκεται στην κίνηση των πακέτων.	Δε μπορεί να ανιχνεύσει τη συνέπεια της επίθεσης.
	Είναι συσκευές συγκεκριμένου σκοπού, που δύσκολα παραβιάζονται.	Ο μεγάλος όγκος δεδομένων μπορεί να δημιουργήσει προβλήματα ανίχνευσης.
Host-Based	Είναι δυνατή η ανάλυση της κρυπτογραφημένης επικοινωνίας.	Απαιτείται η εγκατάσταση επιπρόσθετου λογισμικού, άρα περισσότεροι πόροι και διαχειριστικός φόρτος.
	Δεν απαιτούν εξειδικευμένο υλικό.	Μπορούν να επηρεαστούν και τα ίδια από τις επιθέσεις.
	Έχουν πρόσβαση σε καταγραφές συστήματος ώστε η ανάλυση να είναι πιο ακριβής.	Δεν μπορούν να εγκατασταθούν σε ειδικού σκοπού συσκευές ή σε μη συμβατά λειτουργικά συστήματα.

Πίνακας 3.3 *Τύποι IDS.*

Δεν υπάρχει χρυσός κανόνας για την επιλογή του τύπου IDS. Η επιλογή γίνεται ανάλογα με το δίκτυο και τις απαιτήσεις προστασίας του. Στην περίπτωση που απαιτούνται και οι δύο περιπτώσεις, υπάρχουν τα υβριδικά συστήματα (Hybrid Detection) τα οποία συνδυάζουν και τους δύο τύπους.

3.2.5.2 Ανίχνευση υπογραφών

Στην περίπτωση της ανίχνευσης υπογραφών (signatures), η καταγεγραμμένη κίνηση ελέγχεται και συγκρίνεται με ένα σύνολο κανόνων που υποδεικνύουν μια μη επιθυμητή κατάσταση. Ένας τέτοιος κανόνας θα μπορούσε να είναι: «Οι χρήστες δεν πρέπει να τοποθετούν αρχεία στο home directory άλλων χρηστών».

Έτσι, αν ένας χρήστης δοκιμάσει να εγγράψει ένα αρχείο στο home directory ενός άλλου χρήστη, το IDS θα θεωρήσει τη συμπεριφορά ύποπτη και θα ενημερώσει το διαχειριστή.

Άλλες υπογραφές, σε επίπεδο δικτύου, μπορούν να αναφέρουν περιπτώσεις που δεν πρέπει να παρατηρούνται σε ένα IP πακέτο, όπως για παράδειγμα η ύπαρξη πακέτων με ίδια διεύθυνση προέλευσης και προορισμού (source & destination address). Η επίθεση αυτού του είδους είναι γνωστή ως Land attack.

3.2.5.3 Ανίχνευση συμπεριφοράς

Στην περίπτωση της ανίχνευσης υπογραφών, μια εισβολή ανιχνεύεται και καταγράφεται εφόσον το IDS είναι ενημερωμένο με την αντίστοιχη υπογραφή. Αν η υπογραφή δεν υπάρχει, τότε η επίθεση δεν θα γίνει αντιληπτή. Αντιθέτως, στην περίπτωση του ελέγχου συμπεριφοράς (behavior), το IDS εντοπίζει συμπεριφορές που δεν ταιριάζουν με τη φυσιολογική χρήση του συστήματος. Η φυσιολογική χρήση «μαθαίνεται» από το IDS κατά

τη διάρκεια της ως τότε λειτουργίας του. Έτσι, αν παρατηρηθεί μια απόκλιση στη συμπεριφορά του συστήματος, όπως αυξημένη δραστηριότητα, ασυνήθιστες αιτήσεις πρόσβασης, αυξημένος αριθμός συνόδων, κ.ά. το IDS θεωρεί πως υπάρχει επίθεση.

Η ανίχνευση συμπεριφοράς λειτουργεί σωστά σε στατικά περιβάλλοντα, όπου υπάρχουν σχετικά επαναλαμβανόμενα μοτίβα λειτουργίας. Αντιθέτως, σε δυναμικά περιβάλλοντα μπορεί να οδηγήσει σε περίπτωση λανθασμένου συναγερμού (false positive), όταν μια συμπεριφορά δεν έχει προηγουμένως καταγραφεί ως νόμιμη.

3.2.5.4 Συστήματα Πρόληψης Εισβολών

Τα συστήματα IDS ανιχνεύουν τις πιθανές εισβολές και ενημερώνουν το διαχειριστή ώστε να προβεί στις απαραίτητες ενέργειες. Η διαδικασία, όμως, αυτή μπορεί να χρειαστεί αρκετό χρόνο, με αποτέλεσμα να προκληθεί ζημιά από μια εισβολή. Σε αντιστοιχία, μπορεί κανείς να σκεφτεί ένα συναγερμό που θα ειδοποιήσει τον κάτοικο ενός σπιτιού, αφού ο διαρρήκτης είναι ήδη μέσα σε αυτό. Για το λόγο αυτό, η δεύτερη γενιά συστημάτων ανίχνευσης εισβολών παρέχει και τη δυνατότητα πρόληψης (Intrusion Prevention Systems – IPS). Η αντίδραση μπορεί να είναι είτε άμεση ή έμμεση. Στην άμεση αντίδραση (inline), το ίδιο το IPS απορρίπτει ή αναδρομολογεί τα πακέτα που ανήκουν στη δικτυακή κίνηση της επίθεσης. Στην περίπτωση της έμμεσης αντίδρασης, το IPS δίνει εντολή σε άλλα συστήματα, με τα οποία συνδέεται (όπως firewalls), να προβούν στις απαραίτητες ενέργειες.

Το μειονέκτημα της χρήσης ενός IPS είναι η περίπτωση ενός false positive, όπου η αντίδραση μπορεί να αποτρέψει μια νόμιμη ενέργεια. Ως αντίστοιχο παράδειγμα, μπορεί κανείς να φανταστεί την ενεργοποίηση της αυτόματης πυρόσβεσης σε ένα γραφείο, χωρίς όμως να υπάρχει φωτιά.

3.2.5.5 Honeypots

Για την αποφυγή ζημίας από επιθέσεις, ή για τη μελέτη πραγματικών επιθέσεων είναι δυνατή η ανάπτυξη ενός κόμβου ή δικτύου δολώματος, γνωστού ως honeypot ή honeynet. Ένα honeypot σκόπιμα περιέχει ευπάθειες με σκοπό να δελεάσει το δυνητικό επιτιθέμενο, ώστε να τον προτρέψει στο να επιτεθεί σε αυτό και να μην ασχοληθεί με τα υπόλοιπα συστήματα, με στόχο:

- Να ανιχνευτεί η επίθεση.
- Να μελετηθεί η επίθεση.
- Να εντοπιστεί ο επιτιθέμενος.
- Η ζημιά να περιοριστεί στο honeypot.

3.3 Ασύρματη Δικτύωση

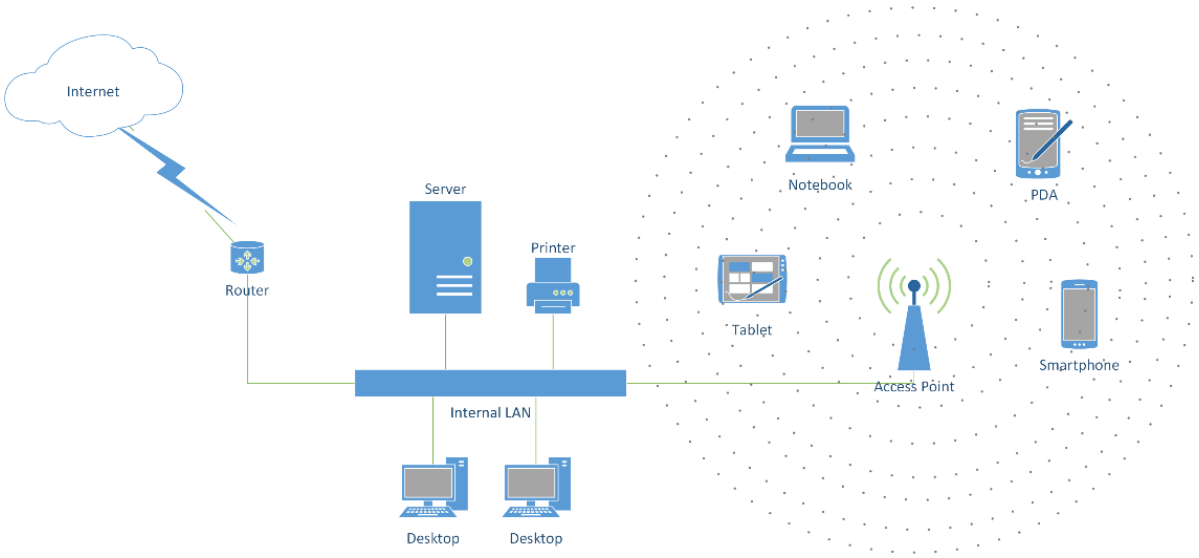
Η ασύρματη δικτύωση παρέχει τη δυνατότητα μεταφοράς δεδομένων χωρίς τη σύνδεση των κόμβων σε φυσικό μέσο (όπως καλώδια χαλκού ή οπτικές ίνες), αλλά με τη χρήση ηλεκτρομαγνητικών κυμάτων που μεταδίδονται στον αέρα. Με τη χρήση τεχνολογιών ασύρματης δικτύωσης, είναι δυνατή η επέκταση του δικτύου και η εξυπηρέτηση κόμβων σε σημεία όπου δεν υπάρχει εγκατάσταση δομημένης καλωδίωσης ή οποιοσδήποτε άλλος τρόπος ενσύρματης σύνδεσης.

Το 1997, η ένωση IEEE παρουσίασε το πρότυπο 802.11 το οποίο περιγράφει ένα σύνολο προδιαγραφών και πρωτοκόλλων που καθορίζουν τον τρόπο επικοινωνίας στο επίπεδο πρόσβασης δικτύου. Κατά την υλοποίηση ασύρματων δικτύων IEEE 802.11, οι λειτουργίες των ανώτερων επιπέδων (δικτύου, μεταφοράς και εφαρμογής) δεν διαφοροποιούνται, επιτρέποντας την απρόσκοπτη λειτουργία των ιδίων πρωτοκόλλων.

Αρχικά, το εύρος ζώνης των ασύρματων συνδέσεων με χρήση του προτύπου IEEE 802.11 ήταν ιδιαίτερα χαμηλό σε σχέση με την ενσύρματη σύνδεση (μόλις 2 Mbps). Με το πέρασμα των χρόνων παρουσιάστηκαν επεκτάσεις του προτύπου οι οποίες επιτρέπουν συνδέσεις με ταχύτητες της τάξεως των Gbps (802.11ac). Η περιγραφή του προτύπου και των επεκτάσεών του είναι εκτός του σκοπού του παρόντος εγχειριδίου.

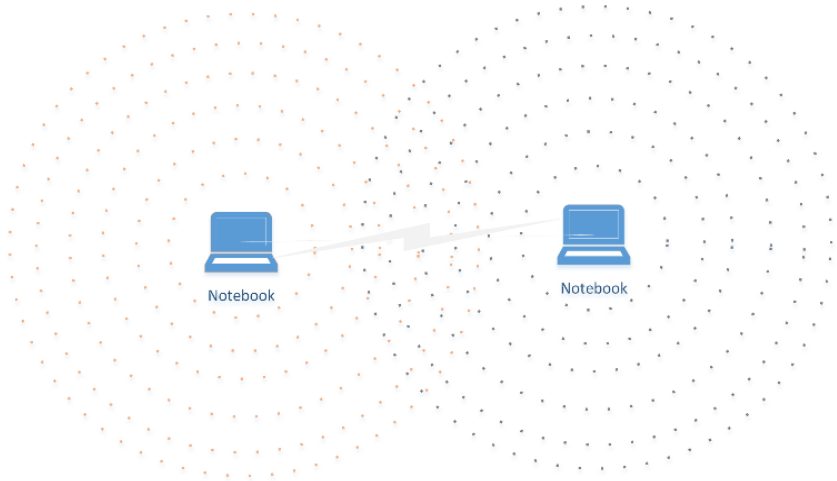
Οι τοπολογίες που συναντώνται συνήθως στα δίκτυα που υλοποιούν το πρότυπο 802.11, είναι οι ακόλουθες:

- Infrastructure Mode, όπου η επικοινωνία μεταξύ των κόμβων γίνεται μέσω ενός κεντρικού σημείου πρόσβασης (access point).



Εικόνα 3.10 *Infrastructure mode.*

- Ad-hoc Mode, όπου εδραιώνονται συνδέσεις απευθείας μεταξύ των τερματικών συσκευών.



Εικόνα 3.11 *Ad-hoc mode.*

3.3.1 Ζητήματα ασφάλειας

Ένα ασύρματο δίκτυο παρουσιάζει το πλεονέκτημα της άμεσης επέκτασης ενός ενσύρματου δικτύου και της ευκολίας διασύνδεσης για κινητούς κυρίως κόμβους (όπως φορητοί υπολογιστές, κινητά τηλέφωνα, tablets κοκ). Καθώς όμως η πληροφορία διακινείται στον αέρα, χωρίς φυσικούς περιορισμούς, μπορεί, πέρα από το νόμιμο αποδέκτη, να αποκτήσει πρόσβαση σε αυτή οποιοσδήποτε άλλος βρίσκεται στην εμβέλεια εκπομπής. Ένας κακόβουλος χρήστης, έχοντας πρόσβαση στο κοινό μέσο, θα μπορούσε να υλοποιήσει επιθέσεις με σκοπό:

- Να υποκλέψει δεδομένα (Sniffing)
  Ο κακόβουλος χρήστης μπορεί να καταγράψει το σύνολο της διακινούμενης πληροφορίας και, στη συνέχεια, να ανακτήσει τα δεδομένα που επιθυμεί να παρακολουθήσει (eavesdropping) ή για να τα χρησιμοποιήσει ώστε να υποκλέψει μια σύνοδο με χρήση επιθέσεων session hijacking, replay attacks ή MAC spoofing.

- Να τροποποιήσει τα μεταδιδόμενα δεδομένα (Man-in-the-Middle)
  Ο κακόβουλος χρήστης μπορεί να υλοποιήσει επίθεση ενδιάμεσου με σκοπό να παρεισφρήσει στην επικοινωνία και να τροποποιήσει τα μεταδιδόμενα δεδομένα.

- Να διακόψει την υπηρεσία (Denial of Service)
  Ο κακόβουλος χρήστης μπορεί να παρεμβάλει μεγάλο όγκο δεδομένων στις χρησιμοποιούμενες συχνότητες, με σκοπό την άρνηση εξυπηρέτησης.

- Να υποκλέψει στοιχεία πρόσβασης (Wireless Phishing)
  Ο κακόβουλος χρήστης μπορεί να τοποθετήσει ένα δικό του access point με ίδιο SSID με αυτό του δικτύου-στόχου. Έτσι, όταν ο πελάτης προσπαθήσει να συνδεθεί σε αυτό, νομίζοντας ότι συνδέεται στο υποτιθέμενο access point, ο επιτιθέμενος θα μπορέσει να καταγράψει τα μεταδιδόμενα στοιχεία αυθεντικοποίησης.

Η αντιμετώπιση των επιθέσεων αυτών απαιτεί την υλοποίηση αντίμετρων που περιλαμβάνουν:

- Μέριμνα κατά τη φυσική σχεδίαση του ασύρματου δικτύου.

- Υλοποίηση τεχνικών και μεθόδων προστασίας των δεδομένων.

3.3.2 Θέματα σχεδίασης

Η αντιμετώπιση των κινδύνων σε ένα ασύρματο δίκτυο, είναι μια διαδικασία που ξεκινά ήδη από το σχεδιασμό του. Για να οργανωθεί όμως το σχέδιο άμυνας ενός δικτύου, θα πρέπει να γίνει πρώτα κατανοητό ποιο είναι το «οχυρό» που πρέπει να προστατευτεί. Έτσι, είναι βασικό να γνωρίζει κανείς πως λειτουργεί η επιμέρους τεχνολογία ασύρματης δικτύωσης, την οποία επιλέγει να χρησιμοποιήσει. Άρα, το πρώτο βήμα είναι η σε βάθος μελέτη των αρχών που διέπουν τη λειτουργία των ασύρματων δικτύων, κάτι που ξεφεύγει από τους σκοπούς του παρόντος εγχειριδίου, αλλά θα αναφερθούν ορισμένοι γενικοί σχεδιαστικοί κανόνες.

3.3.2.1 Ελάχιστη περιοχή κάλυψης

Ένα ασύρματο δίκτυο δεν περιορίζεται εντός των φυσικών ορίων ενός χώρου, όπως οι τοίχοι ενός δωματίου, αλλά είναι διαθέσιμο σε μία περιοχή η έκταση της οποίας εξαρτάται από:

- Την ισχύ εκπομπής.
- Το είδος του δικτύου.
- Τη συχνότητα εκπομπής.
- Τον τύπο και την απολαβή της κεραίας.
- Το φυσικό περιβάλλον.
- Τις παρεμβολές.
- Την απόσταση.

Κατά το σχεδιασμό, θα πρέπει να υπολογιστεί η επιθυμητή απόσταση κάλυψης, να οριστεί κατάλληλα η ισχύς εκπομπής και να επιλεγεί η κατάλληλη για τον τύπο κάλυψης κεραία. Στόχος των παραπάνω είναι η

περιοχή κάλυψης να μην υπερβαίνει την επιθυμητή περιοχή, αλλά επίσης η επιθυμητή περιοχή να καλύπτεται επαρκώς ώστε να μην υπάρχει πρόβλημα διαθεσιμότητας του δικτύου.

Η πρακτική που πολλές φορές ακολουθείται με τη λάθος τοποθέτηση κεραιών (π.χ. εγκατάσταση μιας omnidirectional κεραίας, που παρέχει μια θεωρητικά ομοιόμορφη κάλυψη προς όλες τις κατευθύνσεις, εκτός του κέντρου της επιθυμητής περιοχής κάλυψης ή για περιπτώσεις που επιθυμούμε κάλυψη προς μια μόνο κατεύθυνση) ή η χρήση κεραιών με μεγάλη απολαβή, επιτρέπει στον επιτιθέμενο να εκτελέσει ενέργειες από μεγάλη απόσταση, χωρίς να γίνει αντιληπτή η φυσική του παρουσία.

3.3.2.2 Ορισμός service identifier

Το Service Set Identifier (SSID) χαρακτηρίζει το δίκτυο και το διαφοροποιεί από τα υπόλοιπα. Για το σκοπό αυτό, είναι συνετό το SSID να τροποποιείται, έτσι ώστε να προσδιορίζει με σαφήνεια το δίκτυο. Υπάρχει ακόμη η δυνατότητα της αποφυγής εκπομπής του SSID, σε περίπτωση που δεν είναι επιθυμητή η ανίχνευση του δικτύου ώστε να τραβήξει την προσοχή ενός κακόβουλου χρήστη. Στην περίπτωση επιθυμίας για την αποφυγή εκπομπής του, το SSID θα πρέπει να οριστεί με τέτοιο τρόπο ώστε να μην είναι προβλέψιμο ή να μη διατηρηθεί κάποια προεπιλογή του κατασκευαστή που να διευκολύνει τον επιτιθέμενο στο να το μαντέψει. Ακόμη, η αλλαγή του SSID μπορεί να αποτρέψει μια επίθεση Wireless Phishing, στην οποία ο επιτιθέμενος παρουσιάζει στους clients ένα SSID που τους οδηγεί σε σύνδεση με ένα δικό του δίκτυο, αντί για αυτό που πραγματικά επιθυμούν.

3.3.2.3 Απενεργοποίηση ad-hoc συνδέσεων

Πολλές από τις συσκευές που χρησιμοποιούνται καθημερινά, παρέχουν τη δυνατότητα ασύρματης ad-hoc σύνδεσης με αυτές. Όταν μια τέτοια συσκευή συνδέεται με το υπόλοιπο δίκτυο, θα πρέπει να ληφθεί κατάλληλη μέριμνα ώστε είτε η δυνατότητα αυτή να απενεργοποιηθεί ή να παραμετροποιηθεί με κατάλληλο τρόπο έτσι ώστε να μην είναι δυνατή η χρήση της από έναν κακόβουλου χρήστη για διείσδυση μέσω αυτής στο υπόλοιπο δίκτυο.

3.3.2.4 Έλεγχος ενσύρματων σημείων σύνδεσης

Αν και με την πρώτη ματιά, η συγκεκριμένη προτροπή μοιάζει να μην αφορά το ασύρματο δίκτυο, έχουν καταγραφεί περιπτώσεις όπου νόμιμοι χρήστες του δικτύου συνδέουν σε θύρες δικτύου access points που προμηθεύονται από το εμπόριο για να συνδέσουν τις κινητές τους συσκευές (rogue access points). Η σύνδεση access points χωρίς τις κατάλληλες γνώσεις παραμετροποίησης, μπορεί να αποτελέσει κερκόπορτα για κάποιον επιτιθέμενο. Για την αποφυγή τέτοιων καταστάσεων, πρέπει οι μεταγωγείς (switches) να ρυθμιστούν έτσι ώστε να μην είναι δυνατή η σύνδεση οποιασδήποτε συσκευής σε οποιαδήποτε θύρα (port security).

3.3.2.5 Απομόνωση πελάτη

Σε ένα ασύρματο δίκτυο, κυρίως όταν αυτό αφορά ένα δημόσια διαθέσιμο δίκτυο, συνδέονται αρκετά διαφορετικοί χρήστες. Στο δίκτυο αυτό θα πρέπει να μην επιτρέπεται η ανταλλαγή δεδομένων μεταξύ των τερματικών συσκευών των χρηστών, ώστε να μη μπορεί ένας επιτιθέμενος που είναι συνδεδεμένος, ακόμη και ως νόμιμος χρήστης, να αποκτήσει πρόσβαση στα δεδομένα που είναι αποθηκευμένα στις συσκευές των υπόλοιπων χρηστών (client isolation).

3.3.3 Προστασία δεδομένων

Τα δεδομένα σε ένα ασύρματο δίκτυο, όπως αναφέρθηκε προηγουμένως, μεταδίδονται στον αέρα μέσω ηλεκτρομαγνητικών κυμάτων. Για το λόγο αυτό, θα πρέπει να ληφθεί μέριμνα ώστε να μην είναι διαθέσιμα σε όλους όσοι βρίσκονται στην εμβέλεια κάλυψης του δικτύου. Στο πέρασμα των ετών έχουν προταθεί και υλοποιηθεί διάφορες λύσεις αυθεντικοποίησης και κρυπτογράφησης δεδομένων στο ασύρματο μέσο. Στη συνέχεια θα αναφερθούν οι πιο γνωστές και αυτές που συναντώνται σήμερα.

3.3.3.1 Wired Equivalent Privacy

Στόχος της δημιουργίας του Wired Equivalent Privacy (WEP) δεν ήταν η μέγιστη δυνατή προστασία των ιδιοτήτων της ασφάλειας, αλλά το να παρέχει προστασία αντίστοιχη με αυτή που παρέχεται από ένα ενσύρματο μέσο (όπως εξάλλου δηλώνει και το όνομά του). Έτσι, τα δεδομένα που διακινούνται μεταξύ του access point και των χρηστών κρυπτογραφούνται. Το WEP παρέχει και τη δυνατότητα αυθεντικοποίησης, πέρα από την προστασία της ακεραιότητας και της εμπιστευτικότητας των δεδομένων.

Στο WEP χρησιμοποιείται ένα κοινό κλειδί μεταξύ του access point και του σταθμού (τερματικού). Το κλειδί αυτό διαμοιράζεται από το διαχειριστή του access point με κάθε ασύρματο κόμβο, για την αυθεντικοποίηση και την κρυπτογράφηση της επικοινωνίας.

Υπάρχουν δύο επιλογές αυθεντικοποίησης:

- Open System authentication, όπου ουσιαστικά δεν γίνεται αυθεντικοποίηση και κάθε αίτημα για σύνδεση στο δίκτυο ικανοποιείται από το access point.

- Shared-key authentication, όπου ακολουθείται μια διαδικασία πρόκλησης-απόκρισης (challenge-response), ως εξής:

    - Ο σταθμός αποστέλλει ένα αίτημα στο access point.

    - Το access point δημιουργεί μια τυχαία ακολουθία 128 bits (challenge).

    - Ο σταθμός κρυπτογραφεί την ακολουθία αυτή με χρήση του αλγορίθμου RC4 και του κοινού κλειδιού και αποστέλλει το αποτέλεσμα (κρυπτογράφημα) στο access point.

    - Το access point αποκρυπτογραφεί το κρυπτογράφημα με χρήση του ίδιου αλγόριθμου και του κοινού κλειδιού. Αν το αποτέλεσμα είναι ίδιο με την αρχική ακολουθία, σημαίνει πως το κλειδί μεταξύ των δύο είναι κοινό (το γιατί θα το μελετήσετε αργότερα στο κεφάλαιο 6), άρα ο σταθμός αυθεντικοποιείται.

Η αυθεντικοποίηση στο WEP, βασίζεται στην επαλήθευση της ύπαρξης ενός κοινού κλειδιού μεταξύ του σταθμού και του access point. Ίσως, η αρχική απάντηση στην ερώτηση ποιόν από τους δύο τρόπους αυθεντικοποίησης θα επιλέγατε (Open ή Shared key) θα ήταν πως ο δεύτερος είναι προτιμότερος, καθώς ελέγχεται η πρόσβαση στο δίκτυο και μόνο χρήστες που γνωρίζουν το κοινό κλειδί μπορούν να την αποκτήσουν. Αν το σκεφτούμε όμως καλύτερα, κατά τη διαδικασία της αυθεντικοποίησης ο επιτιθέμενος μπορεί να ανακτήσει (μέσω sniffing) και την αρχική ακολουθία και την κρυπτογραφημένη απάντηση. Έχοντας αυτά τα δύο, εύκολα μπορεί να εξάγει το κλειδί. Άρα, μπορεί με τη σειρά του όχι μόνο να αυθεντικοποιηθεί ώστε να χρησιμοποιήσει το ασύρματο δίκτυο για πρόσβαση στο Διαδίκτυο, αλλά και να υποκλέψει και αποκρυπτογραφήσει το σύνολο της κίνησης που διέρχεται από το access point. Οπότε, η απάντηση είναι ότι, παραδόξως, ασφαλέστερο είναι να επιλεγεί το Open Systems Authentication για την προστασία της εμπιστευτικότητας και ακεραιότητας των δεδομένων (ένας κακόβουλος χρήστης θα μπορέσει να συνδεθεί αλλά όχι να ανταλλάξει δεδομένα).

Η κρυπτογράφηση των frames στο WEP γίνεται ως εξής:

- Ο αποστολέας υπολογίζει το CRC του αρχικού μηνύματος, την τιμή του οποίου συνενώνει (concatenate) με το μήνυμα.

- Στη συνέχεια, δημιουργεί ένα διάνυσμα αρχικοποίησης (initialization vector - IV) 24 bit, το οποίο συνενώνει με το κλειδί μήκους 40 ή 104 bit, ανάλογα. Η συνένωση αυτή τροφοδοτείται σε μια ψευδογεννήτρια τυχαίων αριθμών (Pseudo-random Number Generator – PRNG) που χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης ροής RC4, ώστε να παραχθεί μια κλειδοροή ίση με το μήκος του μηνύματος.

- Το αποτέλεσμα της πράξης XOR μεταξύ του μηνύματος και της κλειδοροής αποτελεί το κρυπτογράφημα (cipher text) το οποίο συνενώνεται με το IV και αποστέλλεται στον παραλήπτη.

Το WEP παρουσιάζει σημαντικές αδυναμίες, όπως:

- Δεν υπάρχει διαχείριση κλειδιών συνόδου, οπότε η διανομή πρέπει να γίνεται «χέρι με χέρι» από το διαχειριστή.

- Το μέγεθος του IV είναι μόλις 24 bit. Άρα, υπάρχουν μόνο 2^{24}, δηλαδή λίγο περισσότερα από 16 εκατομμύρια, διαφορετικά πιθανά IV. Έτσι, σε συνδυασμό με την αυξημένη δικτυακή κίνηση, είναι πιθανή η επανεμφάνιση πακέτων με ίδιο IV σε σύντομο διάστημα. Αν ο επιτιθέμενος καταφέρει να εντοπίσει δύο πακέτα με το ίδιο IV (το οποίο στέλνεται ως ανοικτό κείμενο συνενωμένο με το κρυπτοκείμενο), μπορεί για παράδειγμα να εφαρμόσει μια επίθεση κλειδοροής (keystream attack). Σε μια τέτοια επίθεση, βασιζόμενος στο γεγονός ότι το αποτέλεσμα της XOR σε δύο μηνύματα με κρυπτοκείμενο είναι ίδιο με το αποτέλεσμα της XOR στα δύο μηνύματα με το καθαρού κειμένου από το οποίο προέκυψαν, μπορεί να αποκαλύψει το περιεχόμενο του ενός μηνύματος γνωρίζοντας το περιεχόμενο του άλλου μηνύματος.

- Επειδή ισχύει: $CRC(x \oplus y)=CRC(x) \oplus CRC(y)$, Ο επιτιθέμενος μπορεί να κάνει αλλαγές στο μήνυμα, τέτοιες ώστε η τιμή του CRC να είναι η ίδια.

Οι παραπάνω λόγοι, κατέστησαν σύντομα το WEP ακατάλληλο για χρήση σε ασύρματα δίκτυα και προτάθηκε η αντικατάστασή του από το WPA.

3.3.3.2 Wi-Fi Protected Access

Το Wi-Fi Protected Access (WPA) αποτελεί υποσύνολο του προτύπου 802.11i και παρουσιάστηκε από τη Wi-Fi Alliance με σκοπό να θεραπεύσει προσωρινά τις αδυναμίες του WEP και να μπορεί να εκτελείται στο ίδιο υλικό που εκτελούνταν το τελευταίο. Έπρεπε, ακόμη, να είναι συμβατό με το επερχόμενο 802.11i. Οι βασικές διαφορές του από το WEP είναι:

- Η αυθεντικοποίηση μπορεί να γίνει είτε με χρήση του πρωτοκόλλου 802.1X και χρήση ενός RADIUS Server (Enterprise Mode) είτε βασισμένη στη χρήση ενός συνθηματικού (passphrase) για απλές οικιακές εγκαταστάσεις.

- Εισήχθη το πρωτόκολλο TKIP, που αποτελεί ένα σύνολο αλγορίθμων με σκοπό την αντιμετώπιση των αδυναμιών του WEP, π.χ. όσον αφορά τα IV και τη μη ανανέωση των κλειδιών συνόδου.

Το WPA συνεχίζει να χρησιμοποιεί τον αλγόριθμο RC4, με μεγαλύτερο όμως μήκος κλειδιού (128 bits) και ουσιαστικά αποτελεί μια βελτίωση του WEP.

3.3.3.3 IEEE 802.11i - WPA2

Το πρωτόκολλο WPA2 αποτελεί την υλοποίηση του προτύπου 802.11i. Αντικαθιστά τον αλγόριθμο RC4 με τον AES, ο οποίος χρησιμοποιείται και κατά την αυθεντικοποίηση και κατά την κρυπτογράφηση. Αν και έχει διορθώσει πολλές από τις ευπάθειες των WEP και WPA, είναι ευάλωτο σε επιθέσεις Rollback, RSN IE poisoning και De-Association.

Βιβλιογραφία

Ciampa, M. (2014). Security+ guide to network security fundamentals (5th Ed). Clifton Park, NY: Cengage Learning.

Garg, V. K. (2007). Wireless communications and networking. Amsterdam ; Boston: Elsevier Morgan Kaufmann.

Rhodes-Ousley, M. (2013). Information security: the complete reference (2nd. Ed). New York ;London: McGraw-Hill Education.

Wang, J., & Kissel, Z. A. (2015). Introduction to network security: theory and practice (Second edition). Hoboken, NJ : Singapore: Wiley ; HEP.

Κριτήρια αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Με τον όρο defense in-depth αναφερόμαστε:
α) Στο μοντέλο Lollipop.
β) Στο μοντέλο Onion.
γ) Στο μοντέλο καταρράκτη (Waterfall).
δ) Στη χρήση όλων των τύπων firewall.

2. Οι βασικές κατηγορίες firewalls είναι:
α) Φιλτράρισμα πακέτων (Packet Filters).
β) Φιλτράρισμα κυκλώματος (Circuit-level Filters).
γ) Πύλες κυκλώματος (Circuit-level Gateways).
δ) Πύλες εφαρμογών (Application-level Gateways).

3. Ένα packet filter:
α) Εξετάζει τα δεδομένα που περιέχει το πακέτο (payload).
β) Εξετάζει τις κεφαλίδες επιπέδου δικτύου και μεταφοράς.
γ) Εξετάζει τις κεφαλίδες φυσικού επιπέδου, επιπέδου δικτύου και μεταφοράς.
δ) Εξετάζει τις κεφαλίδες επιπέδου δικτύου, μεταφοράς και εφαρμογής.

4. Ένα stateful packet filter:
α) Δεν χρησιμοποιεί λίστες ελέγχου πρόσβασης αλλά μόνο πίνακες καταστάσεων.
β) Δεν ελέγχει αυτόνομα κάθε πακέτο.
γ) Χρησιμοποιείται μόνο για εδραιωμένες συνδέσεις.
δ) Επιτρέπει μόνον εξερχόμενες συνδέσεις.

5. Η χρήση proxy servers επιτρέπει:
α) Την εξέταση των δεδομένων (payload) κάθε πακέτου.
β) Τη δημιουργία κυκλώματος.
γ) Τη χρήση ενός honeypot.
δ) Τη χρήση του πρωτοκόλλου SOCKS.

6. Ένα bastion host:
α) Χρησιμοποιείται για να τραβήξει την προσοχή των επιτιθέμενων.
β) Είναι απαραβίαστο.
γ) Χρησιμοποιεί πολύπλοκες εφαρμογές λογισμικού.
δ) Είναι καλό να εκτελεί σταθερές (stable) εκδόσεις του λειτουργικού συστήματος.

7. Ο έλεγχος συμπεριφοράς σε ένα IDS:
α) Αξιοποιεί γνωστές υπογραφές.
β) Χρησιμοποιείται για να καθορίσει τη συμπεριφορά των συστημάτων.
γ) Λειτουργεί καλύτερα σε δυναμικά περιβάλλοντα.
δ) Δεν απαιτεί τη χρήση υπογραφών.

8. Κατά το σχεδιασμό ενός ασύρματου δικτύου:
α) Στόχος είναι η κάλυψη όσο το δυνατόν μεγαλύτερης επιφάνειας.
β) Δεν λαμβάνεται υπόψη η ασφάλεια.
γ) Γίνεται προσπάθεια περιορισμού της εμβέλειας.
δ) Κανένα από τα παραπάνω.

9. Στο WEP, το κοινό κλειδί συνόδου:
α) Παράγεται με τη χρήση μονόδρομων συναρτήσεων.
β) Μπορεί να αποκαλυφθεί κατά τη διαδικασία αυθεντικοποίησης.
γ) Δεν χρησιμοποιείται κατά την αυθεντικοποίηση.
δ) Κανένα από τα παραπάνω.

10. Κατά την ανάπτυξη ενός ασύρματου δικτύου. ποιο πρωτόκολλο θα επιλέγατε για την κρυπτογράφηση των δεδομένων;
α) WPA2
β) WPA
γ) WEP
δ) RADIUS

Κεφάλαιο 4. Προγραμματισμός στο Διαδίκτυο

Σύνοψη
Η ανάπτυξη αξιόπιστων διαδικτυακών εφαρμογών που θα λειτουργούν διασφαλίζοντας την ικανοποίηση των βασικών ιδιοτήτων ασφάλειας, είναι ένα ζήτημα που απασχολεί τους ειδικούς του χώρου της Τεχνολογίας Λογισμικού και της Ασφάλειας Πληροφοριών. Ο κώδικας, που γράφεται σήμερα, δίνει στις εφαρμογές αυτές ικανότητες δικτυακής σύνδεσης, έτσι ώστε να εκμεταλλεύονται οι χρήστες τους τις δυνατότητες του Διαδικτύου και να χρησιμοποιούν απομακρυσμένες υπηρεσίες. Η αρχιτεκτονική που ακολουθείται, συνήθως, είναι αυτή του πελάτη/εξυπηρετητή, αν και τα τελευταία χρόνια εμφανίζει ιδιαίτερη άνοδο αυτή των ομότιμων κόμβων (peep-to-peer). Όμως, τα περιστατικά ασφάλειας που σχετίζονται με αδυναμίες των διαδικτυακών εφαρμογών είναι δυστυχώς αρκετά συχνά. Για αυτό, καταβάλλεται μια συντονισμένη προσπάθεια ώστε τα περιστατικά αυτά να καταγράφονται συστηματικά για να συσσωρεύεται γνώση και να λαμβάνονται μέτρα που θα βοηθούν τις επόμενες γενιές προγραμματιστών ώστε να αποφεύγουν τα ίδια προγραμματιστικά λάθη και παραλείψεις κατά την ανάπτυξη των διαδικτυακών εφαρμογών.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου, απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1).

4.1 Εισαγωγή

Στο χώρο της Ασφάλειας Πληροφοριών, η παρατήρηση ότι δεν υπάρχει το ασφαλές πληροφοριακό σύστημα αποτελεί βασική αρχή, καθώς τα πληροφοριακά συστήματα αλλάζουν διαρκώς. Αυτό δε σημαίνει ότι πρέπει να δεχτούμε αυτή τη διαπίστωση μοιρολατρικά και να παραιτηθούμε από κάθε προσπάθεια προστασίας του πληροφοριακού μας συστήματος. Αντιθέτως, υπάρχουν οδηγίες και κατευθυντήριες γραμμές, τις οποίες οφείλουμε να ακολουθήσουμε προκειμένου να επιτύχουμε τον υψηλότερο βαθμό ασφάλειας, ανάλογα με τα μέσα που διαθέτουμε.

Μια διαδικτυακή εφαρμογή (Web application) είναι εκτεθειμένη σε περισσότερους κινδύνους από ότι μια εφαρμογή που είναι εγκατεστημένη και λειτουργεί τοπικά στο δικό μας υπολογιστή ή εντός ενός τοπικού δικτύου. Οι τεχνολογίες διασύνδεσης τις οποίες χρησιμοποιούμε ώστε να καταστήσουμε την εφαρμογή μας περισσότερο λειτουργική, δίνουν ταυτόχρονα τη δυνατότητα σε κακόβουλους χρήστες να έρθουν σε άμεση επικοινωνία μαζί της και έτσι μπορούν να εκμεταλλευτούν τις τυχόν ευπάθειες, οι οποίες προέκυψαν από προγραμματιστικά σφάλματα και παραλείψεις.

Προφανώς, οι προγραμματιστές δεν έχουν σκοπό να γράψουν κώδικα που να περιέχει ευπάθειες. Ωστόσο, αυτό συμβαίνει για διάφορους λόγους. Οι κυριότεροι λόγοι για τους οποίους οι προγραμματιστές καταλήγουν στο να γράψουν κώδικα που περιέχει ή προκαλεί ευπάθειες στη διαδικτυακή εφαρμογή, είναι:

- Η ασφάλεια δεν αποτελεί συνήθως σημαντική προτεραιότητα των προγραμματιστών και μόλις τα τελευταία χρόνια έχει καταστεί σημαντικό χαρακτηριστικό των εφαρμογών. Επιπλέον, οι παλαιότεροι προγραμματιστές είναι αρκετά πιθανό να μην έχουν διδαχθεί τεχνικές ασφαλούς προγραμματισμού.

- Μερικές γλώσσες προγραμματισμού (όπως για παράδειγμα η C) διαθέτουν εγγενείς ιδιότητες που οδηγούν στην ανάπτυξη ευάλωτου κώδικα, όπως για παράδειγμα οι άμεσες αναφορές και εγγραφές στη μνήμη σε δομές δεδομένων, όπως η στοίβα (stack), ή ο σωρός (heap).

- Η ασφάλεια, όντας κατά κανόνα μη λειτουργική απαίτηση, απαιτεί επιπρόσθετο φόρτο εργασίας, με αποτέλεσμα αρκετοί προγραμματιστές να ικανοποιούν μόνο τα απαραίτητα λειτουργικά χαρακτηριστικά της εφαρμογής που αναπτύσσουν.

- Μόλις τα τελευταία χρόνια ξεκίνησε η ευαισθητοποίηση των τελικών χρηστών σε θέματα ασφάλειας, ώστε να επιζητούν την ύπαρξη χαρακτηριστικών ασφάλειας προκειμένου να χρησιμοποιήσουν μια διαδικτυακή εφαρμογή.

- Απαιτείται μεγαλύτερος χρόνος και κόστος για την ανάπτυξη της εφαρμογής, ειδικότερα αν ο κύκλος ανάπτυξης ακολουθεί ένα μοντέλο (όπως για παράδειγμα το σπειροειδές) που περιλαμβάνει στάδια ελέγχου και αποτίμησης της επικινδυνότητας.

4.2 Αρχές Ασφαλούς Προγραμματισμού

Έχουν προταθεί από ανεξάρτητους οργανισμούς (όπως ο οργανισμός OWASP) ή ομάδες ασφάλειας (όπως η ομάδα CERT του πανεπιστημίου Carnegie Mellon), ορισμένες αρχές ασφαλούς προγραμματισμού οι οποίες συνοψίζονται ως εξής:

- Κάθε επιπλέον ιδιότητα που προστίθεται σε μια εφαρμογή, προσθέτει στη συνολική επικινδυνότητα της εφαρμογής αυτής. Πρέπει να επιδιώκεται η μείωση της λεγόμενης «επιφάνειας επίθεσης» (attack surface), προσθέτοντας εκείνα τα ελάχιστα χαρακτηριστικά, τα οποία είναι απαραίτητα προκειμένου να ικανοποιηθούν οι προδιαγραφές λειτουργικότητάς της. Αυτή η αρχή είναι γνωστή ως **Αρχή της Ελάχιστης Επιφάνειας Επίθεσης (Minimum Attack Surface Principle)**.

- Φροντίζουμε ώστε η εφαρμογή να εγκαθίσταται με τις ρυθμίσεις ασφάλειας εξ' ορισμού (by default) ενεργοποιημένες σε μέγιστο βαθμό. Στη συνέχεια, δίνεται στο χρήστη η δυνατότητα μείωσης του επιπέδου ασφάλειας της εφαρμογής, εφόσον το επιθυμεί και με δική του ευθύνη.

- Εφαρμόζουμε, γενικά, την **Αρχή του Ελάχιστου Προνομίου (Principle of Least Privilege)**, που ορίζει ότι στον κάθε χρήστη θα πρέπει να αποδίδεται το ελάχιστο σύνολο προνομίων το οποίο απαιτείται για να μπορεί να εκτελέσει μια εργασία του.

- Είναι καλό να προσθέτουμε περισσότερους από ένα μηχανισμούς ασφάλειας αν κάτι τέτοιο δεν επηρεάζει σημαντικά την απόδοση ή τη λειτουργικότητα της εφαρμογής μας. Αν μια ευπάθεια μειώνεται με την εφαρμογή ενός μηχανισμού ασφάλειας, τότε σίγουρα θα είναι δυσκολότερο να την εκμεταλλευτεί κάποιος επίδοξος εισβολέας έχοντας να υπερνικήσει επιπρόσθετους (δυο ή περισσοτέρους) μηχανισμούς ασφάλειας. Σε εφαρμογές διαδικτύου κάτι τέτοιο θα σήμαινε, για παράδειγμα, το να σχεδιάζονται φόρμες εισαγωγής στοιχείων με πολλαπλά επίπεδα επαλήθευσης. Με αυτό τον τρόπο ο χρήστης αυθεντικοποιείται για να εκτελέσει μια εργασία της εφαρμογής, αλλά όχι για το σύνολο των διαθέσιμων εργασιών. Η εκτέλεση μιας επόμενης εργασίας απαιτεί την εκ νέου αυθεντικοποίηση του χρήστη. Είναι ιδιαίτερα σημαντικός ο τρόπος διαχείρισης από τον ίδιο τον κώδικα (resilience) μιας πιθανής αστοχίας της εφαρμογής, καθώς πρέπει να προληφθεί οποιαδήποτε παρενέργεια που θα μπορούσε να οδηγήσει σε δημιουργία ευπάθειας. Για παράδειγμα, στο παρακάτω τμήμα κώδικα Java το οποίο συναντάμε στον ιστότοπο https://www.owasp.org, ο κακός χειρισμός εξαίρεσης (exception handling) οδηγεί σε απόδοση του ρόλου του διαχειριστή (administrator) στον τελικό χρήστη που εκτελεί την εφαρμογή, αν το τμήμα του κώδικα badCode() αποτύχει:

```
/*
Αν το τμήμα κώδικα badCode ή το τμήμα κώδικα isUserInRole
αποτύχει, τότε ο χρήστης παραμένει σε ρόλο administrator, όπως
αρχικά του είχε αποδοθεί στην πρώτη γραμμή κώδικα.
*/
isAdmin = true;
try {
     badCode();
```

```
    isAdmin = isUserInRole( "Administrator" );
}
catch (Exception ex) {
log.write(ex.toString());
}
```

- Δεν πρέπει να εμπιστευόμαστε χωρίς έλεγχο υπηρεσίες οι οποίες προσφέρονται από πληροφοριακά συστήματα τρίτων οργανισμών. Δεν είναι βέβαιο ότι κάθε οργανισμός διαθέτει μια πολιτική ασφάλειας η οποία καθορίζει τα πλαίσια της ασφαλούς λειτουργίας των πληροφοριακών του συστημάτων. Ακόμη και αν υπάρχει πολιτική ασφάλειας, τότε αυτή πιθανώς να απέχει από τα δικά μας πρότυπα και επιθυμητά επίπεδα ασφάλειας. Όλα τα εξωτερικά πληροφοριακά συστήματα θα πρέπει να αντιμετωπίζονται και να ελέγχονται με την ίδια αυστηρότητα.

- Η πιστή εφαρμογή της **Αρχής του Διαχωρισμού Καθηκόντων (Separation of Duties)** είναι σημαντική, γιατί με τον κατάλληλο διαχωρισμό (π.χ. των διεργασιών και των ρόλων) είναι ευκολότερο να ορίζουμε ρητά τα δικαιώματα της κάθε διεργασίας ή ρόλου που εμπλέκεται στην επιτέλεση μιας εργασίας, χωρίς να δημιουργούμε γκρίζες περιοχές αμφισβήτησης δικαιωμάτων.

- Θα πρέπει να αποφεύγεται η απόκρυψης του τρόπου λειτουργίας των μηχανισμών ασφάλειας, η οποία είναι γνωστότερη ως «**security by obscurity**». Η μυστικοπάθεια σε ότι αφορά τις υπάρχουσες ευπάθειες ενός πληροφοριακού συστήματος ή τους μηχανισμούς ασφάλειας (π.χ. κρυπτογραφικοί αλγόριθμοι), καθιστά το σύστημα «ασφαλές» μέχρι του σημείου γνωστοποίησης ενός τέτοιου «μυστικού». Παράδειγμα προς μίμηση αποτελεί το λειτουργικό σύστημα Linux, του οποίου ο κώδικας διατίθεται ελεύθερα, ώστε πολλές χιλιάδες ερευνητών να έχουν την ευκαιρία να τον ελέγξουν για τυχόν σφάλματα, τα οποία θα προκαλούσαν τη δημιουργία ευπαθειών. Ένας έλεγχος του κώδικα και του τρόπου λειτουργίας των μηχανισμών ασφάλειας από μεγάλο αριθμό ερευνητών σίγουρα υπόσχεται καλύτερα αποτελέσματα από τον αντίστοιχο έλεγχο που θα διεξήγαγε μια μικρή ομάδα μερικών δεκάδων ανθρώπων (π.χ. κρυπταναλυτών).

- Σε συνδυασμό με την Αρχή της Ελάχιστης Επιφάνειας Επίθεσης, προτείνεται η εφαρμογή της **Αρχής της Απλότητας**, που ορίζει ότι μεταξύ δύο λύσεων ο μηχανικός λογισμικού (software engineer) θα πρέπει να επιλέξει την απλούστερη λύση. Η αρχή αυτή είναι γνωστή και ως το «Ξυράφι του Όκαμ» (Occam's Razor).

4.3 Κατηγορίες Ευπαθειών

Οι περισσότερες ευπάθειες που παρουσιάζονται στις διαδικτυακές εφαρμογές ανήκουν σε μία από τις παρακάτω κατηγορίες:

- Υπερχείλιση ενταμιευτήρα (buffer overflow)
- Μη επικυρωμένη είσοδος (invalidated input) χρήστη
- Συνθήκες ανταγωνισμού (race conditions)
- Προβλήματα ελέγχου πρόσβασης (access control)
- Αποθήκευση σε σύστημα διαχείρισης βάσεων δεδομένων (ΣΔΒΔ)

4.3.1 Υπερχείλιση ενταμιευτήρα

Μια τέτοια υπερχείλιση (overflow) συμβαίνει όταν μια διεργασία της εφαρμογής προσπαθεί να εγγράψει δεδομένα πέρα από το τέλος (ή, περιστασιακά, πριν από την αρχή) ενός ενταμιευτήρα (buffer). Ο ενταμιευτήρας είναι ένα τμήμα της μνήμης RAM που χρησιμοποιείται από τη διεργασία μια δεδομένη χρονική στιγμή.

Γενικότερα, μια υπερχείλιση μνήμης μπορεί να προκαλέσει την κατάρρευση (break) μιας διεργασίας, μπορεί να θέσει σε κίνδυνο τα δεδομένα που αυτή χειρίζεται, ή ακόμη μπορεί να βοηθήσει σε μια προσπάθεια περαιτέρω κλιμάκωσης των προνομίων πρόσβασης που απέκτησε ένας επιτιθέμενος σε ένα υπολογιστικό σύστημα. Συνολικά, το 20% των επιθέσεων που έχουν αναφερθεί στις Ηνωμένες Πολιτείες της Αμερικής από την ομάδα ετοιμότητας US-CERT αφορούν περιπτώσεις υπερχείλισης ενταμιευτήρα.

Πιο αναλυτικά, κάθε διεργασία αποθηκεύει στη μνήμη RAM την είσοδο που καταχωρεί ο χρήστης χρησιμοποιώντας μια από τις ακόλουθες δομές δεδομένων:

- **Στοίβα (Stack)**, που υλοποιείται σε ένα τμήμα του χώρου διευθύνσεων μνήμης (memory address space) που χρησιμοποιεί η διεργασία και το οποίο αφορά μια μεμονωμένη κλήση συνάρτησης, μεθόδου, ή άλλης ισοδύναμης λειτουργίας.

- **Σωρός (Heap)**, που αποτελεί έναν γενικής χρήσης αποθηκευτικό χώρο για τη διεργασία. Τα δεδομένα, που αποθηκεύονται στο σωρό παραμένουν διαθέσιμα για το χρονικό διάστημα εκτέλεσης της διεργασίας ή έως ότου το λειτουργικό σύστημα αποφασίσει ότι η διεργασία δεν τα χρειάζεται πλέον.

Γενικότερα, επιθέσεις τύπου υπερχείλισης ενταμιευτήρα συμβαίνουν όταν κανείς εκμεταλλευτεί επιτυχώς τους περιορισμούς ή/και την ελλιπή διαχείριση των παραπάνω δομών δεδομένων.

4.3.2 Μη επικυρωμένη είσοδος από χρήστη

Κατά γενικό κανόνα, ο κώδικας της εφαρμογής θα πρέπει να ελέγχει όλα τα στοιχεία εισόδου που εισάγονται (input data) από τον χρήστη προκειμένου να επικυρώνεται ότι καταχωρήθηκαν οι κατάλληλες και επιτρεπτές τιμές δεδομένων στο πλαίσιο της επιθυμητής λειτουργικότητας της εφαρμογής.

Μια εφαρμογή η οποία δεν εκτελεί έλεγχο κατά την καταχώρηση δεδομένων εισόδου από μη αξιόπιστη πηγή προέλευσης αποτελεί ένα πιθανό στόχο επίθεσης από κακόβουλους χρήστες. Στο πλαίσιο αυτής της θεώρησης, κάθε χρήστης μιας εφαρμογής είναι μια μη αξιόπιστη πηγή προέλευσης και ο έλεγχος των εισηγμένων δεδομένων είναι επιβεβλημένος.

Τα κυριότερα σημεία ελέγχου από τον κώδικα της εφαρμογής, κατά τη διαδικασία επικύρωσης, είναι τα παρακάτω:

- Όρια τιμών: Για κάθε πεδίο (field) θα πρέπει να ορίζεται ένα κάτω και ένα άνω όριο επιτρεπτών τιμών εισόδου. Π.χ. ένα πεδίο το οποίο δέχεται τιμή χρηματικού ποσού θα πρέπει να ελέγχεται ώστε η τιμή αυτή να μην είναι αρνητική ή να μην ξεπερνάει ένα άνω όριο.

- Μήκος εισόδου: Για κάθε πεδίο θα πρέπει να έχει τεθεί ένα όριο στο μήκος της σειράς αλφαριθμητικών χαρακτήρων που μπορεί να δεχθεί. Π.χ. ένα πεδίο στο οποίο καταχωρείται η ηλικία του χρήστη, δεν θα πρέπει να δέχεται τιμή που το μήκος της υπερβαίνει τους 2 χαρακτήρες.

- Ανυπαρξία τιμής: Η γλώσσα προγραμματισμού C χρησιμοποιεί τη δεκαεξαδική τιμή 0x00 (null byte) ως διακριτικό τερματισμού μιας σειράς αλφαριθμητικών χαρακτήρων. Επομένως, το null byte δε θα πρέπει να περιέχεται στην τιμή εισόδου, αφού οι χαρακτήρες που το ακολουθούν θα μπορούσαν να χρησιμοποιηθούν εσφαλμένα σε μια επόμενη δραστηριότητα της εφαρμογής και να προκαλέσουν πιθανώς μια απρόβλεπτη συμπεριφορά.

Για την επικύρωση των εισαγόμενων δεδομένων συνήθως χρησιμοποιείται μια από τις ακόλουθες δύο τεχνικές:

- Μαύρη Λίστα: Αναγνώριση μη έγκυρων δεδομένων και αφαίρεσή τους. Για το σκοπό αυτό διαθέτουμε μια μαύρη λίστα (black list) με πιθανά δεδομένα εισόδου, τα οποία δεν θεωρούνται έγκυρα. Στη συνέχεια, κάθε τιμή εισόδου ελέγχεται έναντι των περιεχομένων της μαύρης λίστας. Όσα δεδομένα συμπίπτουν, απορρίπτονται.

- Λευκή Λίστα: Αναγνώριση έγκυρων δεδομένων και αφαίρεση των υπόλοιπων. Για το σκοπό αυτό, διαθέτουμε μια λευκή λίστα (white list) με πιθανά δεδομένα εισόδου τα οποία θεωρούνται έγκυρα. Στη συνέχεια, κάθε τιμή εισόδου ελέγχεται έναντι των περιεχομένων της λευκής λίστας και όσα δεδομένα συμπίπτουν γίνονται δεκτά, ενώ όλα τα υπόλοιπα απορρίπτονται.

4.3.3 Συνθήκες ανταγωνισμού

Συνθήκη ανταγωνισμού (race condition) έχουμε όταν δύο νήματα (threads) προσπαθούν να προσπελάσουν το ίδιο αντικείμενο ταυτόχρονα και η συμπεριφορά του προγράμματος εξαρτάται από το ποιο νήμα προηγείται στη σειρά προσπέλασης. Η σειρά αυτή δεν εμπίπτει σε μια ντετερμινιστική ακολουθία, άρα όταν δεν ελέγχεται (π.χ. synchronized) είναι μη προβλέψιμη και εξαρτάται από το λειτουργικό σύστημα.

Πέρα από τα προβλήματα στη λειτουργία της εφαρμογής, οι επιτιθέμενοι μπορούν μερικές φορές να επωφεληθούν από μικρά χρονικά κενά κατά την επεξεργασία του κώδικα για να παρέμβουν στην εξέλιξη των εργασιών, τις οποίες στη συνέχεια εκμεταλλεύονται. Ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί μια τέτοια κατάσταση για να εισάγει κατάλληλο κώδικα. Για παράδειγμα, να αλλάξει το όνομα ενός αρχείου και να επηρεάσει την ομαλή λειτουργία της διεργασίας.

4.3.4 Προβλήματα ελέγχου πρόσβασης

Με τη διαδικασία του ελέγχου πρόσβασης (access control) ελέγχουμε συνήθως στη βάση της επιβεβαιωμένης ταυτότητάς του (authentication) αν ο νόμιμος χρήστης της εφαρμογής είναι εξουσιοδοτημένος (authorization) και επομένως του επιτρέπεται να εκτελέσει μια εργασία σε συγκεκριμένους πόρους του πληροφοριακού συστήματος μετά από αίτημά του. Οι μηχανισμοί ελέγχου πρόσβασης είναι δυνατό να επιβάλλονται και να ελέγχονται από το λειτουργικό σύστημα, το σύστημα διαχείρισης βάσεων δεδομένων (ΣΔΒΔ), την ίδια την εφαρμογή, μια υπηρεσία, ένα πρωτόκολλο επικοινωνίας, κ.ά.

Οι εγγενείς ευπάθειες των μηχανισμών αυθεντικοποίησης, εξουσιοδότησης ή/και των κρυπτογραφικών μηχανισμών, που πιθανώς χρησιμοποιούνται για τον έλεγχο πρόσβασης, οφείλονται κυρίως σε σχεδιαστικά σφάλματα ή σε αστοχίες της συγγραφής κώδικα της εφαρμογής. Κατά την ανάπτυξη των διαδικτυακών εφαρμογών, σημαντικό ρόλο κατέχει η αρχιτεκτονική της εφαρμογής που εφαρμόζεται (π.χ. μοντέλο πελάτη/εξυπηρετητή), καθώς και η γλώσσα προγραμματισμού.

4.3.5 Αποθήκευση σε Σύστημα Διαχείρισης Βάσεων Δεδομένων

Κατά τη λειτουργία μιας διαδικτυακής εφαρμογής, συνήθως αποθηκεύονται και ανακτώνται δεδομένα σε /από ένα σύστημα διαχείρισης βάσεων δεδομένων (ΣΔΒΔ). Η επικοινωνία με το ΣΔΒΔ πραγματοποιείται με ανταλλαγή συμβολοσειρών οι οποίες είναι είτε δεδομένα της εφαρμογής είτε εντολές επεξεργασίας τους ή εντολές ελέγχου του ΣΔΒΔ. Στη συνέχεια, το ΣΔΒΔ χρησιμοποιεί ένα διερμηνευτή ο οποίος αποκωδικοποιεί τις εισερχόμενες συμβολοσειρές διαβάζοντας ένα-προς-ένα τους χαρακτήρες και αποφασίζοντας για το είδος της πληροφορίας που περιέχεται στη συμβολοσειρά (δεδομένα εφαρμογής ή εντολή προς εκτέλεση).

Πρόβλημα ασφάλειας παρουσιάζεται όταν ο προγραμματιστής προσπαθεί να αποθηκεύσει δεδομένα στο ΣΔΒΔ και ο διερμηνευτής μεταφράζει εσφαλμένα ένα τμήμα των δεδομένων ως εντολή προς εκτέλεση. Σε μια τέτοια περίπτωση υπάρχει ο κίνδυνος ένας κακόβουλος χρήστης να κατορθώσει να εκμεταλλευτεί μια τέτοια ευπάθεια και να εισάγει εντολές προς εκτέλεση, δημιουργώντας ρήγμα στην ασφάλεια της εφαρμογής. Αυτό το ιδιαίτερα διαδεδομένο είδος επίθεσης ονομάζεται **ψεκασμός κώδικα SQL (SQL Injection).**

Κατά την επίθεση ψεκασμού κώδικα SQL ο επιτιθέμενος εισάγει κατάλληλα διαμορφωμένες συμβολοσειρές ώστε να προκαλέσει την εκτέλεση εντολών SQL από το ΣΔΒΔ που πλήττουν την

εμπιστευτικότητα ή την ακεραιότητα των δεδομένων της εφαρμογής. Η επιτυχία της επίθεσης εξαρτάται από την ύπαρξη αποτελεσματικού κώδικα λογισμικού εφαρμογής για την κατάλληλη επεξεργασία και έλεγχο των εισαγόμενων από τον τελικό χρήστη χαρακτήρων (input validation).

4.4. Μελέτη Περίπτωσης: Java

Η γλώσσα προγραμματισμού Java αποτελεί μια αξιόλογη περίπτωση για την εφαρμογή των παραπάνω αρχών ασφαλούς διαδικτυακού προγραμματισμού. Οι διαδικτυακές εφαρμογές που αναπτύσσονται με τη γλώσσα αυτή μπορούν να εκτελεστούν από πολλούς χρήστες με διαφορετικά δικαιώματα πρόσβασης, χωρίς να δημιουργούνται παρενέργειες, με ή χωρίς πρόθεση από τον τελικό χρήστη. Αυτό επιτυγχάνεται με τη βοήθεια ενός ειδικού υποσυστήματος της γλώσσας το οποίο ονομάζεται επιβεβαιωτής ενδιάμεσου κώδικα (bytecode verifier). Ο επιβεβαιωτής ελέγχει τον ενδιάμεσο κώδικα που παράγεται κατά την εκτέλεση μιας εφαρμογής εντοπίζοντας τα «ύποπτα» σημεία, των οποίων η εκτέλεση θα μπορούσε να προκαλέσει ευπάθειες στο υπολογιστικό σύστημα.

Ωστόσο, ενώ η αρχιτεκτονική της Java μπορεί να προστατέψει το υπολογιστικό σύστημα από κακόβουλα προγράμματα που εκτελούνται μέσω του διαδικτύου, είναι ανυπεράσπιστη σε υλοποιήσεις εφαρμογών με προγραμματιστικά σφάλματα. Τέτοια σφάλματα μπορεί να οδηγήσουν σε ανεπιθύμητη χρήση αρχείων του συστήματος, εκτυπωτών, κάμερας, μικροφώνου και άλλων περιφερειακών. Είναι δυνατό, επίσης, τέτοια σφάλματα να καταστήσουν το υπολογιστικό σύστημα υποχείριο («ζόμπι») ενός επιτιθέμενου, δηλαδή να το μετατρέψουν σε έναν ενδιάμεσο σταθμό γενικότερων επιθέσεων, όπως επιθέσεων υποκλοπής προσωπικών δεδομένων από μια συντονισμένη επίθεση που εξαπολύουν πολλά υπολογιστικά συστήματα μέσω του Διαδικτύου.

Η γλώσσα προγραμματισμού Java διαθέτει εγγενώς μηχανισμούς ασφάλειας, οι οποίοι υπερνικούν το συνηθισμένο πρόβλημα της υπερχείλισης ενταμιευτήρα. Ωστόσο, υπάρχουν αρκετά σημεία στα οποία θα πρέπει να δώσει ιδιαίτερη προσοχή ο προγραμματιστής, προκειμένου να αναπτύξει προγράμματα χωρίς ευπάθειες. Τα κυριότερα σημεία στα οποία θα πρέπει να δώσει έμφαση είναι τα παρακάτω:

- **Απλός σχεδιασμός**: Κατά την ανάπτυξη του λογισμικού εφαρμογής θα πρέπει να επιλέγεται πάντα ο απλούστερος σχεδιασμός, ώστε για τα λάθη που πιθανώς να προκύψουν να είναι εύκολος ο εντοπισμός των αιτίων τους.

- **Ασφάλεια από την αρχή**: Η ασφάλεια θα πρέπει να απασχολεί τον προγραμματιστή από το αρχικό στάδιο της σχεδίασης της εφαρμογής. Η προσπάθεια εισαγωγής μηχανισμών ασφάλειας σε μια εφαρμογή λογισμικού κατά τη διάρκεια ενός επόμενου σταδίου δεν είναι πάντα αποτελεσματική και είναι πιθανό να οδηγήσει σε περαιτέρω σφάλματα. Για παράδειγμα, χαρακτηρίζοντας μια κλάση ως final, προστατεύεται το λογισμικό από πιθανούς κακόβουλους χρήστες οι οποίοι θα επιδίωκαν να δημιουργήσουν νέες κλάσεις-κληρονόμους, ή να κάνουν override μεθόδους αυτής της κλάσης. Επίσης, η χρήση του SecurityManager σε ένα τμήμα κώδικα, υποδηλώνει πως αυτή η περιοχή κώδικα θα ελεγχθεί σχολαστικά.

- **Περιορισμός Προνομίων**: Παρά τις προσπάθειες για συγγραφή ασφαλούς κώδικα, είναι σχεδόν βέβαιο ότι θα συνεχίσουν να υπάρχουν ατέλειες/σφάλματα στα διάφορα προϊόντα λογισμικού διαδικτυακών εφαρμογών. Γι' αυτό το λόγο, είναι προτιμότερο ο κώδικας να εκτελείται με μειωμένα προνόμια, ώστε ακόμη και αν υπάρχουν σφάλματα τα οποία θα μπορούσε να εκμεταλλευτεί μια πιθανή απειλή για να εξαπολύσει μια επιτυχημένη επίθεση, να μη μπορέσει σε μια τέτοια περίπτωση η επίθεση να «εξαπλωθεί» στο υπόλοιπο υπολογιστικό σύστημα. Τα προνόμια εκτέλεσης του κώδικα Java μπορούν να δηλωθούν είτε στατικά, με το μηχανισμό ασφάλειας της Java ο οποίος χρησιμοποιεί αρχεία πολιτικής (policy files), ή δυναμικά, με τη χρήση του μηχανισμού java.security.AccessController.doPrivileged. Οι εφαρμογές Rich Internet (RIA) μπορούν να προσδιορίζουν τα απαιτούμενα προνόμια εκτέλεσης μέσω της χρήσης ενός εφαρμογιδίου (applet) ή μέσω του JNLP. Επίσης, ένα υπογεγραμμένο αρχείο jar μπορεί να δηλώνει στο αρχείο Manifest ένα χαρακτηριστικό, το οποίο θα προσδιορίζει αν απαιτείται να εκτελεστεί με πλήρη δικαιώματα ή με περιορισμένα

δικαιώματα στο πλαίσιο ενός προστατευόμενου περιβάλλοντος (sandbox). Και στις δύο αυτές περιπτώσεις, κάθε παραβίαση της ασφάλειας θα ενεργοποιήσει την παρέμβαση του περιβάλλοντος JRE (Java Runtime Environment), με ταυτόχρονη κλήση του χειριστή εξαιρέσεων.

- **Καθορισμός ορίων εμπιστοσύνης**: Για να είμαστε βέβαιοι ότι ένα σύστημα προστατεύεται επαρκώς θα πρέπει να γνωρίζουμε τα όρια που το καθορίζουν, σε σχέση με κάθε άλλο εξωτερικό σύστημα, το οποίο ανήκει στο εξωτερικό περιβάλλον λειτουργίας του συστήματος μας (όπως για παράδειγμα το διαδίκτυο). Ως όρια του συστήματος, ορίζουμε τα σημεία εκείνα από τα οποία τα δεδομένα εξέρχονται στο εξωτερικό περιβάλλον ή εισέρχονται στο σύστημα μας προερχόμενα από το εξωτερικό περιβάλλον. Ειδικότερα, τα δεδομένα τα οποία διαπερνούν αυτά τα όρια, κατευθυνόμενα προς το εσωτερικό του συστήματος, θα πρέπει να «αποστειρώνονται» (sanitize) και να επικυρώνονται (validate) πριν χρησιμοποιηθούν από τον κώδικα μιας διαδικτυακής εφαρμογής.

- **Αντοχή σε επιθέσεις άρνησης εξυπηρέτησης**: Οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service) στοχεύουν στην άσκοπη κατανάλωση πόρων του υπολογιστικού συστήματος μέχρι του σημείου κατάρρευσης από την πλευρά του εξυπηρετητή, λόγω εξάντλησης των διαθέσιμων πόρων του. Οι συνηθισμένοι πόροι εξυπηρετητή, που αποτελούν στόχους εκμετάλλευσης, είναι η επεξεργαστική ισχύς, η μνήμη RAM, ο αποθηκευτικός χώρος δίσκου και το εύρος ζώνης δικτύου (bandwidth) που του διατίθεται.

Απαιτείται ιδιαίτερη προσοχή κυρίως στις ακόλουθες περιπτώσεις:

- Δημιουργία διανυσματικών αρχείων γραφικών (vector graphics) πολύ μεγάλου μεγέθους (αρχεία svg ή font).

- Σφάλματα υπερχείλισης σε περιπτώσεις ακεραίων τιμών.

- Ένα γραφικό αντικείμενο, το οποίο έχει δημιουργηθεί από τη σάρωση ενός κειμένου, μπορεί να έχει απαιτήσεις σε μνήμη και χωρητικότητα αποθηκευτικού χώρου. πολλές φορές. μεγαλύτερη από ότι το αρχικό κείμενο.

- Αποσυμπίεση υπερσυμπιεσμένων αρχείων («Βόμβες zip»), όπως για παράδειγμα οι εικόνες GIF. Όταν αποσυμπιέζονται τέτοια αρχεία, είναι ασφαλέστερο να τίθεται όριο στο μέγεθος των δεδομένων που τελικά παράγονται.

- Αυθαίρετη κατανάλωση χρόνου από επεξεργασία εκφράσεων XPath.

- Απεριόριστη χρήση μνήμης ή επεξεργαστικής ισχύος από τη διαδικασία σειριοποίησης ή αποσειριοποίησης (java serialization/deserialization).

Η αποδέσμευση των πόρων συστήματος μετά τη χρήση τους (όταν πλέον δεν είναι απαραίτητοι), είναι σημαντική ιδιαίτερα στην περίπτωση ανοικτών αρχείων, κλειδωμάτων (locks) και μνήμης η οποία δεσμεύτηκε ρητά. Η αποδέσμευση των πόρων ενός υπολογιστικού συστήματος είναι απαραίτητη για να μπορούμε να εξυπηρετήσουμε καλύτερα το σκοπό της εφαρμογής μας, χωρίς να επιβαρύνουμε το υπολογιστικό σύστημα.

Το μοτίβο (pattern) **Execute Around Method** παρέχει έναν εξαιρετικό τρόπο διαχείρισης του ζεύγους ενεργειών απόκτησης - απελευθέρωσης πόρων. Στην έκδοση 8 της γλώσσας Java, το μοτίβο αυτό χρησιμοποιείται με τη χρήση της ιδιότητας lambda. Για παράδειγμα:

```
/*
το μοτίβο Execute around method χρησιμοποιείται για να
εκτελέσουμε, μετά από κλήση, διεργασίες οι οποίες είναι
```

```
επαναλαμβανόμενες κατά τη διάρκεια λειτουργίας της εφαρμογής
μας.
*/

long sum = readFileBuffered(InputStream in -> {
     long current = 0;
    for (;;) {
          int b = in.read();
        if (b == -1) {
                return current;
        }
        current += b;
    }
});
```

Η σύνταξη try-with-resource, που παρουσιάστηκε στην έκδοση 7 της γλώσσας Java, χειρίζεται αυτόματα την απελευθέρωση πολλών τύπων πόρων. Για παράδειγμα:

```
/*
Η σύνταξη try-with-resource επιβεβαιώνει ότι μετά την κλήση της
μεθόδου, οι πόροι που χρησιμοποιήθηκαν θα αποδεσμευτούν
αυτόματα.
*/

public R readFileBuffered(InputStreamHandler handler) throws
IOException {
     try (final InputStream in = Files.newInputStream(path)) {
          handler.handle(new BufferedInputStream(in));
    }
}
```

Πόροι οι οποίοι δεν μπορούν να χρησιμοποιήσουν αυτές τις νέες δομές θα πρέπει να χρησιμοποιούν το συνηθισμένο τρόπο κτήσης και απελευθέρωσης πόρων. Για παράδειγμα:

```
/*
αυτόματα αποδεσμεύονται πόροι οι οποίοι εφαρμόζουν το
java.lang.AutoCloseable. Οι υπόλοιποι πόροι πρέπει ρητά να
αποδεσμευτούν με τη κλήση unlock()
*/

public R locked (Action action) {
     lock.lock();
     try {
          return action.run();
     } finally {
          lock.unlock();
    }
}
```

Επίσης, είναι σημαντικό να αδειάζουν όλοι οι ενταμιευτήρες εξόδου (output buffers). Αν αποτύχει το άδειασμα των ενταμιευτήρων, θα πρέπει να γίνεται ρίψη εξαίρεσης.

```
/*
```

```
Η εντολή out.flush() στο πλαίσιο της εντολής try επιβεβαιώνει
ότι αν το άδειασμα του ενταμιευτήρα δεν επιτύχει, τότε θα γίνει
ρίψη εξαίρεσης
*/

public void writeFile(OutputStreamHandler handler) throws
IOException {
     try       (final       OutputStream       rawOut       =
Files.newOutputStream(path)) {
          final     BufferedOutputStream     out     =     new
BufferedOutputStream(rawOut);
        handler.handle(out);
        out.flush();
    }
}
```

4.4.1 Ευαίσθητα δεδομένα

Αρκετές φορές, οι μηχανισμοί εξαίρεσης μπορεί να εκθέσουν δεδομένα τα οποία επιθυμούμε να προστατεύσουμε. Για παράδειγμα, αν μια μέθοδος καλέσει τον κατασκευαστή (constructor) java.io.FileInputStream για να αναγνώσει ένα αρχείο ρυθμίσεων και το αρχείο δεν υπάρχει, τότε επιστρέφεται μια εξαίρεση java.io.FileNotFoundException, η οποία περιέχει τη διαδρομή του αρχείου. Η διάδοση αυτής τη εξαίρεσης προς τα πίσω στην καλούσα μέθοδο, μπορεί να αποκαλύψει τη δομή του συστήματος αρχείων. Αρκετές επιθέσεις στηρίζονται στη γνώση αυτών των διαδρομών του συστήματος αρχείων.

Ακόμη, είναι πιθανό σε μια τέτοια διαδρομή να περιέχονται στοιχεία, όπως το όνομα χρήστη ή ο οικείος φάκελός του (home directory). Ο μηχανισμός SecurityManager μπορεί να προστατεύει αυτή την πληροφορία όταν δηλώνεται σε ιδιότητες συστήματος, όπως είναι το user.home. Ωστόσο, η πληροφορία αυτή θα μπορούσε να ξεφύγει από τον έλεγχο του SecurityManager σε περίπτωση ενεργοποίησης μιας εξαίρεσης και να παρουσιαστεί στον τελικό χρήστη. Χρειάζεται, επομένως, ιδιαίτερη προσοχή στη διαχείριση των εξαιρέσεων, ακόμη και για τις περιπτώσεις όπου γίνεται χρήση βιβλιοθηκών οι οποίες μια δεδομένη στιγμή δεν χρησιμοποιούν ευαίσθητα δεδομένα, αλλά είναι πιθανό μα επόμενη έκδοσή τους να τα χρησιμοποιεί.

Οι εξαιρέσεις μπορούν επίσης να αφορούν ευαίσθητα δεδομένα σχετικά με τις ρυθμίσεις και τα εσωτερικά χαρακτηριστικά του υπολογιστικού συστήματος. Γι' αυτό, δεν πρέπει να επιστρέφονται στους τελικούς χρήστες πληροφορίες εξαίρεσης, εκτός και αν το επιβάλλει σε ειδικές περιπτώσεις το περιεχόμενο των σχετικών μηνυμάτων. Για παράδειγμα, δεν πρέπει να επιστρέφονται μηνύματα εξαιρέσεως σχετικά με ίχνη στοίβας (stack traces) μέσα σε σχόλια κώδικα HTML. Ακόμη υπάρχουν άλλου είδους πληροφορίες, όπως είναι τα δεδομένα προσωπικού χαρακτήρα (π.χ. αριθμός κοινωνικής ασφάλισης, αριθμός αστυνομικής ταυτότητας κ.λπ.), τα οποία δεν πρέπει να διατηρούνται στο σύστημα περισσότερο από όσο απαιτείται για την ορθή λειτουργία των διεργασιών του συστήματος. Για παράδειγμα, η αποθήκευση και διατήρηση τέτοιων πληροφοριών σε αρχεία καταγραφής μητρώου (log files) θα πρέπει να συνοδεύεται από βοηθητικές ενέργειες ασφάλειας. Τα αρχεία καταγραφής θα πρέπει να εξαιρούνται από πιθανές ενέργειες αναζήτησης ή να διαγράφεται η σχετική πληροφορία όταν περατωθεί το χρονικό διάστημα χρήσης της.

Οι ευαίσθητες πληροφορίες απαιτούν ιδιαίτερο χειρισμό και στην περίπτωση όπου κρατούνται μόνο στη μνήμη, καθώς και εκεί αποτελούν στόχο κακόβουλων ενεργειών. Θα πρέπει να φροντίζουμε να πραγματοποιούμε εκκαθάριση της μνήμης όταν καταχωρούνται ευαίσθητες πληροφορίες.

4.4.2 Ψεκασμός εντολών

Είναι πλέον σύνηθες το φαινόμενο κατασκευής αλφαριθμητικών τα οποία προορίζονται για χρήση απλού κειμένου, αλλά χρησιμοποιούνται με τέτοιο τρόπο ώστε να καταλήγουν να αποτελέσουν εκτελέσιμες εντολές. Για αυτό, θα πρέπει να αποφεύγεται η χρήση δυναμικής δημιουργίας εντολών SQL, καθώς ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί το γεγονός ότι χρησιμοποιώντας το χαρακτήρα «΄» (quote) μπορεί να προσθέσει στη συμβολοσειρά εισόδου μια εντολή SQL, η οποία στη συνέχεια θα εκτελεστεί από τη διεργασία.

Για παραμετροποιημένες εντολές SQL μέσω του Java Database Connectivity (JDBC), συστήνεται να γίνεται ορθή χρήση του αντικειμένου java.sql.PreparedStatement ή του αντικειμένου java.sql.CallableStatement και όχι του αντικειμένου java.sql.Statement. Ακόμη, προτιμότερη είναι η χρήση μιας έτοιμης βιβλιοθήκης διαχείρισης βάσης δεδομένων, έτσι ώστε να πραγματοποιείται ορθή χρήση των απαραίτητων εντολών SQL.

Ένα παράδειγμα ορθής χρήσης του αντικειμένου java.sql.PreparedStatement παρουσιάζεται στο παρακάτω τμήμα κώδικα:

```
String sql = "SELECT * FROM User WHERE userId = ?";
PreparedStatement stmt = con.prepareStatement(sql);
stmt.setString(1, userId);
ResultSet rs = prepStmt.executeQuery();
```

Δεδομένα τα οποία προέρχονται από μη αξιόπιστη πηγή προέλευσης (όπως ο τελικός χρήστης) θα πρέπει να εξετάζονται προσεκτικά, πριν εισαχθούν σε αρχεία HTML ή XML. Μια αποτυχία ελέγχου τέτοιων δεδομένων θα μπορούσε να οδηγήσει σε επιθέσεις τύπου Cross-Site Scripting (XSS) ή XML Injection. Προσοχή απαιτείται κυρίως στην περίπτωση των Java Server Pages (JSP). Οι κυριότεροι τρόποι χειρισμού τέτοιων δεδομένων είναι το φιλτράρισμα (έλεγχος και επικύρωση), η αποφυγή αποστολής τους και η κωδικοποίηση επικίνδυνων χαρακτήρων, οι οποίοι μπορεί να μεταφραστούν ως χαρακτήρες ελέγχου. Και σε αυτή την περίπτωση, η χρήση έτοιμων βιβλιοθηκών αποτελεί εφαρμογή μιας ορθής πρακτικής ασφάλειας.

Σε περιβάλλον Unix χρειάζεται ιδιαίτερη προσοχή όταν η διαδικτυακή εφαρμογή παράγει ως έξοδο αλφαριθμητικά σε γραμμή κελύφους (shell), όπου υπάρχει το ενδεχόμενο ένας ή περισσότεροι χαρακτήρες να θεωρηθούν ως διακόπτες (options) σε μια εντολή προς εκτέλεση (π.χ. προς το λειτουργικό σύστημα). Σε αυτές τις περιπτώσεις, συνηθίζεται η κωδικοποίηση τέτοιων χαρακτήρων σε μια μορφή όπως η Base64.

Τα αρχεία εικόνων τύπου BMP μπορεί να περιέχουν αναφορές σε τοπικά αρχεία ICC (International Color Consortium). Ενώ το περιεχόμενο των αρχείων ICC είναι απίθανο να παρουσιάζει κάποιο ενδιαφέρον, η προσπάθεια να διαβαστούν τα αρχεία μπορεί να είναι ένα ζήτημα, καθώς τα αρχεία αυτά συνήθως βρίσκονται αποθηκευμένα σε περιοχές κρίσιμες για τη λειτουργία του συστήματος. Γι' αυτό, είτε αποφεύγουμε τα αρχεία τύπου BMP, ή μειώνουμε τα προνόμιά, έτσι ώστε να μην επιτρέπεται η πρόσβαση σε αρχεία ICC.

Μερικά τμήματα Swing μεταφράζουν τμήματα κώδικα τα οποία ξεκινούν με <html> ως κώδικα HTML. Για να αποφύγουμε τον πιθανό κίνδυνο από μη έμπιστο κώδικα, ορίζουμε την ιδιότητα html.disable σε κάθε τέτοιο τμήμα θέτοντας την τιμή Boolean.TRUE. Για παράδειγμα:

```
label.putClientProperty("html.disable", true);
```

4.4.3 Προσβασιμότητα και επεκτασιμότητα

Τα Containers μπορεί να κρύβουν κώδικα υλοποίησης, τροποποιώντας την ιδιότητα ασφάλειας package.access. Αυτή η ιδιότητα εμποδίζει μη έμπιστες κλάσεις να συνδεθούν και να κληθούν από φορτωτές κλάσεων (class loaders) στην καθορισμένη ιεραρχία πακέτου. Πρέπει να λαμβάνεται μέριμνα για να διασφαλιστεί ότι τα πακέτα δεν είναι προσβάσιμα από μη έμπιστα περιβάλλοντα πριν οριστεί αυτή η ιδιότητα. Το παρακάτω παράδειγμα υποδεικνύει την ορθή χρήση της ιδιότητας package.access:

```
private static final String PACKAGE_ACCESS_KEY =
"package.access";

static {

     //Ανάγνωση ιδιότητας package.access
     String packageAccess =
java.security.Security.getProperty(PACKAGE_ACCESS_KEY);

     //Ορθή χρήση ιδιότητας package.access
```

```
        java.security.Security.setProperty(PACKAGE_ACCESS_KEY,((
    packageAccess == null || packageAccess.trim().isEmpty()) ? ""
    :(packageAccess                    +                    ","))
    +"xx.example.product.implementation.");
    }
```

Ένας ακόμη σημαντικός παράγοντας ασφάλειας, που πρέπει να εξετάζεται, είναι η επεκτασιμότητα των κλάσεων και των μεθόδων. Πρέπει ρητά να δηλώνονται με χαρακτηρισμό final οι κλάσεις που δεν πρέπει να επεκτείνονται. Όπως, για παράδειγμα, στο τμήμα κώδικα που ακολουθεί:

```
//Η κλάση SensitiveClass δεν μπορεί να επεκταθεί
public final class SensitiveClass {

     //Η μέθοδος Behavior δεν μπορεί να επεκταθεί
     private final Behavior;

     // Απόκρυψη κατασκευαστή
     private SensitiveClass(Behavior behavior) {
          this.behavior = behavior;
     }

     //Guarded construction.
     public static SensitiveClass newSensitiveClass(Behavior
behavior) {
          // ... validate any arguments ...

          // ... perform security checks ...

          return new SensitiveClass(behavior);
    }
}
```

4.4.4 Επαλήθευση εισόδου

Ενώ ο κώδικας Java υπόκειται σε έλεγχο πραγματικού χρόνου για τους τύπους, τα όρια πινάκων, τη χρήση βιβλιοθηκών κ.ά., ο εκτελέσιμος κώδικας (native code), δηλαδή ο κώδικας που έχει συμβολομεταφραστεί για μια συγκεκριμένη οικογένεια επεξεργαστών δεν υπόκειται σε κανένα έλεγχο, με αποτέλεσμα να υπάρχει ο κίνδυνος υπερχείλισης ενταμιευτήρα κατά την εκτέλεσή του. Γι' αυτό το λόγο, δε θα πρέπει να δηλώνονται ως δημόσιες (public) οι μέθοδοι του εκτελέσιμου κώδικα. Τέτοιες μέθοδοι θα πρέπει να δηλώνονται ως private και να χρησιμοποιούνται μέσω μιας public μεθόδου wrapper, όπως παρουσιάζεται στο παράδειγμα κώδικα που ακολουθεί:

```
public final class NativeMethodWrapper {

     // Η μέθοδος nativeOperation δηλώνεται ιδιωτική
     private native void nativeOperation(byte[] data, int
offset, int len);

     // Η μέθοδος doOperation δηλώνεται δημόσια για να
χρησιμοποιηθεί ως διεπαφή της μεθόδου nativeOperation
     public void doOperation(byte[] data, int offset, int len)
{
          data = data.clone();

        /*
```

```
          Επικύρωση δεδομένων εισόδου. Το άθροισμα offset+len
μπορεί να προκαλέσει υπερχείλιση ακεραίου. Για παράδειγμα αν
offset=1 and len=Integer.MAX_VALUE, τότε offset+len ==
Integer.MIN_VALUE το οποίο είναι μικρότερο από το data.length.
Επίσης, βρόγχοι της μορφής for (int i=offset; i<offset+len;
++i) { ... } δεν θα προκαλούν πλέον εξαίρεση
          */

          if (offset < 0 || len < 0 || offset > data.length -
len) {
               throw new IllegalArgumentException();
          }
          nativeOperation(data, offset, len);
     }
}
```

4.4.5 Κατασκευή αντικειμένων

Κατά τη διάρκεια κατασκευής τους τα αντικείμενα βρίσκονται σε μια ιδιαίτερη κατάσταση όπου υπάρχουν αλλά δεν μπορούν να χρησιμοποιηθούν. Σε περίπτωση που ένας κατασκευαστής (constructor) σε μια non-final κλάση επιστρέψει μια εξαίρεση (exception), παρέχεται η δυνατότητα σε ένα κακόβουλο χρήστη για να προσπαθήσει να αποκτήσει πρόσβαση σε μια μερικώς αρχικοποιημένη έκδοση της κλάσης. Σε μια τέτοια κατάσταση, δεν έχουν αποδοθεί τιμές σε όλες τις μεταβλητές της μεθόδου και δεν έχουν αρχικοποιηθεί ολοκληρωμένα όλες οι μέθοδοι. Γι' αυτό, πρέπει να είμαστε βέβαιοι ότι μια non-final κλάση παραμένει εντελώς αχρησιμοποίητη, έως ότου ο κατασκευαστής της ολοκληρώσει την εκτέλεσή του επιτυχώς.

Ο έλεγχος ορθής δημιουργίας μιας non-final κλάσης μπορεί να γίνει κατά την κλήση this() ή super(), όπως στο παράδειγμα που ακολουθεί:

```
public abstract class ClassLoader {
     protected ClassLoader() {

     //έλεγχος ορθής δημιουργίας αντικειμένου
     this(securityManagerCheck());
     }

     private ClassLoader(Void ignored) {
          // ... συνέχεια αρχικοποίησης ...
     }

     private static Void securityManagerCheck() {
          SecurityManager              security              =
System.getSecurityManager();
          if (security != null) {
               security.checkCreateClassLoader();
          }
          return null;
     }
}
```

Για συμβατότητα με παλαιότερες εκδόσεις της γλώσσας Java, είναι θεμιτή η χρήση μιας αρχικοποιημένης σημαίας (initialized flag). Ο ορισμός της σημαίας θα πρέπει να είναι η τελευταία ενέργεια του κατασκευαστή πριν την επιτυχή ολοκλήρωση της εκτέλεσής του. Για παράδειγμα:

```
public abstract class ClassLoader {
```

```
        //ορισμός σημαίας
        private volatile boolean initialized;

        protected ClassLoader() {

              // χρειάζεται άδεια για τη δημιουργία ClassLoader
              securityManagerCheck();
              init();

              // Τελευταία ενέργεια του κατασκευαστή
              this.initialized = true;
        }

        protected final Class defineClass(...) {
              //έλεγχος κατάστασης σημαίας
              checkInitialized();
                    //...
              }

        private void checkInitialized() {
              if (!initialized) {
                    throw   new   SecurityException("NonFinal   not
initialized");
              }
        }
}
```

4.4.6 Serialization και Deserialization

Η διαδικασία serialization (σειριοποίησης ή αποτύπωσης σε σειριακή μορφή) παρέχει μια διεπαφή στις κλάσεις, η οποία παρακάμπτει τους μηχανισμούς ελέγχου πρόσβασης της γλώσσας Java. Κάνοντας μια κλάση serializable, ουσιαστικά δημιουργούμε μια δημόσια διεπαφή για όλα τα πεδία αυτής της κλάσης. Το serialization μπορεί, επίσης, να προσθέσει ένα κρυφό δημόσιο κατασκευαστή της κλάσης. Αυτό το ενδεχόμενο θα πρέπει να εξεταστεί κατά την προσπάθεια περιορισμού της αυτόματης κατασκευής αντικειμένων.

Όταν ένα αντικείμενο γίνει serialized, τότε οι μηχανισμοί ελέγχου πρόσβασης της Java παύουν να επιβάλλονται και οι επιτιθέμενοι μπορούν να προσπελάσουν ιδιωτικά πεδία ενός αντικειμένου, αναλύοντας τη serialized ροή του. Για το λόγο αυτό, δεν πρέπει να σειριοποιούνται κλάσεις οι οποίες περιέχουν ευαίσθητα δεδομένα.

Τρόποι αντιμετώπισης περιπτώσεων με ευαίσθητα δεδομένα σε serialized κλάσεις είναι οι παρακάτω:

- Ορισμός των ευαίσθητων πεδίων ως transient.
- Κατάλληλος ορισμός του πεδίου serialPersistentFields.
- Υλοποίηση writeObject και χρήση ObjectOutputStream.putField.
- Υλοποίηση writeReplace.
- Υλοποίηση της διεπαφής Externalizable.

Η διαδικασία deserialization (αποσειριοποίηση ή αναδόμηση από σειριακή μορφή) θα πρέπει να αντιμετωπίζεται ως διαδικασία κατασκευής αντικειμένου. Η διαδικασία deserialization δημιουργεί μια νέα εκδοχή της κλάσης, χωρίς την κλήση του κατασκευαστή αυτής της κλάσης. Θα πρέπει να γίνεται χρήση της ObjectInputStream.readFields για να προστατέψουμε τα περιεχόμενα της κλάσης, όπως στο παράδειγμα που ακολουθεί:

```
public final class ByteString implements java.io.Serializable
{
```

```
     private static final long serialVersionUID = 1L;
     private byte[] data;
     public ByteString(byte[] data) {

          // Δημιουργία αντιγράφου πριν την εκχώρηση
          this.data = data.clone();
     }

     private  void  readObject(java.io.ObjectInputStream  in)
throws java.io.IOException, ClassNotFoundException {

          // Προστασία των περιεχομένων της κλάσης με χρήση
της readFields
          java.io.ObjectInputStreadm.GetField    fields    =
in.readFields();
          this.data = ((byte[])fields.get("data")).clone();
     }
     //...
}
```

Σε μια μέθοδο readObject, θα πρέπει να διενεργούμε τους ίδιους ελέγχους εισόδου, όπως και σε έναν κατασκευαστή. Επίσης, είναι προτιμότερο να δημιουργούμε αντίγραφα αντικειμένων που έχουν προκύψει από deserialization, πριν αυτά οριστούν ως εσωτερικά πεδία σε μια υλοποίηση της readObject, Για παράδειγμα:

```
public final class Nonnegative implements java.io.Serializable
{
     private static final long serialVersionUID = 1L;
     private int value;

     public Nonnegative (int value) {
          // έλεγχος πριν την εκχώρηση
          this.data = nonnegative(value);
     }

     private static int nonnegative(int value) {
          if (value < 0) {
               throw new IllegalArgumentException (value + "
is negative");
          }
     return value;
     }

     // έλεγχος εισόδου
     private  void  readObject(java.io.ObjectInputStream  in)
throws java.io.IOException, ClassNotFoundException {
          java.io.ObjectInputStreadm.GetField fields =
          in.readFields();
          this.value = nonnegative(field.get(value, 0));
     }

     //...
}
```

Αν μια serializable κλάση επιβάλει τον έλεγχο του SecurityManager κατά τη χρήση του κατασκευαστή της, τότε θα πρέπει να επιβάλλουμε τον ίδιο έλεγχο σε μια μέθοδο readObject ή readObjectData. Για παράδειγμα:

```
public final class SensitiveClass implements
java.io.Serializable {
     public SensitiveClass() {

          /*
          Χρειάζεται άδεια για να γίνει instantiation του
SensitiveClass. Επιβολή ελέγχου από το securityManager
          */

          securityManagerCheck();
          // ...
     }

     /*
     Υλοποίηση readObject για επιβολή ελέγχων κατά τη διάρκεια
της αποσειριοποίησης. Ο ίδιος έλεγχος επιβάλλεται και για την
readObject
     /*

    private void readObject(java.io.ObjectInputStream in) {

        // διπλός έλεγχος από κατασκευαστή
        securityManagerCheck();
          //...
     }
}
```

Αν μία serializable κλάση επιτρέπει, μέσω μιας public μεθόδου, αλλαγή της εσωτερικής της κατάστασης και η αλλαγή αυτή ελέγχεται από τον SecurityManager, τότε θα πρέπει επίσης να επιβληθεί ο αντίστοιχος έλεγχος σε μια υλοποίηση της μεθόδου readObject. Για παράδειγμα:

```
public final class SecureName implements java.io.Serializable
{

     // Ιδιωτική εσωτερική κατάσταση
     Private String name;
     private static final String DEFAULT = "DEFAULT";

     public SecureName() {

     // Απόδοση αρχικής τιμής στο πεδίο name
     name = DEFAULT;

/*
Επιτρέπεται στους καλούντες να αλλάζουν την ιδιωτική εσωτερική
κατάσταση. Η δημόσια μέθοδος SetName μπορεί να επιφέρει αλλαγή
στην εσωτερική κατάσταση της κλάσης SecureName
*/

     public void setName(String name) {
          if (name!=null ? name.equals(this.name): (this.name
== null)) {

          // Καμία αλλαγή
```

```
            return;
            } else {
                  /*
                  Χρειάζεται άδεια για αλλαγή ονόματος. Επιβολή
ελέγχου από το securityManager
                  */
                  securityManagerCheck();
                  inputValidation(name);
                  this.name = name;
            }
      }


      /* Υλοποίηση readObject για επιβολή ελέγχων κατά τη
διάρκεια της αποσειριοποίησης
      private void readObject(java.io.ObjectInputStream in) {
            java.io.ObjectInputStream.GetField fields =
            in.readFields();
            String name = (String) fields.get("name", DEFAULT);

            /*
            Αν το αποσειριοποιημένο όνομα δεν ταιριάζει με την
εξ ορισμού τιμή που κανονικά δημιουργήθηκε κατά το χρόνο
κατασκευής, επανάληψη ελέγχων
            */
            if (!DEFAULT.equals(name)) {
                  securityManagerCheck();
                  inputValidation(name);
            }
            this.name = name;
      }
}
```

4.4.7 Έλεγχος πρόσβασης

Ένα ενδιάμεσο (cached) αποτέλεσμα δεν πρέπει να αποστέλλεται σε μια κλάση ή μέθοδο, η οποία δεν έχει τα απαραίτητα προνόμια να το δημιουργεί. Επειδή ο υπολογισμός των προνομίων μπορεί να περιέχει σφάλματα, είναι θεμιτή η χρήση του API AccessController για να επιβάλλουμε τον περιορισμό, όπως στο παράδειγμα που ακολουθεί:

```
private static final Map cache;
public static Thing getThing(String key) {
      // Try cache.
      CacheEntry entry = cache.get(key);
      if (entry != null) {

      /*
      Επιβεβαίωση ότι υπάρχουν οι απαιτούμενες άδειες πριν την
επιστροφή του cached αποτελέσματος.
      */

      AccessController.checkPermission(entry.getPermission());
      return entry.getValue();
      }
```

```
        // Επιβεβαίωση ότι δεν γίνεται αναβάθμιση αδειών

        Permission perm = getPermission(key);
        AccessController.checkPermission(perm);

        // Δημιουργία νέας τιμής με ακριβείς άδειες

        PermissionCollection perms =
    perm.newPermissionCollection();
        perms.add(perm);
        Thing value = AccessController.doPrivileged(
              new PrivilegedAction<Thing>() {
                    public Thing run() {
                          return createThing(key);
                    }
              },
              new AccessControlContext(
                    new ProtectionDomain[] {
                          new ProtectionDomain(null, perms)
                    }
              )
        );
        cache.put(key, new CacheEntry(value, perm));
        return value;
    }
```

Βιβλιογραφία

Checklist: Security Review for Managed Code. (n.d.). Retrieved 30 September 2015, from https://msdn.microsoft.com/en-us/library/ff648189.aspx

Gong, L., Ellison, G., & Dageforde, M. (2003). Inside Java 2 platform security: architecture, API design, and implementation (2nd ed). Boston: Addison-Wesley.

Long, F. (2014). Java coding guidelines: 75 recommendations for reliable and secure programs. Upper Saddle River, NJ: Addison-Wesley.

Long, F., & Carnegie-Mellon University (Eds.). (2012). The CERT Oracle secure coding standard for Java. Upper Saddle River, NJ: Addison-Wesley.

Secure Coding Guidelines for Java SE. (n.d.). Retrieved 30 September 2015, from http://www.oracle.com/technetwork/java/seccodeguide-139067.html

Secure Coding Principles - OWASP. (n.d.). Retrieved 30 September 2015, from https://www.owasp.org/index.php/Secure_Coding_Principles

The Java® Language Specification. (n.d.). Retrieved 30 September 2015, from https://docs.oracle.com/javase/specs/jls/se8/html/

The Java® Virtual Machine Specification. (n.d.). Retrieved 30 September 2015, from https://docs.oracle.com/javase/specs/jvms/se8/html/

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποια γλώσσα διαθέτει εγγενείς αδυναμίες που προκαλούν υπερχείλιση ενταμιευτήρα;
α) Java
β) C
γ) Python
δ) HTML

2. Ποιοι οργανισμοί εκδίδουν αρχές ασφαλούς διαδικτυακού προγραμματισμού;
α) CERT, Carnegie Mellon
β) NIST
γ) OWASP
δ) Όλοι οι παραπάνω

3. Η αντιμετώπιση "security by obscurity'
α) επιλύει όλα τα προβλήματα.
β) επιλύει τα προβλήματα, μέχρι να «ανακαλυφθούν» τα υπάρχοντα σφάλματα.
γ) είναι αρχή ασφαλούς προγραμματισμού.
δ) Δεν ισχύει κάποιο από τα παραπάνω.

4. Ποιο από τα παρακάτω δεν είναι κατηγορία ευπάθειας;
α) Υπερχείλιση ενταμιευτήρα.
β) Χρήση κρυπτογραφικών μηχανισμών.
γ) Συνθήκες ανταγωνισμού.
δ) Μη επαληθευμένη είσοδος χρήστη.

5. Μια επίθεση υπερχείλισης ενταμιευτήρα εκμεταλλεύεται την αποθήκευση σε:
α) stack.
β) heap.
γ) buffer.
δ) όλα τα παραπάνω.

6. Κατά τον έλεγχο εισόδου, ελέγχουμε:
α) τα όρια τιμών.
β) το μήκος της εισόδου.
γ) την ύπαρξη null bytes.
δ) κανένα από τα παραπάνω.

7. Ο περιορισμός προνομίων στη Java επιτελείται από το:
α) java.securityManager.AccessController.doPrivileged
β) java.security.AccessManager.doPrivileged
γ) java.security.AccessController.doPrivileged
δ) java.security.AccessController.restrictPrivileged

8. Ποια από τα παρακάτω απαιτούν ιδιαίτερη προσοχή:
α) Δημιουργία BMP αρχείων.
β) Χρήση υπερσυμπιεσμένων αρχείων.
γ) Εκφράσεις XPath.
δ) Όλα τα παραπάνω.

9. Κατά τη δυναμική δημιουργία SQL εντολών είναι θεμιτή η χρήση:
α) java.sql.StealthStatement
β) java.sql.PreparedStatement
γ) java.sSecureSQL.PreparedStatement
δ) java.sql.Statement

10. Μηχανισμός ασφάλειας της Java είναι το:
α) SecurityManager
β) SecurityGuardManager
γ) SecurityGuard
δ) TotalSecurityManager

Κεφάλαιο 5. Ασφάλεια Διαδικτυακών Εφαρμογών

Σύνοψη
Σε αυτό το κεφάλαιο παρουσιάζονται έννοιες που αφορούν την ασφάλεια των διαδικτυακών εφαρμογών (Web applications), στο πλαίσιο μιας σχετικής θεματολογίας και ορολογίας. Ακόμη, παρουσιάζεται ένα σύνολο δοκιμασμένων αρχών ασφάλειας, οι οποίες βασίζονται σε συστάσεις διεθνών οργανισμών και εταιρειών ανάπτυξης λογισμικού ιστού. Τεκμηριώνεται, επίσης, η αναγκαιότητα υιοθέτησης μιας ολιστικής προσέγγισης σχετικά με τα ζητήματα ασφάλειας, ώστε να αντιμετωπίζονται σε όλα τα επίπεδα αρχιτεκτονικής μιας διαδικτυακής εφαρμογής και να επιτυγχάνεται αποτελεσματικότερα ο στόχος της προστασίας της. Τέλος, το κεφάλαιο αυτό παρουσιάζει και ορίζει τις συνηθέστερες κατηγορίες διαμόρφωσης εξυπηρετητή, ανάλογα με τις προσφερόμενες υπηρεσίες του και τις κατηγορίες ευπαθειών μιας διαδικτυακής εφαρμογής.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας, καθώς και των αρχών και πρακτικών προγραμματισμού στο Διαδίκτυο (Κεφάλαια. 1 και 4).

5.1 Εισαγωγή

Η αναφορά σε ζητήματα ασφάλειας διαδικτυακών εφαρμογών, φέρνει στο μυαλό μας εικόνες επιτιθέμενων σε ιστότοπους, οι οποίοι «αρπάζουν» στοιχεία πιστωτικών καρτών ή εκτελούν επιθέσεις άρνησης εξυπηρέτησης (denial of service). Ωστόσο, αυτό είναι μόνο ένα μέρος του συνολικότερου προβλήματος, το οποίο καλούμαστε να αντιμετωπίσουμε όταν επιθυμούμε να προστατεύσουμε μια διαδικτυακή εφαρμογή. Όπως έχει αναφερθεί σε προηγούμενα κεφάλαια, η ασφάλεια πληροφοριών είναι περισσότερο μια διαδικασία παρά μια απλή εφαρμογή τεχνολογιών και μηχανισμών προστασίας.

Ο μηχανισμός του τείχους προστασίας (firewall), για παράδειγμα, προσφέρει προστασία περιορίζοντας την πρόσβαση σε συγκεκριμένες θύρες (ports), αλλά δεν αποτελεί μια ολοκληρωμένη λύση στο πρόβλημα της ασφάλειας. Ομοίως, η χρήση της τεχνολογίας Secure Sockets Layer (SSL) είναι εξαιρετική για την κρυπτογραφημένη μεταφορά ευαίσθητων δεδομένων μέσω του ανασφαλούς Διαδικτύου, αλλά δε μας προστατεύει εκτελώντας και επικύρωση αυτών των δεδομένων στο πλαίσιο της λειτουργίας μιας διαδικτυακής εφαρμογής.

Μπορούμε να ομαδοποιήσουμε τα απαραίτητα χαρακτηριστικά ασφάλειας μιας διαδικτυακής εφαρμογής σε διαδικασίες όπως:

- **Εμπιστευτικότητα**: Είναι η διαδικασία διασφάλισης της ανάγνωσης των δεδομένων μόνον από εξουσιοδοτημένους χρήστες. Η κρυπτογράφηση χρησιμοποιείται συχνά για να επιβάλλει προστασία της εμπιστευτικότητας.

- **Ακεραιότητα:** Είναι η διαδικασία διασφάλισης της τροποποίησης ή διαγραφής των δεδομένων μόνον από εξουσιοδοτημένους χρήστες. Η αναγνώριση της προσβολής της ακεραιότητας των δεδομένων, συνήθως παρέχεται με τη χρήση συναρτήσεων κατακερματισμού.

- **Διαθεσιμότητα**: Σημαίνει ότι οι πόροι (π.χ. υπολογιστικοί, αποθηκευτικοί, δικτυακοί) παραμένουν διαθέσιμοι όποτε τους χρειάζονται οι εξουσιοδοτημένοι χρήστες.

- **Αυθεντικοποίηση**: Είναι η διαδικασία της επιβεβαίωσης της ταυτότητας των πελατών. Πελάτες μπορεί να είναι οι τελικοί χρήστες, άλλες υπηρεσίες, διαδικασίες, ή υπολογιστές.

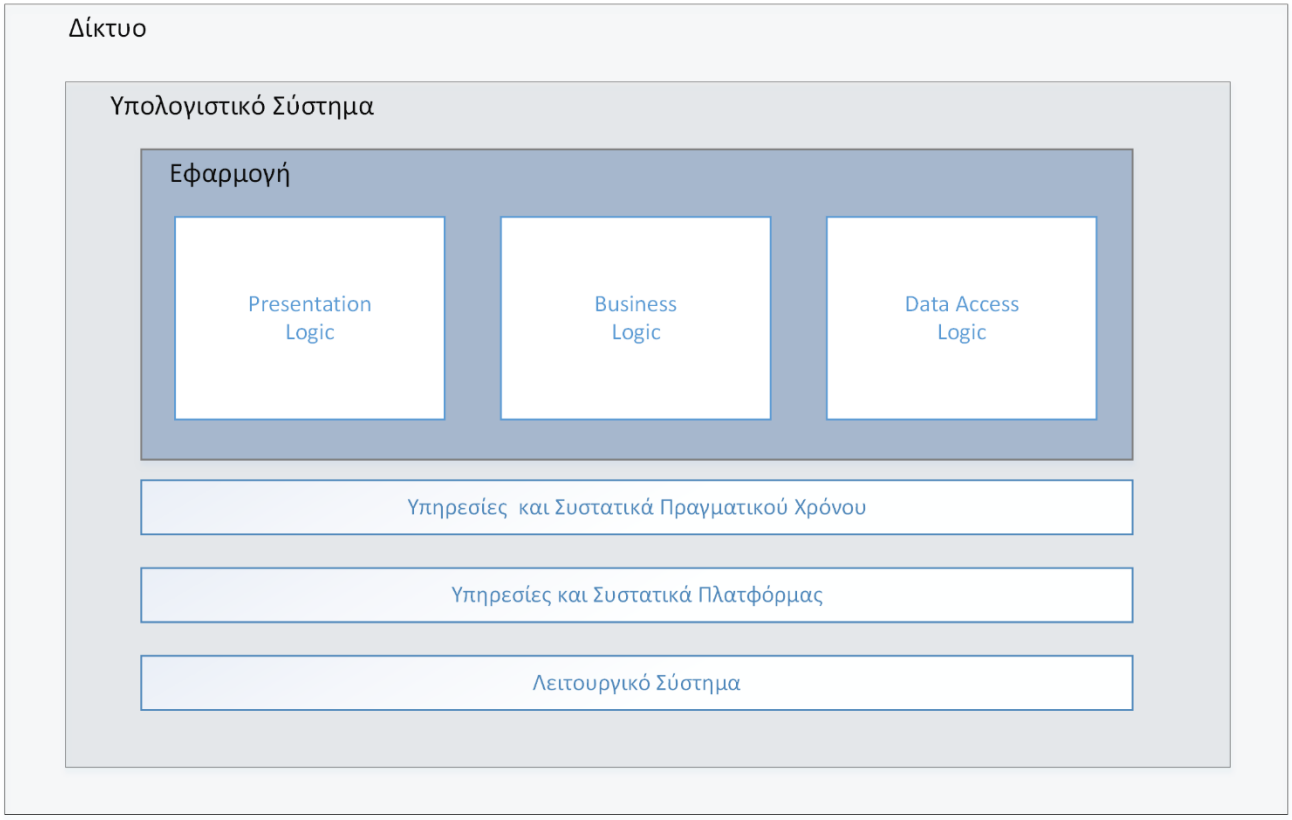
- **Εξουσιοδότηση**: Είναι η διαδικασία που διέπει τα μέσα και τις λειτουργίες ελέγχου πρόσβασης σε πόρους από αυθεντικοποιημένους πελάτες. Οι πόροι περιλαμβάνουν αρχεία, βάσεις δεδομένων, πίνακες, κ.ά., σε συνδυασμό με πόρους σε επίπεδο συστήματος, όπως κλειδιά μητρώου (registry keys) και δεδομένα ρυθμίσεων (configuration data).

- **Αδυναμία Αποποίησης**: Ένα αποτελεσματικό σύστημα επιθεώρησης και καταγραφής μπορεί να είναι το κλειδί για μια υπηρεσία αδυναμίας αποποίησης. Μια υπηρεσία αδυναμίας αποποίησης εγγυάται ότι ο πελάτης δεν μπορεί να αποποιηθεί (αρνηθεί) την ευθύνη για την εκτέλεση μιας ενέργειας από μέρους του (π.χ. μιας ηλεκτρονικής συναλλαγής).

5.2 Παράγοντες Ασφάλειας

Για την ανάπτυξη μιας ασφαλούς διαδικτυακής εφαρμογής, προτείνεται η υιοθέτηση μιας ολιστικής προσέγγισης ασφάλειας, σε συνδυασμό με την πιστή εφαρμογή αρχών, κανόνων και πρακτικών ασφάλειας σε τρία επίπεδα:

- Επίπεδο δικτύου.
- Επίπεδο υπολογιστικού συστήματος.
- Επίπεδο εφαρμογής.



Εικόνα 5.1 *Ολιστική προσέγγιση ασφάλειας.*

Η ασφαλής ανάπτυξη και λειτουργία μιας διαδικτυακής εφαρμογής βασίζεται στην ύπαρξη μιας ασφαλούς υποδομής δικτύου. Η υποδομή δικτύου περιλαμβάνει ενεργά συστατικά, όπως δρομολογητές (routers), τείχη προστασίας (firewalls), μεταγωγείς (switches). Μια ασφαλής δικτυακή υποδομή θα πρέπει να εγγυάται προστασία σε επίπεδο πρωτοκόλλων επικοινωνίας (π.χ. του TCP/IP), αλλά ταυτόχρονα να αποτελεί και το πεδίο εφαρμογής ικανών μέτρων προστασίας, καθώς προσφέρει το απαραίτητο περιβάλλον στο οποίο θα τοποθετηθεί ένα υπολογιστικό σύστημα στο οποίο θα εκτελεστεί μια διαδικτυακή εφαρμογή.

Για την προστασία ενός υπολογιστικού συστήματος μπορούν να χρησιμοποιηθούν διαφορετικές τεχνικές και αντίμετρα, ανάλογα με το ρόλο και τις υπηρεσίες που προσφέρει. Τέτοιοι ρόλοι είναι ο

εξυπηρετητής ιστού (web server), ο εξυπηρετητής εφαρμογών (application server) και ο εξυπηρετητής βάσεων δεδομένων (database server).

Σημεία τα οποία θα πρέπει να εξετάζονται προσεκτικά σε όλους τους τύπους εξυπηρετητών, είναι τα παρακάτω:

Αναβαθμίσεις και ανανεώσεις λογισμικού	Πολλές ευπάθειες αντιμετωπίζονται με την αναβάθμιση του λογισμικού το οποίο έχουμε εγκαταστήσει στον εξυπηρετητή μας. Το πρώτο και ευκολότερο βήμα για την προστασία ενός εξυπηρετητή είναι η πιστή εφαρμογή μιας διαδικασίας εγκατάστασης ενημερωμένων εκδόσεων του λογισμικού που χρησιμοποιείται.
Υπηρεσίες	Το σύνολο των προσφερόμενων υπηρεσιών καθορίζεται από το ρόλο του εξυπηρετητή και τις εφαρμογές που φιλοξενεί. Με την απενεργοποίηση περιττών και σπάνια χρησιμοποιούμενων υπηρεσιών, μειώνεται η «επιφάνεια επίθεσης».
Δικτυακές Συνδέσεις	Για τη μείωση της «επιφάνειας επίθεσης» είναι απαραίτητη η απενεργοποίηση όλων των περιττών ή αχρησιμοποίητων συνδέσεων δικτύου.
Λογαριασμοί Χρηστών	Ο αριθμός των λογαριασμών που έχουν πρόσβαση σε ένα εξυπηρετητή θα πρέπει να περιορίζεται στο ελάχιστο επίπεδο. Επιπλέον, θα πρέπει να εφαρμόζονται κατάλληλες πολιτικές λογαριασμού, όπως πολιτική ορθής χρήσης, ισχυρού συνθηματικού κλπ.
Αρχεία και Κατάλογοι	Η πρόσβαση στα αρχεία και τους καταλόγους θα πρέπει να περιορίζεται στη βάση καθορισμένων δικαιωμάτων πρόσβασης που επιβάλλονται από το σύστημα αρχείων του εξυπηρετητή, ώστε να επιτρέπεται η πρόσβαση μόνο στους απαραίτητους λογαριασμούς υπηρεσιών και χρηστών, σύμφωνα με την Αρχή του Ελάχιστου Προνομίου.
Διαμοιρασμοί	Όλοι οι κατάλογοι οι οποίοι διαμοιράζονται, ενώ δεν είναι απαραίτητοι, θα πρέπει να αφαιρεθούν από το σύστημα αρχείων του εξυπηρετητή.
Θύρες	Υπηρεσίες οι οποίες εκτελούνται σε έναν εξυπηρετητή, χρησιμοποιούν συγκεκριμένες θύρες για να δέχονται τα εισερχόμενα αιτήματα. Οι ανοιχτές θύρες σε ένα διακομιστή, πρέπει να είναι γνωστές και να ελέγχονται τακτικά για να διασφαλίζεται ότι δεν είναι ενεργές και διαθέσιμες για επικοινωνία υπηρεσίες που δεν παρέχουν ικανό επίπεδο ασφαλούς λειτουργίας.
Έλεγχος και Καταγραφή	Η Ελεγκτική (auditing) είναι μια σημαντική βοήθεια για τον εντοπισμό εισβολών ή ακόμη και επιθέσεων σε εξέλιξη. Η Καταγραφή (logging) αποδεικνύεται ιδιαίτερα χρήσιμη κατά τη συλλογή στοιχείων που μπορούν να αξιοποιηθούν κατάλληλα στο πλαίσιο μιας ανάλυσης εγκληματολογικών ευρημάτων (forensics) με σκοπό την διαλεύκανση του τρόπου επιτυχούς πραγματοποίησης μιας εισβολής και των συνεπειών που προκάλεσε στον εξυπηρετητή.

Πίνακας 5.1 *Σημεία εξέτασης για την ασφάλεια εξυπηρετητών.*

Η ασφάλεια μιας διαδικτυακής εφαρμογής και η διαδικασία μελέτης και ανάλυσής της συνεπικουρείται από μια καλή ταξινόμηση των ευπαθειών που είναι πιθανό να εντοπισθούν. Με αυτό τον τρόπο μπορούμε να αντιμετωπίσουμε συλλογικά ομάδες ευπαθειών με κοινά μέτρα προστασίας. Για να μετρηθεί η αντοχή των μηχανισμών ασφάλειας μιας διαδικτυακής εφαρμογής θα πρέπει να μπορούμε να αξιολογήσουμε τις κατηγορίες κατάταξης των ευπαθειών της εφαρμογής, ώστε να δημιουργήσουμε το προφίλ ασφάλειας της εφαρμογής και στη συνέχεια να χρησιμοποιήσουμε αυτό το προφίλ για να καθορίσουμε την αντοχή της σε ενδεχόμενες επιθέσεις.

Ορισμένες κατηγορίες ευπαθειών μιας διαδικτυακής εφαρμογής εμπίπτουν στις κατηγορίες παρουσιάζονται στον Πίνακα 5.2.

Επικύρωση Δεδομένων Εισόδου	Η επικύρωση των δεδομένων εισόδου αναφέρεται στον τρόπο με τον οποίο η εφαρμογή μας φιλτράρει και είτε αποδέχεται είτε απορρίπτει δεδομένα εισόδου, πριν χρησιμοποιηθούν σε επόμενες λειτουργίες.

Αυθεντικοποίηση	Αυθεντικοποίηση είναι η διαδικασία κατά την οποία μια οντότητα αποδεικνύει την ταυτότητά της, συνήθως μέσω διαπιστευτηρίων (credentials), όπως όνομα χρήστη (username) και συνθηματικό (password).
Εξουσιοδότηση	Εξουσιοδότηση είναι το η διαδικασία αντιπαραβολής των χορηγημένων δικαιωμάτων πρόσβασης έναντι συγκεκριμένου αιτήματος πρόσβασης σε αντικείμενα της εφαρμογής.
Διαχείριση Αρχείων Ρυθμίσεων	Αφορά στη διαφύλαξη των ιδιοτήτων ασφάλειας των αρχείων ρυθμίσεων (configuration files) της εφαρμογής (π.χ. ρυθμίσεις σύνδεσης με τη βάση δεδομένων κ.ά.)
Ευαίσθητα Δεδομένα	Αναφέρεται στο τρόπο με τον οποίο η εφαρμογή χειρίζεται τα ευαίσθητα δεδομένα κατά την επεξεργασία, αποθήκευση και μετάδοσή τους.
Διαχείριση Συνόδου	Μια σύνοδος (session) αναφέρεται σε μια αλληλουχία σχετικών αλληλεπιδράσεων μεταξύ χρήστη και εφαρμογής. Η διαχείριση της συνόδου αναφέρεται στον τρόπο με τον οποίο η εφαρμογή χειρίζεται και προστατεύει αυτές τις αλληλεπιδράσεις.
Κρυπτογραφία	Η αξιοποίηση κρυπτογραφικών τεχνικών από την εφαρμογή για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
Διαχείριση Παραμέτρων	Η διαχείριση παραμέτρων αφορά τόσο τον τρόπο διασφάλισης από την εφαρμογή της προστασίας των τιμών των παραμέτρων από πιθανές αλλοιώσεις, όσο και τον τρόπο με τον οποίο τις χειρίζεται.
Διαχείριση Εξαιρέσεων	Όταν μια κλήση μεθόδου αποτύχει, πρέπει η εφαρμογή να παρέχει προστασία των πληροφοριών εξαίρεσης που επιστρέφονται.

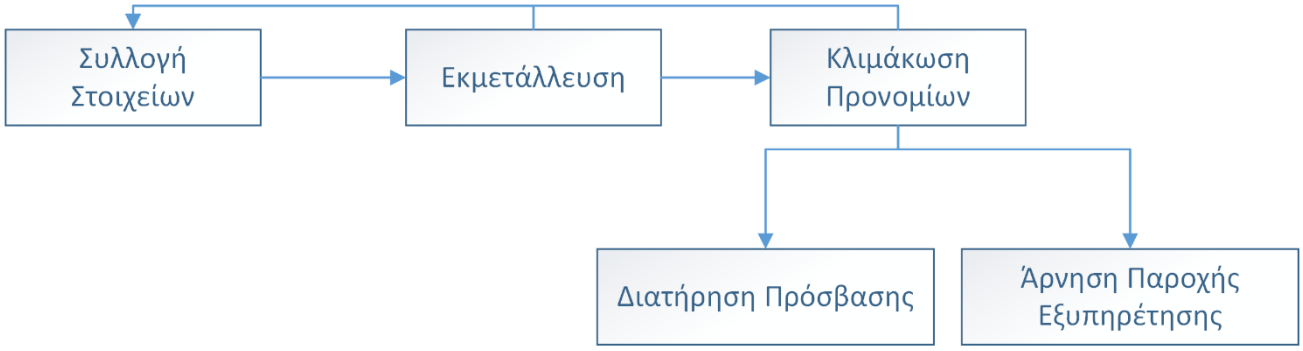
Πίνακας 5.2 *Κατηγορίες ευπαθειών διαδικτυακής εφαρμογής.*

Αρκετές από τις γενικές αρχές ασφαλούς προγραμματισμού, που έχουν αναλυθεί εκτενώς στο Κεφάλαιο 4, αποτελούν τη βάση για την προσέγγιση ασφάλειας που περιγράφεται σε αυτό το κεφάλαιο.

5.3 Παράγοντες Επιθέσεων

5.3.1 Μεθοδολογία επίθεσης

Η κατανόηση μιας τυπικής μεθοδολογίας που χρησιμοποιείται από τους επιτιθέμενους κατά τη διάρκεια μιας επίθεσης σε μια διαδικτυακή εφαρμογή, μας δίνει αρκετά από τα απαραίτητα εφόδια γνώσης, ώστε να λάβουμε κατάλληλα μέτρα προστασίας (είτε αμυντικού είτε ακόμη και επιθετικού χαρακτήρα). Τα βασικά στάδια μιας τυπικής μεθοδολογίας επίθεσης σε μια διαδικτυακή εφαρμογή απεικονίζονται στην Εικόνα 5.2.



Εικόνα 5.2 *Μεθοδολογία επίθεσης.*

Στο στάδιο της συλλογής στοιχείων, ο επιτιθέμενος συλλέγει πληροφορίες για τον επικείμενο στόχο του, προσπαθώντας να εξακριβώσει τα χαρακτηριστικά του. Τα χαρακτηριστικά αυτά μπορεί να περιλαμβάνουν υποστηριζόμενες υπηρεσίες και πρωτόκολλα επικοινωνίας, σε συνδυασμό με τις γνωστές αδυναμίες τους και

τα πιθανά σημεία διείσδυσης. Ο επιτιθέμενος χρησιμοποιεί τις πληροφορίες που συγκεντρώνονται από μια τέτοια έρευνα προκειμένου να τις αξιολογήσει και να προγραμματίσει το επόμενο στάδιο της επίθεσής του.

Έχοντας εντοπίσει και αναλύσει ένα πιθανό στόχο, το επόμενο βήμα είναι να εκμεταλλευτεί τις αδυναμίες του και να διεισδύσει σε αυτόν. Εάν η δικτυακή υποδομή και το υπολογιστικό σύστημα είναι καλά προστατευμένα, τότε η διαδικτυακή εφαρμογή αποτελεί το συνηθέστερο σημείο για την εξαπόλυση της επίθεσης. Ο ευκολότερος τρόπος διείσδυσης του επιτιθέμενου στην εφαρμογή είναι από την ίδια είσοδο την οποία χρησιμοποιούν και οι νόμιμοι χρήστες. Για παράδειγμα, μέσω της σελίδας σύνδεσης (Sign In) στην εφαρμογή.

Εφόσον ο επιτιθέμενος καταφέρει να θέσει σε κίνδυνο την εφαρμογή, παρακάμπτοντας τους περιορισμούς και αποκτώντας πρόσβαση στο υπολογιστικό σύστημα (π.χ. με ψεκασμό κώδικα), θα προσπαθήσει αμέσως μετά να κλιμακώσει τα προνόμια πρόσβασής του. Συγκεκριμένα, θα αναζητήσει την απόκτηση διαχειριστικών προνομίων, δηλαδή προνομίων πρόσβασης που παρέχονται σε λογαριασμούς που είναι μέλη της ομάδας διαχειριστών του συγκεκριμένου υπολογιστικού συστήματος (εξυπηρετητή). Εναλλακτικά, θα αναζητήσει την απόκτηση προνομίων από λογαριασμούς υψηλού επιπέδου που προσφέρουν αντίστοιχα προνόμια.

Στη συνέχεια, έχοντας αποκτήσει πρόσβαση στο σύστημα, ο εισβολέας λαμβάνει μέτρα για να καταστήσει τις μελλοντικές του προσπάθειες διείσδυσης ευκολότερες, καθώς επίσης και να καλύψει τα ίχνη της τρέχουσας διείσδυσής του. Κοινές προσεγγίσεις για την επίτευξη ευκολότερης μελλοντικής πρόσβασης περιλαμβάνουν τη κρυφή εγκατάσταση προγραμμάτων πίσω πόρτας (backdoor). Η κάλυψη των ιχνών του εισβολέα τυπικά περιλαμβάνει την εκκαθάριση των αρχείων καταγραφής και τη διαγραφή των εργαλείων λογισμικού που εγκατέστησε προσωρινά. Εφόσον, λοιπόν, τα αρχεία καταγραφής ελέγχου είναι ο πρωταρχικός στόχος για τον εισβολέα, αυτά θα πρέπει να προστατεύονται και να αναλύονται σε τακτική βάση.

Αν ο επιτιθέμενος δεν καταφέρει να αποκτήσει πρόσβαση, είναι πιθανό να θελήσει να εφαρμόσει μια επίθεση άρνησης εξυπηρέτησης, ώστε να αποτρέψει άλλους εξουσιοδοτημένους χρήστες από τη χρήση της εφαρμογής. Ένα παράδειγμα τέτοιας επίθεσης, είναι η επίθεση πλημμύρας (SYN flood attack), όπου ο επιτιθέμενος αποστέλλει πολύ μεγάλο όγκο αιτήσεων TCP με ενεργοποιημένο το flag SYN, προκειμένου να προκαλέσει την εξάντληση της λίστας αναμονής σύνδεσης στον εξυπηρετητή και να αποτρέψει έτσι τους εξουσιοδοτημένους χρήστες από τη δημιουργία νέων συνδέσεων με τον εξυπηρετητή.

5.3.2 Απειλές

Τα είδη απειλών για μια διαδικτυακή εφαρμογή μπορούν να ταξινομηθούν στις παρακάτω κατηγορίες:

- **Πλαστογράφηση**: Είναι η προσπάθεια του επιτιθέμενου να αποκτήσει πρόσβαση σε ένα σύστημα, χρησιμοποιώντας μια ψεύτικη ταυτότητα χρήστη. Για παράδειγμα, αυτό μπορεί να επιτευχθεί με τη χρήση κλεμμένων διαπιστευτηρίων ή με μια ψεύτικη διεύθυνση IP (IP spoofing).

- **Αλλοίωση**: Αφορά τη μη εξουσιοδοτημένη τροποποίηση των δεδομένων της εφαρμογής. Για παράδειγμα, τροποποίηση μεταδιδόμενων δεδομένων μεταξύ δύο εξυπηρετητών.

- **Αποποίηση**: Σχετίζεται με τη δυνατότητα των χρηστών να αρνούνται ότι έπραξαν συγκεκριμένες ενέργειες (π.χ. ηλεκτρονικές συναλλαγές). Χωρίς επαρκή έλεγχο και καταγραφή, οι επιθέσεις αποποίησης είναι δύσκολο να αποδειχθούν.

- **Δημοσιοποίηση πληροφοριών**: Είναι η ανεπιθύμητη έκθεση ευαίσθητων δεδομένων. Τέτοια δεδομένα μπορεί να βρίσκονται αποθηκευμένα σε κρυφά πεδία φόρμας συμπλήρωσης στοιχείων, σε σχόλια ενσωματωμένα στον κώδικα ιστοσελίδων, τα οποία περιλαμβάνουν λεπτομέρειες σύνδεσης στη βάση δεδομένων ή λεπτομέρειες σχετικά με τη διαχείριση εξαιρέσεων και μπορεί να οδηγήσουν σε αποκάλυψη κρίσιμων λεπτομερειών για την εσωτερική δομή της εφαρμογής. Οποιαδήποτε από αυτές τις πληροφορίες μπορεί να είναι πολύ χρήσιμη για τον εισβολέα.

- **Άρνηση παροχής εξυπηρέτησης**: Αφορά τη διαδικασία κατά την οποία ένα σύστημα ή μια εφαρμογή δεν είναι διαθέσιμη στους εξουσιοδοτημένους χρήστες της. Για παράδειγμα, μια επίθεση άρνησης εξυπηρέτησης θα μπορούσε να επιτευχθεί με «βομβαρδισμό» ενός εξυπηρετητή με αιτήματα τα οποία καταναλώνουν όλους τους διαθέσιμους πόρους του.

- **Κλιμάκωση δικαιωμάτων**: Επιχειρείται όταν ένας χρήστης με περιορισμένα δικαιώματα χρησιμοποιεί την ταυτότητα ενός προνομιούχου χρήστη για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε μια εφαρμογή. Για παράδειγμα, ένας εισβολέας με περιορισμένα δικαιώματα μπορεί να αναβαθμίσει το επίπεδο πρόσβασής του ή το επίπεδο των προνομίων του και να αναλάβει τον έλεγχο μιας εξαιρετικά κρίσιμης διεργασίας.

Τυπικές μέθοδοι αντιμετώπισης των παραπάνω απειλών, αλλά και κατάλληλα αντίμετρα, παρουσιάζονται στον Πίνακα 5.3.

ΑΠΕΙΛΗ	ΑΝΤΙΜΕΤΡΟ
Πλαστογράφηση	Χρήση ισχυρών μηχανισμών ελέγχου ταυτότητας. Αποφυγή αποθήκευσης μυστικών (για παράδειγμα, διαπιστευτηρίων) μέσα σε απλό κείμενο. Αποφυγή μετάδοσης διαπιστευτηρίων σύνδεσης σε μορφή απλού κειμένου μέσω απροστάτευτης δικτυακής σύνδεσης.
Αλλοίωση	Αξιοποίηση μηχανισμών συναρτήσεων κατακερματισμού. Χρήση ψηφιακών υπογραφών. Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της ακεραιότητας του κάθε μεταδιδόμενου μηνύματος.
Αποποίηση	Τήρηση και προστασία αρχείων καταγραφής. Χρήση ψηφιακών υπογραφών.
Δημοσιοποίηση πληροφοριών	Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση ανθεκτικής κρυπτογράφησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της εμπιστευτικότητας των μεταδιδόμενων μηνυμάτων. Αποφυγή αποθήκευσης μυστικών μέσα σε απλό κείμενο.
Άρνηση εξυπηρέτησης	Παρακολούθηση, διαχείριση και ρύθμιση της χρήσης των πόρων του υπολογιστικού συστήματος. Επικύρωση και φιλτράρισμα των δεδομένων εισόδου.
Κλιμάκωση προνομίων	Εφαρμογή της Αρχής του Ελάχιστου Προνομίου. Χρήση επαρκών λογαριασμών για την εκτέλεση των διεργασιών και την πρόσβαση στους πόρους.

Πίνακας 5.3 *Μέθοδοι αντιμετώπισης απειλών και αντίμετρα.*

Μία τεχνική αντιμετώπισης των απειλών είναι η αντιστοίχισή τους με τις ευπάθειες με τις οποίες λογικά σχετίζονται, έτσι ώστε να μπορεί να δοθεί προτεραιότητα σε απειλές οι οποίες θεωρούνται κρισιμότερες ανά περίπτωση. Στον παρακάτω Πίνακα 5.4, επιχειρείται ένας τέτοιος συσχετισμός μεταξύ ευπαθειών και απειλών:

ΕΥΠΑΘΕΙΑ	ΑΠΕΙΛΗ
Επικύρωση δεδομένων εισόδου	Υπερχείλιση ενταμιευτήρα. Ενδεχόμενο επίθεσης XSS. Ψεκασμός SQL εντολών
Αυθεντικοποίηση	Ενδεχόμενο επίθεσης ωμής βίας (brute force) Ενδεχόμενο επίθεσης λεξικού (dictionary) Επανάληψη ψηφιακού μπισκότου (cookie replay). Αλλοίωση δεδομένων.
Εξουσιοδότηση	Κλιμάκωση προνομίων. Δημοσιοποίηση πληροφοριών. Αλλοίωση δεδομένων.

Διαχείριση αρχείων ρυθμίσεων	Μη εξουσιοδοτημένη πρόσβαση σε εργαλεία διαχειριστικού ελέγχου. Μη εξουσιοδοτημένη χρήση λογαριασμών με υψηλά προνόμια.
Ευαίσθητα δεδομένα	Πρόσβαση σε αποθηκευμένα δεδομένα. Παρακολούθηση δικτυακής κίνησης. Αλλοίωση δεδομένων.
Διαχείριση Συνόδου	Υφαρπαγή συνόδου. Επανάληψη συνόδου. Ενδεχόμενο επίθεσης του ενδιάμεσου (MITM).
Κρυπτογραφία	Αδύναμοι μηχανισμοί κρυπτογραφίας. Κακή διαχείριση κλειδιών.\ Παραγωγή αδύναμων κλειδιών
Διαχείριση παραμέτρων	Διαχείριση αλφαριθμητικών ερωτημάτων SQL. Διαχείριση δεδομένων εισόδου σε φόρμες εισαγωγής στοιχείων. Διαχείριση ψηφιακών μπισκότων (cookies) και κεφαλίδων HTTP.
Διαχείριση εξαιρέσεων	Δημοσιοποίηση πληροφοριών. Αποποίηση.
Έλεγχος και Καταγραφή	Αποποίηση. Κάλυψη ιχνών επίθεσης.

Πίνακας 5.4 *Συσχετισμός ευπαθειών και απειλών*.

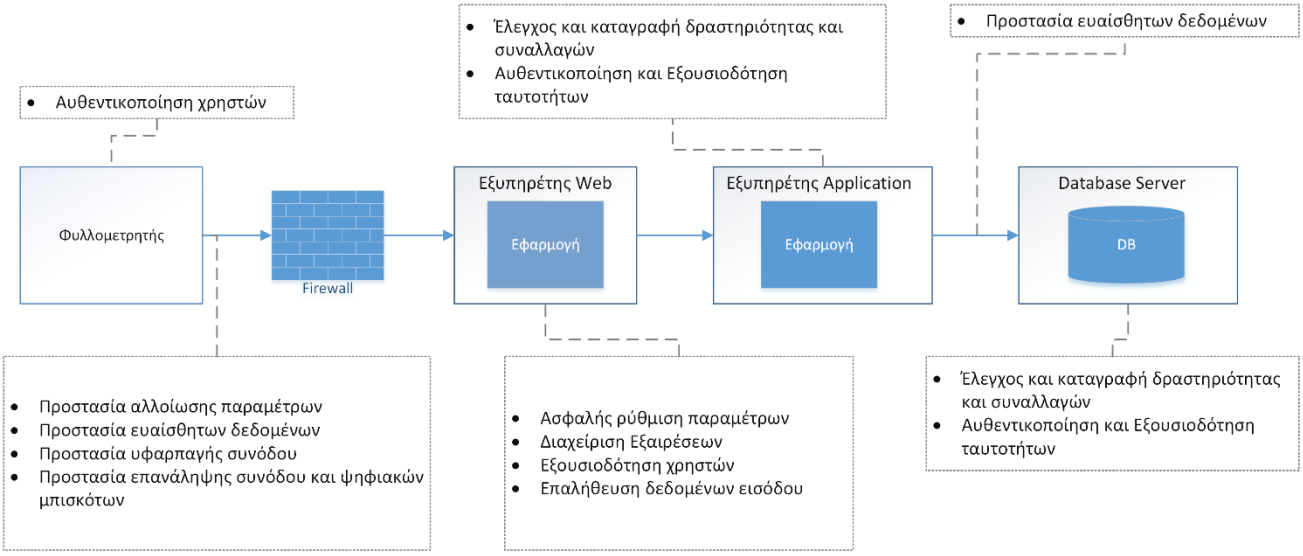
5.4 Ασφαλής Σχεδιασμός Διαδικτυακών Εφαρμογών

Κατά το σχεδιασμό μιας διαδικτυακής εφαρμογής πρέπει να ακολουθείται μια συστηματική προσέγγιση έχοντας κατά νου τους κρισιμότερους τομείς, στους οποίους η εφαρμογή μπορεί να είναι ευάλωτη σε επιθέσεις. Για παράδειγμα, ζητήματα επικύρωσης δεδομένων εισόδου, αυθεντικοποίησης και εξουσιοδότησης, χρήση κρυπτογραφίας και προστασίας ευαίσθητων δεδομένων κ.ά.

Η διαδικασία ασφαλούς ανάπτυξης διαδικτυακών εφαρμογών παρουσιάζει σημαντικές προκλήσεις για τους σχεδιαστές και τους προγραμματιστές. Για παράδειγμα, το ότι το πρωτόκολλο HTTP λειτουργεί χωρίς επίβλεψη της κατάστασης σύνδεσης (stateless), σημαίνει ότι ο εντοπισμός της κατάστασης κάθε χρήστη ανά σύνοδο είναι ευθύνη της εφαρμογής. Για να συμβεί αυτό, η εφαρμογή θα πρέπει να είναι σε θέση να προσδιορίσει το χρήστη, χρησιμοποιώντας κάποια μορφή ελέγχου ταυτότητας. Δεδομένου ότι συνήθως οι επόμενες αποφάσεις εξουσιοδότησης λαμβάνονται με βάση την ταυτότητα του χρήστη, είναι σημαντικό η διαδικασία αυθεντικοποίησης να είναι προστατευμένη και ο μηχανισμός χειρισμού της συνόδου που χρησιμοποιείται για την παρακολούθηση εξουσιοδοτημένων χρηστών να είναι εξίσου καλά προστατευμένος.

Ο σχεδιασμός ασφαλών μηχανισμών αυθεντικοποίησης και διαχείρισης συνόδου είναι μόνο μερικά από τα ζητήματα που αντιμετωπίζουν οι σχεδιαστές και οι προγραμματιστές διαδικτυακών εφαρμογών. Άλλες προκλήσεις σχετίζονται με τη μετάδοση δεδομένων μέσω ανασφαλών δικτύων. Ακόμη. η πρόληψη αλλοίωσης των παραμέτρων και η αποκάλυψη των ευαίσθητων δεδομένων αποτελούν κορυφαία ζητήματα ασφάλειας.

Στην Εικόνα 5.3, εμφανίζεται μια τυπική αρχιτεκτονική μιας διαδικτυακής εφαρμογής, συσχετιζόμενη με επιμέρους ζητήματα που πρέπει να απασχολούν τον σχεδιαστή και τον προγραμματιστή με σκοπό την ασφαλή ανάπτυξή της.



Εικόνα 5.3 *Επιμέρους ζητήματα ασφάλειας διαδικτυακής εφαρμογής.*

Κατά τη φάση του σχεδιασμού μιας διαδικτυακής εφαρμογής, θα πρέπει να εξεταστεί η πολιτική, καθώς και οι διαδικασίες ασφάλειας του οργανισμού, σε σχέση με την υπολογιστική και δικτυακή υποδομή στη βάση της οποίας πρόκειται να αναπτυχθεί η εφαρμογή. Τις περισσότερες φορές, ο σχεδιασμός της εφαρμογής απαιτεί μια ισορροπία μεταξύ των απαιτήσεων ασφάλειας και των λειτουργικών ή άλλων απαιτήσεων. Η έγκαιρη αναγνώριση των περιορισμών κατά τη φάση του σχεδιασμού, μπορεί να οδηγήσει στην αποφυγή δυσάρεστων εκπλήξεων.

Η πολιτική ασφάλειας καθορίζει το πλαίσιο των επιτρεπτών λειτουργιών της εφαρμογής. Πρέπει να είμαστε βέβαιοι ότι λειτουργούμε εντός του πλαισίου που καθορίζεται από την πολιτική ασφαλείας κατά το σχεδιασμό της εφαρμογής, προκειμένου να αποφευχθούν προβλήματα κατά τη μετέπειτα διαδικασία ανάπτυξης της εφαρμογής. Ακόμη, πρέπει να είμαστε βέβαιοι ότι έχουμε κατανοήσει τη δομή του δικτύου που παρέχεται από το περιβάλλον που θα φιλοξενήσει την εφαρμογή, καθώς και τις βασικές απαιτήσεις ασφάλειας σε ό,τι αφορά τους κανόνες φιλτραρίσματος, τους περιορισμούς χρήσης θυρών, τα υποστηριζόμενα πρωτόκολλα επικοινωνίας, κ.ά.

Απαιτείται να αντιληφθούμε πως τα τείχη προστασίας και οι πολιτικές ελέγχου τους είναι πιθανό να επηρεάσουν την ανάπτυξη της εφαρμογής μας. Για παράδειγμα, μπορεί να υπάρχουν τείχη προστασίας για διαχωρισμό του εσωτερικού εταιρικού δικτύου από το Διαδίκτυο. Ακόμη, μπορεί να υπάρχουν επιπλέον τείχη προστασίας μεταξύ του εξυπηρετητή βάσεων δεδομένων και του εξυπηρετητή εφαρμογών. Ο κάθε επιμέρους σχηματισμός μπορεί να επηρεάσει τις ρυθμίσεις των θυρών επικοινωνίας και, ως εκ τούτου, τις επιλογές μηχανισμών ελέγχου ταυτότητας για τον εξυπηρετητή ιστού, τον εξυπηρετητή εφαρμογών, αλλά και τον εξυπηρετητή βάσεων δεδομένων.

Στο στάδιο του σχεδιασμού, πρέπει να προσδιορίζονται τα πρωτόκολλα επικοινωνίας, οι θύρες και οι υπηρεσίες που μπορούν να έχουν πρόσβαση σε πόρους του εσωτερικού δικτύου μέσω των εξυπηρετητών ιστού του περιμετρικού δικτύου. Πρέπει να καταγράφονται τυχόν παραδοχές που έγιναν σχετικά με την ασφάλεια του δικτύου ή της εφαρμογής, καθώς επίσης και ποιο συστατικό λογισμικού ή μηχανισμός ασφάλειας θα είναι υπεύθυνος για την αντιμετώπιση της εναπομένουσας επικινδυνότητας. Μια τέτοια προσέγγιση αποτρέπει την παράλειψη μηχανισμών ασφαλείας, ως αποτέλεσμα της αλληλοεπικάλυψης αρμοδιοτήτων μεταξύ διαφορετικών ειδικοτήτων και ομάδων στελεχών κατά την ανάπτυξη της διαδικτυακής εφαρμογής.

5.4.1 Επικύρωση δεδομένων εισόδου

Η σωστή επικύρωση των δεδομένων εισόδου είναι ένα από τα ισχυρότερα μέτρα άμυνας κατά των επιθέσεων σε μια διαδικτυακή εφαρμογή. Ο προγραμματιστής μιας διαδικτυακής εφαρμογής επιφορτίζεται με την ευθύνη της δημιουργίας της πρώτης γραμμής άμυνας, όπου με τη χρήση κατάλληλων αντιμέτρων πρέπει να βοηθήσει στην πρόληψη επιθέσεων XSS, ψεκασμού εντολών SQL, υπερχείλισης ενταμιευτήρα κ.ά.

Για το σκοπό αυτό:

- Υποθέτουμε ότι όλες οι είσοδοι προέρχονται από μη αξιόπιστη πηγή.
- Χρησιμοποιούμε έναν εξυπηρετητή αυθεντικοποίησης.
- Φιλτράρουμε, περιορίζουμε και απορρίπτουμε όλες τις εισόδους.

5.4.2 Αυθεντικοποίηση

Τρεις πτυχές που πρέπει να εξετάζονται, είναι οι εξής:

- Εντοπισμός των σημείων της εφαρμογής όπου απαιτείται έλεγχος ταυτότητας. Αυτό, συνήθως, συμβαίνει σε σημεία όπου χρειάζεται να ξεπεραστεί ένα όριο εμπιστοσύνης.

- Επαλήθευση της ταυτότητας του χρήστη που εκτελεί μια κλήση. Αυτό, συνήθως, γίνεται με χρήση ζεύγους username και password.

- Προσδιορισμός της ταυτότητας του χρήστη σε επόμενες κλήσεις. Αυτό απαιτεί κάποια μορφή χρήσης token για παρουσίαση της ελεγμένης ταυτότητας.

Οι πρακτικές που ακολουθούνται για την αντιμετώπιση των ζητημάτων αυθεντικοποίησης είναι :

- Διαχωρισμός δημόσιων και περιορισμένων (ιδιωτικών) ζωνών χρήσης της εφαρμογής.

- Χρήση πολιτικών αποκλεισμού για τους λογαριασμούς των τελικών χρηστών.

- Υποστήριξη περιόδου λήξης του κάθε συνθηματικού.

- Δυνατότητα άμεσης απενεργοποίησης λογαριασμών.

- Να μην αποθηκεύονται συνθηματικά σε αποθηκευτικό χώρο του τελικού χρήστη.

- Να απαιτείται η χρήση ισχυρών συνθηματικών.

- Να μη μεταδίδονται απροστάτευτα συνθηματικά μέσω του δικτύου.

- Να προστατεύονται τα ψηφιακά μπισκότα (cookies) ταυτότητας.

5.4.3 Εξουσιοδότηση

Η εξουσιοδότηση καθορίζει τις ενέργειες που μπορεί να εκτελέσει μια οντότητα, η οποία έχει επαληθεύσει την ταυτότητά της. Μια λανθασμένη εξουσιοδότηση μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών και σε αλλοίωση δεδομένων.

Οι συνηθέστερες πρακτικές που ακολουθούνται για ζητήματα εξουσιοδότησης είναι :

- Χρήση πολλαπλών ελέγχων εξουσιοδότησης.
- Περιορισμός των δικαιωμάτων του χρήστη.
- Χρήση επιπέδων εξουσιοδότησης.

5.4.4 Διαχείριση ρυθμίσεων

Θα πρέπει να εξετάσουμε προσεκτικά τον τρόπο διαχείρισης των ρυθμίσεων και των παραμέτρων της εφαρμογής μας. Οι περισσότερες εφαρμογές παρέχουν δυνατότητες σε χρήστες και διαχειριστές για να ρυθμίζουν τον τρόπο λειτουργίας της εφαρμογής και να διαχειρίζονται τα χαρακτηριστικά της, όπως το

περιεχόμενο μιας ιστοσελίδας, τους λογαριασμούς και το προφίλ του κάθε χρήστη, ρυθμίσεις σύνδεσης με τη βάση δεδομένων κλπ. Οι συνέπειες της παραβίασης της ασφάλειας λόγω της εκμετάλλευσης λανθασμένων ή αντικρουόμενων ρυθμίσεων μπορεί να είναι ιδιαίτερα σοβαρές για ολόκληρη την εφαρμογή.

Οι συνηθέστερες πρακτικές που ακολουθούνται για ζητήματα διαχείρισης των ρυθμίσεων είναι:

- Διασφάλιση της ελεγχόμενης πρόσβασης στις διεπαφές διαχείρισης.
- Προστασία του χώρου όπου αποθηκεύονται οι ρυθμίσεις.
- Ανάπτυξη διαφορετικών επιπέδων διαχείρισης για κάθε ρόλο / χρήστη.
- Χρήση λογαριασμών με ελάχιστα δικαιώματα για κάθε ξεχωριστή υπηρεσία.

5.4.5 Προστασία ευαίσθητων δεδομένων

Οι εφαρμογές που επεξεργάζονται και αποθηκεύουν προσωπικά δεδομένα χρηστών, όπως αριθμούς πιστωτικών καρτών, διευθύνσεις, ιατρικά αρχεία, κ.λπ., θα πρέπει να λαμβάνουν ειδικά μέτρα για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων αυτών. Επιπλέον, πρέπει να προστατεύονται επαρκώς τα ευαίσθητα δεδομένα που χρησιμοποιούνται από την εφαρμογή, όπως τα συνθηματικά και οι ρυθμίσεις σύνδεσης με το σύστημα διαχείρισης βάσεων δεδομένων. Η προστασία των ευαίσθητων δεδομένων θα πρέπει να αφορά τη λήψη μέτρων τόσο για τα δεδομένα που επεξεργάζονται, όσο και για αυτά που αποθηκεύονται ή μεταδίδονται μέσω του δικτύου.

Πρακτικές που ακολουθούνται για την προστασία των ευαίσθητων δεδομένων είναι, συνήθως, οι παρακάτω:

- Αποθήκευση μόνο των ευαίσθητων δεδομένων που είναι απαραίτητα για την εκάστοτε λειτουργία της εφαρμογής.
- Αποφυγή αποθήκευσης ευαίσθητων δεδομένων μέσα στον κώδικα της εφαρμογής.
- Κρυπτογραφημένη αποθήκευση των ρυθμίσεων σύνδεσης σε συστήματα διαχείρισης βάσεων δεδομένων, συνθηματικών, κλειδιών κρυπτογράφησης κλπ.
- Εκτεταμένη χρήση κρυπτογραφικών τεχνικών.

5.4.6 Διαχείριση συνόδου

Οι διαδικτυακές εφαρμογές αναπτύσσονται με βάση το πρωτόκολλο HTTP, το οποίο, όπως αναφέρθηκε, λειτουργεί χωρίς επίβλεψη της κατάστασης σύνδεσης του χρήστη, έτσι ώστε η διαχείριση μιας συνόδου να είναι ευθύνη τη ίδιας της εφαρμογής. Επιπλέον, η ασφάλεια συνόδου είναι ζωτικής σημασίας για τη συνολική ασφάλεια μιας διαδικτυακής εφαρμογής.

Οι ακόλουθες πρακτικές βελτιώνουν την ασφάλεια της διαχείρισης συνόδου μιας διαδικτυακής εφαρμογής:

- Εφαρμογή πρωτοκόλλου SSL για την προστασία των μεταδιδόμενων δεδομένων.
- Κρυπτογράφηση των ψηφιακών μπισκότων αυθεντικοποίησης.
- Περιορισμός χρόνου ζωής μιας ενεργής συνόδου.
- Προστασία από το ενδεχόμενο υφαρπαγής κατάστασης μιας συνόδου από μη εξουσιοδοτημένους χρήστες.

5.4.7 Χρήση κρυπτογραφίας

Οι διαδικτυακές εφαρμογές συχνά χρησιμοποιούν κρυπτογραφικές μεθόδους για να προστατεύσουν τα δεδομένα κατά την αποθήκευση ή τη μετάδοσή τους. Οι ακόλουθες πρακτικές βελτιώνουν την ασφάλεια των διαδικτυακών εφαρμογών όταν χρησιμοποιούμε κρυπτογραφία:

- Δεν χρησιμοποιούμε δικές μας μεθόδους κρυπτογράφησής αλλά προτιμούμε έτοιμες ολοκληρωμένες και δοκιμασμένες λύσεις.
- Χρησιμοποιούμε το σωστό αλγόριθμο και με το κατάλληλο μήκος κλειδιού, εφόσον υποστηρίζεται μεταβλητό μήκος.
- Προστατεύουμε επαρκώς τα κρυπτογραφικά κλειδιά.

5.4.8 Αλλοίωση παραμέτρων

Με τις επιθέσεις χειραγώγησης παραμέτρων ο εισβολέας αποσκοπεί στο να τροποποιεί τα δεδομένα που αποστέλλονται μεταξύ του χρήστη και της διαδικτυακής εφαρμογής. Αυτά τα δεδομένα μπορεί να είναι αλφαριθμητικά ερωτήματος, πεδία φόρμας, cookies, ή κεφαλίδες HTTP κ.ά. Οι ακόλουθες πρακτικές προστατεύουν τη χειραγώγηση παραμέτρων μιας διαδικτυακής εφαρμογής:

- Κρυπτογράφηση ψηφιακών μπισκότων κατάστασης.
- Επικύρωση των δεδομένων εισόδου.
- Προσεκτικός έλεγχος των κεφαλίδες HTTP.

5.4.9 Διαχείριση εξαιρέσεων

Ο ασφαλής χειρισμός εξαιρέσεων μπορεί να βοηθήσει στην πρόληψη ορισμένων επιθέσεων σε επίπεδο εφαρμογής, όπως για παράδειγμα άρνησης εξυπηρέτησης. Ακόμη, μπορεί να χρησιμοποιηθεί για να αποτρέψει την αποκάλυψη πολύτιμων πληροφοριών στον τελικό χρήστη. Για παράδειγμα, χωρίς τον κατάλληλο χειρισμό εξαίρεσης, πληροφορίες όπως οι λεπτομέρειες για το σύστημα διαχείρισης βάσεων δεδομένων, το λειτουργικό σύστημα, τα ονόματα των αρχείων και οι πληροφορίες διαδρομής, πιθανά ερωτήματα SQL και άλλες πληροφορίες που έχουν αξία για έναν εισβολέα, υπάρχει το ενδεχόμενο να επιστραφούν στον τελικό χρήστη, που θεωρείται μη αξιόπιστος.

Μια καλή προσέγγιση είναι να σχεδιαστεί μια κεντρική λύση διαχείρισης εξαιρέσεων και καταγραφής τους, έτσι ώστε να υποστηριχθεί αποτελεσματικά η εργασία των διαχειριστών του συστήματος. Οι ακόλουθες πρακτικές βοηθούν στη διασφάλιση του σωστού χειρισμού εξαιρέσεων από μια διαδικτυακή εφαρμογή:

- Δεν επιτρέπουμε την επιστροφή κρίσιμων πληροφοριών στον χρήστη.
- Καταγράφουμε λεπτομερώς τα μηνύματα λάθους.
- Υπάρχει χειρισμός για όλες τις εξαιρέσεις.

5.4.10 Έλεγχος και καταγραφή

Θα πρέπει να ελέγχουμε και να καταγράφουμε όλες τις δραστηριότητες σε όλα τα επίπεδα λειτουργίας της εφαρμογής. Αξιοποιώντας και αναλύοντας τα αρχεία καταγραφής, μπορούμε να εντοπίσουμε ύποπτες δραστηριότητες. Μάλιστα, σε ορισμένες περιπτώσεις μπορεί να μας παρέχει κάποιες πρώτες ενδείξεις για μια επικείμενη επίθεση.

Ακόμη, τα αρχεία καταγραφής βοηθούν στην αντιμετώπιση της αποποίησης από τελικούς χρήστες. Τα αρχεία καταγραφής είναι πιθανό να απαιτούνται σε νομικές διαδικασίες για να αποδείξουμε την τέλεση παράνομων πράξεων. Σε γενικές γραμμές, ο έλεγχος των αρχείων καταγραφής θεωρείται πιο έγκυρος και χρήσιμος αν πραγματοποιείται στον πραγματικό χρόνο λειτουργίας της εφαρμογής.

Οι ακόλουθες πρακτικές βελτιώνουν τη διαδικασία ελέγχου και καταγραφής:

- Έλεγχος και καταγραφή σε όλα τα επίπεδα λειτουργίας της εφαρμογής μας.
- Λεπτομερής καταγραφή κύριων συμβάντων.
- Διασφάλιση και προστασία των αρχείων καταγραφής.
- Περιοδική δημιουργία αντιγράφων και ανάλυση των αρχείων καταγραφής.

Βιβλιογραφία

Curphey, M., & Araujo, R. (2006). Web Application Security Assessment Tools. IEEE Security & Privacy, 4(4), 32–41.

Graff, M., & Van Wyk, K. R. (2003). Secure coding: principles and practices. Beijing ; Cambridge: O'Reilly.

Harwood, M., & Harwood, M. (2015). Internet security: how to defend against attackers on the web (Second Edition). Burlington, MA: Jones & Bartlett Learning.

Improving Web Application Security: Threats and Countermeasures. (n.d.). Retrieved 30 September2015, from https://msdn.microsoft.com/en-us/library/ff649874.aspx

Manico, J., & Detlefsen, A. (2015). Iron-clad Java: building secure web applications. New York: McGraw-Hill Education.

Scheller, F., Jänchen, M., Lampe, J., Prümke, H. J., Blanck, J., & Palecek, E. (1975). Studies on electron transfer between mercury electrode and hemoprotein. Biochimica Et Biophysica Acta, 412(1), 157–167.

Shema, M. (2012). Hacking web apps: detecting and preventing web application security problems. Amsterdam ; Boston: Syngress.

Stuttard, D., & Pinto, M. (2011). The web application hacker's handbook: finding and exploiting security flaws (2nd ed). Indianapolis, IN : Chichester: Wiley ; John Wiley [distributor].

Sullivan, B., & Liu, V. (2012). Web application security: a beginner's guide. New York: McGraw-Hill.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Κατά την ολιστική προσέγγιση ασφάλειας μιας διαδικτυακής εφαρμογής εξετάζουμε την ασφάλεια:
α) στο επίπεδο δικτύου.
β) στο επίπεδο υπολογιστικού συστήματος.
γ) στο επίπεδο διαδικτυακής εφαρμογής.
δ) σε όλα τα επίπεδα.

2. Φροντίζουμε
α) να ενεργοποιούμε όσα περισσότερα πρωτόκολλα επικοινωνίας μπορεί να χρησιμοποιήσει ο εξυπηρετητής.
β) να ενεργοποιούμε μόνο όσα πρωτόκολλα επικοινωνίας απαιτούνται για την ομαλή λειτουργία της διαδικτυακής μας εφαρμογής.
γ) να μην ενεργοποιούμε κανένα πρωτόκολλο επικοινωνίας στον εξυπηρετητή μας.
δ) σε κάθε περίπτωση να ενεργοποιούμε μόνον ένα πρωτόκολλο επικοινωνίας στον εξυπηρετητή μας.

3. Σε μια τυπική επίθεση σε διαδικτυακή εφαρμογή, η πρώτη φάση αφορά
α) τη συλλογή στοιχείων.
β) την εκμετάλλευση.
γ) την κλιμάκωση προνομίων.
δ) τη διατήρηση πρόσβασης.

4. Κατά τη μελέτη ασφάλειας ενός εξυπηρετητή εξετάζουμε:
α) τις αναβαθμίσεις λογισμικού.
β) τις υπηρεσίες που παρέχει.
Γ) τις ανοικτές θύρες του.
δ) όλα τα παραπάνω.

5. Ποια από τις παρακάτω επιλογές δεν αποτελεί απειλή;
α) Αλλοίωση.
β) Αποποίηση.
γ) Αυθεντικοποίηση.
δ) Πλαστογράφηση.

6. Ο έλεγχος και η καταγραφή αποτελούν μέτρα προστασίας για την αντιμετώπιση
α) της αποποίησης.
β) της δημοσιοποίησης πληροφοριών.
γ) της άρνησης παροχής υπηρεσίας.
δ) της αναβάθμισης δικαιωμάτων πρόσβασης.

7. Ο φυλλομετρητής του τελικού χρήστη θα πρέπει να επικοινωνεί πρώτα με:
α) τον εξυπηρετητή ιστού.
β) το τείχος προστασίας.
γ) τον εξυπηρετητή εφαρμογής.
δ) τον εξυπηρετητή βάσης δεδομένων.

8. Η χρήση ψηφιακών υπογραφών σε ποια είδη απειλής αποτελεί απάντηση;
α) Πλαστογράφηση.
β) Αλλοίωση.
γ) Αποποίηση.
δ) Αποκάλυψη.

9. Η ευπάθεια της διαχείρισης εξαιρέσεων είναι απαραίτητη, από άποψη ασφάλειας,:
α) γιατί δεν πρέπει να συμβαίνουν εξαιρέσεις.
β) γιατί δεν πρέπει να επιστρέφονται λεπτομέρειες της διαδικτυακής εφαρμογής στον τελικό χρήστη.
γ) γιατί η διαχείριση εξαιρέσεων πρέπει να πραγματοποιείται από τον τελικό χρήστη.
δ) για όλους τους παραπάνω λόγους.

10. Ποια από τα παρακάτω μέτρα προστασίας χρησιμοποιούνται για τη διαχείριση συνόδου;
α) Χρήση τεχνολογίας SSL.
β) Κρυπτογράφηση ψηφιακών μπισκότων αυθεντικοποίησης.
γ) Περιορισμός χρόνου ζωής ενεργής/ανενεργής συνόδου.
δ) Όλα τα παραπάνω.

Κεφάλαιο 6. Εισαγωγή στην κρυπτολογία

Σύνοψη
Το κεφάλαιο αποτελεί εισαγωγή στη γνωστική περιοχή της κρυπτολογίας, ως μιας γενικότερης περιοχής που περιλαμβάνει την κρυπτογραφία και την στεγανογραφία. Θα παρατεθούν και θα εξεταστούν συνοπτικά οι δύο αυτές βασικές υποπεριοχές και θα γίνει αναφορά σε έννοιες της θεωρίας πληροφορίας που θα μας χρειαστούν στη συνέχεια. Ο αναγνώστης θα έχει την ευκαιρία να κατανοήσει βασικές έννοιες τη εφαρμοσμένης κρυπτογραφίας, καθώς και να κάνει τα πρώτα βήματα στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης, καθώς και προσπάθειες κρυπτανάλυσης, χρησιμοποιώντας απλούς κλασσικούς αλγόριθμους με τη βοήθεια του εκπαιδευτικού εργαλείου Cryptool.

Προαπαιτούμενη γνώση
Για την κατανόηση των εννοιών που περιλαμβάνονται στο κεφάλαιο δεν απαιτείται κάποια εξειδικευμένη προηγούμενη γνώση.

6.1 Εισαγωγή

Ο όρος κρυπτολογία (cryptology) είναι ετυμολογικά μια σύνθετη λέξη που αποτελείται από τα λήμματα «κρυπτός» και «λόγος» και δηλώνει τη μυστικότητα του λόγου που μπορεί να είναι προφορικός ή με τη μορφή ενός γραπτού κειμένου. Η μυστικότητα των περιεχομένων αφορά την προστασία της εμπιστευτικότητας (confidentiality) της πληροφορίας που περιέχεται σε αυτά. Σήμερα, με τον όρο κρυπτολογία ορίζεται η επιστημονική περιοχή που περιλαμβάνει την **κρυπτογραφία** (cryptography) και την **κρυπτανάλυση** (cryptanalysis).

Η κρυπτογραφία ασχολείται με την μετατροπή των δεδομένων με τέτοιο τρόπο ώστε να καθίσταται αδύνατη η ανάγνωση και ερμηνεία του μεταδιδόμενου κρυπτογραφημένου μηνύματος. Σχετική με την κρυπτογραφία είναι η περιοχή της **στεγανογραφίας (steganography)**. Η λέξη προέρχεται από τις λέξεις «στεγανός» και «γραφή» και δηλώνει την προσπάθεια απόκρυψης της ύπαρξης ενός μηνύματος που είναι κρυμμένο μέσα στα μηνύματα μιας φανερής (φαινομενικά απροστάτευτης) επικοινωνίας μεταξύ δυο οντοτήτων. Η κύρια διαφορά με την κρυπτογραφία είναι ότι η στεγανογραφία στοχεύει στην απόκρυψη της ύπαρξης του κρίσιμου μηνύματος, το οποίο δεν είναι απαραίτητο να είναι κρυπτογραφημένο.

Η πρώτη εμφάνιση τεχνικών κρυπτογραφίας συναντάται περίπου 4.000 χρόνια πριν, στα πρώιμα στάδια του Αιγυπτιακού πολιτισμού, όταν οι συγγραφείς της εποχής περιέγραφαν τη ζωή των βασιλιάδων με ασυνήθιστες ιερογλυφικές αναπαραστάσεις. Ως αποτέλεσμα αυτής της ενέργειας, η ανάγνωση των ιερογλυφικών ήταν δυνατή μόνο από όσους γνώριζαν τον μυστικό κώδικα που είχε χρησιμοποιηθεί κατά τη συγγραφή τους, ενώ για όλους τους άλλους οι παραστάσεις ήταν ακατανόητες. Η διεργασία μετασχηματισμού ενός **αρχικού κειμένου** (plaintext) σε μια ακατάληπτη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου ονομάζεται **κρυπτογράφηση**.

Ένας **κρυπτογραφικός αλγόριθμος** (Cipher/Encryption algorithm) περιγράφει τη μέθοδο μετασχηματισμού μηνυμάτων σε μια μορφή τέτοια που να μην επιτρέπεται σε μη εξουσιοδοτημένα μέρη η αποκάλυψη του περιεχομένου τους. Οι αρχαίοι Σπαρτιάτες χρησιμοποίησαν την κρυπτογραφία και εκμεταλλεύτηκαν τις τεχνικές της για στρατιωτικούς σκοπούς. Αναφέρεται χαρακτηριστικά η χρήση της «σκυτάλης», η οποία ήταν μια ξύλινη ράβδος πάνω στην οποία περιτυλίγονταν ένας πάπυρος σε μορφή ταινίας. Το μήνυμα αποτυπωνόταν στον τυλιγμένο γύρω από την σκυτάλη πάπυρο, κατά μήκος της ράβδου, οπότε όταν ο πάπυρος ξετυλίγονταν, η ανάγνωση του κειμένου κατά μήκος του πάπυρου κατέληγε να μην αποδίδει ένα καταληπτό νόημα. Το αρχικό μήνυμα ήταν δυνατό να διαβαστεί μόνο από κάποιον ο οποίος διέθετε σκυτάλη ίδιας διαμέτρου, ώστε να προσαρμόσει πάνω της εκ νέου τον πάπυρο και να αποκρυπτογραφήσει το μήνυμα. Σε αυτή την περίπτωση, η διάμετρος της σκυτάλης αποτελεί το **κλειδί** (key) κρυπτογράφησης, το οποίο μαζί με τον κρυπτογραφικό αλγόριθμο αποτελεί το μέσο για το μετασχηματισμό του αρχικού μηνύματος σε **κρυπτοκείμενο** (cipher text).

Στην Εικόνα 6.1 (Πηγή: https://commons.wikimedia.org/wiki/File:Skytale.png) παρουσιάζεται η λειτουργία της Σπαρτιατικής σκυτάλης.

Εικόνα 6.1 *Λειτουργία Σπαρτιατικής σκυτάλης.*

Η διαδικασία που εκτελείται από μια εξουσιοδοτημένη οντότητα για την ανάκτηση του αρχικού κειμένου από το κρυπτοκείμενο, ονομάζεται **αποκρυπτογράφηση** (Decryption/Decipherment).

6.2 Κρυπτογραφία

Στόχος της κρυπτογραφίας είναι να παρέχει υπηρεσίες ασφάλειας, όπως:

- Εμπιστευτικότητα (confidentiality).
- Ακεραιότητα (integrity).
- Αυθεντικοποίηση (authentication).
- Αδυναμία αποποίησης (non-repudiation).

Επιπλέον, είναι επιθυμητές οι παρακάτω ιδιότητες για ένα κρυπτοσύστημα και τα συστατικά μέρη του:

- Πρέπει να χρησιμοποιούνται αποδοτικοί αλγόριθμοι για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης.

- Το σύστημα πρέπει να είναι εύχρηστο και να μην προκαλεί σύγχυση στον χρήστη.

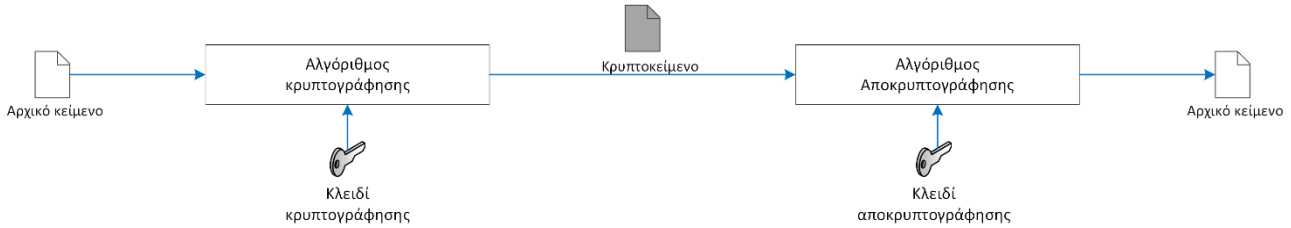
- Η προστασία που παρέχει το σύστημα πρέπει να προϋποθέτει μόνο τη μυστικότητα των κλειδιών και όχι των αλγορίθμων που χρησιμοποιούνται.

Η τελευταία ιδιότητα, γνωστή ως αρχή του Kerckhoff, εκφράστηκε το 1883 από τον Auguste Kerckhoff (1853-1903) και ορίζει πως σε αντίθεση με την αντίληψη πως σε ένα **κρυπτογραφικό σύστημα** οι λεπτομέρειες σχεδιασμού και υλοποίησης πρέπει να είναι κρυφές (security through obscurity), αυτό θα πρέπει να σχεδιάζεται έτσι ώστε να είναι ασφαλές όταν ο «αντίπαλος» γνωρίζει κάθε λεπτομέρεια, εκτός από τις παραμέτρους που σχεδιάζονται να είναι μυστικές, όπως τα κλειδιά κρυπτογράφησης / αποκρυπτογράφησης.

6.2.1 Κρυπτογραφικό σύστημα

Σε ένα κρυπτογραφικό σύστημα, τα δεδομένα που περιέχονται σε ένα μήνυμα με τη μορφή ενός αρχικού κειμένου (plaintext), κρυπτογραφούνται και το παραγόμενο μήνυμα αποτελεί το κρυπτοκείμενο (ciphertext). Στη συνέχεια, το κρυπτοκείμενο αποστέλλεται στον παραλήπτη, όπου αποκρυπτογραφείται για να αναπαραχθεί

το αρχικό κείμενο. Η κρυπτογράφηση ενός μηνύματος γίνεται με τη βοήθεια ενός αλγόριθμου κρυπτογράφησης που χρησιμοποιεί ένα κλειδί κρυπτογράφησης. Ανάλογα, κατά την αποκρυπτογράφηση χρησιμοποιείται ένας αλγόριθμος αποκρυπτογράφησης και είτε το ίδιο είτε ένα άλλο κλειδί αποκρυπτογράφησης. Ένα τυπικό κρυπτοσύστημα απεικονίζεται στο σχήμα της Εικόνας 6.2:



Εικόνα 6.2 *Τυπικό κρυπτοσύστημα.*

Ένα κρυπτογραφικό σύστημα θεωρείται ασφαλές όταν ικανοποιούνται τα ακόλουθα κριτήρια:

- Το **κόστος** της παραβίασης του κρυπτομηνύματος, δηλαδή της ανάκτησης του κλειδιού αποκρυπτογράφησης, υπερβαίνει την αξία των πληροφοριών που τελικά λαμβάνονται ως αποτέλεσμα της κρυπτανάλυσης.

- Ο **χρόνος** που απαιτείται για τη διαδικασία της κρυπτανάλυσης υπερβαίνει την ωφέλιμη διάρκεια ζωής των λαμβανομένων πληροφοριών.

6.2.2 Κρυπτανάλυση

Στόχος της κρυπτανάλυσης είναι η εύρεση του κλειδιού αποκρυπτογράφησης που χρησιμοποιήθηκε για την ασφαλή ανταλλαγή μηνυμάτων με τη χρήση ενός κρυπτοσυστήματος. Ο ρόλος του **κρυπταναλυτή**, επομένως, έρχεται σε πλήρη αντίθεση με το ρόλο του **κρυπτογράφου**, καθώς ο πρώτος προσπαθεί να παραβιάσει ένα κρυπτοσύστημα το οποίο χρησιμοποιεί ο δεύτερος.

Για την εύρεση του κλειδιού αποκρυπτογράφησης, ο κρυπταναλυτής μπορεί να χρησιμοποιήσει τεχνικές όπως:

- **Επίθεση Ωμής Βίας (Brute-Force Attack)**: Ο επιτιθέμενος, μέσω εξαντλητικής αναζήτησης, προσπαθεί να αποκαλύψει το κλειδί αποκρυπτογράφησης, δοκιμάζοντας όλους τους πιθανούς συνδυασμούς στοιχείων του αλφαβήτου που χρησιμοποιήθηκε κατά τον ορισμό του. Ξεκινώντας από το ελάχιστο δυνατό μήκος κλειδιού (εφόσον το μήκος κλειδιού μπορεί να είναι μεταβλητό), δοκιμάζει να αποκρυπτογραφήσει το κρυπτοκείμενο με όλες τις πιθανές τιμές του κλειδιού. Μόλις τις εξαντλήσει, αυξάνει κατά ένα το μήκος του δοκιμαζόμενου κλειδιού και συνεχίζει με τον ίδιο τρόπο. Η υπολογιστική ισχύς των σημερινών υπολογιστών, παρέχει σημαντικά πλεονεκτήματα τα οποία μπορούν να πολλαπλασιαστούν με διατάξεις υπολογιστών που εκτελούν μια τέτοια επίθεση παράλληλα (π.χ. με κατανομή του πεδίου ορισμού του κλειδιού). Για αυτό, λαμβάνοντας υπόψη την τρέχουσα τεχνολογική στάθμη και εξέλιξη, επιβάλλεται η χρήση κλειδιών μεγάλου μήκους για την ενίσχυση της ανθεκτικότητας των κρυπτογραφικών αλγορίθμων (αυτό κυρίως αφορά τους λεγόμενους συμμετρικούς αλγορίθμους).

- **Επίθεση Στατιστικής Ανάλυσης (Statistical Analysis Attack)**: Ο κρυπταναλυτής προσπαθεί να εκμεταλλευτεί, προς όφελός του, εγγενή χαρακτηριστικά της γλώσσας στην οποία έχει γραφτεί το αρχικό κείμενο. Για παράδειγμα, έστω ότι το γράμμα Ε είναι το πλέον χρησιμοποιούμενο στην Αγγλική γλώσσα. Ξεκινώντας από αυτή τη γνώση, ο κρυπταναλυτής αναλύει στατιστικά το κρυπτοκείμενο και προσπαθεί να αντιστοιχίσει το συχνότερα εμφανιζόμενο γράμμα με το γράμμα Ε. Συνεχίζει με παρόμοιο τρόπο, χρησιμοποιώντας

παρόμοια στατιστικά χαρακτηριστικά, π.χ. για άλλα γράμματα ή συνδυασμούς γραμμάτων (όπως δυάδες, τριάδες κ.λπ.), ώστε σε συνδυασμό με άλλες τεχνικές, όπως η αυτοσυσχέτιση (autocorrelation), να οδηγηθεί σε χρήσιμες πληροφορίες και συμπεράσματα για τα χαρακτηριστικά του κλειδιού (π.χ. μέγεθος) και τελικά στην εύρεση της τιμής του. Μια ακόμη τεχνική που μπορεί να τον βοηθήσει, στο πλαίσιο της γενικότερης ανάλυσης που πραγματοποιεί ο κρυπταναλυτής, είναι η αναζήτηση και ο εντοπισμός επαναλαμβανόμενων μοτίβων (pattern) που έχουν σχέση, για παράδειγμα, με τυπικές εκφράσεις που χρησιμοποιούνται στη σύνταξη επαγγελματικών επιστολών (π.χ. τυπική έκφραση του αρχικού χαιρετισμού).

Μπορούμε να διακρίνουμε τις επιθέσεις κρυπτανάλυσης, με βάση την πληροφορία που διαθέτει ο κρυπταναλυτής, ως εξής:

- **Μόνο κρυπτοκειμένου (ciphertext only)**: Ο επιτιθέμενος γνωρίζει μόνο τον αλγόριθμο κρυπτογράφησης και το σύνολο ή μέρος του κρυπτοκειμένου. Αυτό το είδος επίθεσης είναι και το πιο συνηθισμένο, καθώς ο επιτιθέμενος σχετικά εύκολα μπορεί να υποκλέψει το κρυπτοκείμενο, παρακολουθώντας το κανάλι επικοινωνίας μεταξύ των δύο οντοτήτων που επικοινωνούν με χρήση κρυπτογραφίας

- **Γνωστού αρχικού κειμένου (known plaintext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει επιπροσθέτως να αποκτήσει ένα ή περισσότερα ζεύγη από το σύνολο ή μέρος του αρχικού κειμένου και κρυπτοκειμένου, που έχουν κρυπτογραφηθεί με το κλειδί κρυπτογράφησης.

- **Επιλεγμένου αρχικού κειμένου (chosen plaintext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει να εισάγει ένα δικό του αρχικό κείμενο, το οποίο αφού κρυπτογραφηθεί με το κλειδί κρυπτογράφησης, θα πάρει τη μορφή ενός κρυπτοκειμένου το οποίο, στη συνέχεια, θα επιδιώξει π.χ. να υποκλέψει. Με κατάλληλη διαμόρφωση του αρχικού κειμένου, ο κρυπταναλυτής μπορεί να καταφέρει να οδηγηθεί σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

- **Επιλεγμένου κρυπτοκειμένου (chosen ciphertext)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο αποκρυπτογράφησης και καταφέρνει να εισάγει επιλεγμένα κρυπτοκείμενα τα οποία αφού αποκρυπτογραφηθούν παράγουν αρχικά κείμενα που μπορεί να τον οδηγήσουν σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

- **Επιλεγμένου κειμένου (chosen text)**: Ο επιτιθέμενος γνωρίζει τον αλγόριθμο κρυπτογράφησης και καταφέρνει να εισάγει δικά του αρχικά κείμενα τα οποία κρυπτογραφούνται, ενώ καταφέρνει να εισάγει και επιλεγμένα κρυπτοκείμενα τα οποία αποκρυπτογραφούνται με γνωστό αλγόριθμο αποκρυπτογράφησης για να παράγουν αρχικά κείμενα τα οποία μαζί με τα κρυπτοκείμενα των δικών του αρχικών κειμένων μπορεί να τον οδηγήσουν σε συμπεράσματα σχετικά με την τιμή του κλειδιού.

6.2.3 Κλειδί

Σε ένα κρυπτογραφικό σύστημα, η ανάκτηση του αρχικού κειμένου, το οποίο πρέπει να παραμείνει μυστικό από τρίτους, προϋποθέτει την ανάκτηση του κλειδιού αποκρυπτογράφησης. Όπως αναφέρθηκε προηγουμένως, μια μη εξουσιοδοτημένη οντότητα μπορεί να έχει τη δυνατότητα π.χ. να εκτελέσει μια εξαντλητική αναζήτηση έτσι ώστε:

- Στην περίπτωση που έχει αποκτήσει δεδομένα που αποτελούν μέρος του αρχικού κειμένου και του κρυπτοκειμένου να δοκιμάσει όλα τα πιθανά κλειδιά μέχρι να βρει το σωστό το οποίο, στη συνέχεια, θα χρησιμοποιήσει για την αποκρυπτογράφηση κάθε επόμενου κρυπτοκειμένου.

- Στην περίπτωση που έχει αποκτήσει μόνο δεδομένα που αποτελούν μέρος του κρυπτοκειμένου, να δοκιμάσει όλα τα πιθανά κλειδιά μέχρι να βρει ένα με το οποίο το παραγόμενο αποτέλεσμα της αποκρυπτογράφησης να έχει λογική σημασία. Εικάζοντας πως αυτό είναι το σωστό κλειδί, στη συνέχεια, θα το χρησιμοποιήσει για την αποκρυπτογράφηση των υπόλοιπων τμημάτων κρυπτοκειμένου.

Ένα κλειδί αποτελείται από μια σειρά bit. Για την αποφυγή του εντοπισμού του κλειδιού μέσω της εξαντλητικής αναζήτησης (brute force attack), το πλήθος των πιθανών τιμών (συνδυασμών από bit) που μπορεί να πάρει ένα κλειδί, πρέπει να είναι τεράστιο προκειμένου να αντιμετωπίζονται οι επιθέσεις αυτές στη βάση των κριτηρίων κόστους και χρόνου που αναφέρθηκαν προηγουμένως. Έτσι, για μήκος κλειδιού της τάξης των 64bit, οι πιθανές τιμές κλειδιού είναι 2^{56}, δηλαδή μπορούν να παραχθούν περισσότερα από $7x10^{16}$ διαφορετικά κλειδιά.

Αν θεωρήσουμε πως ένας επεξεργαστής έχει τη δυνατότητα δοκιμής 60 εκατομμυρίων κλειδιών το δευτερόλεπτο, τότε ένα κλειδί μήκους 56 bit θα ανακτηθεί σε περίπου από 1.200.000.000 δευτερόλεπτα. Όμως, μοιράζοντας το χώρο αναζήτησης σε περισσότερους επεξεργαστές (π.χ. 1536 του Deep Crack που χρησιμοποιήθηκε για παρόμοιο σκοπό το 1998) ο χρόνος μειώνεται σε 781.875 δευτερόλεπτα, δηλαδή 217 ώρες, άρα μόλις 9 μέρες. Η αύξηση του μήκους του κλειδιού στα 64bit, αυξάνει το χώρο αναζήτησης σε περισσότερα από 10^{19} κλειδιά και τον απαιτούμενο χρόνο στις 2317 μέρες (περίπου 6 έτη)!

Στον πίνακα 6.1 μπορείτε να δείτε ενδεικτικά την αύξηση του χρόνου αναζήτησης σε σχέση με το μήκος του κλειδιού και τον αριθμό n των επεξεργαστικών μονάδων.

Μήκος κλειδιού	**Χώρος αναζήτησης**	**Απαιτούμενος χρόνος με $6x10^7$ κλειδιά ανά sec**
56	$7,2x10^{16}$	38 έτη / n
64	$1,8x10^{19}$	9749 έτη / n
128	$3,4x10^{38}$	$1,8x10^{23}$ έτη / n
256	$1,16x10^{77}$	$6,1x10^{61}$ έτη / n
512	$1,36x10^{154}$	$7,1x10^{138}$ έτη / n

Πίνακας 6.1 *Χρόνοι εξαντλητικής αναζήτησης κλειδιών.*

6.2.4 Αλγόριθμοι κρυπτογράφησης

Οι κρυπτογραφικοί αλγόριθμοι διακρίνονται ως προς:

- το είδος των κλειδιών που χρησιμοποιούν και
- τον τρόπο επεξεργασίας του αρχικού και του κρυπτογραφημένου κειμένου.

6.2.4.1 Είδος κλειδιών

Κατηγοριοποιώντας τους αλγορίθμους κρυπτογράφησης ως προς το είδος των κλειδιών, διακρίνουμε τους συμμετρικούς (symmetric) αλγορίθμους και τους ασύμμετρους (asymmetric) ή δημοσίου κλειδιού (public key).

Στους συμμετρικούς κρυπτογραφικούς αλγορίθμους, η κρυπτογράφηση και η αποκρυπτογράφηση γίνεται χρησιμοποιώντας (συμμετρικά) το ίδιο κλειδί, αλλά με αντίστροφες λειτουργίες. Η οντότητα Α κρυπτογραφεί το αρχικό κείμενο με το κλειδί Κ και αποστέλλει το κρυπτοκείμενο, ενώ η οντότητα Β παραλαμβάνει το κρυπτοκείμενο και χρησιμοποιεί το ίδιο κλειδί Κ για να το αποκρυπτογραφήσει και να ανακτήσει το αρχικό κείμενο (Εικόνα 6.3). Η συμμετρική κρυπτογραφία ονομάζεται και κρυπτογραφία μυστικού κλειδιού.

Εικόνα 6.3 *Συμμετρική κρυπτογραφία.*

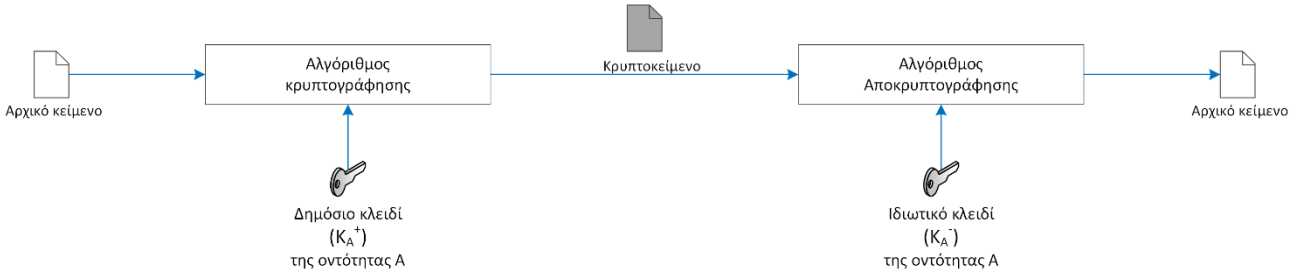
Έστω, P είναι το αρχικό κείμενο το οποίο επιθυμεί να κρυπτογραφήσει η οντότητα A, C είναι το κρυπτοκείμενο που παράγεται και K το κοινό μυστικό κλειδί που χρησιμοποιεί ο αλγόριθμος κρυπτογράφησης E. Η διαδικασία $E_k(P)$ δημιουργεί το κρυπτοκείμενο C με είσοδο το αρχικό κείμενο P και το κλειδί K, ενώ ο αλγόριθμος αποκρυπτογράφησης D ακολουθεί τη διαδικασία $D_k(C)$ για να ανακτήσει το αρχικό κείμενο P με είσοδο το κρυπτοκείμενο C και το κλειδί K.

Σημαντική προϋπόθεση είναι η πρότερη συμφωνία μεταξύ των δυο οντοτήτων για την τιμή του κοινού μυστικού κλειδιού (secret key), το οποίο θα πρέπει να έχει περιορισμένη διάρκεια ισχύος, συνήθως στα όρια μιας συνόδου επικοινωνίας. Για αυτό και το κλειδί αυτό ονομάζεται κλειδί συνόδου (session key). Επομένως, για να επικοινωνήσουν μεταξύ τους ανά δυο (2) συνολικά n οντότητες, θα χρειαστούν n (n-1) / 2 κλειδιά συνόδων. Ο πιο διαδεδομένος αλγόριθμος συμμετρικής κρυπτογραφίας είναι ο DES, ο οποίος επινοήθηκε το 1977 και θα μελετηθεί στο επόμενο κεφάλαιο.

Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν διαφορετικό κλειδί για την κρυπτογράφηση (π.χ. το δημόσιο κλειδί του παραλήπτη) και διαφορετικό για την αποκρυπτογράφηση (π.χ. το ιδιωτικό κλειδί του παραλήπτη). Κάθε οντότητα που συμμετέχει σε ένα κρυπτοσύστημα δημοσίου κλειδιού, διαθέτει ένα δικό της ζεύγος κλειδιών, με μεγάλη διάρκεια ισχύος που εξαρτάται από το σκοπό χρήσης του (π.χ. για κρυπτογράφηση ή για υπογραφή).

Οι ασύμμετροι αλγόριθμοι λειτουργούν ικανοποιώντας δυο (2) βασικές απαιτήσεις:

- **Είναι υπολογιστικά ανέφικτο να υπολογιστεί το ένα κλειδί γνωρίζοντας το άλλο κλειδί του ίδιου κατόχου.** Η ιδιότητα αυτή επιτρέπει να δημοσιοποιηθεί το ένα κλειδί (δημόσιο κλειδί) και να διατηρηθεί το άλλο πραγματικό μυστικό, ώστε να το γνωρίζει μόνον ο ιδιοκτήτης του (ιδιωτικό κλειδί). Λόγω αυτού του σχήματος λειτουργίας, οι αλγόριθμοι αυτοί ονομάζονται αλγόριθμοι δημοσίου κλειδιού, οπότε:
    - Το δημόσιο κλειδί (K^+) κάθε οντότητας είναι διαθέσιμο σε όλες τις άλλες οντότητες.
    - Το ιδιωτικό κλειδί (K^-) είναι αυστηρά γνωστό μόνο στη μια οντότητα που κατέχει το ζεύγος των κλειδιών στο οποίο ανήκει.
- **Κάθε αρχικό κείμενο που κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται μόνο με το άλλο κλειδί του ίδιου ζεύγους.** Έτσι, μια οντότητα A μπορεί να κρυπτογραφήσει ένα μήνυμα το οποίο προορίζεται για την οντότητα B, χρησιμοποιώντας το δημόσιο κλειδί της οντότητας B. Στη συνέχεια, το κρυπτοκείμενο που παράγεται αποστέλλεται στον παραλήπτη (B), όπου μόνον αυτός μπορεί να το αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό κλειδί του. Με τον τρόπο αυτό εξασφαλίζεται η εμπιστευτικότητα του μηνύματος.



Εικόνα 6.4 *Εφαρμογή κρυπτογραφίας δημοσίου κλειδιού για προστασία της εμπιστευτικότητας*.

6.2.4.2 Τρόπος επεξεργασίας

Κατηγοριοποιώντας τους αλγόριθμους κρυπτογράφησης ως προς τον τρόπο επεξεργασίας, διακρίνουμε τις περιπτώσεις αλγορίθμων δέσμης (block) και ροής (stream).

6.2.4.2.1 Επεξεργασία Δέσμης

Οι αλγόριθμοι δέσμης μετατρέπουν το αρχικό κείμενο (μήνυμα) σε δέσμες σταθερού μήκους, π.χ. των 64 bit, τις οποίες στη συνέχεια κρυπτογραφούν. Σε μια σύνοδο κρυπτογράφησης, όλες οι δέσμες δεδομένων ενός μηνύματος κρυπτογραφούνται με το ίδιο κλειδί.

Οι αλγόριθμοι δέσμης προϋποθέτουν ότι είναι γνωστό το αρχικό μήνυμα πριν την κρυπτογράφησή του. Επομένως, δεν μπορούν να χρησιμοποιηθούν π.χ. για την κρυπτογραφημένη μετάδοση μιας συνομιλίας σε πραγματικό χρόνο, χωρίς την εισαγωγή αισθητής καθυστέρησης στη μετάδοσή της.

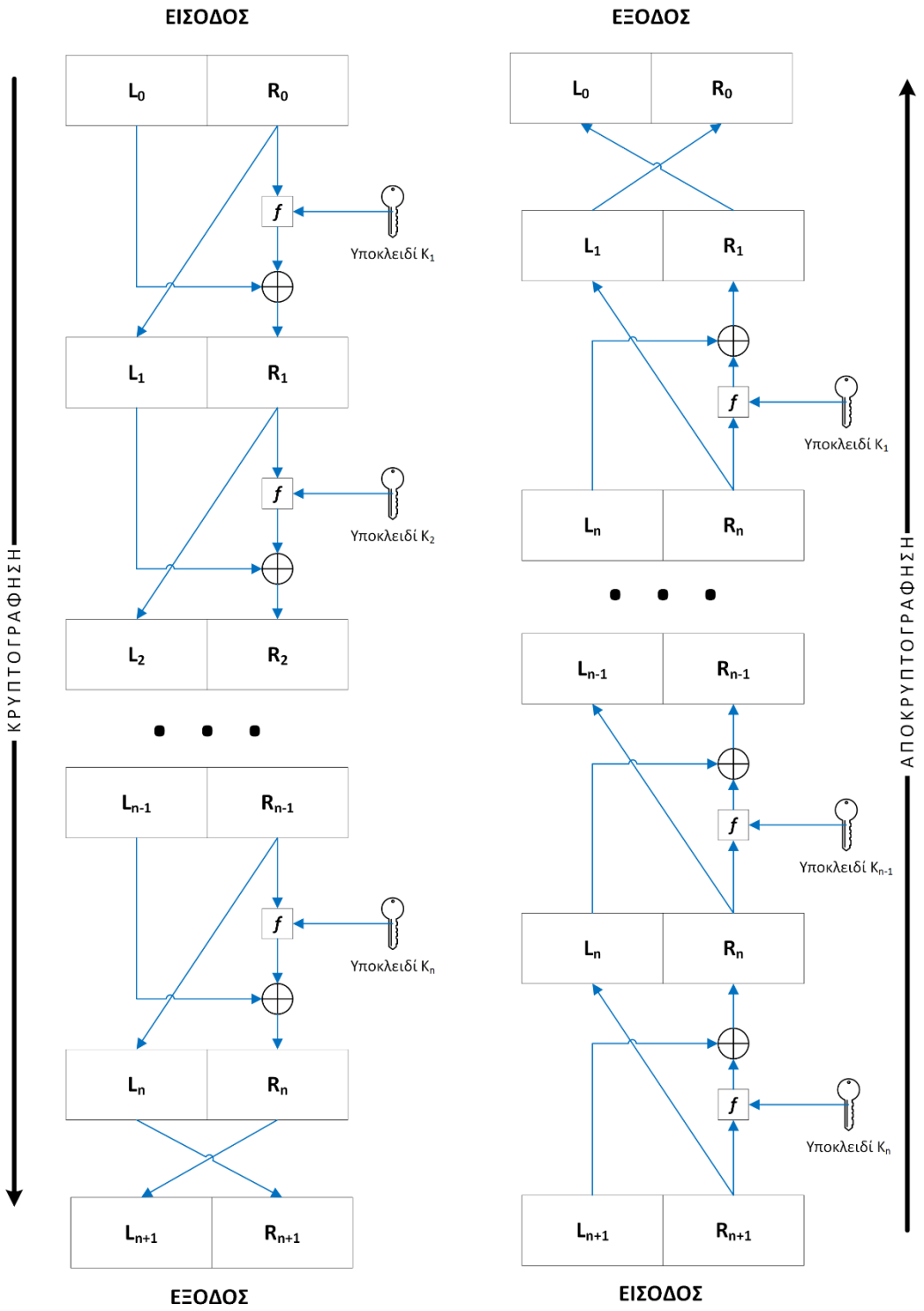
Ορισμένοι συμμετρικοί αλγόριθμοι δέσμης ανήκουν στην οικογένεια αλγορίθμων με δομή Feistel. Η δομή Feistel αποτελείται από μια σειρά πανομοιότυπων κύκλων επεξεργασίας. Σε κάθε κύκλο (round) επεξεργασίας, τα δεδομένα της δέσμης υποβάλλονται σε επεξεργασία, όπου χρησιμοποιείται ένα διαφορετικό υποκλειδί (sub-key), που προκύπτει από το συμμετρικό κλειδί.

Συγκεκριμένα, από το συμμετρικό κλειδί K υπολογίζονται τόσα υποκλειδιά (K_i, i=1 … n), όσοι και οι n κύκλοι επεξεργασίας. Κατά την κρυπτογράφηση, πρώτα χωρίζεται η δέσμη του αρχικού κειμένου σε δυο ίσα μέρη: L_0 και R_0. Στη συνέχεια, εκτελούνται οι κύκλοι επεξεργασίας, όπως φαίνεται στην Εικόνα 6.5. Πιο συγκεκριμένα, σε κάθε κύκλο:

- το τρέχον δεξί μέρος δέσμης γίνεται το επόμενο αριστερό: $L_i = R_{i-1}$
- στο τρέχον δεξί μέρος της δέσμης εφαρμόζεται η συνάρτηση f με το υποκλειδί K_i, ενώ το αποτέλεσμα γίνεται είσοδος μαζί με το τρέχον αριστερό μέρος της δέσμης σε μια πράξη XOR που παράγει στην έξοδό της το επόμενο δεξί μέρος της δέσμης: $R_i = L_{i-1} \oplus f_{Ki}(R_{i-1})$.

Επειδή η κυκλική συνάρτηση είναι αντιστρέψιμη, κατά την αποκρυπτογράφηση ακολουθείται η ακριβώς αντίστροφη διαδικασία:

- το τρέχον αριστερό μέρος δέσμης θα γίνει το επόμενο δεξί: $R_i = L_{i-1}$
- στο τρέχον αριστερό δεξί μέρος της δέσμης εφαρμόζεται η συνάρτηση f με το υποκλειδί K_i, ενώ το αποτέλεσμα γίνεται είσοδος μαζί με το τρέχον δεξί μέρος της δέσμης σε μια πράξη XOR που παράγει στην έξοδό της το επόμενο αριστερό μέρος της δέσμης: $L_i = R_{i-1} \oplus f_{Ki}(L_{i-1})$.

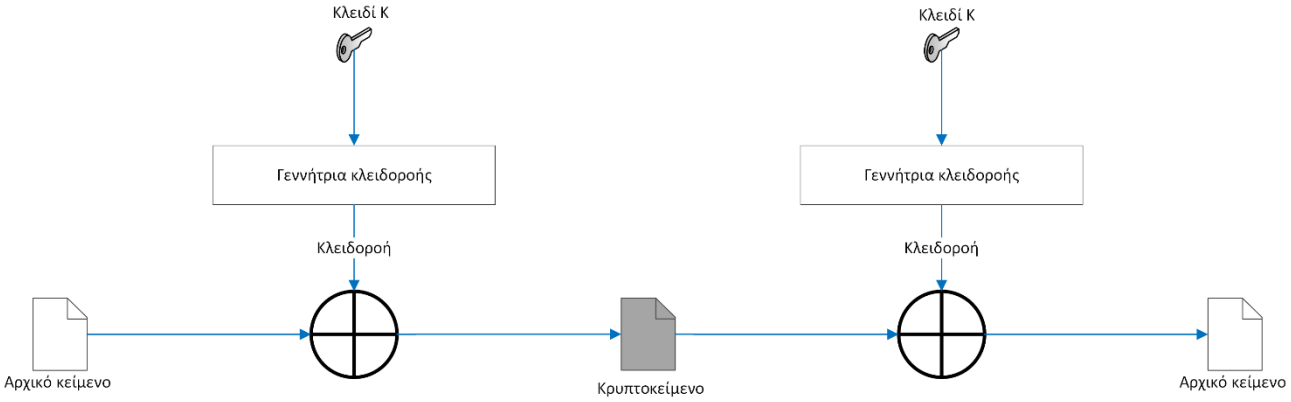


Εικόνα 6.5 *Δομή Feistel.*

6.2.4.2.2 Επεξεργασία Ροής

Οι αλγόριθμοι ροής κρυπτογραφούν το αρχικό κείμενο, το οποίο θεωρείται ότι έχει τη μορφή μιας ροής από bit, εφαρμόζοντας την πράξη XOR μεταξύ κάθε bit της ροής του μηνύματος και μιας άλλης ροής, γνωστής ως κλειδοροής (key stream). Επομένως, η ανθεκτικότητα της παρεχόμενης κρυπτογράφησης εξαρτάται από την γεννήτρια της κλειδοροής, η οποία λειτουργεί επίσης στη βάση της τιμής ενός μυστικού κλειδιού.

Στην Εικόνα 6.6, περιγράφεται η λειτουργία ενός αλγορίθμου ροής, όπου το μυστικό κλειδί K αποτελεί την είσοδο σε μια γεννήτρια κλειδοροής:



Εικόνα 6.6 *Λειτουργία αλγόριθμου ροής.*

Κάθε bit της κλειδοροής συνδυάζεται με ένα bit του αρχικού κειμένου, χρησιμοποιώντας την λογική πράξη XOR, ως εξής:

```
11001100  αρχικό κείμενο
01101100  κλειδοροή
----------
10100000  κρυπτοκείμενο
```

Για τη σωστή αποκρυπτογράφηση απαιτείται η παραγωγή της ίδιας ακριβώς κλειδοροής στη μεριά του παραλήπτη:

```
10100000  κρυπτοκείμενο
01101100  κλειδοροή
----------
11001100  αρχικό κείμενο
```

Μια ανθεκτική σε επίθεση αυτοσυσχέτισης (correlation attack) κλειδοροή θα πρέπει να χαρακτηρίζεται από τις ακόλουθες ιδιότητες:

- Θα πρέπει να έχει μεγάλη περίοδο επανάληψης. Στην πραγματικότητα, η κλειδοροή παράγεται από μια γεννήτρια ψευδοτυχαίων αριθμών, όπως για παράδειγμα οι γεννήτριες Linear Congruence Generator (LCG) και Inverse Congruence Generator (LCG). Μια τέτοια γεννήτρια χρησιμοποιεί μια συνάρτηση που παράγει μια ντετερμινιστική ακολουθία από bit, η οποία είναι αναπόφευκτο από κάποια στιγμή και μετά να επαναλαμβάνεται. Όσο πιο αργά έρθει αυτή η στιγμή, τόσο μεγαλύτερη είναι η περίοδος επανάληψης.

- Θα πρέπει να ομοιάζει όσο γίνεται περισσότερο τις ιδιότητες μιας ακολουθίας πραγματικά τυχαίων αριθμών. Για παράδειγμα, θα πρέπει να επιδιώκεται ώστε να περιέχει ίσο περίπου αριθμό από 0 και 1. Το NIST έχει ορίσει στο Special Publication 800-22 ένα εκτενές σύνολο στατιστικών ελέγχων για την επιβεβαίωση της τυχαιότητας (randomness tests) μιας ακολουθίας bit που παράγεται από μια γεννήτρια.

- Θα πρέπει να έχει μεγάλη γραμμική ισοδυναμία (linear equivalence). Επειδή η παραγωγή μιας τέτοιας ακολουθίας γίνεται με τη χρήση γραμμικών μεθόδων, όπου κάθε επόμενο bit προκύπτει από το γραμμικό συνδυασμό των bit ενός ή περισσότερων καταχωρητών (όπως π.χ. στην

περίπτωση του LCG) της γεννήτριας, όσο μεγαλύτερο το πλήθος αυτών των bit, τόσο μεγαλύτερη η γραμμική ισοδυναμία.

Με μια προσεκτικά σχεδιασμένη γεννήτρια ψευδοτυχαίων αριθμών, ένας αλγόριθμος ροής μπορεί να είναι το ίδιο ασφαλής όσο και ένας αλγόριθμος δέσμης ίδιου μήκους κλειδιού. Ένα ακόμη πλεονέκτημα των αλγόριθμων ροής σχετίζεται με το γεγονός ότι είναι πιο γρήγοροι, σε σχέση με τους αλγορίθμους δέσμης.

Καταλήγοντας, θα λέγαμε ότι για εφαρμογές που χειρίζονται ροές δεδομένων, όπως για παράδειγμα δεδομένα τα οποία διακινούνται σε ένα κανάλι επικοινωνίας ή δεδομένα τα οποία μεταφέρονται από έναν φυλλομετρητή (Web browser), ένας αλγόριθμος ροής είναι η προτιμότερη επιλογή. Για εφαρμογές οι οποίες διαχειρίζονται δέσμες δεδομένων, όπως οι εφαρμογές μεταφοράς αρχείων, εφαρμογές email και εφαρμογές διαχείρισης βάσεων δεδομένων, οι αλγόριθμοι δέσμης είναι καταλληλότεροι.

6.2.4.3 Ανθεκτικότητα

Με βάση τις υποθέσεις για την χειρότερη περίπτωση, γίνονται δοκιμές με σκοπό να βρεθούν τρόποι για να «σπάσει» το κρυπτογραφημένο κείμενο, δηλαδή να βρεθεί το μυστικό κλειδί αποκρυπτογράφησής του. Σε αυτή την περίπτωση, ο σχεδιαστής ή ο χρήστης που προτίθεται να χρησιμοποιήσει ένα προϊόν κρυπτογράφησης παίζει το ρόλο του κρυπταναλυτή.

Οι κρυπτογραφικοί αλγόριθμοι θεωρείται ότι είναι ισχυροί, εφόσον οι προσπάθειες εξειδικευμένων κρυπταναλυτών δεν μπορούν να καταλήξουν σε τρόπους για να τους σπάσουν με συμβατικά μέσα και σε λογικούς χρόνους, καθώς δεν υπάρχουν φορμαλιστικές μέθοδοι που να αποδεικνύουν την ασφάλεια που παρέχουν οι περισσότεροι κρυπτογραφικοί αλγόριθμοι.

Νέοι κρυπτογραφικοί αλγόριθμοι σχεδιάζονται συνεχώς και είτε σπάζουν ή αντέχουν καλά. Για το λόγο αυτό η επιλογή του κατάλληλου αλγόριθμου αποκτά ιδιαίτερη βαρύτητα στην υλοποίηση ενός κρυπτογραφικού συστήματος.

6.3 Στεγανογραφία

Η στεγανογραφία, αποτελεί έναν κλάδο της κρυπτολογίας όπου, σε αντίθεση με την κρυπτογραφία, στόχος δεν είναι η μετατροπή του μηνύματος σε ακατανόητη μορφή αλλά η απόκρυψη της ύπαρξής του.

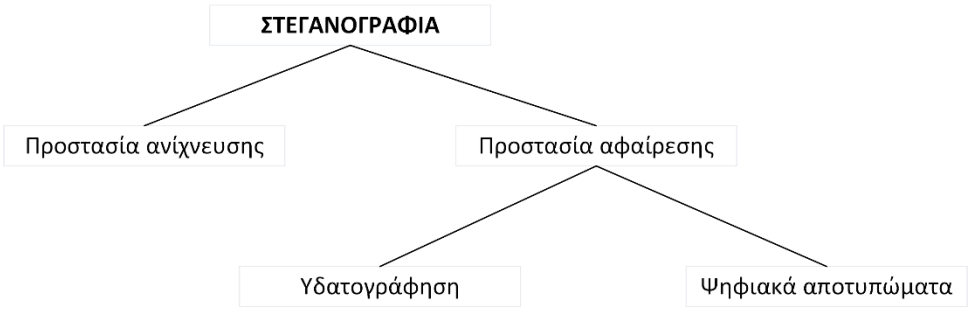
Ένα από τα αρχαιότερα παραδείγματα στεγανογραφικής τεχνικής αναφέρεται στον Ηρόδοτο, όπου περιγράφει την περίπτωση ενός σκλάβου, ο οποίος στάλθηκε στην Ιωνία με ένα μυστικό μήνυμα ζωγραφισμένο στο κεφάλι του. Ο σκλάβος απέκρυψε το μήνυμα αφήνοντας τα μαλλιά του να αποκτήσουν ικανό μάκρος έτσι ώστε να είναι αδύνατη η θέαση του μηνύματος. Στη συνέχεια, ταξίδεψε στη Μίλητο, όπου ξυρίζοντας εκεί το κεφάλι του φανέρωσε το μυστικό μήνυμα στον Αρισταγόρα που ήταν και ο τελικός αποδέκτης του. Ένα άλλο παράδειγμα στεγανογραφικής τεχνικής αποτελεί η χρήση του αόρατου μελανιού. Σε αυτή την περίπτωση, η ύπαρξη του μηνύματος αποκρύπτεται αξιοποιώντας την ιδιότητα του ειδικού μελανιού να μην γίνεται αντιληπτό από το ανθρώπινο μάτι σε κανονικές συνθήκες. Σήμερα, χρησιμοποιούνται τεχνικές με παρόμοιο αποτέλεσμα, ώστε να αποκρύπτεται η ύπαρξη των μεταδιδόμενων ηλεκτρονικών μηνυμάτων.

Οι στεγανογραφικές τεχνικές μπορούν να χρησιμοποιηθούν για διάφορους σκοπούς, όπως:

- Διαφύλαξη της εμπιστευτικότητας ενός μηνύματος.
- Προστασία πληροφορίας από μη εξουσιοδοτημένη τροποποίηση.
- Έλεγχος πρόσβασης κατά τη διανομή ηλεκτρονικού περιεχομένου.

Μια ακόμη χρήση της στεγανογραφίας στις μέρες μας, είναι η προστασία των πνευματικών δικαιωμάτων ηλεκτρονικού περιεχομένου, όπου το κρυφό μήνυμα επιβεβαιώνει την ταυτότητα του νόμιμου ιδιοκτήτη του. Η Ψηφιακή Υδατογράφηση (Digital Watermarking) και τα Ψηφιακά Αποτυπώματα (Digital Fingerprinting) είναι δύο κατηγορίες στις οποίες διαχωρίζεται η τεχνική του ηλεκτρονικού «σημαδέματος» ενός ηλεκτρονικού αρχείου με τεχνικές στεγανογραφίας.

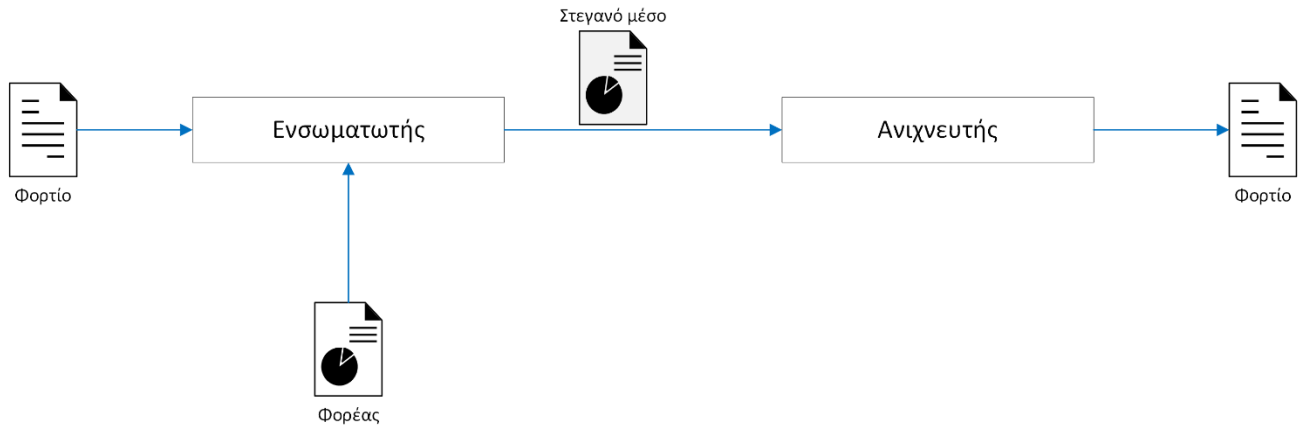
Στην Εικόνα 6.7 απεικονίζεται μια κατηγοριοποίηση των σύγχρονων στεγανογραφικών τεχνικών.



Εικόνα 6.7 *Κατηγοριοποίηση σύγχρονων στεγανογραφικών τεχνικών.*

Το κριτήριο, με βάση το οποίο γίνεται ο διαχωρισμός, προκύπτει από το στόχο της στεγανογραφικής μεθόδου. Στόχος μπορεί να είναι η προστασία ανίχνευσης της ύπαρξης των δεδομένων στο μήνυμα ή η προστασία της αφαίρεσής τους από το μήνυμα (τα ίδια τα δεδομένα δηλώνουν το νόμιμο ιδιοκτήτη τους). Στην περίπτωση κατά την οποία στόχος είναι η προστασία αφαίρεσης, οι τεχνικές διακρίνονται σε παραγωγή υδατογραφημάτων (watermarking), που αφορούν το σύνολο των δεδομένων, ή αποτυπωμάτων (fingerprinting), που προσδιορίζουν μοναδικά κάθε αντικείμενο. Το αποτύπωμα, συνήθως, παράγεται με τη βοήθεια μιας **συνάρτησης συνόψισης**. Οι συναρτήσεις αυτές θα μελετηθούν στο Κεφάλαιο 8.

Ένα γενικό περιγραφικό σχήμα για τη διαδικασία ψηφιακής υδατογράφησης παρατίθεται στην Εικόνα 6.8. Παρατηρούμε ότι στον **ενσωματωτή** (embedder) υπάρχουν δύο είσοδοι: μια για το **φορτίο** (payload), το οποίο αποτελεί το κυρίως μήνυμα που επιθυμούμε να μεταφέρουμε, καθώς και μια για τον **φορέα** (cover work), στον οποίο θέλουμε να ενσωματώσουμε το φορτίο (ώστε να αποκρυφτεί η ύπαρξή του). Η παραγόμενη έξοδος, γνωστή ως **στεγανό μέσο** (stego work), μεταφέρεται στον παραλήπτη και αποτελεί την είσοδο στον **ανιχνευτή** (detector), ο οποίος είναι επιφορτισμένος με την ευθύνη ανίχνευσης της ύπαρξης φορτίου. Αν ανιχνευτεί φορτίο, τότε αυτό παρουσιάζεται στον παραλήπτη.



Εικόνα 6.8 *Διαδικασία ψηφιακής υδατογράφησης.*

Η στεγανογραφία βασίζεται σε τρεις κύριες αρχές, οι οποίες αποτελούν και ένα μέτρο της αποδοτικότητας μιας στεγανογραφικής τεχνικής:

- **Ποσότητα Πληροφορίας:** Όσο περισσότερη πληροφορία (μεγαλύτερο φορτίο) μπορούμε να αποκρύψουμε, τόσο πιο αποδοτική είναι η στεγανογραφική τεχνική.

- **Δυσκολία Ανίχνευσης:** Μια στεγανογραφική τεχνική θα πρέπει να είναι ανθεκτική σε προσπάθειες ανίχνευσης. Υπάρχει οπωσδήποτε μια άμεση σχέση μεταξύ της ποσότητας πληροφορίας που μπορούμε να κρύψουμε και της δυσκολίας ανίχνευσης που προσφέρει η μέθοδος που χρησιμοποιούμε. Όσο περισσότερη πληροφορία, για παράδειγμα, προσπαθούμε

να κρύψουμε ενσωματώνοντάς την στο στεγανό μέσο, τόσο πιο εύκολη γίνεται η ανίχνευση της κρυμμένης πληροφορίας.

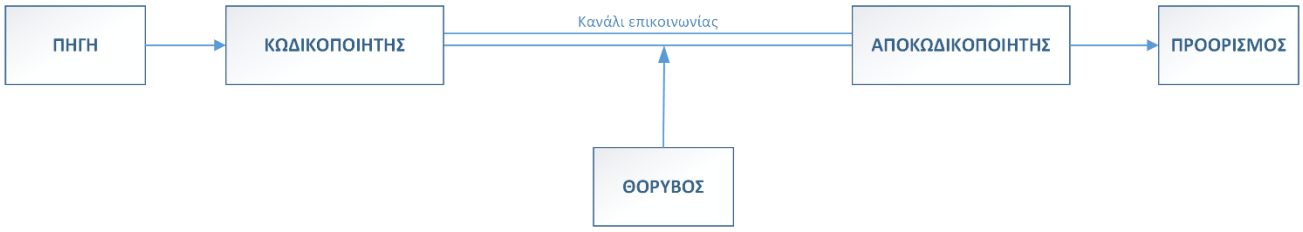
- **Δυσκολία Αφαίρεσης Πληροφορίας**: Πρέπει να είναι πολύ δύσκολη, αν όχι αδύνατη, η αφαίρεση του κρυμμένου μηνύματος (φορτίου) από το στεγανό μέσο, χωρίς αυτό να γίνεται αντιληπτό από το νόμιμο παραλήπτη.

6.4 Χρήσιμες Έννοιες από τη Θεωρία Πληροφορίας

Το 1948 και το 1949 ο Claude Shannon δημοσίευσε δύο εργασίες του με τίτλους: «The Mathematical Theory of Communication» και «Communication Theory of Secrecy Systems», οι οποίες αποτέλεσαν τα θεμέλια για τη γνωστική περιοχή που σήμερα ονομάζεται Θεωρία Πληροφορίας (Information Theory). Η Θεωρία Πληροφορίας διαδραματίζει σπουδαίο ρόλο στη σύγχρονη κρυπτογραφία, καθώς μελετάει ζητήματα τα οποία αφορούν άμεσα τις διαδικασίες που εκτελούν οι κρυπτογραφικοί αλγόριθμοι.

Η συνδυασμένη αξιοποίηση της Θεωρίας Πληροφορίας και της Πολυπλοκότητας Αλγορίθμων, στο πλαίσιο μελέτης της ανθεκτικότητας των κρυπτογραφικών αλγόριθμων, είναι η αναζήτηση και απόδειξη των ελάχιστων ορίων σε χρόνο και χώρο οι οποίοι απαιτούνται προκειμένου να επιλυθεί ένα δεδομένο υπολογιστικό πρόβλημα. Όπως αναφέρθηκε προηγουμένως, ένα κρυπτογραφικό σύστημα είναι ασφαλές αν ο κρυπτογραφικός αλγόριθμος το προστατεύει με τέτοιο τρόπο ώστε να είναι **υπολογιστικά ανέφικτο** να καταφέρει κάποιος τρίτος να υπερνικήσει αυτή την προστασία με λογικούς πόρους (δηλαδή, σε εύλογο χρονικό διάστημα και χρησιμοποιώντας περιορισμένο χώρο αποθήκευσης). Επομένως, η εύρεση των ελάχιστων αυτών ορίων είναι σημαντική για να διασφαλιστεί ότι ο κρυπτογραφικός αλγόριθμος εξυπηρετεί το σκοπό του, ακόμη και αν αποδεδειγμένα μπορεί με κάποιο τρόπο να υπερνικηθεί. Αν οι πόροι που απαιτούνται ικανοποιούν τις απαιτήσεις, τότε ο κρυπτογραφικός αλγόριθμος κρίνεται ανθεκτικός.

Η Θεωρία Πληροφορίας εστιάζει στην επικοινωνία μεταξύ των οντοτήτων, οι οποίες συμμετέχουν σε ένα επικοινωνιακό σύστημα, όπως απεικονίζεται στην Εικόνα 6.9.



Εικόνα 6.9 *Επικοινωνιακό σύστημα.*

Ο σκοπός ενός επικοινωνιακού συστήματος είναι η μεταφορά πληροφορίας από μια πηγή (source) σε ένα συγκεκριμένο προορισμό (destination). Οι οντότητες που συμμετέχουν σε ένα επικοινωνιακό σύστημα, όπως αυτές εμφανίζονται στην αφαιρετική αναπαράσταση της Εικόνας 6.9, είναι οι παρακάτω:

- **Πηγή (Source)**: Είναι η οντότητα η οποία παράγει το μήνυμα πληροφορίας το οποίο πρέπει να μεταδοθεί.

- **Κωδικοποιητής (Encoder)**: Μεταφράζει το μήνυμα σε μια μορφή κατάλληλη για μεταφορά μέσω του **καναλιού επικοινωνίας (communication channel)**. Για παράδειγμα, στις ψηφιακές επικοινωνίες η μορφή αυτή είναι μια ακολουθία δυαδικών ψηφίων.

- **Κανάλι επικοινωνίας (communication channel)**: Είναι το μέσο (ο δίαυλος επικοινωνίας), το οποίο χρησιμοποιείται για τη μεταφορά του κωδικοποιημένου μηνύματος, όπως αυτό έχει προκύψει από τον κωδικοποιητή.

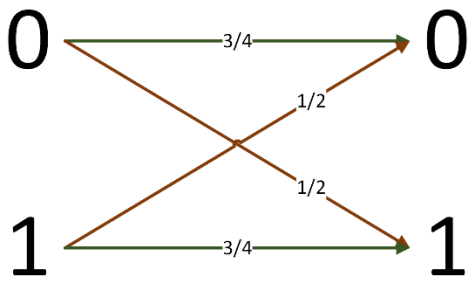
- **Κανάλι μεταφοράς**: Μπορεί να υπόκειται σε παρέμβαση **θορύβου (noise)**, με αποτέλεσμα να υπάρχουν αλλοιώσεις του μηνύματος κατά τη μεταφορά του. Για παράδειγμα, η επιθυμητή μεταφορά του bit με τιμή 1 μπορεί να έχει ως αποτέλεσμα να φτάσει στον προορισμό το bit με τιμή 0.

- **Αποκωδικοποιητής (Decoder)**: Παραλαμβάνει το κωδικοποιημένο μήνυμα από την έξοδο του καναλιού και το αποκωδικοποιεί έτσι ώστε να είναι καταληπτό από τον προορισμό.

- **Προορισμός (Destination)**: Λαμβάνει το μεταφερθέν μήνυμα πληροφορίας. Είναι ο τελικός αποδέκτης της επικοινωνίας, που λαμβάνει χώρα στο επικοινωνιακό σύστημα.

Η Θεωρία Πληροφορίας αναζητά σε ένα επικοινωνιακό σύστημα και εξετάζει λύσεις για πρακτικά ερωτήματα, όπως για παράδειγμα: «Ποιος είναι ο βέλτιστος τρόπος συμπίεσης των δεδομένων προς αποστολή;», «Ποιο είναι το καταλληλότερο σχήμα κωδικοποίησης που μπορούμε να χρησιμοποιήσουμε;». Οι απαντήσεις σε τέτοιου είδους ερωτήματα βασίζονται σε θεωρίες με ισχυρά μαθηματικά θεμέλια, οι οποίες αναπτύχθηκαν και συνεχίζουν να αναπτύσσονται, ή να βελτιώνονται, καθώς οι ανάγκες αλλάζουν με την πάροδο του χρόνου.

Ας θεωρήσουμε το ακόλουθο παράδειγμα. Έστω ότι υπάρχει μια πηγή, η οποία παράγει μια ακολουθία bit με ρυθμό 1 bit/sec. Τα bit με τιμή 0 και τα bit με τιμή 1 παράγονται με ίσες πιθανότητες και ανεξάρτητα το ένα από το άλλο. Η επικοινωνία λαμβάνει χώρα πάνω σε ένα κανάλι με θόρυβο. Ας υποθέσουμε ότι ο θόρυβος προκαλείται με τρόπο τέτοιο ώστε ένα bit να μπορεί να παραληφθεί στον προορισμό με λάθος τιμή (δηλαδή με τιμή διαφορετική από αυτή με την οποία στάλθηκε από την πηγή) με πιθανότητα ¼ (0,25). Το επικοινωνιακό αυτό σύστημα απεικονίζεται στην Εικόνα 6.10



Εικόνα 6.10 *Επικοινωνία σε κανάλι με θόρυβο*.

Σε ένα τέτοιο σύστημα, μπορεί κάποιος να κρίνει ότι η πιθανότητα λάθους 0,25 είναι πολύ μεγάλη και ότι πρέπει να αντιμετωπίσει αυτό το πρόβλημα. Μια λύση θα ήταν η επαναλαμβανόμενη εκπομπή του ίδιου bit περισσότερες από μια φορές. Έστω, ότι στέλνουμε το bit με τιμή 1 τρεις φορές. Τότε ο προορισμός θα μπορούσε να αποφανθεί ποια είναι η σωστή τιμή του bit που αρχικά στάλθηκε, βασιζόμενος στην πιθανότητα σωστής ή λανθασμένης μετάδοσης. Αν ο προορισμός παραλάβει την ακολουθία bit 110 τότε ακόμη και διαισθητικά αντιλαμβανόμαστε ότι πιθανότερο είναι ότι αρχικά η πηγή είχε ως στόχο να μεταδώσει το bit με τιμή 1, αφού η παραλαβή δύο αλλοιωμένων τιμών έχει λιγότερες πιθανότητες από την παραλαβή δύο σωστών.

Το θεμελιώδες θεώρημα της Θεωρίας Πληροφορίας αναφέρει πως προκειμένου να έχουμε μεγάλη αξιοπιστία κατά τη μετάδοση πληροφοριών, χωρίς να μειώσουμε το ρυθμό μετάδοσης κοντά στο μηδέν, αρκεί να τον μειώσουμε ως την τιμή η οποία ονομάζεται Χωρητικότητα Καναλιού (Channel Capacity). Η κωδικοποίηση έχει ακριβώς αυτό τον στόχο. Να αντιστοιχίσει σε μια ακολουθία πραγματικών bit προς αποστολή μια σειρά συμβόλων, η οποία ονομάζεται κωδική λέξη (code word) και είναι κατάλληλη για τη μετάδοση πάνω από κανάλι με θόρυβο. Για την αποδοτικότερη μετάδοση των πραγματικών bit του μηνύματος είναι σύνηθες η κωδική λέξη να αντιστοιχεί σε μια δέσμη (block) από bit και όχι σε ένα μόνο bit. Στην

κρυπτογραφία, χρησιμοποιείται η έννοια της εντροπίας ως ένα μαθηματικό μέτρο της πληροφορίας που μεταφέρεται μέσω ενός μηνύματος.

Με την εργασία του 1949, ο Shannon κατάφερε να μετρήσει τη «μυστικότητα» ενός αλγόριθμου κρυπτογράφησης χρησιμοποιώντας την αβεβαιότητα του αρχικού κειμένου, δεδομένης της κατοχής του κρυπτοκειμένου. Ένα κρυπτοσύστημα, από το οποίο έχουμε στη διάθεση μας όση ποσότητα κρυπτοκειμένου επιθυμούμε αλλά παρόλα αυτά δεν μπορούμε να μάθουμε κάτι παραπάνω για το αρχικό κείμενο, λέμε ότι προσφέρει «τέλεια μυστικότητα» (**perfect secrecy**).

Συνήθως, όσο μεγαλύτερη ποσότητα κρυπτοκειμένου έχουμε στη διάθεση μας, τόσο μειώνεται η αβεβαιότητα του αρχικού κειμένου, μέχρι του σημείου που γίνεται μηδενική, οπότε μπορούμε να ανακτήσουμε το αρχικό κείμενο. Ωστόσο, από έναν κρυπτογραφικό αλγόριθμο απαιτείται να είναι υπολογιστικά ανέφικτη δυνατότητα εξαγωγής συμπερασμάτων για το αρχικό κείμενο, λαμβάνοντας υπόψη τους υπολογιστικούς πόρους που μπορούν να διατίθενται στους κρυπταναλυτές.

Η Θεωρία Πληροφορίας μετράει την ποσότητα πληροφορίας που περιέχεται σε ένα μήνυμα με το πλήθος των bit που απαιτούνται για να κωδικοποιήσουμε όλα τα ενδεχόμενα μηνύματα. Για παράδειγμα, για να κωδικοποιήσουμε το σύνολο {ΑΣΠΡΟ, ΜΑΥΡΟ} χρειαζόμαστε 1 bit. Η ποσότητα αυτή της πληροφορίας ενός μηνύματος μετριέται με την εντροπία, η οποία είναι μία συνάρτηση της κατανομής πιθανοτήτων πάνω σε όλες τις ενδεχόμενες τιμές που μπορεί να έχει ένα μήνυμα.

Έστω X_1, …, X_n όλες οι πιθανές εκδοχές ενός μηνύματος *m* με αντίστοιχες πιθανότητες εμφάνισης $p(X_1)$, … , $p(X_n)$, όπου το άθροισμα των $p(X_i)$ είναι 1. Η εντροπία του μηνύματος *m* δίνεται από τον ακόλουθο τύπο:

$$H(X) = -\sum_{i=1}^{n} p(X_i) \log_2 p(X_i) \qquad (6.1)$$

όπου για το λογάριθμο χρησιμοποιούμε ως βάση το 2 και για αυτό το λόγο η μονάδα μέτρησης της εντροπίας είναι το bit.

Ο παραπάνω τύπος, ερμηνευτικά μας λέει ότι με πιθανότητα $p(X_i)$ η εκδοχή μηνύματος X_i μπορεί να αναπαρασταθεί με $\log_2 p(X_i)$ bit πληροφορίας. Για παράδειγμα, έστω η τυχαία μεταβλητή Χ η οποία παίρνει τιμές από το σύνολο Χ = {Α, Β, Γ}, με p(A) = 1/2, p(B) = 1/4 και p(Γ) = 1/4. Τότε, σύμφωνα με τον ορισμό της εντροπίας, θα έχουμε:

$$H(X) = -\frac{1}{2}\log_2\left(\frac{1}{2}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) - \frac{1}{4}\log_2\left(\frac{1}{4}\right) = 1,5\,bit \qquad (6.2)$$

Η εντροπία, στην περίπτωσή μας η τιμή 1.5, μας δίνει και ένα μέτρο των ελάχιστων bit που απαιτούνται προκειμένου να περιγράψουμε πλήρως την τυχαία μεταβλητή Χ. Ο αριθμός αυτός των bit είναι πάντα μεταξύ των τιμών Η(Χ) και Η(Χ) + 1. Για το παράδειγμά μας, οι τιμές Α, Β και Γ της μεταβλητής απαιτούν τελικά 2 bit για να περιγράφουνε, αφού Η(Χ) < 2 < Η(Χ)+1. Άρα, η εντροπία παρέχει το κάτω όριο του αριθμού των bit που απαιτούνται για να περιγράψουμε την τιμή που έλαβε μια τυχαία διακριτή μεταβλητή.

Παρατηρώντας τον τύπο υπολογισμού της εντροπίας, καταλήγουμε στο συμπέρασμα ότι αυτή γίνεται μέγιστη όταν όλα τα ενδεχόμενα της τυχαίας μεταβλητής Χ είναι ισοπίθανα. Ενώ, αντίστοιχα, η εντροπία γίνεται ελάχιστη (ίση με το μηδέν) όταν υπάρχει ενδεχόμενο X_i το οποίο έχει πιθανότητα εμφάνισης ίσο με τη μονάδα (σίγουρο ότι θα συμβεί).

Ο κρυπτογράφος και ο κρυπταναλυτής χρησιμοποιούν την έννοια της εντροπίας με διαφορετικό σκοπό. Ο κρυπτογράφος χρησιμοποιεί έναν αλγόριθμο τέτοιο ώστε να αυξήσει την εντροπία του παραγόμενου κρυπτοκειμένου με σκοπό να καταστήσει δυσκολότερη την αποκρυπτογράφηση, καθώς η αύξηση της εντροπίας σημαίνει μείωση της συντακτικής δομής του παραγόμενου κρυπτοκειμένου. Από την άλλη, ο κρυπταναλυτής επιθυμεί να αναγνωρίσει μια λογική δομή στο κρυπτοκείμενο προκειμένου να οδηγηθεί σε συμπεράσματα, άρα χρησιμοποιεί τεχνικές και μεθόδους τέτοιες ώστε να οδηγηθεί σε ένα κρυπτοκείμενο μειωμένης εντροπίας, δηλαδή αυξημένης λογικής δομής. Για παράδειγμα, όταν ο κρυπταναλυτής γνωρίζει ότι το κρυπτοκείμενο FS%S^# αντιστοιχεί είτε στην τιμή ΑΣΠΡΟ είτε στην τιμή ΜΑΥΡΟ τότε η αβεβαιότητα

είναι μόλις 1 bit. Δηλαδή, ο κρυπταναλυτής χρειάζεται να γνωρίσει μόλις 1 bit προκειμένου να αποφανθεί για την πραγματική τιμή που αντιστοιχεί στο κρυπτοκείμενο που έχει στη διάθεσή του. Στην περίπτωσή μας, το πρώτο bit και μόνο θα αρκούσε για να καταλάβει ο κρυπταναλυτής ποιος είναι ο πρώτος χαρακτήρας: **Α**(ΣΠΡΟ) ή **Μ**(ΑΥΡΟ).

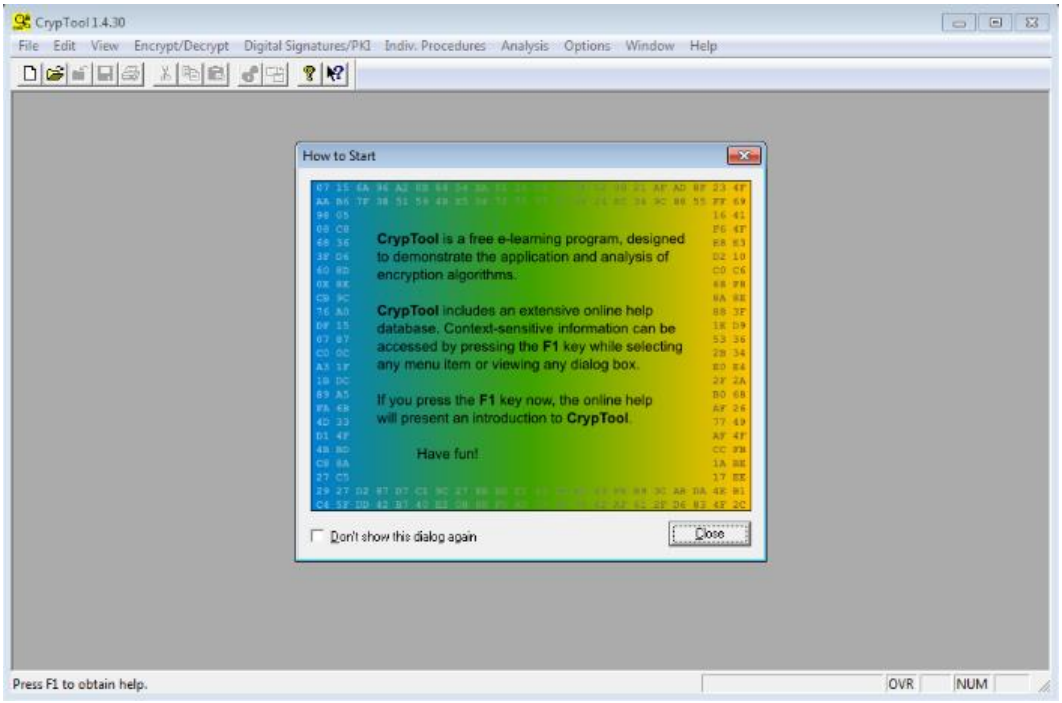
6.5 Μελέτη κλασσικών κρυπτογραφικών αλγορίθμων με το Cryptool

Το Cryptool είναι ένα εκπαιδευτικό λογισμικό που αναπτύχθηκε από τη συνεργασία πανεπιστημίων, στο πλαίσιο ενός εσωτερικού προγράμματος ευαισθητοποίησης μιας τράπεζας. Από τις αρχές της δεκαετίας του 2000 διατίθεται ελευθέρα για χρήση.

Το Cryptool περιλαμβάνει μεταξύ άλλων την υλοποίηση:

- Κλασσικών και σύγχρονων κρυπτογραφικών αλγορίθμων.
- Εργαλείων κρυπτανάλυσης.
- Διαδραστικών παρουσιάσεων αλγορίθμων και κρυπτοσυσκευών.
- Μηχανισμού online βοήθειας.

Στη συνέχεια αυτού του κεφαλαίου, το εργαλείο Cryptool θα χρησιμοποιηθεί για την εφαρμογή και κρυπτανάλυση κλασσικών αλγορίθμων κρυπτογράφησης. Το Cryptool είναι διαθέσιμο στη σελίδα: https://www.cryptool.org/en/ct1-downloads, όπου πέρα από την Αγγλική γλώσσα παρέχεται και στην Ελληνική γλώσσα, μεταφρασμένο από την επιστημονική ομάδα για την έρευνα και ανάπτυξη στην Ασφάλεια Πληροφοριών InfoSec του Πανεπιστημίου Μακεδονίας (http://infosec.uom.gr).



Εικόνα 6.11 *Το λογισμικό Cryptool.*

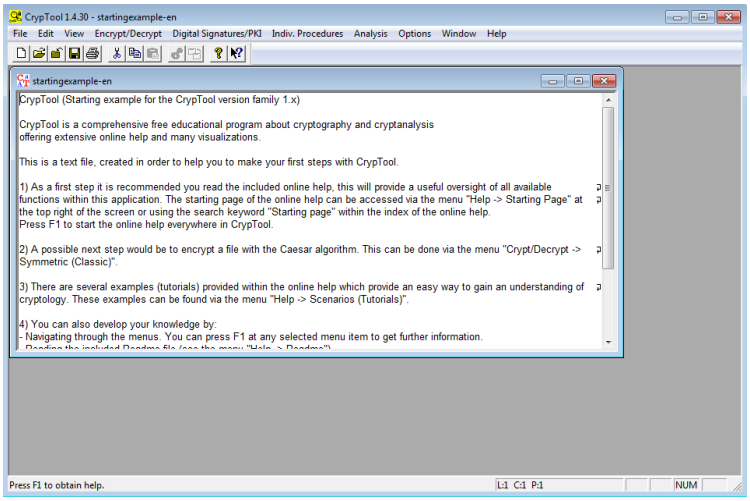
Οι κλασσικοί κρυπτογραφικοί αλγόριθμοι βασίζονται στην εφαρμογή τεχνικών μετατόπισης ή αντικατάστασης χαρακτήρων ενός συγκεκριμένου αλφαβήτου, ώστε το αρχικό κείμενο ως συλλογή χαρακτήρων να μετατραπεί στο κρυπτοκείμενο το οποίο θα έχει μια μορφή ακατανόητη πάλι όμως ως συλλογή χαρακτήρων του ίδιου αλφαβήτου. Ακολουθεί η παρουσίαση ορισμένων από τους πιο γνωστούς κλασσικούς κρυπτογραφικούς αλγορίθμους, με χρήση του εκπαιδευτικού εργαλείου Cryptool.

6.5.1 Αλγόριθμος του Καίσαρα

Ο αλγόριθμος του Καίσαρα ανήκει στην κατηγορία κρυπτογραφικών αλγορίθμων μονοαλφαβητικής αντικατάστασης, όπου το κλειδί είναι ένας χαρακτήρας του οποίου ο αύξων αριθμός θέσης στο αλφάβητο προκαλεί μια μετάθεση όλων των χαρακτήρων στο αλφάβητο. Ο Ιούλιος Καίσαρας στο βιβλίο «The Gallic Wars» περιγράφει έναν αλγόριθμο όπου κάθε γράμμα της αλφαβήτου μετατίθεται τρεις θέσεις δεξιότερα στο αλφάβητο. Η κρυπτογράφηση υλοποιείται με αντικατάσταση κάθε γράμματος του αρχικού κειμένου με το γράμμα που προκύπτει μετά τη μετάθεση. Αντίστοιχα, η αποκρυπτογράφηση γίνεται με αντικατάσταση του κάθε χαρακτήρα σύμφωνα με την αντίστροφη μετάθεση του αρχικού αλφαβήτου.

6.5.1.1 Κρυπτογράφηση

Μετά την εκκίνηση του ανοίγει ένα παράθυρο όπου περιέχεται ένα δείγμα αγγλικού κειμένου (startingexample-en.txt), όπως φαίνεται στην Εικόνα 6.12, το οποίο θα χρησιμοποιηθεί στη συνέχεια ως αρχικό κείμενο.



Εικόνα 6.12 *Το αρχικό κείμενο.*

Από το μενού επιλέγουμε κατά σειρά **Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13** και βεβαιωνόμαστε ότι:

- Στο πεδίο Select Variant είναι επιλεγμένη η επιλογή Caesar.
- Στο πεδίο Options to interpret the alphabet characters είναι επιλεγμένη η πρώτη επιλογή που καθορίζει πως η αρίθμηση ξεκινά από το 0.
- Στο πεδίο Key entry as επιλέγουμε Alphabet character και δίνουμε ως χαρακτήρα-κλειδί τον χαρακτήρα K.

Παρατηρούμε ότι στο κάτω μέρος του παραθύρου εμφανίζεται (και ανανεώνεται καθώς πληκτρολογούμε) η αντιστοίχιση κάθε χαρακτήρα του αλφαβήτου με αυτόν με τον οποίο θα αντικατασταθεί κατά την παραγωγή του κρυπτοκειμένου (κρυπτογράφηση), σύμφωνα με την επιλογή που έχει γίνει για το χαρακτήρα-κλειδί.

Στη συνέχεια, επιλέγουμε Encrypt, οπότε εμφανίζεται ένα νέο παράθυρο με το κρυπτογραφημένο κείμενο. Τι παρατηρείτε στο κείμενο αυτό; Είναι δυνατή η ανάγνωση και κατανόησή του;

- Έχοντας ως ενεργό το παράθυρο με το κρυπτοκείμενο, επιλέγουμε διαδοχικά από το μενού: **Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13**. Χωρίς καμία αλλαγή στις προτεινόμενες (default) ρυθμίσεις, επιλέγουμε Decrypt.

Εμφανίζεται ένα νέο παράθυρο με το αποκρυπτογραφημένο κείμενο, το οποίο όμως δεν είναι όμοιο με το αρχικό μας κείμενο. Γιατί συνέβη αυτό; Γιατί δεν αποκρυπτογραφήθηκε σωστά το κρυπτοκείμενο;

- Κλείνουμε το παράθυρο με το ανεπιτυχώς αποκρυπτογραφημένο κείμενο και επιλέγουμε να είναι ενεργό εκ νέου το παράθυρο με το κρυπτογράφημα.

- Επιλέγουμε διαδοχικά από το μενού**: Encrypt/Decrypt → Symmetric (classic) → Caesar / Rot13**.

- Στο πεδίο Key entry as, επιλέγουμε Alphabet character και δίνουμε το χαρακτήρα-κλειδί που είχαμε επιλέξει κατά την κρυπτογράφηση (K).

- Στη συνέχεια, επιλέγουμε Decrypt.

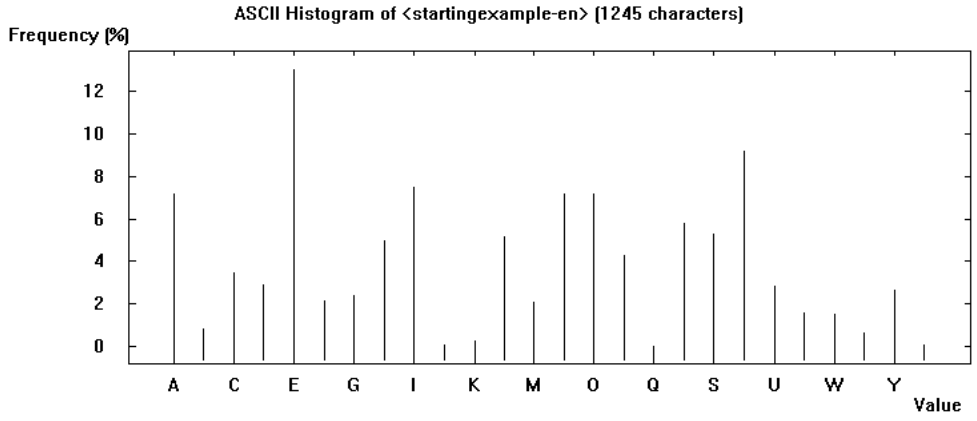
Εμφανίζεται ένα νέο παράθυρο με το αποκρυπτογραφημένο κείμενο. Αυτή τη φορά η αποκρυπτογράφηση έγινε σωστά. Γιατί;

- Επαναλαμβάνουμε τη διαδικασία κρυπτογράφησης / αποκρυπτογράφησης του αρχικού μας κειμένου δίνοντας στο πεδίο Key entry για την επιλογή Number Value την τιμή 8.

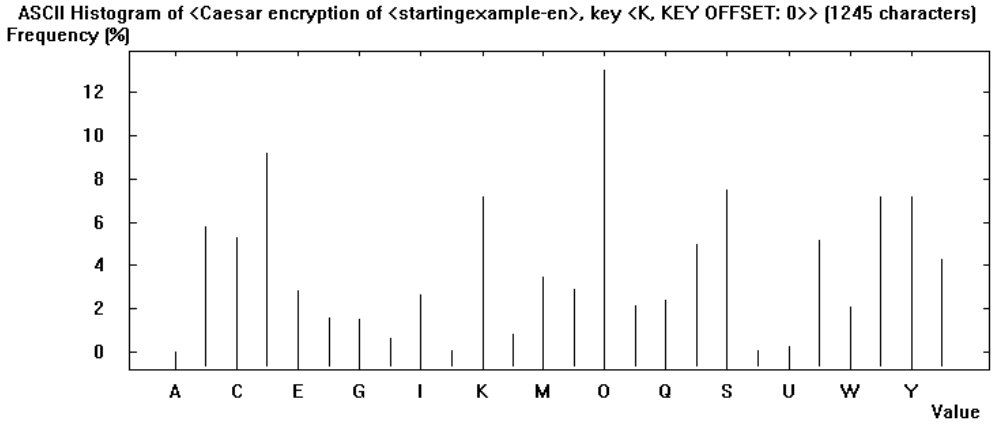
- Επιλέγουμε να είναι ενεργό το παράθυρο με το κρυπτογραφημένο μήνυμα και επιλέγουμε από το μενού κατά σειρά: **Analysis → Tools for Analysis → Histogram**.

- Επιλέγουμε να είναι ενεργό το παράθυρο με το αρχικό κείμενο και επιλέγουμε διαδοχικά από το μενού: **Analysis → Tools for Analysis → Histogram**.

Τι παρατηρείτε συγκρίνοντας τα δύο ιστογράμματα; Μπορείτε να εξάγετε κάποια χρήσιμη πληροφορία κρυπταναλυτικού ενδιαφέροντος (δηλαδή, για το κλειδί αποκρυπτογράφησης);



Εικόνα 6.13 *Ιστόγραμμα αρχικού κειμένου.*



Εικόνα 6.14 *Ιστόγραμμα κρυπτοκειμένου Καίσαρα.*

6.5.1.2 Κρυπτανάλυση μόνο με κρυπτοκείμενο

Η κρυπταναλυτική προσπάθεια έχοντας γνωστό μόνο το υποκλαπέν κρυπτοκείμενο, μπορεί να βοηθηθεί σημαντικά από επιμέρους εργαλεία ανάλυσης που συμπεριλαμβάνει το Cryptool.

Κλείνουμε όλα τα ανοιχτά παράθυρα του Cryptool και από το μενού επιλέγουμε διαδοχικά: **File → New** και εισάγουμε το ακόλουθο κρυπτοκείμενο που γνωρίζουμε ότι προέρχεται από κάποιο αρχικό κείμενο στην Αγγλική γλώσσα, το οποίο έχει κρυπτογραφηθεί με τον αλγόριθμο Caesar. Δυστυχώς όμως, δεν γνωρίζουμε το κλειδί που χρησιμοποιήθηκε:

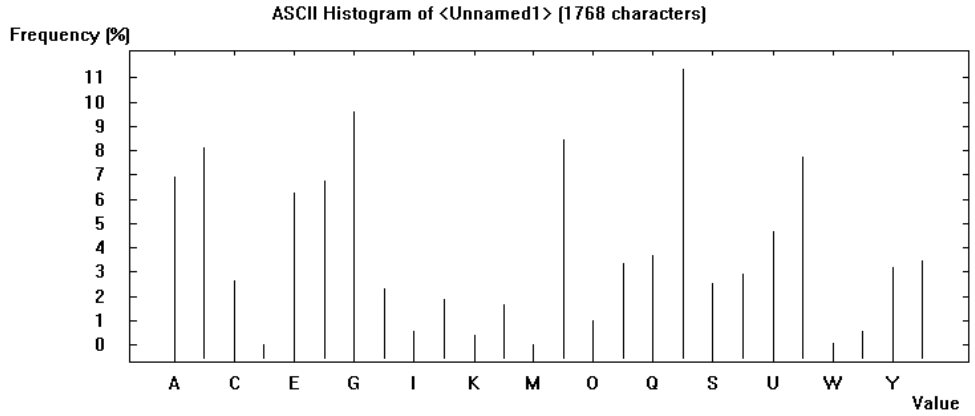
```
Gurer ner n ynetr ahzore bs fgrtnabtencuvp zrgubqf gung zbfg
bs hf ner snzvyvne jvgu (rfcrpvnyyl vs lbh jngpu n ybg bs fcl
zbivrf!), enatvat sebz vaivfvoyr vax naq zvpebqbgf gb frpergvat
n uvqqra zrffntr va gur frpbaq yrggre bs rnpu jbeq bs n ynetr
obql bs grkg naq fcernq fcrpgehz enqvb pbzzhavpngvba. Jvgu
pbzchgref naq argjbexf, gurer ner znal bgure jnlf bs uvqvat
vasbezngvba, fhpu nf:
* Pbireg punaaryf (r.t., Ybxv naq fbzr qvfgevohgrq qravny-bs-
freivpr gbbyf hfr gur Vagrearg Pbageby Zrffntr Cebgbpby, be
VPZC, nf gur pbzzhavpngvbaf punaary orgjrra gur "onq thl" naq
n pbzcebzvfrq flfgrz)
* Uvqqra grkg jvguva Jro cntrf
* Uvqvat svyrf va "cynva fvtug" (r.t., jung orggre cynpr gb
"uvqr" n svyr guna jvgu na vzcbegnag fbhaqvat anzr va gur
p:\jvaqbjf\flfgrz32 qverpgbel?)
* Ahyy pvcuref (r.t., hfvat gur svefg yrggre bs rnpu jbeq gb
sbez n uvqqra zrffntr va na bgurejvfr vaabphbhf grkg)
Fgrtnabtencul gbqnl, ubjrire, vf fvtavsvpnagyl zber
fbcuvfgvpngrq guna gur rknzcyrf nobir fhttrfg, nyybjvat n hfre
gb uvqr ynetr nzbhagf bs vasbezngvba jvguva vzntr naq nhqvb
svyrf. Gurfr sbezf bs fgrtnabtencul bsgra ner hfrq va
pbawhapgvba jvgu pelcgbtencul fb gung gur vasbezngvba vf qbhoyl
cebgrpgrq; svefg vg vf rapelcgrq naq gura uvqqra fb gung na
nqirefnel unf gb svefg svaq gur vasbezngvba (na bsgra qvssvphyg
gnfx va naq bs vgfrys) naq gura qrpelcg vg.
Gurer ner n ahzore bs hfrf sbe fgrtnabtencul orfvqrf gur zrer
abirygl. Bar bs gur zbfg jvqryl hfrq nccyvpngvbaf vf sbe fb-
pnyyrq qvtvgny jngreznexvat. N jngreznex, uvfgbevpnyyl, vf gur
ercyvpngvba bs na vzntr, ybtb, be grkg ba cncre fgbpx fb gung
gur fbhepr bs gur qbphzrag pna or ng yrnfg cnegvnyyl
```

```
nhguragvpngrq. N qvtvgny jngreznex pna nppbzcyvfu gur fnzr
shapgvba; n tencuvp negvfg, sbe rknzcyr, zvtug cbfg fnzcyr
vzntrf ba ure Jro fvgr pbzcyrgr jvgu na rzorqqrq fvtangher fb
gung fur pna yngre cebir ure bjarefuvc va pnfr bguref nggrzcg
gb cbegenl ure jbex nf gurve bja.
Fgrtnabtencul pna nyfb or hfrq gb nyybj pbzzhavpngvba jvguva
na haqretebhaq pbzzhavgl. Gurer ner frireny ercbegf, sbe
rknzcyr, bs crefrphgrq eryvtvbhf zvabevgvrf hfvat fgrtnabtencul
gb rzorq zrffntrf sbe gur tebhc jvguva vzntrf gung ner cbfgrq
gb xabja Jro fvgrf.
```

Από το μενού επιλέγουμε διαδοχικά: **Analysis → Tools for Analysis → Histogram**. Εμφανίζεται το ιστόγραμμα που αντιστοιχεί στο κείμενο αυτό (Εικόνα 6.15).

Στη διεθνή βιβλιογραφία, μπορούμε να εντοπίσουμε αρκετές έρευνες για τη συχνότητα εμφάνισης των γραμμάτων της λατινικής αλφαβήτου, ή συνδυασμών τους (π.χ. digrams, trigrams κ.λπ.), μέσα σε τυπικά κείμενα, συνήθως της κλασσικής λογοτεχνίας. Από τις έρευνες αυτές προκύπτει ότι το πλέον συχνά εμφανιζόμενο γράμμα είναι το «**E**».

Συνδυάζοντας την παραπάνω πληροφορία για το γράμμα «E» και παρατηρώντας τη συχνότητα εμφάνισης των γραμμάτων στο ιστόγραμμα του κρυπτοκειμένου (Εικόνα 6.15), ποιο συμπέρασμα εξάγετε σχετικά με την τιμή της μετατόπισης, άρα και του κλειδιού κρυπτογράφησης (number value) που χρησιμοποιήθηκε για την παραγωγή του κρυπτοκειμένου;



Εικόνα 6.15 *Ιστόγραμμα δεύτερου κρυπτοκειμένου Καίσαρα.*

Επαληθεύστε την υπόθεσή σας, εφαρμόζοντας αποκρυπτογράφηση με το εργαλείο Cryptool. Καταφέρατε να φτάσετε σε αναγνώσιμο και καταληπτό κείμενο; Αν τα έχετε καταφέρει θα πρέπει να διαβάζετε στο Cryptool το παρακάτω κείμενο:

```
There are a large number of steganographic methods that most
of us are familiar with (especially if you watch a lot of spy
movies!), ranging from invisible ink and microdots to secreting
a hidden message in the second letter of each word of a large
body of text and spread spectrum radio communication. With
computers and networks, there are many other ways of hiding
information, such as:
* Covert channels (e.g., Loki and some distributed denial-of-
service tools use the Internet Control Message Protocol, or
ICMP, as the communications channel between the "bad guy" and
a compromised system)
```

* Hidden text within Web pages
* Hiding files in "plain sight" (e.g., what better place to "hide" a file than with an important sounding name in the c:\windows\system32 directory?)
* Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information within image and audio files. These forms of steganography often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in and of itself) and then decrypt it.

There are a number of uses for steganography besides the mere novelty. One of the most widely used applications is for so-called digital watermarking. A watermark, historically, is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function; a graphic artist, for example, might post sample images on her Web site complete with an embedded signature so that she can later prove her ownership in case others attempt to portray her work as their own.

Steganography can also be used to allow communication within an underground community. There are several reports, for example, of persecuted religious minorities using steganography to embed messages for the group within images that are posted to known Web sites.

6.5.2 Αλγόριθμος Vigenere

Ο αλγόριθμος Vigenere ανήκει στην κατηγορία των κρυπτογραφικών αλγορίθμων πολυαλφαβητικής αντικατάστασης, όπου το κλειδί είναι μια μικρή ακολουθία γραμμάτων (π.χ. μια λέξη). Λειτουργεί όπως ο αλγόριθμος του Καίσαρα, αλλά χρησιμοποιεί τόσα διαφορετικά νέα αλφάβητα (μετά τις μεταθέσεις) όσα και τα διαφορετικά γράμματα της λέξης που χρησιμοποιείται ως κλειδί.

6.5.2.1 Κρυπτογράφηση και Αποκρυπτογράφηση

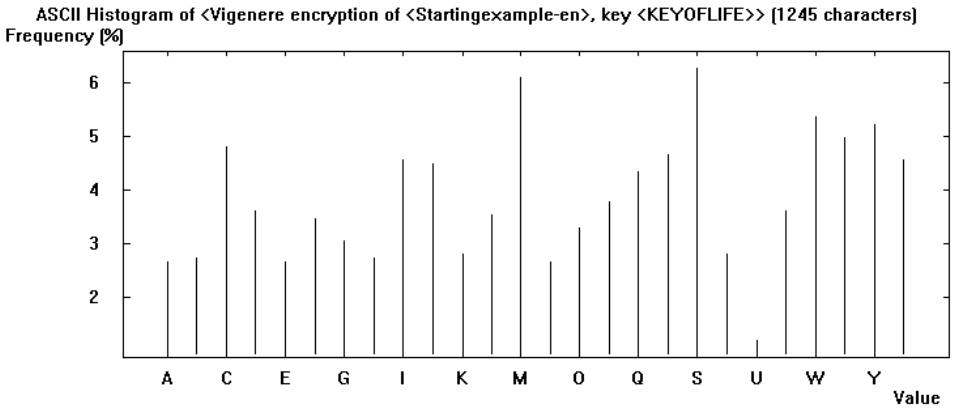
Για την κρυπτογράφηση και την αποκρυπτογράφηση με χρήση του αλγόριθμου Vigenere, θα χρησιμοποιήσουμε εκ νέου το παράδειγμα αγγλικού κειμένου (startingexample-en.txt) ως αρχικό κείμενο, ως εξής:

- Από το μενού επιλέγουμε διαδοχικά **Encrypt / Decrypt → Symmetric (classic) → Vigenere**
- Εισάγουμε τη λέξη-κλειδί KEYOFLIFE και πατάμε το πλήκτρο Encrypt, οπότε εμφανίζεται ένα νέο παράθυρο με το κρυπτογραφημένο κείμενο.

Τι παρατηρείτε στο κείμενο αυτό; Είναι δυνατή η ανάγνωση και κατανόησή του μετά την εφαρμογή του αλγορίθμου κρυπτογράφησης;

Επιλέγουμε να είναι ενεργό το παράθυρο με το κρυπτογραφημένο μήνυμα και επιλέγουμε από το μενού κατά σειρά: **Analysis → Tools for Analysis → Histogram**.

Τι παρατηρείτε συγκρίνοντας τα δύο ιστογράμματα (Εικόνες 6.16 και 6.13); Μπορείτε να εξάγετε κάποια χρήσιμη πληροφορία κρυπταναλυτικού ενδιαφέροντος (δηλαδή, για το κλειδί κρυπτογράφησης);



Εικόνα 6.16 *Ιστόγραμμα κρυπτοκειμένου Vigenere.*

6.5.2.2 Κρυπτανάλυση μόνο με κρυπτοκείμενο

Η κρυπταναλυτική προσπάθεια, έχοντας γνωστό μόνο το υποκλαπέν κρυπτοκείμενο, μπορεί, όπως και στην προηγούμενη περίπτωση, να βοηθηθεί σημαντικά από επιμέρους εργαλεία ανάλυσης που συμπεριλαμβάνονται στο Cryptool. Αυτή τη φορά όμως, τα πράγματα έχουν δυσκολέψει αρκετά, καθώς μια απλή παρατήρηση των συχνοτήτων εμφάνισης των γραμμάτων, όπως διαπιστώσατε ήδη, δεν φαίνεται να βοηθάει ουσιαστικά.

Αυτό συμβαίνει, καθώς η αντικατάσταση είναι πλέον πολυαλφαβητική και όχι μονοαλφαβητική, όπως στην περίπτωση του αλγόριθμου του Καίσαρα. Θα ήταν ιδιαίτερα χρήσιμο να υπήρχε τρόπος να μετατρέψουμε το πρόβλημα της πολυαλφαβητικής αντικατάστασης σε πρόβλημα μονοαλφαβητικής. Για παράδειγμα, θα μας βοηθούσε αν γνωρίζαμε έστω το μήκος του κλειδιού που χρησιμοποιήθηκε κατά την κρυπτογράφηση.

- Κλείνουμε όλα τα ανοιχτά παράθυρα του Cryptool.

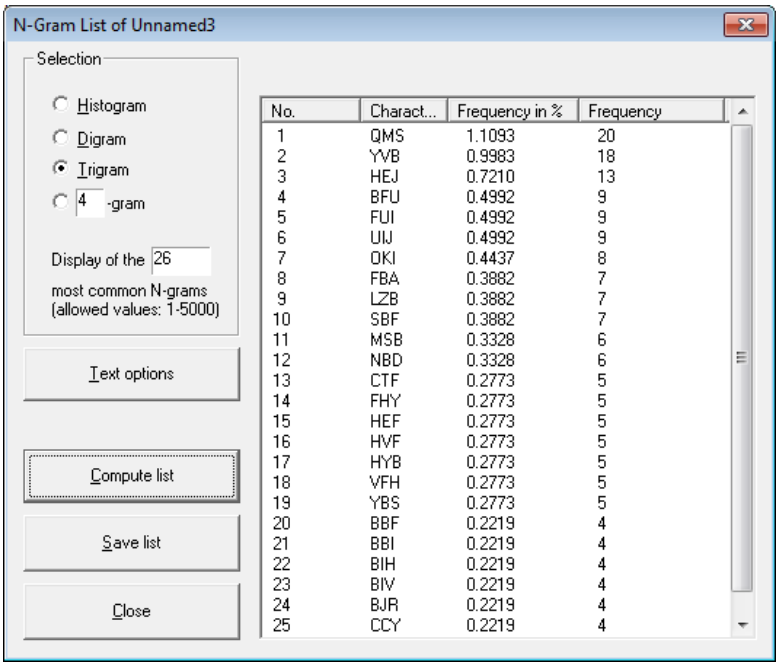
- Από το μενού επιλέγουμε διαδοχικά: **File → New** και εισάγουμε το παρακάτω κρυπτοκείμενο, για το οποίο γνωρίζουμε ότι προέκυψε από αρχικό κείμενο στην Αγγλική γλώσσα με χρήση του αλγόριθμου Vigenere. Όμως, δεν γνωρίζουμε το κλειδί που χρησιμοποιήθηκε, ούτε το μήκος του.

```
TBZJIMTBXYWJJKENZBBOIPWKLHEWCRLVQMSCTFBXHXHSOYOFSAXSTLZBAFMLZ
BDJODQSEJHLTYFYVLRSXSRMZHFYWKMWPGOOSMXWRTMSOJWQXCLSZBFFKJRQTS
XYQENQHJBCJSAFBAYCYJVXASXXQENQHJBPGSEFJBTBBIOVFBXYIOFZFXHTMCT
FGMFGPNBDGMFSERNFBICCYVBTKKJFTMMFYKXXHEFHXSSXLZBYVBPWKLCCFZIG
WOIGPMCRQRYJQLSTFSSAYCINJBNBQMSYFFKDOOIKFYVQMSZMWZPSKXGFSQBNV
XASDNJBSWQHVFHYBSTBJRXSRQWOFSSANHQTPBFQENQHJBFYVXXBBASOQSXWBB
IHLKZVWSMQWBIHEJCTSSONHYJVXASPFGZMWZPSKXPBMOSJGLNHFXBLQCKLSOF
BBFUIJGQNZINBPNGQJRQMSKFHRWOINGQNHEFGQMSEJOOYCCFBBFUIJOKIQXSG
RWSIDPBYORLVQYCCQMXKHBWHXQYFSUFYCSJFQMSQBCJJBXLFBJRQTTFSRLZHT
MSQMSOYVFXKXXDLXGFGZBLSKYZVYVBSOQZFXQWPYHLTYQMSBFUIJWKMWPFFJX
OKIGXNRVTIYJZLSUQTHEJGHDOKIBLYHLYVBJOOYVPYFBYQEKCOYVVTIOBWKLG
XSRCQMQMSBFUIJVLBSSJFTFGZTBCZGBIVBIWASCQPBLBKETVBBOPFBAXSBNBD
YVBHVFHYBSGBFHFSUQMSFWTBJREJXRRDBIRLBBQTPBBWQMHEJAXLOFSIKIWPR
OVJRQMSKFHRWOINGQYCLPHEJSXLZBTBQMSCTZITKFSUAFMRUCKYVBWCLKCCYV
BMCRXSXSRRWUBIVFRODFWKDCRFFBFBBFUIJGQWSQHVCTFQMMLZFTNBDXOKITI
DPRYHEJSXLZBBOPFTOFWATTENGRSYKTKKXSIKOKIKLWZAFBAOIJUSAICTSCKH
SJTFBKCOYVBHVFHYBSTBJRLSHEJHENFAIOVYVBSOQZFXQWPYFLXSBFFIDOKIH
LTYQMSBFUIJCRYCCYVBGOOSMXWRQTOENUERCRSHXNBQMSOJVBMSIIHEJYFSUL
KPFWRPMWDMOYTJBMWJFBAJBZTIOFUBIVFRODFWKXOVNBDDCRFFBFBBFUIJMLZ
```

```
PBQCKLHLYVBXYVFGTJZIFGQMSBFFQMGQWSQHVCTFQMMLZFTNBDXBLBOKITIDH
EJSXLZBQCLPSAFFLZBAGOZPHLBOOIHEJPXWBVFFAFBAZDQTHEJGHDGQNZIMSA
NRKTHCQMQMSKYVBSOQZFXQWPYZFKHBIVFRGQWOFLVQYCTFFAYVBXIKFBANHEF
DMJBBIHEFHQMSBFUIJPBLOKYCQWSJGZBFBAXZLBZVMSPYFBYQEJRENGTNBDXO
QQOPYKFYVXYFFZAMMOKYQODVBXCXWSAFKXDWKYCQMSEJOSJBPNHJFMYJHEFHQ
MSBFUIJGQNZIWSJJAYJFPYVBHVFHYBSGTNHESCPYOILWXNHJFMBASKGSQMOQM
SLHQXXWLSOIQMOJJFXWQXHEJPXWBVFFAGIQFGCFFXXOKDCKJYKTKPMSEFGKJJ
BWFBYIOSSAYCIJOAYVBQWCJCCFQENQHJBEJKXXOKJODQSBASKYVLZUEMSEFRY
JSKPSMYOKIHXRSAFGXHVFHYBSXRXHINYBYVBJODQSMJCMQSTMCEFJBQSXWBBI
HLYVFSYLKHEJAPJZSJGXXGLRSQMWKLHEJMXWSKYQXSFBISZNRBNBCFJLWCCYV
BNFOJOIUCQJBQNOIYVBDQXSPBHCJJKFSBBWG
```

Επιλέγουμε από το μενού: **Analysis → Tools for Analysis → N-Gram**

- Στο πεδίο Selection επιλέγουμε **Trigram** και στη συνέχεια Compute List ώστε να εμφανίσουμε τις συχνότητες εμφάνισης συνδυασμών τριών γραμμάτων, που υπάρχουν στο κρυπτογραφημένο κείμενο (Εικόνα 6.17).



Εικόνα 6.17 *Συχνότητες εμφάνισης συνδυασμών τριών γραμμάτων.*

Αντίστοιχα με τον τρόπο που εργαστήκαμε στην περίπτωση του Καίσαρα, μπορούμε να βρούμε στη διεθνή βιβλιογραφία σχετικές έρευνες για τις συχνότητες εμφάνισης συνδυασμών των γραμμάτων σε κείμενα της Αγγλικής γλώσσας (π.χ. digrams, trigrams κ.λπ.). Από την εξέταση αυτών των ερευνών προκύπτει ότι η πιο συχνά εμφανιζόμενη είναι η τριάδα «THE». Υποθέτοντας πως και στο αρχικό κείμενο η πιο συχνά εμφανιζόμενη τριάδα ήταν η τριάδα «THE», θα μπορούσαμε να εντοπίσουμε τη λέξη-κλειδί. Παρατηρούμε ότι η ακολουθία γραμμάτων «QMS» εμφανίζεται 20 φορές στο κρυπτοκείμενο. Περισσότερες από κάθε άλλη. Υποθέτουμε λοιπόν ότι η τριάδα «QMS» αποτελεί το κρυπτογράφημα της λέξης «THE».

Ας προχωρήσουμε σε μια προσπάθεια επιβεβαίωσης της υπόθεσης αυτής. Για τη διευκόλυνση της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης με τη χρήση του Vigenere, χρησιμοποιείται ο πίνακας Vigenere Square (Πίνακας 6.2) όπου:

- Επιλέγουμε τη γραμμή που αντιστοιχεί σε κάθε χαρακτήρα του αρχικού κειμένου.
- Επιλέγουμε τη στήλη που αντιστοιχεί σε κάθε χαρακτήρα του κλειδιού.

- Το κρυπτογράφημα προκύπτει από το χαρακτήρα που βρίσκονται στην τομή της παραπάνω γραμμής και στήλης.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	R	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	I	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	Z	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	U
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	V
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Z

Πίνακας 6.2 *Ο πίνακας Vigenere Square*.

Ομοίως, γνωρίζοντας το αρχικό κείμενο και το κρυπτογράφημα, εντοπίζουμε τους χαρακτήρες του κλειδιού στις αντίστοιχες στήλες. Για το παράδειγμα που εξετάζουμε, έχουμε:

- Ο χαρακτήρας T για να κρυπτογραφηθεί ως Q θα πρέπει να χρησιμοποιηθεί η σειρά X, άρα ο πρώτος χαρακτήρας από τη λέξη-κλειδί είναι ο X.

- Ο χαρακτήρας H για να κρυπτογραφηθεί ως M θα πρέπει να χρησιμοποιηθεί η σειρά F, άρα ο δεύτερος χαρακτήρας από τη λέξη κλειδί είναι ο F.

- Ο χαρακτήρας E για να κρυπτογραφηθεί ως S θα πρέπει να χρησιμοποιηθεί η σειρά W, άρα ο δεύτερος χαρακτήρας από τη λέξη κλειδί είναι ο W.

Άρα, θεωρούμε πως το κλειδί είναι η ακολουθία «XFW».

Στην εφαρμογή Cryptool επιλέγουμε ως ενεργό το παράθυρο με το κρυπτοκείμενο και επιλέγουμε από το μενού: **Encrypt / Decrypt → Symmetric (classic) → Vigenere**, εισάγουμε ως κλειδί τη λέξη XFW και πατάμε Decrypt.

Παρατηρούμε ότι το αποκρυπτογραφημένο κείμενο παραμένει ακατανόητο και επομένως η λέξη-κλειδί που επιλέξαμε δεν ήταν σωστή. Η επιλογή της προήλθε από την αρχική μας εκτίμηση ότι η λέξη THE

αντιστοιχεί στη λέξη QMS. Συνεχίζοντας τη συλλογιστική, μπορούμε να υποθέσουμε ότι στο συγκεκριμένο κείμενο, η λέξη THE δεν ήταν η πιο συχνά εμφανιζόμενη αλλά ήταν η δεύτερη πιο συχνή.

Προχωράμε με αυτή τη δεύτερη υπόθεση, όπου αντίστοιχα επιλέγουμε το δεύτερο κατά σειρά πιο συχνά εμφανιζόμενο συνδυασμό τριών γραμμάτων: τη λέξη YVB.

- Επαναλαμβάνουμε τα βήματα 5 έως και 7 για να διαπιστώσουμε ότι εμφανίζεται ένα αποκρυπτογραφημένο κείμενο με νόημα και να επιβεβαιώσουμε έτσι την ορθότητα της υπόθεσής μας, για τη λέξη-κλειδί που προκύπτει (FOX).

Η παραπάνω υπόθεση στηρίχθηκε, αρχικά, στη διαπίστωση πως αν υπάρχει σημαντικός αριθμός εμφανίσεων ενός συνδυασμού τριών γραμμάτων, τότε ίσως το μέγεθος της λέξης κλειδιού είναι τρία. Τι θα γινόταν όμως αν το μέγεθος της λέξης-κλειδί ήταν μεγαλύτερο;

Σε μια πιο αποτελεσματική τεχνική, αναζητούμε ακολουθίες γραμμάτων που εμφανίζονται περισσότερο από μια φορά στο κρυπτοκείμενο. Η πιο πιθανή αιτία για αυτές τις επαναλήψεις είναι ότι η ίδια ακολουθία γραμμάτων του αρχικού κειμένου έχει κρυπτογραφηθεί επανειλημμένα, χρησιμοποιώντας το ίδιο μέρος του κλειδιού. Ένα σημαντικό εργαλείο σε αυτή την προσπάθεια είναι το εργαλείο αυτοσυσχέτισης (autocorrelation) που διαθέτει το Cryptool.

Η εύρεση της απόστασης από τη μια εμφάνιση μιας ακολουθίας γραμμάτων μέχρι την επόμενη επανάληψή της, ενδεχομένως, μας παρέχει χρήσιμες πληροφορίες για το μέγεθος του κλειδιού. Η απόσταση αυτή ή κάποια από τις ενδιάμεσες τιμές που προκύπτουν από την παραγοντοποίησή της, μπορεί να ισούται με το μέγεθος του κλειδιού. Αν το γνωρίζαμε αυτό, τότε απλά θα χωρίζαμε το κρυπτογράφημα σε τμήματα ίσα με το μέγεθος του κλειδιού και θα τα τοποθετούσαμε ως τις γραμμές ενός πίνακα με τόσες στήλες όσες και το υποτιθέμενο μέγεθος του κλειδιού. Ένα τέτοιο παράδειγμα βλέπουμε στον πίνακα 6.3, για το αρχικό τμήμα του παραπάνω κρυπτοκειμένου και με την υπόθεση ότι το μέγεθος του κλειδιού είναι 3 γράμματα.

T	B	Z
J	I	M
T	B	X
Y	W	J
J	K	E
N	Z	B
B	O	I
P	W	K
L	H	E

Πίνακας 6.3 *Υπόθεση για κλειδί μεγέθους τριών (3) γραμμάτων.*

Στη συνέχεια, χειριζόμαστε κάθε στήλη (σας θυμίζει την περίπτωση της Σπαρτιατικής σκυτάλης;) ως ξεχωριστό κρυπτοκείμενο και εφαρμόζουμε την κρυπταναλυτική τεχνική της υποενότητας 6.5.1.2 (πρόβλημα μονοαλφαβητικής αντικατάστασης). Αφού ολοκληρώσουμε διαδοχικά για κάθε στήλη, ανατοποθετούμε όλα τα γράμματα του πίνακα σε μια γραμμή, οπότε διαβάζουμε το ανακτημένο αρχικό κείμενο.

Βιβλιογραφία

Kahn, D. (1996). The codebreakers: the story of secret writing (Rev. ed.). New York: Scribner.

Manuel, M. (2008). Cryptography and Security Services: Mechanisms and Applications: Mechanisms and Applications. IGI Global.

Mollin, R. A. (2005). Codes: the guide to secrecy from ancient to modern times. Boca Raton: Chapman & Hall/CRC.

Oppliger, R. (2011). Contemporary Cryptography, Second Edition. Artech House.

Stallings, W. (2014a). Cryptography and network security: principles and practice (Seventh edition). Boston: Pearson.

Κριτήρια Αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Η στεγανογραφία χρησιμοποιείται με σκοπό:
α) Την προστασία της ταυτότητας του αποστολέα.
β) Την προστασία της διαθεσιμότητας της πληροφορίας.
γ) Τη μεταφορά ενός μηνύματος χωρίς η ύπαρξή του να γίνει αντιληπτή.
δ) Την προστασία της ιδιοκτησίας.

2. Ένα υδατογράφημα προκύπτει από την εφαρμογή μεθόδων:
α) Στενογραφίας.
β) Στεγανογραφίας.
γ) Κρυπτογραφίας.
δ) Κρυπτανάλυσης.

3. Η διαδικασία της στεγανάλυσης:
α) Απαιτεί ένα κλειδί κρυπτογράφησης.
β) Απαιτεί ένα κλειδί στεγανογραφίας.
γ) Εφαρμόζεται με σκοπό την αποκάλυψη του μηνύματος.
δ) Εφαρμόζεται με στόχο την απόκρυψη του μηνύματος.

4. Στην κρυπτογραφία μυστικού κλειδιού, για κάθε επικοινωνία μεταξύ δυο οντοτήτων απαιτείται:
α) Ένα κοινό κλειδί.
β) Ένα ζεύγος κλειδιών.
γ) Δύο ζεύγη κλειδιών.
d) Ένα ιδιωτικό κλειδί.

5. Το κλειδί κρυπτογράφησης
α) Είναι μέρος του αλγορίθμου κρυπτογράφησης.
β) Χρησιμοποιείται από τον αλγόριθμο κρυπτογράφησης.
γ) Είναι πάντα δημόσιο.
δ) Είναι κρυπτογραφημένο.

6. Στην κρυπτογραφία δημοσίου κλειδιού:
α) Ότι κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα αποκρυπτογραφείται με το ιδιωτικό κλειδί του παραλήπτη.
β) Ότι κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα.
γ) Ότι κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα.
δ) Ότι κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη αποστολέα αποκρυπτογραφείται με το ιδιωτικό κλειδί του παραλήπτη.

7. Οι κρυπτογραφικοί αλγόριθμοι ροής:
α) Κρυπτογραφούν δέσμες δεδομένων.
β) Κρυπτογραφούν τα δεδομένα bit προς bit.
γ) Είναι ταχύτεροι από τους αλγόριθμους δέσμης.
δ) Δεν απαιτούν κλειδί κρυπτογράφησης.

8. Ο κρυπτογραφικός αλγόριθμος του Καίσαρα:
α) Είναι αλγόριθμος δημοσίου κλειδιού.
β) Χρησιμοποιεί κλειδί κρυπτογράφησης.
γ) Είναι αλγόριθμος πολυαλφαβητικής αντικατάστασης.
δ) Είναι συμμετρικός αλγόριθμος.

9. Ο Binary-Exclusive XOR που περιέχεται στο Cryptool:
α) Είναι αλγόριθμος δέσμης.
β) Είναι αλγόριθμος ροής.
γ) Είναι αλγόριθμος στεγανογραφίας.
δ) Χρησιμοποιεί πύλες XOR σε παράλληλη σύνδεση.

10. Το δημόσιο κλειδί:
α) Παραμένει το ίδιο μυστικό όπως και το ιδιωτικό.
β) Διανέμεται ελεύθερα.
γ) Περιέχει το ιδιωτικό κλειδί.
δ) Χρησιμοποιείται για κρυπτογράφηση μόνο.

Δραστηριότητα 1

Αναζητήστε στη βιβλιογραφία παραδείγματα στεγανογραφικών μεθόδων. Προσπαθήστε να αποκρύψετε το δικό σας μήνυμα με χρήση της στεγανογραφίας.

Δραστηριότητα 2

Δημιουργήστε το δικό σας αλγόριθμο κρυπτογράφησης. Περιγράψτε τον και χρησιμοποιήστε τον για να αποστείλετε ένα κρυπτογραφημένο μήνυμα. Στη συνέχεια εξετάστε πόσο ισχυρός είναι ο αλγόριθμος που σχεδιάσατε.

Δραστηριότητα 3

Στο Cryptool επιλέξτε Individual Procedures → Visualization of Algorithms και επιλέξτε την οπτικοποίηση των αλγόριθμων Caesar και Vigenere για να μελετήσετε μια διαδραστική παρουσίαση των αλγόριθμων.

Δραστηριότητα 4

Στο Cryptool επιλέξτε Individual Procedures → Visualization of Algorithms και επιλέξτε την επιλογή Enigma. Η Enigma αποτέλεσε μια κρυπτομηχανή βασισμένη σε υλικό. Ανατρέξτε στη βιβλιογραφία και με τη βοήθεια της οπτικοποίησης μελετήστε τη χρήση της.

Συγκριτική Αξιολόγηση

Θεωρήστε ότι θέλετε να αποστείλετε μια φωτογραφία σε έναν παραλήπτη, η οποία όμως δεν πρέπει να γίνει αντιληπτή από κανέναν πλην αυτού. Σκεφτείτε και καταγράψτε σε ποιες περιπτώσεις θα ήταν επιθυμητή η αποστολή της ως κρυπτογραφημένου μηνύματος και σε ποιες η αποστολή της μέσα σε μία άλλη φωτογραφία ή άλλο αρχείο, με χρήση τεχνικών στεγανογραφίας.

Κεφάλαιο 7. Σύγχρονοι Κρυπτογραφικοί Αλγόριθμοι

Σύνοψη

Στο κεφάλαιο αυτό, θα παρουσιαστούν ορισμένοι από τους γνωστούς σύγχρονους συμμετρικούς και ασύμμετρους κρυπτογραφικούς αλγορίθμους. Με τον όρο σύγχρονοι, αναφερόμαστε σε αλγόριθμους που χρησιμοποιούνται σήμερα σε υλοποιήσεις κρυπτοσυστημάτων με τη χρήση υπολογιστών. Επομένως, δεν επεξεργαζόμαστε απλά κείμενα, όπως στους κλασσικούς κρυπτογραφικούς αλγορίθμους, αλλά τη δυαδική αναπαράσταση των μηνυμάτων, δηλαδή τα bit με τα οποία αναπαρίσταται κάθε μήνυμα σε έναν υπολογιστή. Μετά την σύντομη παρουσίαση των αλγορίθμων, παρουσιάζεται η χρήση τους με τη βοήθεια του εργαλείου Cryptool, είτε από τη μεριά του νόμιμου χρήστη είτε από τη μεριά του κρυπταναλυτή, έτσι ώστε ο αναγνώστης να αποκτήσει μια ολοκληρωμένη εικόνα για τη δομή και τη λειτουργία των αλγορίθμων αυτών.

Προαπαιτούμενη γνώση

Για την κατανόηση του κεφαλαίου, προτείνεται η ολοκλήρωση της μελέτης του Κεφαλαίου 6, όπου παρατίθενται οι βασικές αρχές της κρυπτογραφίας.

7.1 Εισαγωγή

Η εφαρμογή των δύο κλασσικών κρυπτογραφικών αλγορίθμων που εξετάστηκαν στο προηγούμενο κεφάλαιο είναι εφικτή μόνο σε κείμενα, δηλαδή σε συμβολοσειρές. Επίσης η διαδικασία της κρυπτανάλυσης είναι σχετικά απλή και οδηγεί σε αποτελέσματα σε σύντομο χρονικό διάστημα. Στην περίπτωση που το μήνυμα το οποίο αποστέλλεται από τη μία οντότητα στην άλλη, έχει μια σύνθετη μορφή (π.χ. εκτελέσιμο πρόγραμμα) και οι ανάγκες εμπιστευτικότητας είναι αυξημένες, επιβάλλεται η ψηφιακή επεξεργασία με την εφαρμογή σύγχρονων κρυπτογραφικών αλγορίθμων που έχουν σχεδιαστεί με αντικείμενο τια ανάγκες των σύγχρονων επικοινωνιακών συστημάτων

Το βασικό σενάριο σε μια κρυπτογραφημένη επικοινωνία είναι:

- Έστω δύο επικοινωνούντα μέρη, που τα ονομάζουμε Αλίκη και Βασίλη.
- Η Αλίκη κρυπτογραφεί το αρχικό κείμενο Μ χρησιμοποιώντας ένα κλειδί Κ και παράγει το κρυπτοκείμενο C.
- Το κρυπτοκείμενο C μεταδίδεται στον Βασίλη, ο οποίος το παραλαμβάνει και το αποκρυπτογραφεί για να ανακτήσει το αρχικό κείμενο Μ, εφόσον γνωρίζει το κλειδί αποκρυπτογράφησης.
- Ένας κακόβουλος χρήστης, έστω η Ελένη, μπορεί να καταφέρει να υποκλέψει το κρυπτοκείμενο, ωστόσο ο αλγόριθμος κρυπτογράφησης θα πρέπει να εγγυάται ότι δεν πρόκειται να καταφέρει να το μετατρέψει σε μια μορφή κατανοητή ώστε να μπορέσει να το διαβάσει, διαφυλάσσοντας έτσι τη μυστικότητα του μεταδιδόμενου μηνύματος.

Όπως έχει αναφερθεί στο προηγούμενο κεφάλαιο, το πλεονέκτημα των συμμετρικών αλγορίθμων είναι η ταχύτητα επεξεργασίας ακόμη και όταν πρόκειται για μεγάλα σε μέγεθος μηνύματα, αλλά το μειονέκτημά τους αφορά τον τρόπο διανομής του μυστικού κλειδιού μεταξύ της Αλίκης και του Βασίλη, διαφυλάσσοντας τη μυστικότητά του από την Ελένη. Επιπλέον, όπως είδαμε στο προηγούμενο κεφάλαιο, αν έχουμε n οντότητες που θέλουν να επικοινωνήσουν ανά δυο, απαιτούνται συνολικά n(n-1)/2 μυστικά κλειδιά (π.χ. για 2 μέρη χρειάζεται 1, αλλά για 11 μέρη χρειάζονται 55 κλειδιά). Αυτό σημαίνει ότι το πλήθος των απαιτούμενων κλειδιών που θα πρέπει να διατηρεί κάθε οντότητα αυξάνει γεωμετρικά, όσο αυξάνει το πλήθος των υπόλοιπων οντοτήτων.

Το 1976, οι W.Diffie και M.E.Hellman δημοσίευσαν την εργασία τους με το τίτλο «New Directions in Cryptography», όπου, προσπαθώντας να δώσουν λύση στο παραπάνω μειονέκτημα των συμμετρικών

κρυπτογραφικών αλγορίθμων, πρότειναν μια νέα μέθοδο διανομής κλειδιών, που έγινε γνωστή ως ανταλλαγή κλειδιών των Diffie και Hellman (Diffie–Hellman key exchange) και έβαλε τα θεμέλια της κρυπτογραφίας δημοσίου κλειδιού. Στη νέα προσέγγιση της κρυπτογραφίας δημόσιου κλειδιού, κάθε επικοινωνούν μέρος κατέχει δυο κλειδιά: ένα δημόσιο κλειδί (K+) και ένα ιδιωτικό κλειδί (K-). Έτσι, αν η Αλίκη επιθυμεί να στείλει με ασφάλεια ένα μήνυμα M στο Βασίλη, το κρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί (K_B+) του Βασίλη. Στη συνέχεια, ο Βασίλης είναι ο μόνος ο οποίος μπορεί να αποκρυπτογραφήσει το κρυπτοκείμενο, χρησιμοποιώντας το ιδιωτικό κλειδί του (K_B-). Πλέον, κάθε οντότητα διαθέτει το δικό της ζεύγος κλειδιών, απλοποιώντας το πρόβλημα της επικοινωνίας ανά δυο, όπου για n οντότητες απαιτούνται 2n κλειδιά μόνο. Όμως, η κρυπτογράφηση δημόσιου κλειδιού είναι σημαντικά πιο αργή σε σχέση με τη συμμετρική κρυπτογράφηση, ακόμη και για μικρά σε μέγεθος μηνύματα.

Για τους παραπάνω λόγους, προκύπτει η ανάγκη συνδυασμένης χρήσης των κρυπτογραφιών συμμετρικού κλειδιού και δημοσίου κλειδιού, ώστε όταν πρόκειται να κρυπτογραφηθεί μεγάλη ποσότητα πληροφοριών να χρησιμοποιείται ένα συμμετρικό κρυπτοσύστημα, ενώ για την ασφαλή ανταλλαγή του μυστικού κλειδιού (συνόδου) να χρησιμοποιείται ένα κρυπτοσύστημα δημοσίου κλειδιού.

7.2 Συμμετρικά Κρυπτοσυστήματα

Ένα παράδειγμα συνδυασμένης χρήσης συμμετρικών και ασύμμετρων αλγορίθμων θα μελετήσουμε σε επόμενο κεφάλαιο. Προς το παρόν, ας εξετάσουμε τρεις από τους πιο γνωστούς συμμετρικούς αλγορίθμους, που χρησιμοποιούνται σήμερα ευρέως, δηλαδή τον αλγόριθμο DES (Data Encryption Standard), τη μετεξέλιξή του 3DES (triple-DES) και το νεώτερο αλγόριθμο AES (Advanced Encryption Standard). Ακόμη, θα εξετάσουμε τον ασύμμετρο αλγόριθμο.

7.2.1 DES

Ο κρυπτογραφικός αλγόριθμος Data Encryption Standard (DES) είναι ένας συμμετρικός αλγόριθμος δέσμης, ο οποίος υιοθετήθηκε ως το επίσημο πρότυπο (Federal Information Processing Standard) FIPS 46 των ΗΠΑ το 1977.

Το 1973, στο πλαίσιο ενός προγράμματος που είχε ξεκινήσει ένα χρόνο νωρίτερα, ο οργανισμός NIST (τότε γνωστός ως NBS) δημοσίευσε μια πρόσκληση για υποβολή προτάσεων για ένα νέο αλγόριθμο συμμετρικού κλειδιού, ο οποίος θα αποτελούσε το νέο πρότυπο κρυπτογράφησης σε εθνικό επίπεδο και θα έπρεπε να πληροί τα ακόλουθα κριτήρια:

- Να παρέχει υψηλό επίπεδο ασφάλειας.
- Να είναι πλήρως τεκμηριωμένος και εύκολα κατανοητός
- Η ασφάλειά του να βασίζεται στο κλειδί και όχι στη μυστικότητα του ίδιου του αλγορίθμου.
- Να είναι διαθέσιμος σε όλους τους χρήστες.
- Να είναι προσαρμόσιμος για χρήση σε ποικίλες εφαρμογές.
- Να είναι υλοποιήσιμος με χαμηλό κόστος.
- Να είναι αποδοτικός.
- Να μπορεί να επικυρωθεί.

Αν και αρχικά καμμιά από τις προτάσεις που κατατέθηκαν δεν πληρούσε το σύνολο των κριτηρίων, μετά από μια δεύτερη πρόσκληση, η πρόταση που επικράτησε βασίστηκε στον αλγόριθμο Lucifer της IBM, ο οποίος, μετά από ορισμένες τροποποιήσεις και τη διευθέτηση ορισμένων θεμάτων αδειοδότησης και χρήσης, έγινε δεκτός με το όνομα DES. Ο αλγόριθμος DES δέχτηκε επικρίσεις για δύο κυρίως λόγους:

- Διέθετε μικρό μήκος κλειδιού (56 bits), αρκετά μειωμένο σε σχέση με το κλειδί μήκους 128 bit του Lucifer. Το γεγονός αυτό καθιστούσε τον αλγόριθμο ευάλωτο σε επιθέσεις εξαντλητικής αναζήτησης (brute-force attacks).

- Υπήρχε μυστικότητα και αδιαφάνεια σχετικά με κάποιο τμήμα του σχεδιασμού της εσωτερικής δομής του. Οι επικριτές υποστήριζαν πως το τμήμα της αρχιτεκτονικής του αλγόριθμου που αφορούσε τα S-box (θα παρουσιαστούν στη συνέχεια), τα οποία προέκυψαν από μεταβολή αυτών του Lucifer, επέτρεπε την ύπαρξη «κερκόπορτας» (backdoor), ώστε να παρέχεται η δυνατότητα άμεσης αποκρυπτογράφησης, χωρίς την ανάγκη της γνώσης του κάθε επιμέρους μυστικού κλειδιού. Αργότερα, οι συμμετέχοντες ερευνητές δήλωσαν πως οι αλλαγές στην εσωτερική δομή αφορούσαν όντως μόνο τα S-box, αλλά έγιναν στο πλαίσιο μιας προσπάθειας απομάκρυνσης ορισμένων ευπαθειών που αναγνωρίσθηκαν κατά τη διαδικασία επιβεβαίωσης (validation) του αλγορίθμου.

Ο DES είναι ένας αλγόριθμος που υλοποιεί μια δομή Feistel με 16 κύκλους εκτέλεσης. Σε κάθε κύκλο χρησιμοποιείται ένα υποκλειδί μήκους 48 bit, που παράγεται από το μυστικό κλειδί. Το τελευταίο εκφράζεται συνήθως με τη χρήση 64bit, από τα οποία όμως κάθε όγδοο bit αγνοείται καθώς χρησιμοποιείται μόνο για έλεγχο ισοτιμίας. Το αρχικό κείμενο διαχωρίζεται σε δέσμες (block) των 64 bit και παράγονται δέσμες κρυπτοκειμένου του ίδιου μήκους (64 bit). Αντιστρόφως, κατά την αποκρυπτογράφηση, οι δέσμες κρυπτοκειμένου μήκους 64 bit αποτελούν, μαζί με το ίδιο μυστικό κλειδί, την είσοδο στη διαδικασία αποκρυπτογράφησης και παράγονται δέσμες αρχικού κειμένου με μήκος πάλι 64 bit.

Στη συνέχεια θα περιγραφούν:

- η μεθοδολογία δημιουργίας υποκλειδιών και
- η επεξεργασία της δέσμης του αρχικού κειμένου για την παραγωγή της αντίστοιχης δέσμης του κρυπτογραφήματος.

7.2.1.1 Δημιουργία υποκλειδιών

Για να παραχθούν τα 16 κλειδιά μήκους 48bit, ακολουθείται η εξής διαδικασία:

- Στο αρχικό κλειδί μήκους 64bit, εφαρμόζεται μια αρχική μετάθεση (permutation), όπου κάθε όγδοο bit αγνοείται και τα υπόλοιπα 56 επανατοποθετούνται, σύμφωνα με τον πίνακα PC1 (Permuted Choice One) που φαίνεται στον Πίνακα 7.1.

- Στη συνέχεια, το κλειδί των 56bit χωρίζεται σε δυο τμήματα: το αριστερό C_0 και το δεξί D_0, μήκους 28bit (Πίνακας 7.1).

- Σε κάθε έναν από τους 16 κύκλους εκτέλεσης του DES:
  - Τα τμήματα C_{i-1} και D_{i-1} υπόκεινται σε κυκλική αριστερή ολίσθηση, κατά
    - 1 bit στους κύκλους 1, 2, 9 και 16,
    - 2 bit σε όλους τους υπόλοιπους.

    για να προκύψουν τα τμήματα C_i και D_i
  - Στα τμήματα C_i και D_i συνενώνονται και εφαρμόζεται μια τελική επιλογή και μετάθεση, σύμφωνα με τον πίνακα PC2 (Permuted Choice Two) που φαίνεται στον Πίνακα 7.2, για να προκύψει το υποκλειδί K_i του κύκλου, μήκους 48 bits.

C	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
D	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

Πίνακας 7.1 *Πίνακας PC1.*

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Πίνακας 7.2 *Πίνακας PC2.*

7.2.1.2 Επεξεργασία δέσμης αρχικού κειμένου

Ο αλγόριθμος DES επεξεργάζεται ένα αρχικό κείμενο, αφού πρώτα το χωρίσει σε δέσμες μήκους 64 bit. Σε κάθε δέσμη εφαρμόζεται μια αρχική μετάθεση (Initial Permutation), σύμφωνα με τον πίνακα αρχικής μετάθεσης IP (Πίνακας 7.3). Μετά την αρχική μετάθεση, η κάθε δέσμη χωρίζεται σε δύο υποδέσμες, την αριστερή L_0 που αποτελείται από τα πρώτα 32 bit και τη δεξιά R_0 που αποτελείται από τα υπόλοιπα 32.

Οι υποδέσμες L_0 και R_0 γίνονται είσοδοι σε μια δομή Feister με 16 κύκλους επεξεργασίας, όπου στον i-οστό κύκλο έχουμε:

- Η δεξιά υποδέσμη γίνεται η επόμενη αριστερή υποδέσμη ($L_i = R_{i-1}$).

- Εφαρμόζεται μετάθεση και επέκταση της δεξιάς υποδέσμης R_{i-1}, ώστε να αποκτήσει μήκος 48bit, σύμφωνα με τον πίνακα Επέκτασης Μετάθεσης (Expansion Permutation), που φαίνεται στον Πίνακα 7.4.

- Υπολογίζεται η πράξη XOR με εισόδους τα R_{i-1} και K_i.

- Το αποτέλεσμα της πράξης XOR, μήκους 48bit, χωρίζεται σε 8 εξάδες και κάθε μια χρησιμοποιείται ως είσοδος ενός από τα 8 S-box, που φαίνονται στον Πίνακα 7.5, το οποίο παράγει έξοδο μήκους 4bit, ως εξής:

    - Από την εξάδα bit, επιλέγεται το πρώτο και το έκτο bit για να διαμορφώσουν μια δυάδα bit, η οποία καθορίζει τη γραμμή του S-box.

    - Από την εξάδα bit, επιλέγονται τα τέσσερα ενδιάμεσα bit για να διαμορφώσουν μια δυάδα bit, η οποία καθορίζει τη στήλη του S-box.

    - Το περιεχόμενο του κελιού του S-box που καθορίζεται από την παραπάνω γραμμή και στήλη, θα αποτελέσει την έξοδο του S-box.

  Έτσι, αν η εξάδα 100110 αποτελέσει την είσοδο του πρώτου S-box (S1), τότε θα επιλεγεί το περιεχόμενο του κελιού, που αντιστοιχεί στη δεύτερη γραμμή (10) και στην τρίτη στήλη (0011), είναι 8. Άρα, στην έξοδο το αποτέλεσμα θα είναι τα bit: 1000. Για την επιλογή γραμμής και στήλης θυμηθείτε ότι μετράμε ξεκινώντας από το μηδέν (0).

- Στη συνέχεια, οι οκτώ τετράδες από bit συνενώνονται (συνολικά 8x4 = 32bit) και εφαρμόζεται μια τελική μετάθεση, σύμφωνα με τον πίνακα μετάθεσης P που φαίνεται στον Πίνακα 7.6, για να προκύψει η νέα δεξιά υποδέσμη R_{i-1}.

- Η επόμενη δεξιά υποδέσμη προκύπτει από τον υπολογισμό της πράξης XOR με εισόδους τα R_{i-1} και L_{i-1} ($R_i = R_{i-1} \oplus L_{i-1}$).

- Στα 64 bit που τελικά προκύπτουν από τη συνένωση των υποδεσμών L_{16} και R_{16}, εφαρμόζεται μια μετάθεση, σύμφωνα με τον ανάστροφο πίνακα της αρχικής μετάθεσης (Inverse Permutation – IP^{-1}), που φαίνεται στον Πίνακα 7.6, ώστε να προκύψει η κρυπτογραφημένη δέσμη.

L_0	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
R_0	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

Πίνακας 7.3 *Πίνακας IP.*

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Πίνακας 7.4 *Πίνακας επέκτασης E.*

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Πίνακας 7.5 *S-boxes.*

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Πίνακας 7.6 *Πίνακας μετάθεσης P.*

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Πίνακας 7.7 *Πίνακας Inverse Permutation IP^{-1}.*

7.2.1.3 3DES

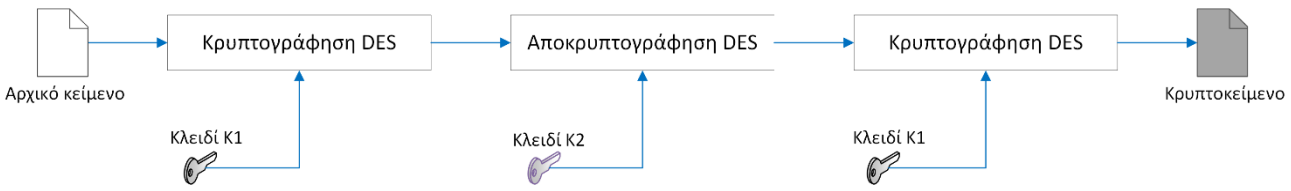
Όπως αναφέρθηκε παραπάνω, το μικρό σε μέγεθος μήκος κλειδιού του DES διευκολύνει τις επιθέσεις εξαντλητικής αναζήτησης (brute-force attack). Η αρχική προσέγγιση προς τη βελτίωση του αλγορίθμου ήταν η χρήση ενός δεύτερου, ώστε το αποτέλεσμα της πρώτης κρυπτογράφησης με DES να κρυπτογραφείται εκ νέου με DES αλλά με το δεύτερο κλειδί, ώστε από το αρχικό μήνυμα M να προκύψει το κρυπτογράφημα $C=E_{DES}(K_2, E_{DES}(K_1,M))$. Με αυτό τον τρόπο, υλοποιείται ο Double DES και το μήκους του κλειδιού πλέον θεωρείται ότι αυξήθηκε στα 112bit.

Τα προβλήματα που ενδέχεται να παρουσιάζει η προσέγγιση αυτή είναι:

- Η περίπτωση να υπάρχει κλειδί K', τέτοιο ώστε $C=E_{DES}(K_2, E_{DES}(K_1,M))= E_{DES}(K',M)$. Στην περίπτωση αυτή θα αρκούσε η εύρεση ενός κλειδιού K'. Η περίπτωση αυτή έχει αποκλειστεί από τους Campbell και Wiener το 1992.

- Είναι δυνατό να υπάρχει $X=E_{DES}(K_1,M)=D_{DES}(K_2,C)$. Για ένα γνωστό ζεύγος M, C, κρυπτογραφούμε το M για κάθε πιθανή τιμή του K_1. Στη συνέχεια, αποκρυπτογραφούμε το C με κάθε πιθανή τιμή του K_2. Αν από τη διαδικασία προκύψουν δύο ίδια αποτελέσματα υποθέτουμε πως έχουμε εντοπίσει τα κλειδιά K_1 και K_2. Η επίθεση αυτή, γνωστή Meet-in-the-middle είναι ο βασικότερος λόγος εγκατάλειψης του Double DES και υιοθέτησης του 3DES (Triple-DES).

Για την αντιμετώπιση της επίθεσης αυτής, προτάθηκε η χρήση τριών επιπέδων κρυπτογράφησης. Συγκεκριμένα, το κρυπτογράφημα προκύπτει από μια διαδικασία κρυπτογράφησης με το κλειδί K_1, αποκρυπτογράφησης με το κλειδί K_2 και εκ νέου κρυπτογράφησης με το K_1, όπως φαίνεται στην Εικόνα 7.1. Με τον τρόπο αυτό, ο χώρος αναζήτησης αυξάνει στα 2^{112} κλειδιά.



Εικόνα 7.1 *Triple DES.*

Η επιλογή της διαδικασίας αποκρυπτογράφησης στο δεύτερο βήμα δεν αποτελεί πρόβλημα, ενώ επιλέχθηκε για να είναι δυνατή η αποκρυπτογράφηση κρυπτοκειμένων που είχαν δημιουργηθεί με τον απλό DES, αφού αρκεί $K_1=K_2$. Τέλος, έχει προταθεί και η εφαρμογή 3DES με τρία κλειδιά, όπου ο χώρος αναζήτησης

εκτείνεται πλέον στα 2^{168} κλειδιά. Στην περίπτωση αυτή κατά τη φάση της τελευταίας κρυπτογράφησης, χρησιμοποιείται το κλειδί K_3.

7.2.2 AES

Το 1997, ο οργανισμός NIST ξεκίνησε την αναζήτηση του αντικαταστάτη του αλγορίθμου DES. Στις προδιαγραφές που καθορίσθηκαν, περιλαμβάνονταν τα εξής σημεία:

- Ο αλγόριθμος θα έπρεπε να είναι αδιαβάθμητος και ελεύθερα διαθέσιμος.
- Ο αλγόριθμος θα έπρεπε να είναι συμμετρικός αλγόριθμος δέσμης.
- Ο αλγόριθμος θα έπρεπε να υποστηρίζει κλειδιά μεταβλητού μήκους 128, 192 και 256 bits.

Από το σύνολο των αλγορίθμων που προτάθηκαν, προκρίθηκαν στη δεύτερη φάση αξιολόγησης οι ακόλουθοι πέντε:

- MARS, της εταιρίας IBM (ΗΠΑ).
- RC6, του οργανισμού RSA Laboratories (ΗΠΑ).
- Rijndael, των ερευνητών Joan Daemen και Vincent Rijmen (Βέλγιο).
- Serpent, των ερευνητών Ross Anderson (HB), Eli Bihar (Ισραήλ), και Lars Knudsen (Νορβηγία).
- Twofish, των ερευνητών Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, και Niels Ferguson (ΗΠΑ).

Από την αξιολόγηση, μεγαλύτερη βαθμολογία έλαβε τελικά ο αλγόριθμος Rijndael, με το όνομά του να αποδίδεται σε λογοπαίγνιο με τα επώνυμά των ερευνητών που τον πρότειναν.

Στον Πίνακα 7.8, συνοψίζονται οι παράμετροι λειτουργίας του αλγόριθμου Rijndael:

Μήκος Κλειδιού (Word/Byte/Bit)	4/16/128	6/24/192	8/32/256
Μήκος Δέσμης (Word/Byte/Bit)	4/16/128	4/16/128	4/16/128
Πλήθος κύκλων επεξεργασίας	10	12	14
Μήκος Υποκλειδιού (Word/Byte/Bit)	4/16/128	4/16/128	4/16/128

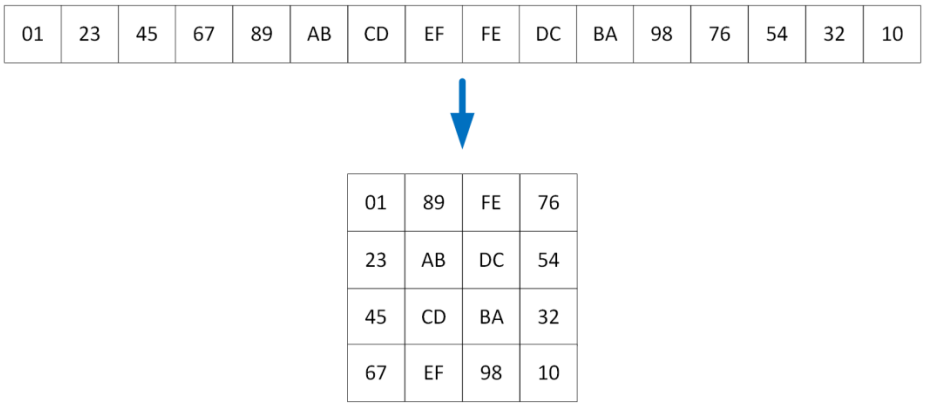
Πίνακας 7.8 *Παράμετροι λειτουργίας του αλγόριθμου Rijndael.*

Ο κρυπτογραφικός αλγόριθμος Rijndael προτυποποιήθηκε με την ονομασία Advanced Encryption Standard (AES) (FIPS 197) για μήκος κλειδιού και δέσμης στα 128 bit και παρουσιάστηκε από τον οργανισμό National Institute of Standards and Technology (NIST) το 2001.

Ο αλγόριθμος AES σχεδιάστηκε με τις ακόλουθες ιδιότητες:

- αντοχή σε όλες τις μέχρι τότε γνωστές επιθέσεις,
- ταχύτητα εκτέλεσης και οικονομία κώδικα κατά την υλοποίηση σε όλες τις διαθέσιμες πλατφόρμες,
- απλότητα στη σχεδίαση.

Σύμφωνα με τον AES, το αρχικό κείμενο τμηματοποιείται σε δέσμες μήκους 128bit. Τα bit κάθε δέσμης τοποθετούνται σε ένα δισδιάστατο πίνακα 4 x 4 byte, που ονομάζονται state (Εικόνα 7.2). Στον αλγόριθμο Rijndael, οι πίνακες αυτοί έχουν πάντα 4 γραμμές και αριθμό στηλών που εξαρτάται από το μήκος της δέσμης και το μήκος του κλειδιού.



Εικόνα 7.2 *Τοποθέτηση byte σε πίνακα State.*

Η κρυπτογράφηση με χρήση του AES ακολουθεί τα βήματα:

- Επέκταση του μυστικού κλειδιού σε υποκλειδιά.
- Μια αρχική πρόσθεση (XOR) υποκλειδιού (AddRoundKey).
- Έναν αριθμό κύκλων που περιλαμβάνει την αντικατάσταση byte (Sub Bytes), την ολίσθηση γραμμών (Shift Rows), την ανάμειξη byte (Mix Bytes) και την πρόσθεση υποκλειδιού (AddRoundKey).
- Ένα τελικό κύκλο που περιλαμβάνει την αντικατάσταση byte (Sub Bytes), την ολίσθηση γραμμών (Shift Rows) και την πρόσθεση υποκλειδιού (AddRoundKey).

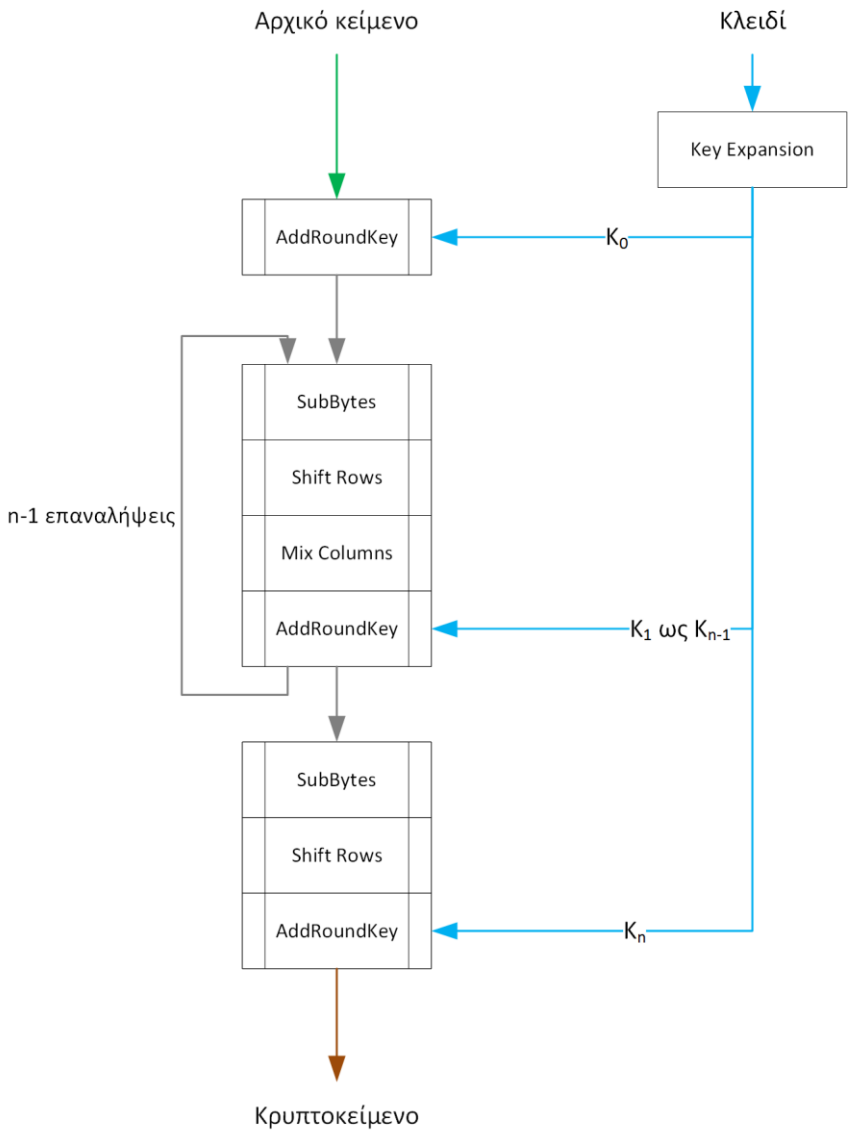
Ο αριθμός των κύκλων επεξεργασίας καθορίζεται από το μήκος της δέσμης και το μήκος του κλειδιού, όπως φαίνεται στον Πίνακα 7.9.

	Κλειδί 128 bit	**Κλειδί 192 bit**	**Κλειδί 256 bit**
Δέσμη 128 bit	10	12	14
Δέσμη 192 bit	12	12	14
Δέσμη 256 bit	14	14	14

Πίνακας 7.9 *Αριθμός απαιτούμενων κύκλων*

Ομοίως με παραπάνω, καθώς ο AES προτυποποιεί τον αλγόριθμο Rijndael για μήκος δέσμης των 128 bit, μπορούμε να έχουμε 10, 12 ή 14 κύκλους για μήκος κλειδιού 128, 192 και 256 bits αντίστοιχα.

Η διαδικασία κρυπτογράφησης απεικονίζεται συνοπτικά στην Εικόνα 7.3.



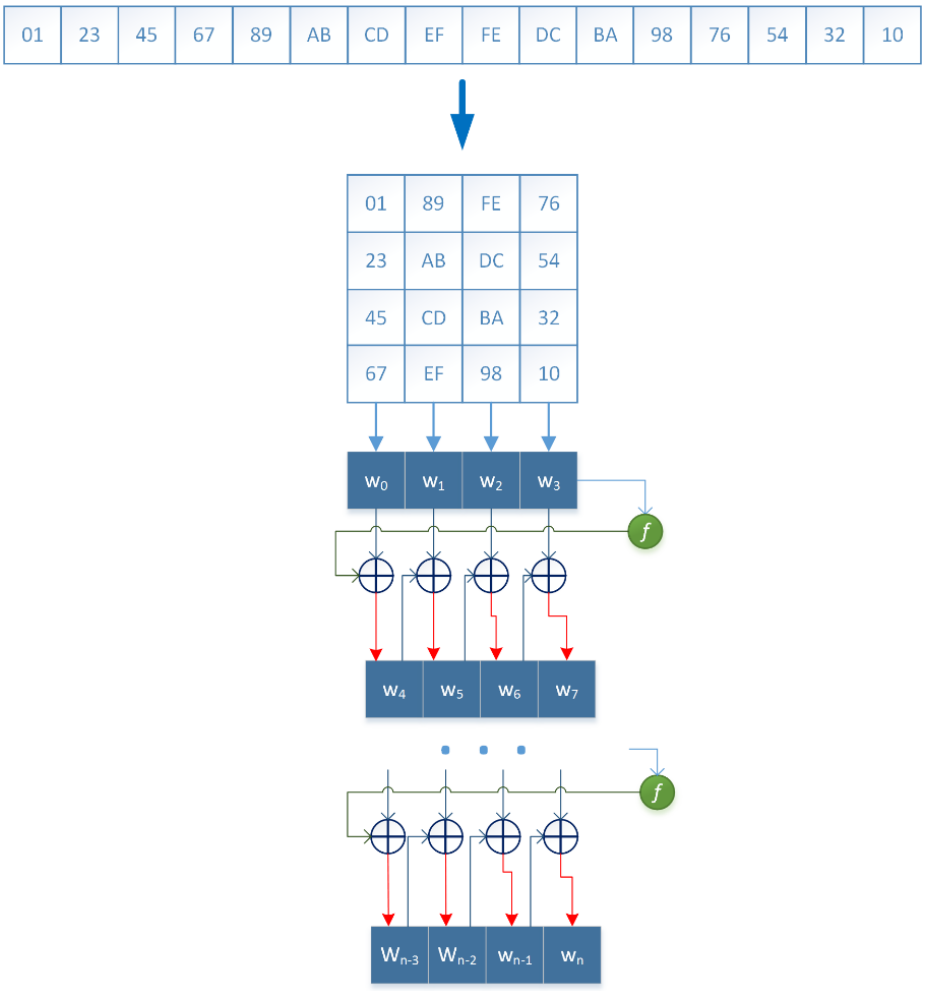
Εικόνα 7.3 *Συνοπτική παρουσίαση του AES.*

7.2.2.1 Επέκταση κλειδιού

Τα bit του μυστικού κλειδιού τοποθετούνται αρχικά σε στήλες του πίνακα ανά 32, σχηματίζοντας k στήλες με μέγεθος λέξης (word) των 32bit. Από τις αρχικές λέξεις (ο αριθμός τους είναι ίσος με το λόγο του μήκους κλειδιού προς το μήκος της λέξης) θα προκύψουν $N_w(N_r+1)$ λέξεις υποκλειδιών, όπου N_w ο αριθμός των αρχικών λέξεων και N_r ο αριθμός των επαναλήψεων, ως εξής:

- Οι πρώτες k λέξεις (του πρώτου υποκλειδιού) προκύπτουν απευθείας από το μυστικό κλειδί.
- Για κάθε ένα από τα υπόλοιπα N_r υποκλειδιά:
    - Κάθε μια από τις επόμενες λέξεις που δεν είναι σε θέση πολλαπλάσια του k προκύπτει από το αποτέλεσμα της εφαρμογής της πράξης XOR μεταξύ της αμέσως προηγούμενης και της λέξης που βρίσκεται k θέσεις πιο πίσω.
    - Κάθε λέξη σε θέση πολλαπλάσια του k προκύπτει από το αποτέλεσμα της XOR μεταξύ της λέξης που βρίσκεται k θέσεις πιο πίσω και της εξόδου μιας συνάρτησης f με είσοδο την προηγούμενη λέξη.

Η παραπάνω διαδικασία γίνεται κατανοητή με τη βοήθεια της Εικόνας 7.4.



Εικόνα 7.4 *Διαδικασία επέκτασης κλειδιού.*

Οι παραπάνω n λέξεις σχηματίζουν n/k υποκλειδιά. Στην περίπτωση ενός μυστικού κλειδιού K μήκους 128 bit, δημιουργούνται 4x(10+1)=44 λέξεις, από τις οποίες προκύπτουν 44/4=11 υποκλειδιά (K_0=K), που χρησιμοποιούνται όπως φαίνεται στην Εικόνα 7.3, για n=10.

Η συνάρτηση f που χρησιμοποιείται κατά την επέκταση κλειδιού για κάθε ένα από τα υπόλοιπα N_r υποκλειδιά (πέραν του πρώτου), υλοποιείται ως εξής:

- Η λέξη εισόδου υπόκειται σε κυκλική αριστερή μετατόπιση κατά μια θέση. Έτσι τα τέσσερα byte που την αποτελούν (B_0, B_1, B_2, B_3) αναδιατάσσονται ως εξής: (B_1, B_2, B_3, B_0)

- Με τη χρήση του S-box, που φαίνεται στον Πίνακα 7.10, πραγματοποιείται αντικατάσταση για κάθε byte της λέξης με το byte που βρίσκεται στη θέση του S-box που καθορίζεται από τη γραμμή που υποδεικνύουν τα πρώτα 4bit του προς αντικατάσταση byte και τη στήλη που υποδεικνύουν τα τέσσερα τελευταία 4bit. Για παράδειγμα, το byte 7C θα αντικατασταθεί από το byte 10.

- Κατόπιν, εφαρμόζεται η πράξη XOR με εισόδους τη λέξη που προκύπτει μετά την αντικατάσταση και την λέξη Rcon που αντιστοιχεί στο κάθε ένα από τα υπόλοιπα N_r

υποκλειδιά (πέραν του πρώτου). Οι τιμές αυτές φαίνονται στον πίνακα 7.11. Το αποτέλεσμα θα αποτελέσει την έξοδο της συνάρτησης f.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Πίνακας 7.10 *AES S-Box.*

Δημιουργία Nr υποκλειδιού	**Rcon**
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1B 00 00 00
10	36 00 00 00
11	6C 00 00 00
12	D8 00 00 00
13	AB 00 00 00
14	4D 00 00 00

Πίνακας 7.11 *Λέξεις Rcon.*

7.2.2.2 Διαδικασία κρυπτογράφησης

Αφού υπολογιστούν τα υποκλειδιά, για κάθε δέσμη αρχικού κειμένου εκτελούνται οι ακόλουθοι μετασχηματισμοί, όπως φαίνεται στην Εικόνα 7.3.

7.2.2.2.1 AddRoundKey

Εφαρμόζεται η πράξη XOR με εισόδους την τρέχουσα δέσμη και το εκάστοτε υποκλειδί.

7.2.2.2.2 SubBytes

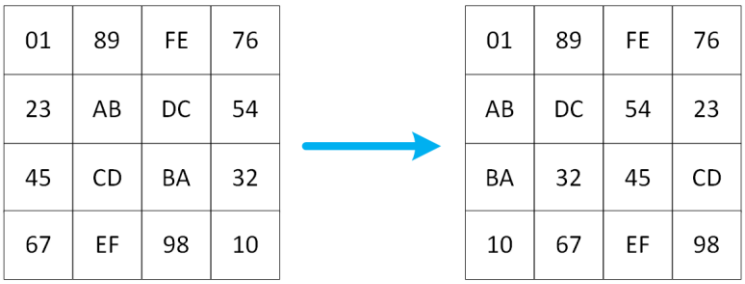
Τα byte κάθε λέξης της δέσμης, αντικαθίστανται σύμφωνα με το S-box που φαίνεται στον Πίνακα 7.9 και τον τρόπο που περιγράφηκε προηγουμένως, κατά την παρουσίαση της συνάρτησης f.

7.2.2.2.3 ShiftRows

Εκτελούνται κυκλικές αριστερές ολισθήσεις ως εξής:

- Στην πρώτη σειρά δεν έχουμε καμία ολίσθηση.
- Στη δεύτερη σειρά εκτελείται ολίσθηση 1 byte.
- Στη δεύτερη σειρά εκτελείται ολίσθηση 2 byte.
- Στη δεύτερη σειρά εκτελείται ολίσθηση 3 byte.

Ένα παράδειγμα μετασχηματισμού ShiftRows φαίνεται στην Εικόνα 7.5.



Εικόνα 7.5 *Μετασχηματισμός ShiftRows.*

7.2.2.2.4 MixColumns

Για κάθε λέξη S_i (στήλη) της τρέχουσας δέσμης, η αντίστοιχη λέξη S'_i της δέσμης που θα προκύψει υπολογίζεται ως εξής:

$$\begin{pmatrix} S'_{0,i} \\ S'_{1,i} \\ S'_{2,i} \\ S'_{3,i} \end{pmatrix} = \begin{pmatrix} S_{0,i} \\ S_{1,i} \\ S_{2,i} \\ S_{3,i} \end{pmatrix} \otimes \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \tag{7.1}$$

όπου $S_{k,i}$ είναι το κ-οστό byte της λέξης S_i και ⊗ ο πολλαπλασιασμός modulo(x^4-1). Άρα έχουμε:

$$\begin{aligned} S'_{0,i} &= \{02\} S_{0,i} \oplus \{03\} S_{1,i} \oplus S_{2,i} \oplus S_{3,i} \\ S'_{1,i} &= S_{0,i} \oplus \{02\} S_{1,i} \oplus \{03\} S_{2,i} \oplus S_{3,i} \\ S'_{2,i} &= S_{0,i} \oplus S_{1,i} \oplus \{02\} S_{2,i} \oplus \{03\} S_{3,i} \\ S'_{3,i} &= \{03\} S_{0,i} \oplus S_{1,i} \oplus S_{2,i} \oplus \{02\} S_{3,i} \end{aligned} \tag{7.2}$$

όπου ⊕ η πράξη XOR. Επιπλέον, $\{03\} S_{k,i} = \{02\} S_{k,i} \oplus S_{k,i}$. Τέλος, για τον υπολογισμό του $\{02\}S_{k,i}$ ακολουθούμε τα εξής βήματα:

- αν το αριστερότερο bit του $S_{k,i}$ είναι 0, εφαρμόζουμε αριστερή ολίσθηση (left shift) ενός bit (με συμπλήρωση μηδέν από δεξιά),

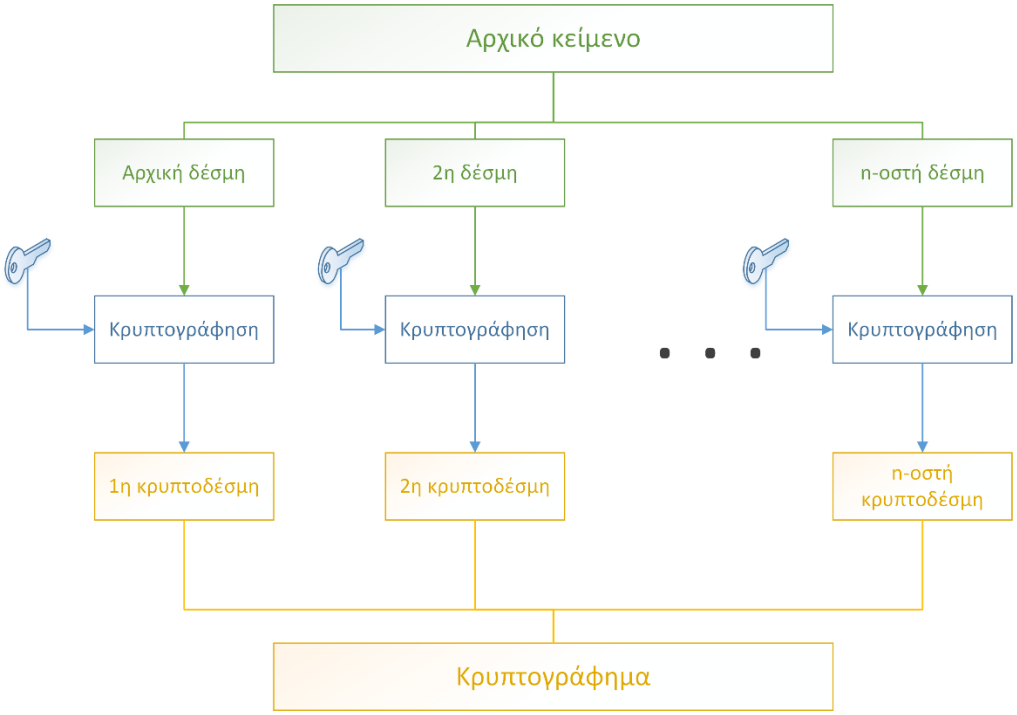
- αν το αριστερότερο bit του $S_{k,i}$ είναι 1, εφαρμόζουμε αριστερή ολίσθηση ενός bit και το αποτέλεσμα αποτελεί κατόπιν τη μια είσοδο της πράξης XOR με δεύτερη είσοδο το byte (00011011).

Έτσι, για παράδειγμα, από τη λέξη D4BF5D30 θα προκύψει η λέξη 046681E5.

7.2.3 Τρόποι λειτουργίας

7.2.3.1 Electronic Codebook (ECB)

Στον DES, όπως περιγράφηκε παραπάνω, το κρυπτογράφημα μιας δέσμης του αρχικού κειμένου εξαρτάται αποκλειστικά από το μυστικό κλειδί και από την ίδια τη δέσμη. Αυτός ο τρόπος λειτουργίας ονομάζεται Electronic CodeBook (ECB). Ο όρος «Codebook» χρησιμοποιείται επειδή για κάθε δέσμη αρχικού κειμένου, με δεδομένο το κλειδί, αντιστοιχεί ένα μοναδικό κρυπτοκείμενο. Θα μπορούσε να το φανταστεί κανείς ως ένα τηλεφωνικό κατάλογο όπου σε κάθε όνομα (αρχικό κείμενο) αντιστοιχεί και ένας τηλεφωνικός αριθμός (κρυπτοκείμενο).



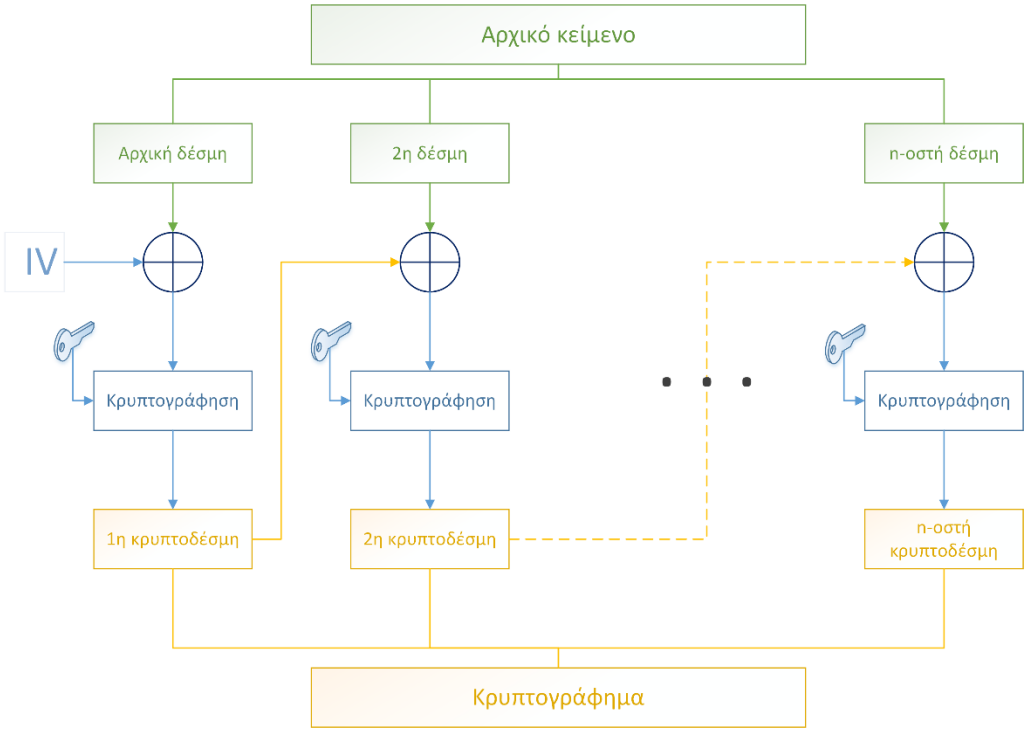
Εικόνα 7.6 *Λειτουργία ECB.*

Γίνεται κατανοητό πως όταν χρησιμοποιείται ο τρόπος λειτουργίας ECB, όποτε μια δέσμη αρχικού κειμένου εμφανίζεται περισσότερες από μια φορές στο μήνυμα, θα παράγεται κάθε φορά το ίδιο κρυπτοκείμενο. Αυτή η πιθανή κατάσταση δεν είναι επιθυμητή, καθώς τέτοιου είδους επαναλήψεις μπορεί να είναι ιδιαίτερα χρήσιμες για τον κρυπταναλυτή.

7.2.3.2 Cipher Block Chaining (CBC)

Μια τεχνική, για να αποφευχθεί το πρόβλημα επαναληπτικότητας που παρουσιάζει ο τρόπος λειτουργίας ECB, είναι η χρησιμοποίηση της κρυπτογραφημένης δέσμης κατά τη διαδικασία κρυπτογράφησης της επόμενης αρχικής δέσμης. Έτσι, η κρυπτοδέσμη i αποτελεί είσοδο της πράξης XOR μαζί με την αρχική δέσμη i+1, όπως φαίνεται στην Εικόνα 7.7.

Για την πρώτη αρχική δέσμη, για την οποία δεν υπάρχει προηγούμενη κρυπτοδέσμη, χρησιμοποιείται ένα διάνυσμα αρχικοποίησης (Initialization Vector - IV) ίσου μήκους με τη δέσμη. Το IV αποστέλλεται στον παραλήπτη, μαζί με το κρυπτογραφημένο μήνυμα, ώστε να είναι δυνατή η αποκρυπτογράφηση.

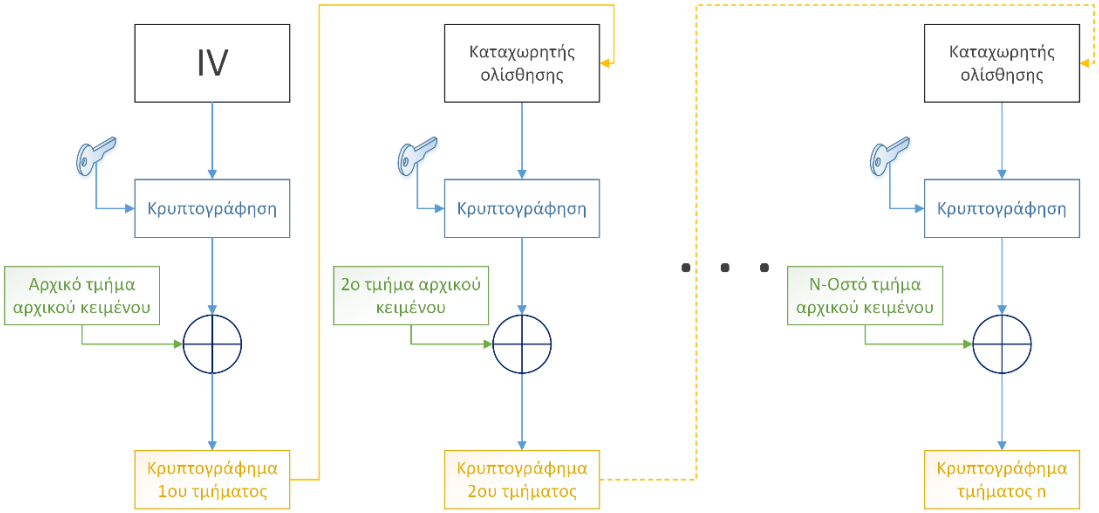


Εικόνα 7.7 *Λειτουργία CBC.*

7.2.3.3 Cipher FeedBack Mode (CFB)

Ένα βασικό πρόβλημα των αλγορίθμων δέσμης είναι η κρυπτογράφηση δεσμών συγκεκριμένου μεγέθους. Έτσι είναι δύσκολο να χρησιμοποιηθούν για μετάδοση ροής δεδομένων σε πραγματικό χρόνο. Στην κατάσταση λειτουργίας CFB, το αρχικό κείμενο χωρίζεται σε τμήματα μικρότερου μεγέθους από αυτό της δέσμης, ακόμη και σε τμήματα του 1 bit (με συνηθέστερη τιμή αυτή του ενός byte). Έστω k το μέγεθος του κάθε τμήματος αρχικού κειμένου. Ακόμη, χρησιμοποιείται ένας καταχωρητής ολίσθησης, μεγέθους μιας δέσμης, στον οποίο δίνεται μια αρχική τιμή, γνωστή ως διάνυσμα αρχικοποίησης (IV).

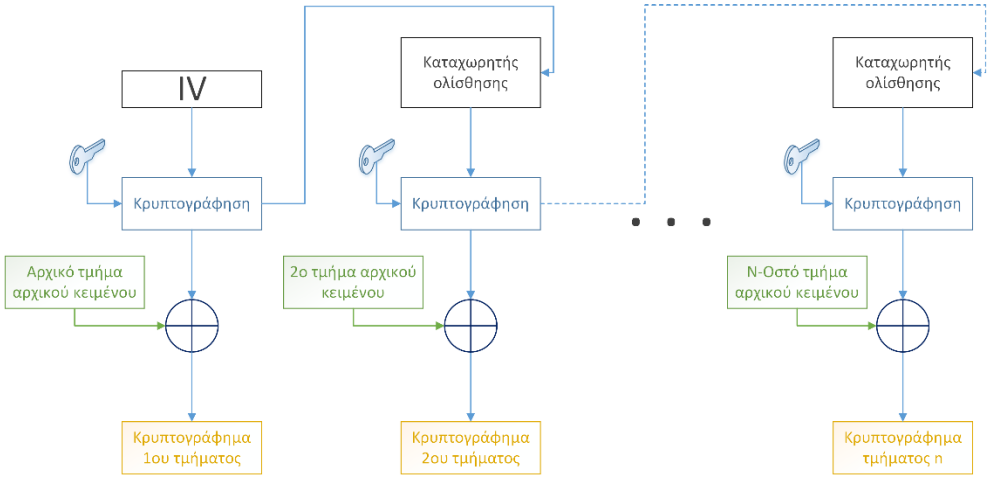
Για κάθε τμήμα αρχικού κειμένου, γίνεται αρχικά κρυπτογράφηση του καταχωρητή ολίσθησης με βάση το κλειδί κρυπτογράφησης (Εικόνα 7.8) και η παραγόμενη κρυπτοδέσμη τοποθετείται σε ένα καταχωρητή κρυπτογράφησης. Από τον καταχωρητή κρυπτογράφησης, επιλέγονται στην συνέχεια τα k αριστερότερα bit, τα οποία μαζί με το τρέχον τμήμα του ανοικτού κειμένου οδηγούνται ως είσοδοι σε μια πράξη XOR, της οποίας η έξοδος αποτελεί το κρυπτογράφημα του τμήματος. Το κρυπτογράφημα του τμήματος τοποθετείται (παρέχοντας ανατροφοδότηση - feedback) στο δεξί μέρος του καταχωρητή ολίσθησης, αφού προηγουμένως έχει εκτελεστεί μια αριστερή ολίσθηση του περιεχομένου του, κατά k bits. Με τον τρόπο αυτό, ένας αλγόριθμος δέσμης μετατρέπεται σε αλγόριθμο ροής.



Εικόνα 7.8 *Λειτουργία CFB.*

7.2.3.4 Output FeedBack Mode (OFB)

Ο τρόπος λειτουργίας OFB μοιάζει αρκετά με τον τρόπο CFB. Η κύρια διαφοροποίηση έγκειται στο ότι η ανατροφοδότηση του καταχωρητή ολίσθησης γίνεται πλέον από τα k αριστερότερα bit του καταχωρητή κρυπτογράφησης (Εικόνα 7.9).



Εικόνα 7.9 *Λειτουργία OFB.*

7.3 Ασύμμετρα Κρυπτοσυστήματα

Όπως είδαμε στην προηγούμενη ενότητα, οι συμμετρικοί κρυπτογραφικοί αλγόριθμοι βασίζονται κυρίως στη χρήση μετασχηματισμών μετάθεσης, αντικατάστασης, μετατόπισης κ.ά. των bit της κάθε δέσμης ή υποδέσμης. Οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι βασίζονται κυρίως στη χρήση μαθηματικών πράξεων και για αυτό ενδείκνυνται για την κρυπτογράφηση / αποκρυπτογράφηση αριθμητικών δεδομένων, μικρού μεγέθους. Όπως αναφέρθηκε και προηγουμένως, για την ασφάλεια των ΤΠΕ γίνεται συμπληρωματική αξιοποίηση των συμμετρικών και των ασύμμετρων κρυπτογραφικών αλγορίθμων προκειμένου να παρέχονται ολοκληρωμένες και αποδοτικές υπηρεσίες ασφάλειας.

Στα ασύμμετρα κρυπτοσυστήματα, όλα τα μέρη έχουν πρόσβαση στα δημόσια κλειδιά όλων, ενώ ταυτόχρονα μόνον τα ίδια πρέπει να έχουν πρόσβαση στα ιδιωτικά τους κλειδιά. Κάθε μέρος μπορεί να δημιουργεί νέα ζεύγη κλειδιών, ανάλογα με τη χρήση τους. Έτσι, αν η χρήση τους είναι για κρυπτογράφηση

μόνο, τότε η παραγωγή νέων ζευγών θα πρέπει να γίνεται σπάνια, ενώ η φύλαξη των ιδιωτικών κλειδιών είναι κρίσιμη και θα πρέπει να υπάρχει διαδικασία ανάκτησης (key escrow) για την περίπτωση απώλειάς τους. Αν όμως η χρήση τους είναι για υπογραφή μόνο, τότε η παραγωγή νέων ζευγών μπορεί να γίνεται όποτε παραστεί ανάγκη, π.χ. όταν υπάρξει κάποιο πρόβλημα με τα ιδιωτικά κλειδιά (για παράδειγμα, διαρροή ή απώλεια).

Σύμφωνα με τα παραπάνω, διακρίνουμε τρεις κατηγορίες στις οποίες μπορούμε να εντάξουμε τα κρυπτοσυστήματα δημοσίου κλειδιού:

- **Κρυπτογράφηση/αποκρυπτογράφηση**: Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη, ο οποίος το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Με αυτό τον τρόπο προστατεύεται η εμπιστευτικότητα του μηνύματος.

- **Ψηφιακή υπογραφή**: Ο αποστολέας υπογράφει το μήνυμα κρυπτογραφώντας το με το ιδιωτικό κλειδί του. Ο παραλήπτης επιβεβαιώνει την ψηφιακή υπογραφή αποκρυπτογραφώντας το κρυπτοκείμενο με το δημόσιο κλειδί του αποστολέα. Η υπογραφή μπορεί να γίνει στο σύνολο του μηνύματος ή μόνο σε ένα μικρό σετ δεδομένων το οποίο παράγεται ως αποτέλεσμα της εφαρμογής μιας συνάρτησης κατακερματισμού (hashing function) πάνω στο σύνολο του μηνύματος. Με αυτό τον τρόπο προστατεύεται η αυθεντικότητα του αποστολέα και η ακεραιότητα του μηνύματος.

- **Ανταλλαγή κλειδιών**: Τα δύο επικοινωνούντα μέρη συνεργάζονται ώστε να ανταλλάξουν με ασφάλεια (εξασφαλίζοντας την εμπιστευτικότητα) ένα συμμετρικό κλειδί συνόδου.

Από τους γνωστούς αλγόριθμους κάποιοι είναι κατάλληλοι και για τις τρεις κατηγορίες κρυπτογραφικών ενεργειών, ενώ άλλοι για λιγότερες. Στον παρακάτω πίνακα εμφανίζονται με συνοπτικό τρόπο οι δυνατότητες των πιο γνωστών αλγόριθμων δημόσιου κλειδιού:

Αλγόριθμος	**Κρυπτογράφηση**	**Ψηφιακή Υπογραφή**	**Ανταλλαγή Κλειδιών**
RSA	NAI	NAI	NAI
Diffie - Hellman	OXI	OXI	NAI
DSS	OXI	NAI	OXI
Elliptic Curves	NAI	NAI	NAI

Πίνακας 7.12 *Αλγόριθμοι δημοσίου κλειδιού.*

7.3.2 RSA

Ένας από τους πρώτους αλγορίθμους δημοσίου κλειδιού που αναπτύχθηκαν ήταν ο RSA. Το ακρωνύμιο προκύπτει από τα ονόματα των Ron Rivest, Adi Shamir, και Len Adleman που πρότειναν τον συγκεκριμένο αλγόριθμο το 1977. Σύμφωνα με τον αλγόριθμο RSA, η κρυπτογράφηση γίνεται σε δέσμες (blocks) αρχικού κειμένου, το περιεχόμενο των οποίων είναι μια αριθμητική τιμή που πρέπει να είναι μικρότερη από έναν αριθμό n.

Η κρυπτογράφηση ενός τμήματος αρχικού κειμένου m με το δημόσιο κλειδί παράγει το κρυπτογράφημα c ως εξής:

$$c = m^e \bmod n \tag{7.3}$$

Αντιστοίχως, για την αποκρυπτογράφηση, έχουμε:

$$m = c^d \bmod n \tag{7.4}$$

Το ζεύγος {e,n} αποτελεί το δημόσιο κλειδί που είναι γνωστό σε όλους, ενώ το ζεύγος {d,n} το ιδιωτικό που είναι γνωστό μόνο στον ιδιοκτήτη του.

Για να είναι ικανοποιητικός αυτός ο αλγόριθμος θα πρέπει να ισχύουν οι παρακάτω προϋποθέσεις:

- Είναι εφικτό να βρεθούν e, d, n τέτοια ώστε $m^{ed} \text{mod} n = m$ για κάθε $m<n$.
- Είναι σχετικά εύκολο να υπολογιστούν τα m^e και c^d για κάθε $m<n$.
- Είναι αδύνατο να υπολογιστεί το ιδιωτικό κλειδί {d, n}, δηλαδή το d, αν γνωρίζουμε το δημόσιο {e, n}.

Οι δύο πρώτες προϋποθέσεις ικανοποιούνται εύκολα. Η τρίτη προϋπόθεση ικανοποιείται για πολύ μεγάλα p και q και βασίζεται στην υπόθεση πως είναι δύσκολο να παραγοντοποιηθεί ένας μεγάλος αριθμός σε γινόμενο πρώτων αριθμών.

Ας δούμε αρχικά τον τρόπο υπολογισμού των κλειδιών του RSA:

- Επιλέγουμε τυχαία δύο μεγάλους πρώτους αριθμούς p και q.
- Υπολογίζουμε το n=pq.
- Υπολογίζουμε το φ(n)=(p-1)(q-1).
- Βρίσκουμε έναν τυχαίο αριθμό e, σχετικά πρώτο του φ(n). Δύο σχετικά πρώτοι αριθμοί έχουν μέγιστο κοινό διαιρέτη (ΜΚΔ) τη μονάδα.
- Υπολογίζουμε έναν αριθμό d για τον οποίο ισχύει ed=1mod(φ(n)).

Παρατηρούμε ότι η ασφάλεια του αλγορίθμου έγκειται στη δυσκολία εύρεσης των p και q, δεδομένου του e και του n. Ο κρυπταναλυτής πρέπει να εντοπίσει τους αριθμούς p και q ώστε να παράξει το φ(n) και στη συνέχεια από το γνωστό e να υπολογίσει το d. Η διαδικασία εντοπισμού των p και q, η παραγοντοποίηση (factorization) δηλαδή του n, ή αλλιώς του modulus είναι ως σήμερα αδύνατη για τιμή μήκους από 1024bit και πάνω. Για το λόγο αυτό, σε πραγματικά κρυπτοσυστήματα χρησιμοποιούνται ιδιαίτερα μεγάλοι πρώτοι αριθμοί Ένα απλό παράδειγμα χρήσης του RSA, ακολουθεί στη συνέχεια.

- Αρχικά θα πρέπει να δημιουργήσουμε το ζεύγος κλειδιών. Εντοπίζουμε δύο πρώτους αριθμούς, έστω p=7 και q=11.
- Από αυτούς προκύπτει n=pq=77.
- Υπολογίζουμε το φ(n)=(7-1)(11-1)=60.
- Εντοπίζουμε e, τέτοιο ώστε να είναι σχετικά πρώτος αριθμός του 60. Έστω e=13.
- Το δημόσιο κλειδί θα είναι το {13,77}.
- Υπολογίζουμε το ιδιωτικό κλειδί d, τέτοιο ώστε ed mod φ(n) = 1. Ένας τέτοιος αριθμός είναι ο 37. Άρα το ιδιωτικό κλειδί είναι το {37,77}.

Έστω ότι κάποιος θέλει να κρυπτογραφήσει τον αριθμό 3 (3<77) με τη χρήση του RSA και να μας στείλει το κρυπτογράφημα. Για την κρυπτογράφηση θα χρησιμοποιήσει το διαθέσιμο δημόσιο κλειδί και θα υπολογίσει:

$$c = m^e \bmod n = 3^{13} \bmod 77 = 38 \tag{7.5}$$

Άρα θα μας αποστείλει τον αριθμό 38. Για να ton αποκρυπτογραφήσουμε, θα χρησιμοποιήσουμε το ιδιωτικό κλειδί, που μόνοn εμείς κατέχουμε. Άρα έχουμε:

$$m = c^d \bmod n = 38^{37} \bmod 77 = 3 \tag{7.6}$$

7.4 Μελέτη Σύγχρονων Αλγόριθμων με το Cryptool

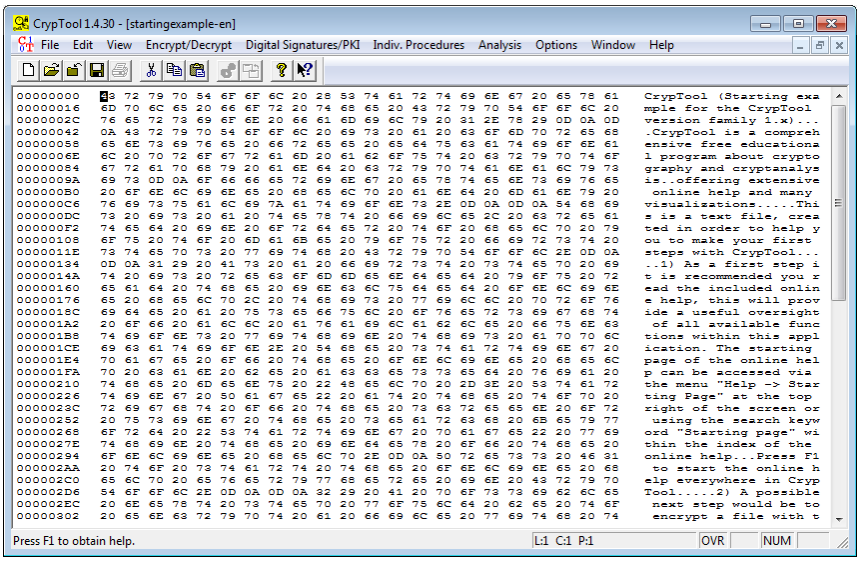
Στη συνέχεια, θα χρησιμοποιήσουμε το λογισμικό Cryptool, αλλά και το προϊόν λογισμικού PGP σε περιβάλλον Linux για μια κοντινότερη στην πραγματικότητα μελέτη των αλγόριθμων που αναφέρθηκαν στις προηγούμενες ενότητες.

7.4.1 Συμμετρικοί αλγόριθμοι

7.4.1.1 Κρυπτογράφηση DES-CBC

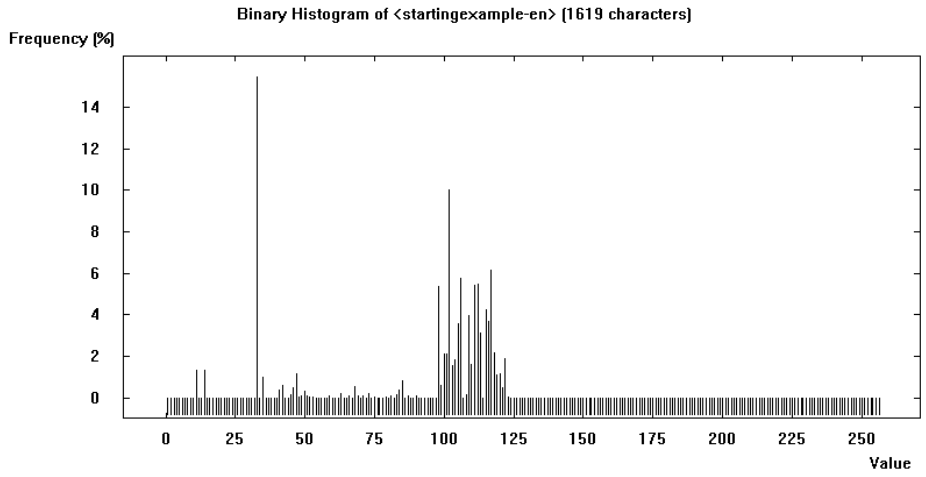
Εκτελούμε το λογισμικό *Cryptool*, οπότε ανοίγει το αρχικό παράθυρο με το αρχείο startingexample-en.txt το οποίο θα χρησιμοποιήσουμε ως αρχικό κείμενο για την κρυπτογράφηση.

Από το μενού επιλέγουμε διαδοχικά **View → As Hexdump**. Με την επιλογή αυτή εμφανίζεται και η δεκαεξαδική αναπαράσταση του αρχείου startingexample-en.txt, παράλληλα με την αναπαράσταση ASCII.



Εικόνα 7.10 *Προβολή HexDump.*

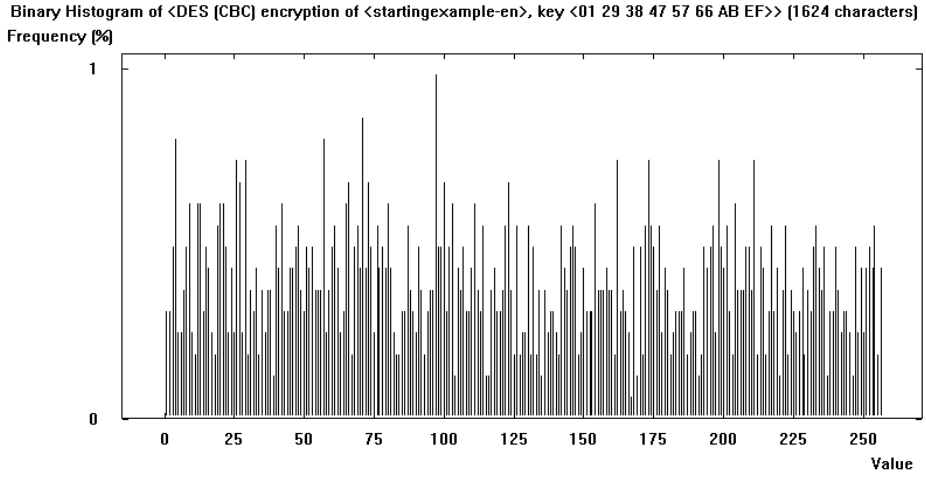
Από το μενού επιλέγουμε διαδοχικά **Analysis → Tools for Analysis → Histogram**. Ανοίγει νέο παράθυρο, όπου εμφανίζεται ένα ιστόγραμμα. Το ιστόγραμμα αυτό εκφράζει με γραφικό τρόπο την κατανομή συχνοτήτων εμφάνισης των χαρακτήρων που περιέχονται στο κείμενο. Παρατηρήστε το ιστόγραμμα. Γιατί περιέχει 256 τιμές (οι χαρακτήρες της λατινικής αλφαβήτου είναι μόλις 26);



Εικόνα 7.11 *Ιστόγραμμα αρχικού κειμένου.*

Εστιάζουμε στο παράθυρο του αρχικού κειμένου και κρυπτογραφούμε το μήνυμα με τον αλγόριθμο DES εκτελώντας τα ακόλουθα βήματα:

- Επιλέγουμε διαδοχικά: **Encrypt/ Decrypt → Symmetric (modern) → DES(CBC)**
- Ως κλειδί κρυπτογράφησης χρησιμοποιούμε το **01 29 38 47 57 66 AB EF** και στη συνέχεια πατάμε το κουμπί **Encrypt**
- Εμφανίζεται νέο παράθυρο με το κρυπτογραφημένο μήνυμα. Εστιάζοντας σε αυτό το παράθυρο επιλέγουμε από το μενού διαδοχικά **Analysis → Tools for Analysis → Histogram**



Εικόνα 7.12 *Ιστόγραμμα κρυπτογραφήματος.*

Παρατηρήστε τα δύο ιστογράμματα (αρχικού κειμένου και κρυπτογραφημένου κειμένου) που εμφανίζονται στις Εικόνες 7.12 και 7.13. Τι παρατηρείτε;

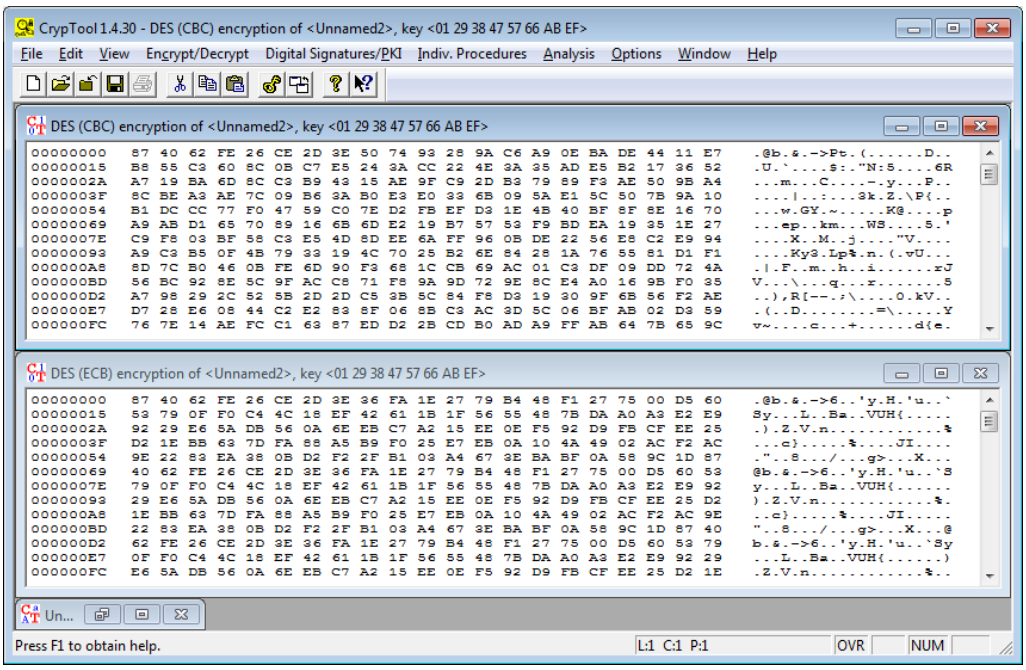
7.4.1.2 Σύγκριση μεθόδων ECB και CBC

Κλείνουμε όλα τα εσωτερικά παράθυρα της εφαρμογής Cryptool και δημιουργούμε νέο αρχικό μήνυμα επιλέγοντας από το μενού **File → New**. Στο νέο παράθυρο γράφουμε τη λέξη «**Cryptography** »

(χρησιμοποιείστε και τον τελευταίο κενό χαρακτήρα) και την επαναλαμβάνουμε πολλές φορές (τουλάχιστον 20 γραμμές κειμένου), αντιγράφοντας και τον κενό χαρακτήρα ώστε να διαχωρίζεται η μια λέξη από την άλλη. Στόχος μας είναι να δημιουργήσουμε ένα κείμενο όπου μία λέξη επαναλαμβάνεται συνεχώς.

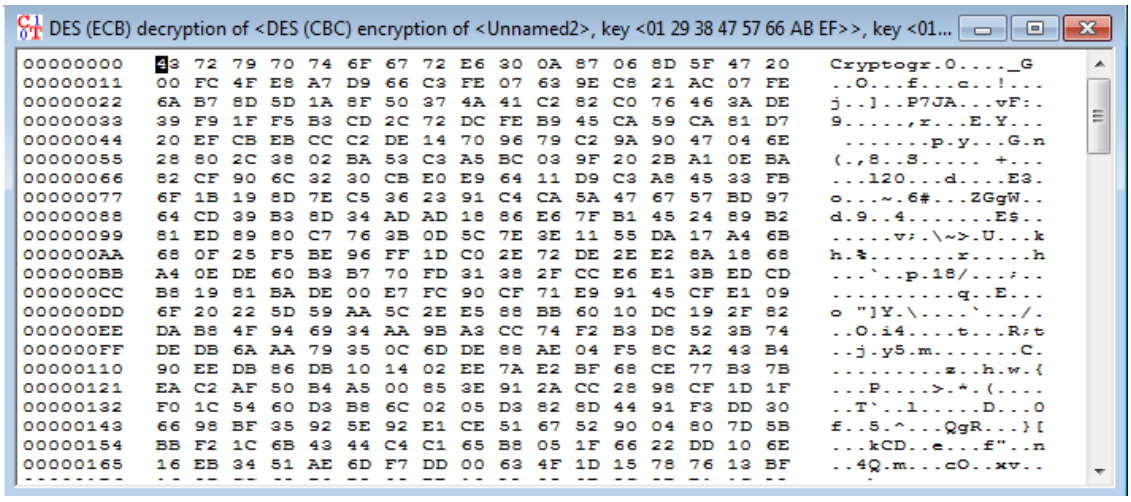
Κρυπτογραφούμε το αρχικό κείμενο πρώτα με τον αλγόριθμο DES (CBC) και κατόπιν με τον αλγόριθμο DES (ECB), χρησιμοποιώντας το ίδιο κλειδί: **01 29 38 47 57 66 AB EF**, όπως είδαμε παραπάνω.

- Συγκρίνετε τα δύο κρυπτογραφημένα μηνύματα (Εικόνα 7.13). Τι παρατηρείτε;



Εικόνα 7.13 *Κρυπτογραφήματα κειμένου με περιοδικότητα.*

Και για τα δύο κρυπτογραφημένα μηνύματα αποκρυπτογραφούμε χρησιμοποιώντας το ίδιο κλειδί: **01 29 38 47 57 66 AB EF**. Επιλέγουμε από το μενού **Encrypt / Decrypt → Symmetric (modern) → DES (ECB)**, εισάγουμε το κλειδί και κατόπιν πατάμε το πλήκτρο Decrypt, δηλαδή αποκρυπτογραφούμε και τα δύο επιλέγοντας λειτουργία ECB (Εικόνα 7.14). Τι «περίεργο» παρατηρούμε; Πώς αιτιολογείται;



Εικόνα 7.14 *Αποκρυπτογράφηση με χρήση ECB σε κρυπτογράφημα CBC.*

7.4.1.3 DES Weak Keys

Η αποτελεσματικότητα ενός συμμετρικού κρυπτοσυστήματος εξαρτάται και από το κλειδί κρυπτογράφησης που χρησιμοποιείται. Ας δούμε ένα παράδειγμα:

- Κλείνουμε όλα τα εσωτερικά παράθυρα της εφαρμογής Cryptool, εκτός από το αρχείο CrypTool-en.txt.

- Επιλέγουμε διαδοχικά: **Encrypt/Decrypt → Symmetric(modern) → DES(ECB)** για να κρυπτογραφήσουμε το αρχείο, εισάγουμε την τιμή: **01 01 01 01 01 01 01 01** ως κλειδί και επιλέγουμε **Encrypt**.

- Επαναλαμβάνουμε την **κρυπτογράφηση** χρησιμοποιώντας το ίδιο κλειδί. Το αρχικό κείμενο εμφανίζεται και πάλι. Είναι σωστή μια τέτοια συμπεριφορά; Γιατί προκύπτει η συμπεριφορά αυτή;

7.4.1.4 Επίθεση Brute Force

Θα χρησιμοποιήσουμε τη μέθοδο brute force για να προσπαθήσουμε να κρυπταναλύσουμε με γνωστό μόνο το κρυπτοκείμενο, που έχει προκύψει με χρήση του αλγόριθμου 3DES.

- Κλείνουμε όλα τα εσωτερικά παράθυρα της εφαρμογής Cryptool και ανοίγουμε το αρχείο Cryptool-en.txt από το directory examples που βρίσκεται στον κατάλογο εγκατάστασης του Cryptool.

- Από το μενού επιλέγουμε: **Encrypt/Decrypt → Symmetric (modern) → Triple DES (CBC)**.

- Δίνουμε ως κλειδί: 01 23 45 67 89 AB CD EF FE DC BA 98 76 54 32 10 (128bits).

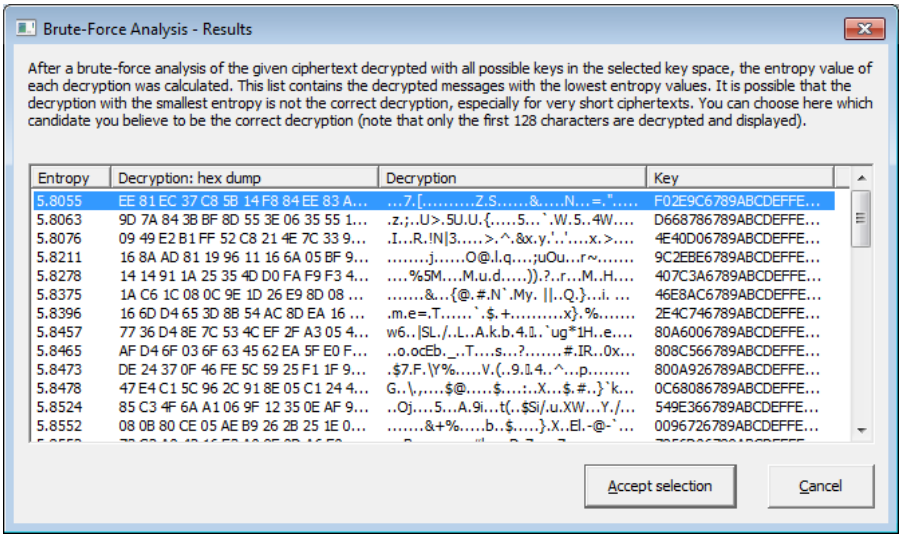
- Πατάμε το κουμπί Encrypt.

Στόχος είναι να βρεθεί το κλειδί του κρυπτοκειμένου εξαπολύοντας μια brute-force επίθεση. Για να εκτελέσουμε την επίθεση:

- Επιλέγουμε: **Analysis → Symmetric Encryption (modern) → Triple DES (CBC)**

- Έστω, για λόγους οικονομίας χρόνου, ότι με κάποιο τρόπο άγνωστα μας είναι μόνο τα 24 πρώτα bits του κλειδιού. Εισάγουμε την τιμή: **** ** ** 67 89 AB CD EF FE DC BA 98 76 54 32 10** ως μοτίβο κλειδιού.

- Πατάμε το κουμπί Start. Μετά από λίγη ώρα θα εμφανιστεί μία λίστα αποτελεσμάτων. Εστιάστε στην πρώτη στήλη που τιτλοφορείται εντροπία (Εικόνα 7.15). Στο προηγούμενο κεφάλαιο είχε γίνει αναφορά σε αυτή. Ποιο από τα αποτελέσματα θα διαλέγατε με βάση αυτή την τιμή; Γιατί;

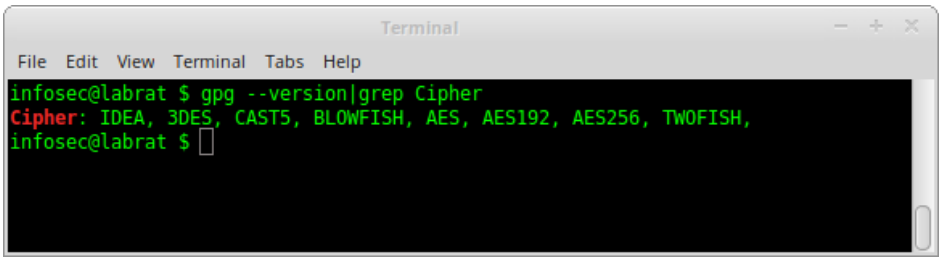


Εικόνα 7.15 *Τιμές εντροπίας.*

7.4.1.5 Χρήση GPG σε Λ.Σ. Linux

Χρησιμοποιήστε μια μηχανή με λειτουργικό σύστημα Linux και εντοπίστε αν υπάρχει εγκατεστημένη η εφαρμογή gpg, εκτελώντας την εντολή **which gpg**. Αν το gpg δεν εντοπιστεί, θα πρέπει να εγκατασταθεί από το διαχειριστή πακέτων της διανομής ή από τον πηγαίο κώδικα. Ενδεικτικά, σε RedHat ή παράγωγα (CentOS, Oracle Linux) εκτελείτε **yum install gpg** ενώ σε Debian διανομές (Debian, Ubuntu, Mint) **apt-get install gpg** με δικαιώματα διαχειριστή.

Για να δούμε ποιους αλγόριθμους συμμετρικής κρυπτογράφησης υποστηρίζει το πρόγραμμα gpg εκτελούμε (Εικόνα 7.16): **gpg --version** ή εναλλακτικά, για να περιορίσουμε την πληροφορία στους αλγόριθμους, εκτελούμε: **gpg --version | grep Cipher**



Εικόνα 7.16 *Υποστηριζόμενοι αλγόριθμοι.*

- Δημιουργούμε το φάκελο **test-symcrypt** με την εντολή:

```
mkdir test-symcrypt
```

- Μεταφερόμαστε στο directory αυτό με την εντολή:

```
cd test-symcrypt
```

- Δημιουργούμε το αρχείο myfile.txt με περιεχόμενο Sample text με την εντολή

```
echo "Sample Text" > myfile.txt
```

- Κρυπτογραφούμε με αλγόριθμο AES256 με την εντολή:

```
gpg --symmetric --cipher-algo aes256 -o myfile.txt.gpg
myfile.txt
```

- Εισάγουμε το επιθυμητό κλειδί (π.χ. «passphrase») για την κρυπτογράφηση και το επιβεβαιώνουμε όταν μας ξαναζητηθεί
- Εκτελούμε **ls –al** για να δούμε τα περιεχόμενα του καταλόγου
- Εμφανίζουμε το περιεχόμενο ενός αρχείου με την εντολή **cat myfile.txt**
- Τι παρατηρούμε για τα δύο αρχεία;
- Αποκρυπτογραφούμε με την εντολή:

```
gpg –d –o myfile-decrypted.txt myfile.txt.gpg
```

Στη συνέχεια, θα κρυπτογραφήσουμε το ίδιο αρχικό κείμενο με τους αλγόριθμους TWOFISH και CAMELLIA256 χρησιμοποιώντας τις παρακάτω εντολές

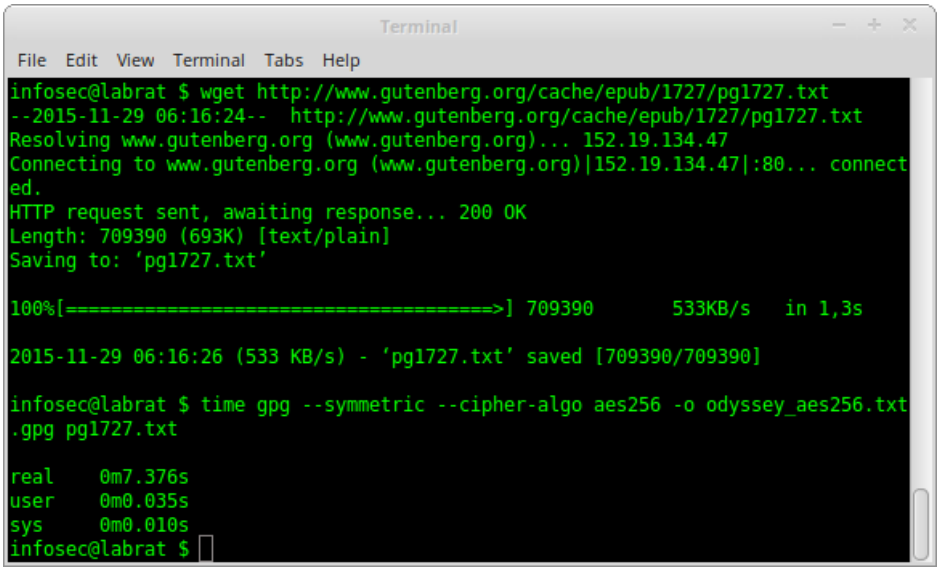
```
gpg --symmetric --cipher-algo TWOFISH myfile.txt

gpg --symmetric --cipher-algo CAMELLIA256 myfile.txt
```

Κατεβάζουμε από το διαδίκτυο ένα κείμενο μεγάλου μεγέθους με την εντολή:

```
wget http://www.gutenberg.org/cache/epub/1727/pg1727.txt
```

Για να μετρήσουμε το χρόνο που απαιτείται για την κρυπτογράφηση, εκτελούμε την εντολή (Εικόνα 7.17):

```
time gpg --symmetric --cipher-algo aes256 -o
odyssey_aes256.txt.gpg pg1727.txt
```



Εικόνα 7.17 *Χρόνοι εκτέλεσης.*

Επαναλάβετε την κρυπτογράφηση για όλους τους προσφερόμενους αλγόριθμους περισσότερες από μια φορές (τουλάχιστον 10) σημειώνοντας το μέσο χρόνο του user στον παρακάτω Πίνακα 7.13:

Αλγόριθμος	Χρόνος (sec)	Μήκος κλειδιού (bits)
DES		
3DES		
CAST5		
BLOWFISH		
AES		
AES192		
AES256		
TWOFISH		
CAMELLIA128		
CAMELLIA256		

Πίνακας 7.13 *Καταγραφή χρόνων εκτέλεσης και μήκος κλειδιού*

Σημειώνεται ότι ο τρόπος μέτρησης της ταχύτητας (time command) των συμμετρικών κρυπτογραφικών αλγόριθμων χρησιμοποιείται μόνο για τις ανάγκες της εργαστηριακής παρουσίασης των αποτελεσμάτων. Ο ορθός τρόπος μέτρησης της ταχύτητας των συμμετρικών κρυπτογραφικών αλγόριθμων θα πρέπει να γίνεται με εξειδικευμένο λογισμικό/υλικό, στη βάση συγκεκριμένου σεναρίου δοκιμών (testing).

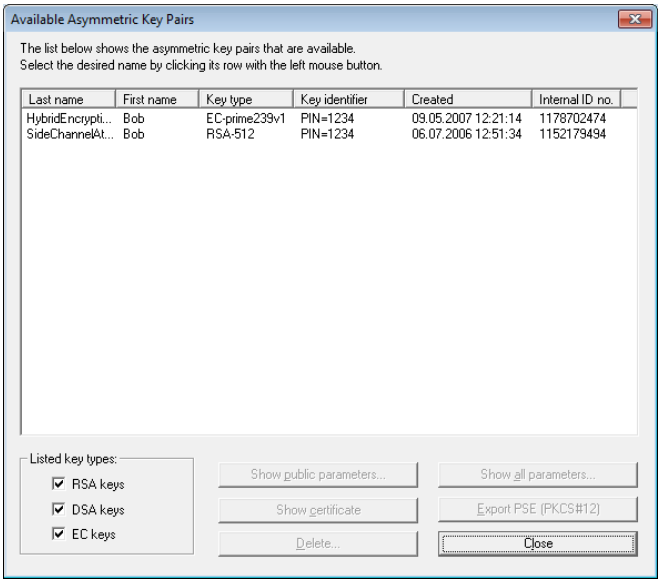
7.4.2 Ασύμμετροι αλγόριθμοι

Ο αλγόριθμος δημόσιου κλειδιού που χρησιμοποιείται συχνότερα, είναι ο RSA, τον οποίο και θα μελετήσουμε στη συνέχεια.

7.4.2.1 Δημιουργία ζεύγους κλειδιών RSA

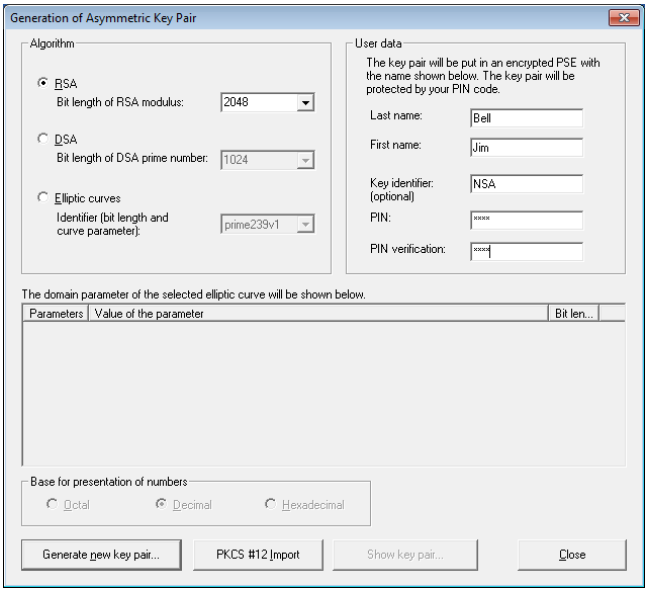
Εκτελούμε το εργαλείο Cryptool και από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Display / Export Keys**

Από το παράθυρο που εμφανίζεται, ενημερωνόμαστε για τα ζεύγη κλειδιών που υπάρχουν στον υπολογιστή μας και για τα οποία είναι ενήμερο το Cryptool (εικόνα 7.18).



Εικόνα 7.18 *Εγκατεστημένα ζεύγη κλειδιών.*

Στη συνέχεια, θα δημιουργήσουμε ένα ζεύγος ιδιωτικού & δημοσίου κλειδιού. Από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Generate / Import Keys (Εικόνα 7.19).**

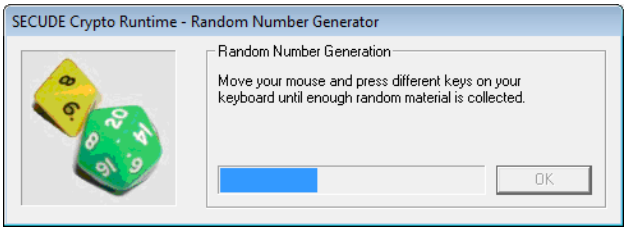


Εικόνα 7.19 *Δημιουργία ζεύγους κλειδιών στο Cryptool.*

Επιλέγουμε τη χρήση του RSA με modulus ίσο με 2048 bits. Εισάγουμε τα στοιχεία μας (User data). Αν, για παράδειγμα, είμαστε ο Jim Bell της NSA, θα μπορούσαμε να εισάγουμε:

- Last name: Bell
- First name: Jim
- Key Identifier: NSA
- PIN: protect

Πατάμε το κουμπί Generate new key pair. Μετά από ελάχιστα δευτερόλεπτα, αφού μετακινήσουμε το ποντίκι ή πατήσουμε τυχαία πλήκτρα ώστε να συλλεγούν τυχαίες τιμές, το ζεύγος κλειδιών δημιουργείται (Εικόνα 7.20).



Εικόνα 7.20 *Εκτέλεση διαδικασίας δημιουργίας ζεύγους κλειδιών στο Cryptool.*

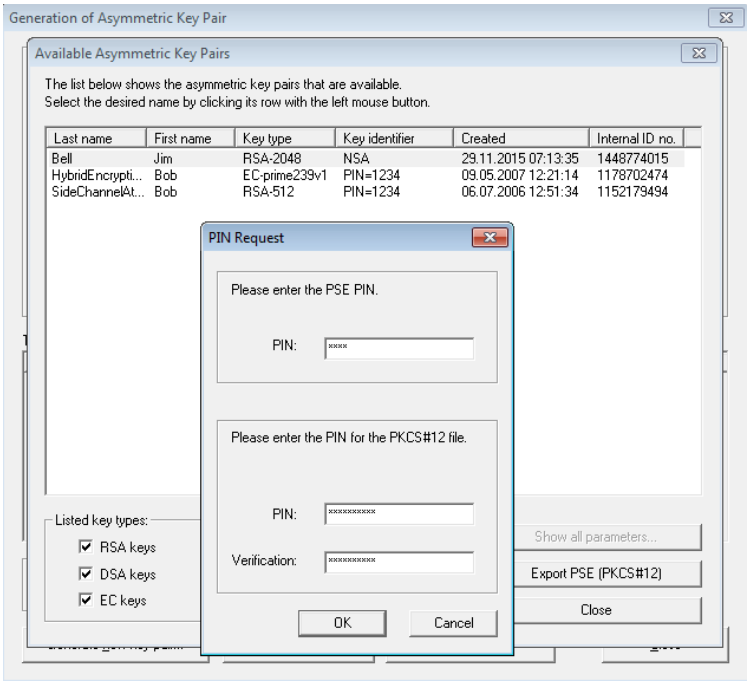
Για να το δούμε, επιλέγουμε το κουμπί **Show key pair…**

7.4.2.2 Εξαγωγή δημοσίου κλειδιού RSA

Στη ασύμμετρη κρυπτογραφία, για να αποστείλει κάποιος ένα κρυπτογραφημένο μήνυμα σε εμάς, θα πρέπει να γνωρίζει το δημόσιο κλειδί μας. Άρα, θα πρέπει με κάποιο τρόπο να το εξάγουμε και να μπορούμε να το διανείμουμε:

- Από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Key Display / Export**
- Επιλέγουμε το ζεύγος κλειδιών που δημιουργήσαμε

Πατάμε το κουμπί Export PSE (PKCS #12) και εισάγουμε το PIN που χρησιμοποιήσαμε κατά τη δημιουργία του ζεύγους κλειδιών. Στη συνέχεια, εισάγουμε PIN για το PKCS#12 αρχείο. Το PIN αυτό χρησιμοποιείται προκειμένου να περιορίσουμε την χρήση του δημοσίου κλειδιού μας σε όσους διαθέτουν το PKCS#12 PIN. Αφού εισάγουμε τις τιμές, αποθηκεύουμε το δημόσιο κλειδί (Εικόνα 7.21).



Εικόνα 7.21 *Εξαγωγή κλειδιού σε αρχείο τύπου PKCS#12.*

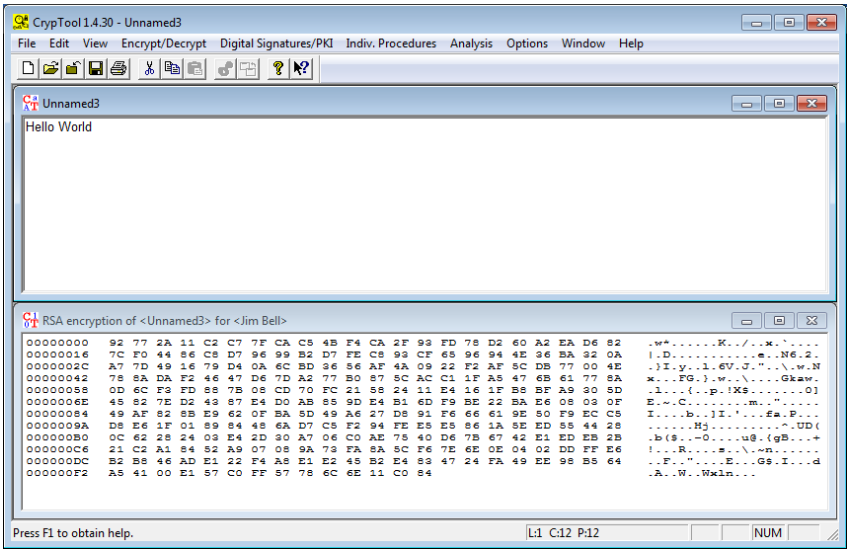
Μπορούμε να αποστείλουμε το δημόσιο αυτό κλειδί με οποιοδήποτε τρόπο σε όλους, όσοι επιθυμούν να το χρησιμοποιήσουν για να επικοινωνήσουν μαζί μας. Σε περιβάλλον του εργαστηρίου, μπορείτε να το αποστείλετε με email σε κάποιο συμφοιτητή/συνεργάτη σας.

7.4.2.3 Εισαγωγή δημοσίου κλειδιού RSA

Έστω ότι έχουμε στην κατοχή μας το δημόσιο κλειδί του προσώπου με το οποίο θα επικοινωνήσουμε. Στο εργαλείο Cryptool, από το μενού επιλέγουμε: **Digital Signatures / PKI → PKI → Key Generation/ import** και Πατάμε το κουμπί **PKCS#12 Import**. Διαλέγουμε από την επιφάνεια εργασίας το δημόσιο κλειδί του άλλου προσώπου που αποθηκεύσαμε και εισάγουμε το απαραίτητο PIN προκειμένου να ολοκληρωθεί η εισαγωγή του δημόσιου κλειδιού

7.4.2.4 Κρυπτογράφηση με χρήση RSA

Από το μενού του Cryptool επιλέγουμε: **File → New** και γράφουμε μία φράση της αρεσκείας μας. Στη συνέχεια από το μενού επιλέγουμε: **Encrypt / Decrypt → Asymmetric → RSA Encryption** και επιλέγουμε το δημόσιο κλειδί του παραλήπτη του κρυπτογραφήματος. Πατάμε Encrypt και εμφανίζεται το μήνυμά μας κρυπτογραφημένο με το δημόσιο κλειδί του άλλου προσώπου (Εικόνα 7.22).



Εικόνα 7.22 *Αρχικό μήνυμα και κρυπτογραφημένο με τον RSA.*

Έχοντας επιλέξει το παράθυρο του κρυπτοκειμένου, από το μενού επιλέγουμε: **File → Save as** και αποθηκεύουμε το αρχείο το οποίο μπορούμε να αποστείλουμε στον παραλήπτη. Προσπαθήστε να αποκρυπτογραφήσετε το αρχείο που μόλις κρυπτογραφήσατε. Είναι δυνατό; Συνάδει το αποτέλεσμα με όσα ξέρετε για την κρυπτογραφία δημόσιου κλειδιού;

7.4.2.5 Αποκρυπτογράφηση αρχείου με RSA

Ανοίξτε στο Cryptool ένα κρυπτογραφημένο μήνυμα που έχει κρυπτογραφηθεί με το δημόσιο κλειδί σας. Από το μενού επιλέξτε: **Encrypt/Decrypt → Asymmetric → RSA Decryption**. Επιλέξτε το μυστικό κλειδί που θα χρησιμοποιήσετε για την αποκρυπτογράφηση, εισάγετε το PIN και πατάτε Decrypt.

- Ποιο κλειδί χρησιμοποιήσατε για την αποκρυπτογράφηση;
- Γιατί υπάρχουν επιπρόσθετα μηδενικά στο τέλος του αρχείου;

Βιβλιογραφία

Delfs, H., & Knebl, H. (2007). Introduction to Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://link.springer.com/10.1007/3-540-49244-5

Konheim, A. G. (2007). Computer security and cryptography. Hoboken, N.J: Wiley-Interscience.

Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of applied cryptography. Boca Raton: CRC Press.

Paar, C., & Pelzl, J. (2010). Understanding cryptography: a textbook for students and practitioners. Heidelberg ; New York: Springer.

Stallings, W. (2014a). Cryptography and network security: principles and practice (Seventh edition). Boston: Pearson.

Stallings, W. (2014b). Network security essentials: applications and standards (Fifth edition). Boston: Pearson.

Stinson, D. R. (2006). Cryptography: theory and practice (3rd ed). Boca Raton: Chapman & Hall/CRC.

Πάγκαλου Γ., Μαυρίδη Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

Κριτήρια αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ο αλγόριθμος DES δέχτηκε επικρίσεις κυρίως για:
α) το μεγάλο μήκος κλειδιού.
β) το μικρό μήκος κλειδιού.
γ) την αργή ταχύτητα κρυπτογράφησης.
δ) την αδιαφάνεια κατά το σχεδιασμό της εσωτερικής του δομής.

2. Ο αλγόριθμος DES-OFB λειτουργεί ως αλγόριθμος:
α) δέσμης.
β) ροής.
γ) συμμετρικός.
δ) ασύμμετρος.

3. Ο αλγόριθμος AES είναι αλγόριθμος:
α) δέσμης.
β) ροής.
γ) συμμετρικός.
δ) ασύμμετρος.

4. Το μήκος δέσμης του AES μπορεί να είναι:
α) 64bit.
β) 128bit.
γ) 256bit.
δ) 512bit.

5. Ο αλγόριθμος DES χρησιμοποιεί δομή Feistel;
α) Ναι.
β) Μόνο σε λειτουργία CBC.
γ) Μόνο σε λειτουργία ECB.
δ) Όχι.

6. Το S-box του AES χρησιμοποιείται στην εκτέλεση του:
α) SubBytes.
β) ShiftColumns.
γ) MixRows.
δ) AddRoundKey.
ε) Key Expansion.

7. Ο RSA θεωρείται ασφαλής για:
α) κάθε πρώτο αριθμό p και q.
β) μεγάλους πρώτους αριθμούς p και q.
γ) κρυπτογραφήματα μεγαλύτερα από 1024 bits.

δ) κλειδιά μεγαλύτερα από 1024 bits.

8. Για ποιο ζεύγος αριθμών ισχύει πως είναι σχετικά πρώτοι
α) 3 και 20
β) 5 **και** 20
γ) 7 **και** 20
δ) 1 **και** 20

9. Η αποκρυπτογράφηση ενός κειμένου που έχει κρυπτογραφηθεί με DES, είναι δυνατή με τη χρήση του 3DES αν:
α) $K_1=K_2$.
β) $K_1<>K_2$.
γ) Ποτέ.
δ) Σε κάθε περίπτωση.

10. Αν το δημόσιο κλειδί του RSA είναι {7,33} το κρυπτογράφημα του αριθμού 2 είναι:
α) 27.
β) 29.
γ) 2.
δ) Δεν ορίζεται.

Δραστηριότητα 1

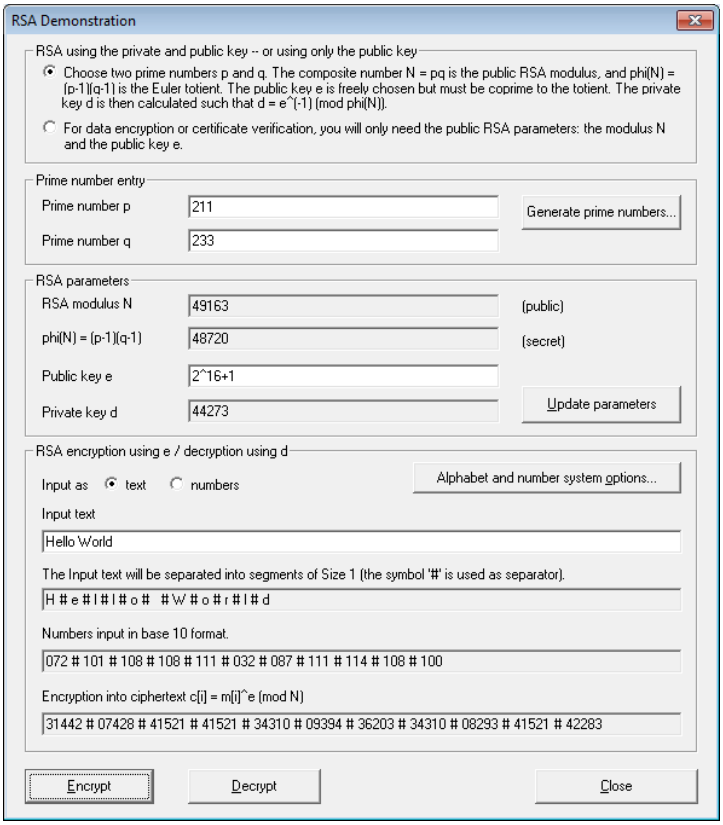
Χρησιμοποιήστε το Cryptool και κρυπτογραφήστε μια εικόνα (θα ανοίξει ως hexdump) με χρήση του DES σε ECB και CBC mode και συγκρίνετε τα κρυπτογραφήματα αφού τα αποθηκεύσετε. Προσπαθήστε η εικόνα σας να είναι σχετικά απλή με επαναλαμβανόμενα μοτίβα.

Δραστηριότητα 2

Στο Cryptool επιλέξτε Individual Procedures → Visualization of Algorithms και επιλέξτε την οπτικοποίηση των αλγόριθμων DES και AES για να μελετήσετε διαδραστικές παρουσίασεις των αλγόριθμων. Στη συνέχεια χρησιμοποιώντας μια γλώσσα προγραμματισμού υλοποιήστε τον DES ή τον 3DES.

Δραστηριότητα 3

Στο Cryptool επιλέξτε Encrypt/Decrypt → Asymmetric → RSA Demonstration και πειραματιστείτε με τη χρήση του RSA (Εικόνα 7.23). Εντοπίστε τον τρόπο με τον οποίο το κείμενο μετατρέπεται σε αριθμητικές τιμές για να κρυπτογραφηθεί.



Εικόνα 7.23 *Οπτικοποίηση του RSA.*

Κεφάλαιο 8. Ακεραιότητα και Αυθεντικότητα Μηνυμάτων

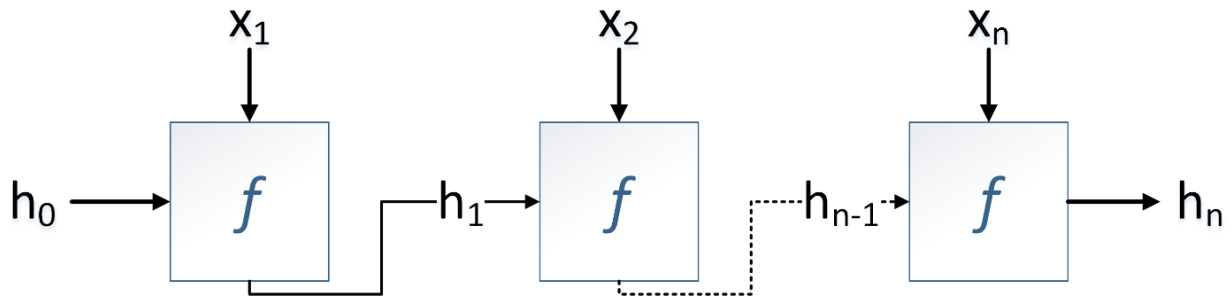
Σύνοψη
Κατά τη μεταφορά δεδομένων με τη μορφή μηνυμάτων στο Διαδίκτυο, κρίσιμο ζητούμενο αποτελεί η ύπαρξη μηχανισμών για την επιβεβαίωση της ακεραιότητας και αυθεντικότητας του κάθε μηνύματος στο σημείο παραλαβής του. Σημαντικό εργαλείο σε αυτή την κατεύθυνση αποτελούν οι μηχανισμοί ελέγχου ακεραιότητας, για παράδειγμα, με τη χρήση κρυπτογραφικών συναρτήσεων κατακερματισμού (cryptographic hash functions), καθώς και ελέγχου αυθεντικότητας του αποστολέα του μηνύματος με πρόσθετες τεχνικές. Στο κεφάλαιο αυτό, θα εξεταστούν τόσο ορισμένοι από τους πιο γνωστούς μηχανισμούς ελέγχου, όσο και ορισμένες από τις πιο γνωστές συναρτήσεις κατακερματισμού, στις οποίες συνήθως βασίζονται.

Προαπαιτούμενη γνώση
Για την παρακολούθηση του κεφαλαίου, είναι απαραίτητη η μελέτη των Κεφαλαίων 6 και 7, όπου παρουσιάζονται οι βασικές αρχές της κρυπτογραφίας και γίνεται αναφορά σε κρυπτογραφικούς αλγόριθμους.

8.1 Συναρτήσεις Κατακερματισμού

Μια συνάρτηση κατακερματισμού (hashing function) *h* δέχεται ως είσοδο μια σειρά m από bit, με οποιοδήποτε μήκος, ενώ παράγει στην έξοδο μια σειρά *h(m)* από bit με ένα προκαθορισμένο σταθερό μήκος, έστω k bit (λειτουργία συμπίεσης). Μια βασική ιδιότητα των συναρτήσεων κατακερματισμού είναι η ευκολία υπολογισμού (ease-of-computation) της εξόδου, γνωστής ως συνόψιση μηνύματος (message digest ή hash value).

Ο υπολογισμός της συνόψισης h ενός μηνύματος m γίνεται με επαναληπτική εφαρμογή μιας συνάρτησης συμπίεσης στις δέσμες x_i, όπου i = 1…n, στις οποίες χωρίζεται το μήνυμα. Ξεκινώντας από μια σταθερή αρχική τιμή συνόψισης h_0, υπολογίζονται οι ενδιάμεσες συνοψίσεις, ως εξής: $h_i = f(x_i \| h_{i-1})$, για i = 1…n, όπου το σύμβολο || σημαίνει συνένωση (concatenation). Η τελευταία υπολογισμένη συνόψιση h_n είναι η τελική συνόψιση h του μηνύματος m. Στον πυρήνα μιας συνάρτησης κατακερματισμού, υπάρχει η συνάρτηση συμπίεσης *f* που δέχεται ως εισόδους σειρές από bit σταθερού μήκους (Εικόνα 8.1).



Εικόνα 8.1 *Λειτουργία συνάρτησης κατακερματισμού.*

8.1.1 Μέγεθος μηνύματος και συμπλήρωση δέσμης

Πριν την εφαρμογή μιας συνάρτησης κατακερματισμού, κάθε είσοδος (μήνυμα), ανεξαρτήτως μήκους (πλήθους από bit), χωρίζεται σε δέσμες x_1, x_2, …, x_n με σταθερό μέγεθος j bit. Επειδή η τελευταία δέσμη πιθανώς να μην έχει μέγεθος j bit, εφαρμόζονται τεχνικές συμπλήρωσης (padding) ως εξής:

- **Μέθοδος 1:** Πρόσθεση όσων μηδενικών (ή κανενός) χρειάζεται για να συμπληρωθεί η τελευταία δέσμη (η παλιότερη μέθοδος).

- **Μέθοδος 2:** Πρόσθεση ενός μηδενικού και κατόπιν τόσων μηδενικών όσων χρειάζεται (μπορεί να προκαλεί τη δημιουργία μιας επιπλέον δέσμης).

- **Μέθοδος 3:** Όπως και η μέθοδος 2, αλλά επιπλέον περιλαμβάνεται ένας αριθμός για το μήκος των δεδομένων πριν το γέμισμα.

Αν δεν γνωστοποιείται, με κάποιο συγκεκριμένο τρόπο στη μεριά του παραλήπτη, το μέγεθος του κατειλημμένου μέρους της τελευταίας δέσμης πριν τη συμπλήρωσή της, τότε πρέπει να χρησιμοποιείται είτε η μέθοδος 2 είτε η μέθοδος 3, που ανιχνεύουν την πιθανή κακοπροαίρετη πρόσθεση/διαγραφή των τελευταίων μηδενικών. Η μέθοδος 1 χρησιμοποιείται σε εφαρμογές όπου το μήκος του κάθε μηνύματος είναι προκαθορισμένο και σταθερό.

8.1.2 Απαιτήσεις ανθεκτικότητας

Οι απαιτήσεις ασφάλειας για την ανθεκτικότητα μιας συνάρτησης κατακερματισμού περιλαμβάνουν τις ακόλουθες ιδιότητες (αντοχές):

- Αντοχή προαπεικόνισης (preimage resistance) ή μονόδρομη συμπεριφορά (one-way): Δεδομένης μια τιμής εξόδου y, είναι γενικά υπολογιστικά ανέφικτο να βρεθεί μια τιμή εισόδου x τέτοια ώστε h(x) = y.

- Αντοχή δεύτερης προαπεικόνισης (second preimage resistance) ή ασθενής αντοχή σε συγκρούσεις (weak collision resistance): Δεδομένης μιας τιμής εισόδου x και της εξόδου h(x), είναι υπολογιστικά ανέφικτο να βρεθεί μια άλλη διαφορετική τιμή εισόδου x’ τέτοια ώστε h(x) = h(x’).

- Αντοχή σε συγκρούσεις (collision resistance) ή σθεναρή αντοχή σε συγκρούσεις (strong collision resistance): Είναι υπολογιστικά ανέφικτο να βρεθούν δυο διαφορετικές τιμές εισόδου x και x’, τέτοιες ώστε h(x) = h(x’).

Σύγκρουση υπάρχει όταν για δυο διαφορετικές εισόδους x και x’ έχουμε h(x) = h(x’), δηλαδή όταν για δυο διαφορετικές εισόδους, η συνάρτηση κατακερματισμού παράγει ίδια έξοδο. Σε μια τέτοια περίπτωση, δίνεται η δυνατότητα σε εισβολείς να μεταβάλλουν τα μηνύματα που υφαρπάζουν κατά τη μετάδοσή τους, χωρίς η μεταβολή αυτή να γίνεται αντιληπτή από τους νόμιμους παραλήπτες τους.

Σημειώνεται, πως είναι υπολογιστικά ανέφικτο να αποδειχθεί ότι μια συνάρτηση κατακερματισμού ικανοποιεί τις παραπάνω ιδιότητες.

8.1.3 Συγκρούσεις και το παράδοξο της ημερομηνίας γέννησης

Όπως είδαμε, αποτελεί σημαντική απαίτηση για μια συνάρτηση κατακερματισμού το να είναι υπολογιστικά ανέφικτη (computationally infeasible) η εύρεση συγκρούσεων (collisions). Το πόσο πιθανό είναι να βρεθούν συγκρούσεις, στο πλαίσιο π.χ. μιας επίθεσης εκτενούς αναζήτησης (brute force attack), εξαρτάται από το επιλεγμένο σταθερό μήκος της παραγόμενης συνόψισης μηνύματος. Στην περίπτωση σύγκρουσης, δίνεται η δυνατότητα σε εισβολείς να μεταβάλλουν τα μηνύματα που υφαρπάζουν κατά τη μετάδοσή τους, χωρίς η μεταβολή αυτή να γίνεται αντιληπτή από τους νόμιμους παραλήπτες τους.

Σχετικό είναι το παράδοξο της ημερομηνίας γέννησης (birthday paradox), που βοηθά στο να αντιληφθούμε ότι η επιλογή του μεγέθους της συνόψισης με έναν απλό υπολογισμό δεν είναι πάντα η καλύτερη λύση. Το παράδοξο αυτό μας λέει ότι αν υποθέσουμε ότι έχουμε μια ομάδα 23 ατόμων, τότε η πιθανότητα να υπάρχουν δυο άτομα με ίδια ημερομηνία γέννησης (365 διαφορετικά ισοπίθανα ενδεχόμενα) είναι μεγαλύτερη του 0,5. Η μικρή τιμή 23 είναι που εκπλήσσει και για το λόγο αυτό μιλάμε για παράδοξο, αφού κανείς θα περίμενε κάτι τέτοιο να συμβαίνει όταν η ομάδα θα αριθμούσε τουλάχιστον (365/2) 183 άτομα.

Πράγματι, ας θεωρήσουμε γενικότερα μια ομάδα *k* ατόμων και έστω *n* το πλήθος των πιθανών ημερομηνιών γέννησής τους (προηγουμένως είχαμε k = 23 και n = 365). Έστω ότι $p_{n,k}$ είναι η πιθανότητα να μην υπάρχουν δυο άτομα με την ίδια ημερομηνία γέννησης στην ομάδα. Υπολογίζεται ότι $p_{n,k} \leq e^{-k(k-1)/(2n)}$ και επομένως, σε μια γενική περίπτωση, όταν:

$$k \geq (1 + \sqrt{1 + 8n \log 2}) / 2 \qquad (8.1)$$

(π.χ. για n = 365, υπολογίζουμε $k \geq 22,99994$) θα έχουμε $p_{n,k} \leq 1/2$.

Η εφαρμογή του παράδοξου της ημερομηνίας γέννησης στο χώρο της κρυπτογραφίας αφορά την επίθεση, όπου αν ένας επιτιθέμενος επιλέξει k το πλήθος σειρές από bit x(i) μήκους n bit (όπου $1 \leq i \leq k$) και υπολογίσει τις συνοψίσεις τους h(x(i)), τότε η πιθανότητα να βρεθούν ίδιες συνοψίσεις για δυο διαφορετικές σειρές από bit είναι μεγαλύτερη από 0,5.

Με το σημερινό τεχνολογικό υπόβαθρο, μια συνόψιση για να είναι πράγματι ελεύθερη-συγκρούσεων θα πρέπει να έχει μήκος τουλάχιστον 160 bit (καλύτερα 256 bit).

8.2 Αλγόριθμοι Παραγωγής Συνοψίσεων Μηνυμάτων

Η παραγωγή συνοψίσεων μηνυμάτων μπορεί να γίνει είτε με αξιοποίηση της κρυπτογραφίας (τυπικό παράδειγμα είναι με DES-CBC), είτε χωρίς αυτήν (τυπικά παραδείγματα είναι ο αλγόριθμος MD5 και η οικογένεια αλγορίθμων SHA).

Στη συνέχεια, παρουσιάζονται γνωστοί αλγόριθμοι παραγωγής συνόψισης μηνύματος, που χρησιμοποιούνται ευρέως σε πραγματικές εφαρμογές.

8.2.1 MD5

Ο αλγόριθμος συνόψισης μηνύματος MD5 (Message-Digest algorithm 5), αναπτύχθηκε από τον Ron Rivest [RFC 1321] το 1991 (για να αντικαταστήσει τον MD4) και χρησιμοποιείται μέχρι και σήμερα, αν και το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ (U. S. Department of Homeland Security) συστήνει τη μετάβαση στην οικογένεια των αλγορίθμων SHA, καθώς ο MD5 θεωρείται ότι δεν είναι ανθεκτικός σε συγκρούσεις (collision resistant) και δεν ενδείκνυται για σοβαρές εφαρμογές, όπως οι ψηφιακές υπογραφές. Ο MD5 χρησιμοποιείται, πλέον, κυρίως για τον έλεγχο της ακεραιότητας αρχείων που διακινούνται μέσω του Διαδικτύου.

Αρχικά, το μήνυμα χωρίζεται σε δέσμες μήκους 512 bit. Ο αλγόριθμος MD5 πραγματοποιεί μια επέκταση της τελευταίας δέσμης του μηνύματος, έτσι ώστε να τη μετατρέψει σε δέσμη μήκους 512 bit, ως εξής:

- Προστίθεται στα δεξιά ένα bit με τιμή 1, για να σηματοδοτήσει την αρχή του επιθέματος (postfix).
- Στη συνέχεια, προστίθενται τόσα bit με τιμή 0, όσα είναι απαραίτητα ώστε το μήκος της δέσμης να γίνει ίσο με 448 bit.
- Τέλος, προσαρτάται η τιμή (με μέγεθος 64-bit) του συνολικού μήκους του μηνύματος πριν την επέκτασή του.

Επιπλέον, ο αλγόριθμος MD5 χρησιμοποιεί μια αρχική συνόψιση (initial seed) τεσσάρων (4) λέξεων (A, B, C, D), μήκους 32-bit η κάθε μια. Οι αντίστοιχες τιμές των τεσσάρων αυτών λέξεων είναι σταθερές και φαίνονται στον Πίνακα 8.1.

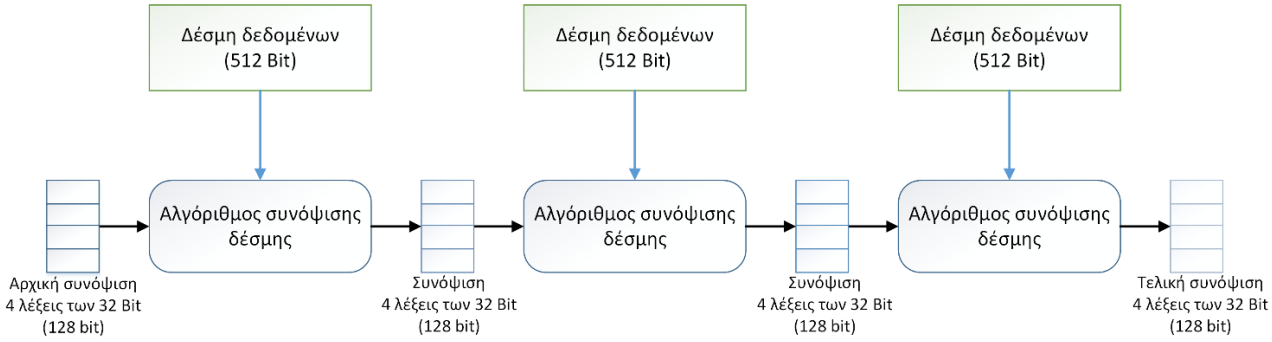
Λέξη A	01	23	45	67
Λέξη B	89	AB	CD	EF

Λέξη C	FE	DC	BA	98
Λέξη D	76	54	32	10

Πίνακας 8.1 *Αρχική συνόψιση MD5.*

Στη συνέχεια, ξεκινώντας από την αρχική συνόψιση (128-bit), που αποτελεί το τρέχον περιεχόμενο του ενταμιευτήρα (buffer) του MD5, σε συνδυασμό με την πρώτη δέσμη του μηνύματος, γίνεται επαναληπτική επεξεργασία του μηνύματος κατά δέσμες των 16-λέξεων (512-bit). Η επεξεργασία αυτή εξελίσσεται στο πλαίσιο μιας διαδικασίας τεσσάρων (4) κύκλων, με λειτουργίες 16 βημάτων σε κάθε κύκλο.

Στο τέλος κάθε επεξεργασίας, γίνεται πρόσθεση του αποτελέσματος στον ενταμιευτήρα εισόδου για να προκύψει μια νέα τιμή. Η τιμή του τελευταίου ενταμιευτήρα είναι το ζητούμενο αποτέλεσμα, δηλαδή η τελική συνόψιση του μηνύματος (message digest).



Εικόνα 8.2 *Συνόψιση μηνύματος τριών δεσμών με τον αλγόριθμο MD5.*

Ο δημιουργός του MD5, Ronald Rivest, διατύπωσε την ακόλουθη εικασία: "Εικάζεται ότι η δυσκολία να έχετε δύο μηνύματα με την ίδια συνόψιση μηνύματος είναι της τάξης των 2^{64} πράξεων και ότι η δυσκολία να βρείτε ένα μήνυμα που έχει μια δεδομένη συνόψιση μηνύματος είναι της τάξης των 2^{128} πράξεων". Από ένα αυθαίρετο 128-bit string x, είναι πολύ δύσκολο να βρεθεί ή να φτιαχτεί μήνυμα m του οποίου η συνόψιση που παράγεται από τον αλγόριθμο MD5 να είναι ίση με μια δεδομένη τιμή x.

Παρόλα αυτά, το 1996 βρέθηκε ένα σχεδιαστικό λάθος του MD5, ενώ το 2004 εντοπίσθηκαν πιο σοβαρές αδυναμίες, διαταράσσοντας ακόμη πιο πολύ την αξιοπιστία του αλγορίθμου για εφαρμογές ασφάλειας. Έκτοτε, έχουν προταθεί τρόποι δημιουργίας αρχείων τα οποία έχουν την ίδια τιμή συνόψισης. Ως αποτέλεσμα, το ενδιαφέρον στράφηκε προς την οικογένεια αλγορίθμων SHA, ξεκινώντας από το πρώτο μέλος της, που είναι γνωστό ως SHA-1.

8.2.2 Οικογένεια αλγορίθμων SHA

Η αρχική προδιαγραφή της οικογένειας SHA, δημοσιεύθηκε το 1993 από το NIST των ΗΠΑ (FIPS PUB 180), με την ονομασία Secure Hash Standard, που είναι γνωστή πλέον ως SHA-0, καθώς γρήγορα αποσύρθηκε από την NSA. Η αναθεωρημένη έκδοσή της δημοσιεύθηκε το 1995 με την ονομασία SHA-1 (FIPS PUB 180-1).

Ο αλγόριθμος SHA-1 (Secure Hash Algorithm 1) είναι ο δεύτερος κορυφαίος αλγόριθμος παραγωγής συνόψισης μηνύματος που χρησιμοποιείται σήμερα. Βασίζεται σε αρχές παρόμοιες με αυτές που χρησιμοποιήθηκαν κατά τη σχεδίαση του MD4, του προγόνου του MD5. Ο SHA-1 παράγει σύνοψη μήκους 160-bit. Το μεγαλύτερο μήκος εξόδου κάνει τον SHA-1 ασφαλέστερο από τον MD5, αν και μια σημαντική διαφορά μεταξύ των δυο αλγορίθμων αφορά το μήκος του μηνύματος εισόδου. Στον SHA-1 αυτό δεν μπορεί να είναι οποιοδήποτε και θα πρέπει να μην ξεπερνά τα $2^{64} - 1$ bit, που είναι βέβαια μια πολύ μεγάλη τιμή.

Ο αλγόριθμος SHA-1 χρησιμοποιεί κι αυτός μια αρχική συνόψιση (initial seed) μήκους 160 bit που αποτελείται από πέντε (5) λέξεις (A, B, C, D, E), με μήκος 32-bit η κάθε μια. Οι σταθερές τιμές τους φαίνονται στον Πίνακα 8.2.

Λέξη A	67	45	23	01
Λέξη B	EF	CD	AB	89
Λέξη C	98	BA	DC	FE
Λέξη D	10	32	54	76
Λέξη E	C3	D2	E1	F0

Πίνακας 8.2 *Αρχική συνόψιση SHA-1.*

Ο αλγόριθμος SHA επεκτείνει αρχικά το μήνυμα, όπως και ο MD5, ώστε το μήκος του να είναι πολλαπλάσιο του 512. Η επαναληπτική επεξεργασία κάθε δέσμης μήκους 512 bit, περιλαμβάνει 4 κύκλους των είκοσι (20) βημάτων. Έτσι, ολόκληρη η διαδικασία παραγωγής συνόψισης περιλαμβάνει 80 βήματα, κάθε ένα από τα οποία τροποποιεί τα δεδομένα 5 καταχωρητών των 32 bit (A, B, C, D, E).

Νεότερες δημοσιεύσεις του NIST (από το 2001 μέχρι σήμερα), καθορίζουν ως νεότερα μέλη της οικογενείας τις ακόλουθες συναρτήσεις κατακερματισμού, γνωστές ως SHA-2: SHA-224, SHA-256, SHA-384,και SHA-512. Οι τιμές που ακολουθούν το ακρωνύμιο SHA, δηλώνουν και το μήκος συνόψισης που παράγει η κάθε μια από αυτές, Στον Πίνακα 8.3, που ακολουθεί, αποτυπώνονται τα βασικά χαρακτηριστικά του κάθε μέλους της οικογένειας αλγορίθμων SHA:

Αλγόριθμος		**Μήκος Συνόψισης**	**Μήκος δέσμης**	**Μέγιστο μήκος εισόδου**	**Μήκος λέξης**	**Κύκλοι x Βήματα**
SHA-0		160	512	2^{64}-1	32	4 x 20
SHA-1		160	512	2^{64}-1	32	4 x 20
SHA2	SHA-224	224	512	2^{64}-1	32	4 x 16
	SHA-256	256	512	2^{64}-1	32	4 x 16
	SHA-384	384	1024	2^{128}-1	64	4 x 20
	SHA-512	512	1024	2^{128}-1	64	4 x 20

Πίνακας 8.3 *Βασικά χαρακτηριστικά της οικογένειας αλγορίθμων SHA.*

Το 2003 παρουσιάστηκε ένα νέο πρότυπο με την ονομασία Secure Hash Standard (SHS), το οποίο πρόσθεσε τρεις (3) νέους αλγορίθμους παραγωγής συνοψίσεων μεγαλύτερου μήκους. Το πρότυπο SHS χρησιμοποιείται από το Digital Signature Algorithm (DSA) για την παραγωγή Ψηφιακών Υπογραφών. Το πρωτόκολλο Secure Shell (SSH), το οποίο αποτελεί και κυβερνητικό πρότυπο (FIPS PUB 180-2), περιλαμβάνει συνολικά τέσσερις SHA αλγόριθμους SHA-1, SHA-256, SHA-384 και SHA-512.

8.3 Εφαρμογές Ελέγχου Ακεραιότητας και Αυθεντικότητας

Κατά τη μεταφορά δεδομένων με τη μορφή μηνυμάτων στο Διαδίκτυο, αποτελεί κρίσιμο ζητούμενο η ύπαρξη μηχανισμών για την επιβεβαίωση της αυθεντικότητας του αποστολέα και της ακεραιότητας του μηνύματος στο σημείο παραλαβής του. Σημαντικό εργαλείο σε αυτή την κατεύθυνση αποτελούν οι συνοψίσεις μηνυμάτων (message digests).

Κατά την παραλαβή ενός ηλεκτρονικού μηνύματος, θα πρέπει να είμαστε σίγουροι ότι το μήνυμα δεν έχει τροποποιηθεί (έλεγχος ακεραιότητας), αλλά και ότι προέρχεται από τον αποστολέα ο οποίος ισχυρίζεται ότι το έστειλε (έλεγχος αυθεντικότητας). Στην καθημερινή μας ζωή, όταν ένα γραπτό μήνυμα (π.χ. μια επιστολή) αποστέλλεται, υπογράφεται από τον αποστολέα με χειρόγραφη υπογραφή, έτσι ώστε ο παραλήπτης να μπορεί να επαληθεύσει την αυθεντικότητα του αποστολέα του μηνύματος.

Η συνόψιση ενός μηνύματος εγγυάται την ακεραιότητά του. Εγγυάται, δηλαδή, πως το μήνυμα δεν έχει υποστεί τροποποίηση. Ωστόσο, η συνόψιση δεν αυθεντικοποιεί και τον αποστολέα του μηνύματος. Όταν η Αλίκη στείλει ένα μήνυμα στον Βασίλης, ο Βασίλης χρειάζεται να γνωρίζει αν το μήνυμα προέρχεται πραγματικά από την Αλίκη.

Η συνόψιση ενός μηνύματος, που συνήθως είναι γνωστή με την ονομασία Κώδικας Ανίχνευσης Μετατροπών (Message Detection Code, MDC), δεν αρκεί για την αυθεντικοποίηση του μηνύματος. Με τον

όρο αυθεντικοποίηση μηνύματος, εννοούμε την αυθεντικότητα της προέλευσης των δεδομένων (data origin authentication) και για το σκοπό αυτό χρειαζόμαστε την εφαρμογή μιας πρόσθετης τεχνικής που παράγει τον Κώδικα Αυθεντικοποίησης Μηνύματος (Message Authentication Code, MAC).

8.3.1 Κώδικας Ανίχνευσης Μετατροπών – MDC

Αρκετές φορές, στην επικοινωνία μέσω Διαδικτύου δεν απαιτείται η διασφάλιση της ιδιότητας της εμπιστευτικότητας, αλλά της ιδιότητας της ακεραιότητας των μεταδιδόμενων δεδομένων. Για παράδειγμα, έστω ότι η Αλίκη επιθυμεί να αποστείλει ένα μήνυμα στο Βασίλη μέσω του ανασφαλούς Διαδικτύου. Για την Αλίκη δεν είναι απαραίτητο να παραμείνει μυστικό το μήνυμα, όσο το να είναι σίγουρη ότι θα παραληφθεί από τον Βασίλη χωρίς να έχει τροποποιηθεί από κάποιον ενδιάμεσο (π.χ. την Ελένη).

Για την προστασία την ακεραιότητας του μηνύματος, οποιουδήποτε σχεδόν μεγέθους, η Αλίκη παρέχει το μήνυμα ως είσοδο σε μια συνάρτηση κατακερματισμού, η οποία ικανοποιεί τις απαιτήσεις αποφυγής συγκρούσεων που αναφέραμε πριν και δημιουργεί μια σταθερού μήκους συνόψιση. Η συνόψιση του μηνύματος μπορεί στη συνέχεια να χρησιμοποιηθεί ως το αποτύπωμα (fingerprint) του μεταδιδόμενου μηνύματος. Η διαδικασία αυτή παρουσιάζεται στην ακόλουθη Εικόνα 8.3:

Εικόνα 8.3 *Παραγωγή συνόψισης μεταδιδόμενου μηνύματος.*

Κατόπιν, η Αλίκη αποστέλλει το μήνυμα και τη συνόψισή του στο Βασίλη. Για την επιβεβαίωση της ακεραιότητας του μηνύματος, ο Βασίλης τροφοδοτεί εκ νέου το παραλαμβανόμενο μήνυμα στην ίδια συνάρτηση κατακερματισμού και αν η παραγόμενη συνόψιση είναι ίδια με την παραληφθείσα συνόψιση (που έστειλε η Αλίκη), τότε μπορεί να είναι βέβαιος ότι δεν πραγματοποιήθηκε τροποποίηση του μηνύματος κατά τη μετάδοσή του.

Ο Κώδικας Ανίχνευσης Μετατροπών (Manipulation Detection Code - MDC), γνωστός και ως Κώδικας Ακεραιότητας Μηνύματος (Message Integrity Code - MIC), αποτελεί το μέσο για τη ανίχνευση μετατροπών σε ένα μήνυμα που μεταφέρθηκε μέσω Διαδικτύου. Για την παραγωγή του χρησιμοποιούνται:

- Μονόδρομες συναρτήσεις κατακερματισμού (one-way hash functions – OWHF) που παρέχουν συμπίεση, ευκολία υπολογισμού, αντοχή προαπεικόνισης και αντοχή δεύτερης προαπεικόνισης.

- Ανθεκτικές σε συγκρούσεις συναρτήσεις κατακερματισμού (collision-resistant hash functions – CRHF) που παρέχουν συμπίεση, ευκολία υπολογισμού, αντοχή δεύτερης προαπεικόνισης και αντοχή σε συγκρούσεις.

Γενικά, παρέχουν μηχανισμούς ακεραιότητας, παράγοντας μια σταθερού μήκους σειρά από bit, που υπολογίζεται χωρίς να χρησιμοποιηθεί κλειδί (unkeyed hash functions).

8.3.2 Κώδικας Αυθεντικοποίησης Μηνυμάτων - MAC

Ο Κώδικας Αυθεντικοποίησης Μηνύματος (Message Authentication Code - MAC) παρέχει αυθεντικοποίηση της πηγής προέλευσης (data origin authentication) και προστασία ακεραιότητας του ίδιου του μηνύματος. Για τον υπολογισμό του χρησιμοποιούνται δυο είσοδοι:

- το μήνυμα
- ένα μυστικό κλειδί κρυπτογράφησης

Κατά τη διαδικασία αυθεντικοποίησης, ο παραλήπτης χρησιμοποιεί το κοινό μυστικό κλειδί που είχε χρησιμοποιήσει και ο αποστολέας κατά τον υπολογισμό του κώδικα MAC.

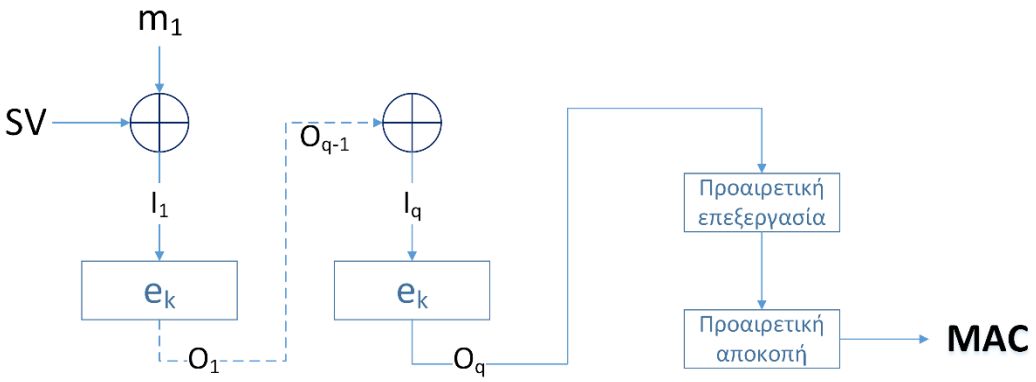
Πιο συγκεκριμένα, χρησιμοποιείται ένα κλειδί και μια κρυπτογραφική συνάρτηση για τον υπολογισμό της τιμής-ελέγχου (MAC) των δεδομένων, που κατόπιν στέλνεται μαζί με τα δεδομένα. Ο υπολογισμός του MAC συμβολίζεται ως εξής:

$$MAC = f_k(m) \tag{8.2}$$

όπου f είναι η κρυπτογραφική συνάρτηση για τον υπολογισμό της τιμής-ελέγχου του μηνύματος m, ενώ k είναι το μυστικό κλειδί κρυπτογράφησης.

Οι πλέον αποδεκτοί μηχανισμοί παραγωγής MAC είναι οι CBC-MAC, που λειτουργούν με αξιοποίηση ενός αλγόριθμου κρυπτογράφησης δέσμης (π.χ. DES, 3DES, αλλά με καθολική πλέον επικράτηση του AES) σε τρόπο λειτουργίας (mode of operation) CBC.

Για την παραγωγή του CBC-MAC χρησιμοποιείται ένα κλειδί και ένας αλγόριθμος δέσμης n-bit για να δώσει ένα m-bit MAC ($m \leq n$). Αρχικά, γίνεται συμπλήρωση (padding) των δεδομένων για να προκύψουν σειρές δεσμών των *n*-bit. Στη συνέχεια, γίνεται κρυπτογράφηση των δεδομένων σε CBC mode. Συγκεκριμένα, για τις δέσμες δεδομένων (μήκους *n*-bit) m_1, m_2, ..., m_q, το MAC υπολογίζεται όπως φαίνεται στην Εικόνα 8.4:



Εικόνα 8.4 *Παραγωγή CBC-MAC.*

Έχουμε:

$$I_1 = m_1 \oplus SV \tag{8.3}$$

και

$$O_1 = e_k(I_1) \tag{8.4}$$

Για i=1,2,3,…,n:

$$I_q = m_q \oplus O_{q-1} \tag{8.5}$$

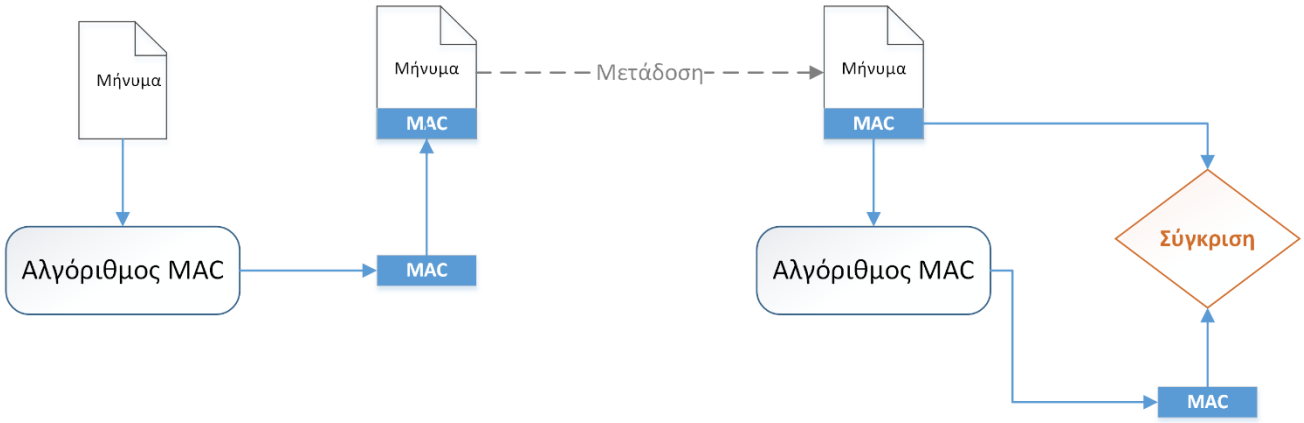
και

$$O_q = e_k(I_q) \tag{8.6}$$

Η έξοδος O_q υπόκειται σε μια προαιρετική επεξεργασία και αποκοπή σε *m* bit για να δώσει τελικά το MAC.

Όπου ⊕ η λογική πράξη XOR και SV (starting variable) είναι μια τυχαία επιλεγμένη τιμή που αποστέλλεται (σε μορφή plaintext) μαζί με το μήνυμα.

Ο κώδικας MAC προϋποθέτει το διαμοιρασμό μεταξύ δύο πλευρών ενός μυστικού κλειδιού, προκειμένου να αυθεντικοποιήσουν την πηγή προέλευσης (origin) των μεταξύ τους μεταδιδόμενων δεδομένων. Η αυθεντικότητα της πηγής προέλευσης των δεδομένων, την οποία εγγυάται η συνάρτηση MAC, απορρέει από το γεγονός ότι δεν είναι δυνατό να αναπαραχθεί η ίδια συνόψιση χωρίς τη γνώση του κλειδιού. Ένας ενδιάμεσος ο οποίος υποκλέπτει το μήνυμα δεν θα μπορέσει να τροποποιήσει τα δεδομένα του μηνύματος και μετά να παράγει σωστό κώδικα MAC. Στην ακόλουθη Εικόνα 8.5, απεικονίζεται ο τρόπο αξιοποίησης του μηχανισμού MAC κατά τη μετάδοση μηνυμάτων.



Εικόνα 8.5 *Αξιοποίηση μηχανισμού MAC.*

Η Αλίκη παράγει τον κώδικα MAC και τον αποστέλλει μαζί με το μήνυμα στο Βασίλη. Ο Βασίλης πραγματοποιεί τον ίδιο υπολογισμό στο παραληφθέν μήνυμα, χρησιμοποιώντας το ίδιο μυστικό κλειδί, προκειμένου να ξαναδημιουργήσει το MAC. Στη συνέχεια, γίνεται σύγκριση του παραληφθέντος και του νέου κώδικα αυθεντικοποίησης. Αν υποθέσουμε ότι μόνο ο παραλήπτης και ο αποστολέας γνωρίζουν το μυστικό κλειδί, τότε ισχύουν οι παρακάτω παρεχόμενες υπηρεσίας ασφάλειας:

- Ακεραιότητα μηνύματος: Ο παραλήπτης είναι βέβαιος ότι το μήνυμα δεν έχει τροποποιηθεί. Αν ένας επιτιθέμενος τροποποιούσε το μήνυμα δεν θα μπορούσε να δημιουργήσει ένα καινούργιο κώδικα MAC, καθώς δεν γνωρίζει το μυστικό κλειδί.

- Αυθεντικότητα πηγής προέλευσης μηνύματος: Ο παραλήπτης είναι βέβαιος ότι το μήνυμα στάλθηκε από τον αποστολέα ο οποίος εμφανίζεται ως κανονικός αποστολέας. Επειδή κανείς άλλος δεν γνωρίζει το μυστικό κλειδί, άρα κανείς άλλος δεν θα μπορούσε να δημιουργήσει το σωστό MAC.

Είναι φανερό ότι τα κλειδιά πρέπει να προστατεύονται ώστε να διασφαλίζεται ότι δεν θα διαρρεύσουν σε τρίτους.

Γνωστός τύπος επίθεσης σε MAC είναι η επίθεση ‘cut-and-paste’. Αν υποθέσουμε ότι ο MAC υπολογίζεται με CBC (CBC-MAC) χωρίς να ακολουθήσουν προαιρετική επεξεργασία και αποκοπή (truncation), τότε για δυο μηνύματα m_1 και m_2 με κώδικες MAC που έχουν υπολογισθεί με το ίδιο μυστικό κλειδί k, είναι δυνατό να υπολογισθεί ένα τρίτο ψευδές μήνυμα, καθώς και ο κώδικας MAC που του αντιστοιχεί, χωρίς ο επιτιθέμενος να γνωρίζει το (μυστικό) κλειδί k. Αυτό γίνεται σε μια περίπτωση επίθεσης όπου είναι γνωστοί οι MAC για δυο μηνύματα μιας δέσμης. Έτσι, αν υποθέσουμε ότι:

$MAC_1 = e_k(m1)$
$MAC_2 = e_k(m2)$

τότε, ο MAC_2 είναι ένας σωστός MAC του νέου μηνύματος *m3* δυο δεσμών $m1 \| m2 \oplus MAC1$, όπου $\oplus$ η λογική πράξη XOR.

Για να αποφεύγονται τέτοιου είδους επιθέσεις σε νόμιμους MAC, απαιτείται η εφαρμογή επεξεργασίας και αποκοπής του μηνύματος, ή να χρησιμοποιείται η τρίτη μέθοδος συμπλήρωσης (padding).

8.3.3 HMAC

Για τον υπολογισμό του κώδικα MAC, μπορούν ακόμη να χρησιμοποιηθούν συναρτήσεις κατακερματισμού (hash-functions), όπου γίνεται αρχικά συνένωση (concatenation) ενός κοινού μυστικού κλειδιού με το μήνυμα που πρόκειται να μεταδοθεί και κατόπιν εφαρμόζεται η συνάρτηση κατακερματισμού. Το αποτέλεσμα του κώδικα MAC σε αυτή την περίπτωση ονομάζεται HMAC (hashed MAC). Για αυτό και οι σχετικοί μηχανισμοί ονομάζονται συναρτήσεις κατακερματισμού με κλειδί (keyed hash functions). Το κλειδί χρησιμοποιείται για να παραμετροποιείται η συμπεριφορά της συνάρτησης κατακερματισμού.

Ένα τέτοιο παράδειγμα αφορά την αξιοποίηση μιας συνάρτησης κατακερματισμού *h* στο πλαίσιο μιας δομής HMAC, όπου για μια τιμή κλειδιού *k* και για ένα μήνυμα *m* υπολογίζουμε:

$$HMAC(m) = h(K1 \| h(K2 \| m)) \tag{8.7}$$

όπου

- *h* είναι η συνάρτηση κατακερματισμού,
- *K1* και *K2* είναι δυο παραλλαγές του μυστικού κλειδιού *k*
- || είναι η συνένωση των επιμέρους ακολουθιών bit.

Οι παραλλαγές *K1* και *K2* του μυστικού κλειδιού *k* μπορούν να προκύπτουν από τη συνένωση ακολουθιών bit συμπλήρωσης (padding) του κλειδιού, ως εξής: $K1 = k \| p1$ και $K2 = k \| p2$.

Το πρότυπο FIPS PUB 198 (από το 2002) περιγράφει τον κώδικα HMAC σαν ένα μηχανισμό αυθεντικοποίησης μηνύματος, ο οποίος χρησιμοποιεί κρυπτογραφικές συναρτήσεις συνόψισης. Ο HMAC μπορεί να χρησιμοποιηθεί με κάθε συνάρτηση συνόψισης σε συνδυασμό με ένα ή περισσότερα κοινά μυστικά κλειδιά.

Βιβλιογραφία

Burnett, S., & Paine, S. (2001). RSA Security's Official Guide to Cryptography. Berkeley, CA, USA: Osborne/McGraw-Hill.

Forouzan, B. A. (2008). Introduction to cryptography and network security. Boston: McGraw-Hill Higher Education.

Konheim, A. G. (2007). Computer Security and Cryptography. Hoboken, NJ, USA: John Wiley & Sons, Inc. Retrieved from http://doi.wiley.com/10.1002/0470083980

Stallings, W. (2014). Network security essentials: applications and standards (Fifth edition). Boston: Pearson.

Stinson, D. R. (2006). Cryptography: theory and practice (3rd ed). Boca Raton: Chapman & Hall/CRC.

Πάγκαλου Γ., Μαυρίδη Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Για μία συνόψιση θα πρέπει να ισχύει ότι:
α) Είναι μοναδική.
β) Είναι υπολογιστικά ανέφικτο να παραχθεί.
γ) Μπορεί να ανακτηθεί από αυτή το μήνυμα.
δ) Κανένα από τα παραπάνω.

2. Η συνόψιση είναι ελεύθερη συγκρούσεων όταν:
α) Έχει μέγεθος 128 bit τουλάχιστον.
β) Μπορούν να υπάρξουν δύο διαφορετικά μηνύματα με ίδιες συνοψίσεις.
γ) Δεν μπορούν να υπάρξουν δύο διαφορετικά μηνύματα με ίδιες συνοψίσεις.
δ) Δεν είναι υπολογιστικά εφικτό να βρεθούν δύο διαφορετικά μηνύματα με ίδιες συνοψίσεις.

3. Ο αλγόριθμος MD5 δημιουργεί συνοψίσεις μήκους:
α) 32 bit
β) 64 bit
γ) 128 bit
δ) 160 bit

4. Η συνόψιση ενός μηνύματος μπορεί να διασφαλίσει:
α) την ακεραιότητά του.
β) τη διαθεσιμότητά του.
γ) την εμπιστευτικότητά του.
d) την αυθεντικότητα προέλευσής του.

5. Για τον υπολογισμό του κώδικα MAC χρησιμοποιείται:
α) κρυπτογραφικός αλγόριθμος ροής.
β) ασύμμετρος κρυπτογραφικός αλγόριθμος.
γ) συνάρτηση κατακερματισμού χωρίς κλειδί.
δ) συμμετρικός κρυπτογραφικός αλγόριθμος.

6. Χρησιμοποιούνται κλειδιά για την παραγωγή του:
α) Message Authentication Code (MAC)
β) Hashed MAC (HMAC)
γ) SHA1 digest
δ) MD5 digest

7. Για τη δημιουργία συνόψισης ενός πολύ μεγάλου όγκου δεδομένων (π.χ. 2^{234} bit), θα επιλέγατε:
α) Τον αλγόριθμο MD5
β) Τον αλγόριθμο SHA1
γ) Τον αλγόριθμο SHA224
δ) Τον αλγόριθμο SHA512

8. Πόσες δέσμες θα δημιουργηθούν για τη δημιουργία συνόψισης ενός αρχείου μεγέθους 1040 bytes με τον αλγόριθμο SHA256;
α) 1
β) 2
γ) 3
δ) 4

9. Ποια από τα παρακάτω προσφέρει ο κώδικας αυθεντικοποίησης MAC;
α) Αυθεντικοποίηση πηγής προέλευσης.
β) Αυθεντικοποίηση προορισμού.
γ) Ακεραιότητα δεδομένων.
δ) Εμπιστευτικότητα δεδομένων.

10. Για την παραγωγή του κώδικα HMAC χρησιμοποιούνται:
α) συναρτήσεις κατακερματισμού και μυστικό κλειδί.
β) συναρτήσεις κατακερματισμού χωρίς μυστικό κλειδί.
γ) συνάρτηση συμπίεσης δεδομένων με μυστικό κλειδί.
δ) συνάρτηση συμπίεσης χωρίς μυστικό κλειδί.

Κεφάλαιο 9. Ψηφιακές Υπογραφές και Ψηφιακά Πιστοποιητικά

Σύνοψη

Η ολοένα και μεγαλύτερη διάδοση της χρήσης ψηφιακών εγγράφων αντί για τα κλασσικά χειρόγραφα έντυπα, κατά την πραγματοποίηση των καθημερινών συναλλαγών των πολιτών με τις κρατικές υπηρεσίες ή των πελατών με τις υπηρεσίες ηλεκτρονικού επιχειρείν, καθιστούν απαραίτητη την αποτελεσματική εφαρμογή τεχνολογιών που θα διασφαλίζουν την ασφάλεια αυτών των συναλλαγών. Τέτοιες τεχνολογίες είναι οι ψηφιακές υπογραφές, οι οποίες παρέχουν διασφάλιση της ακεραιότητας και της αυθεντικότητας ενός ψηφιακού εγγράφου, καθώς και τα ψηφιακά πιστοποιητικά, τα οποία διασφαλίζουν την αυθεντικότητα της κυριότητας ενός δημοσίου κλειδιού. Οι τεχνολογίες αυτές λειτουργούν στο πλαίσιο πρωτοκόλλων και υποδομών ασφάλειας που αξιοποιώντας κρυπτογραφία συμμετρικού και δημοσίου κλειδιού παρέχουν το απαραίτητο πλέγμα υπηρεσιών ασφάλειας για την πραγματοποίηση ασφαλών συναλλαγών.

Προαπαιτούμενη γνώση

Για την κατανόηση του παρόντος κεφαλαίου απαιτούνται, πέραν των βασικών του κεφαλαίου 1, οι γνώσεις που παρέχουν τα προηγούμενα κεφάλαια 6, 7 και 8.

9.1 Ψηφιακές Υπογραφές

Στα κεφάλαια 6 και 7, είδαμε πως η χρήση της κρυπτογραφίας δημόσιου κλειδιού μπορεί να χρησιμοποιηθεί για την προστασία της εμπιστευτικότητας του μεταδιδόμενου μηνύματος εφαρμόζοντας κατά την κρυπτογράφησή του το δημόσιο κλειδί του παραλήπτη. Με τον τρόπο αυτό, όντως διασφαλίζουμε πως από την αρχική κρυπτογράφηση ως την τελική λήψη και αποκρυπτογράφηση του μηνύματος, αυτό δεν έχει διαβαστεί από κάποιον τρίτο. Το δημόσιο όμως κλειδί μπορεί να είναι ελεύθερα διαθέσιμο. Πώς μπορούμε να είμαστε βέβαιοι ότι πράγματι ο αποστολέας είναι αυτός που ισχυρίζεται στο μήνυμα του ότι είναι; Πώς, δηλαδή, θα μπορούσαμε να αποκλείσουμε την περίπτωση το μήνυμα να έχει κρυπτογραφηθεί από κάποιον κακόβουλο τρίτο;

Η αυθεντικοποίηση της πηγής προέλευσης ενός μηνύματος μας επιτρέπει να επαληθεύσουμε την πραγματική ταυτότητα της οντότητας η οποία αποτελεί την πηγή (αποστολέα). Επιπλέον, η δυνατότητα ανίχνευσης πιθανών μετατροπών κατά τη μετάδοσή του, επιτρέπει και τη διαφύλαξη της ακεραιότητάς (integrity) του. Στον πραγματικό κόσμο, αντίστοιχες τεχνικές χρησιμοποιούνται εδώ και χρόνια. Ο συντάκτης ενός εγγράφου, διαβεβαιώνει με την υπογραφή του τον παραλήπτη για την αυθεντικότητα της προέλευσής του. Άρα, με αφορμή τον πραγματικό κόσμο, θα πρέπει να υπάρχει και στις ΤΠΕ μια αντίστοιχη διαδικασία που θα διασφαλίζει την αυθεντικότητα προέλευσης, καθώς και την ακεραιότητα του μηνύματος. Αυτή η διαδικασία είναι γνωστή ως ψηφιακή υπογραφή.

Η χρήση ψηφιακών υπογραφών οφείλει να προσφέρει:

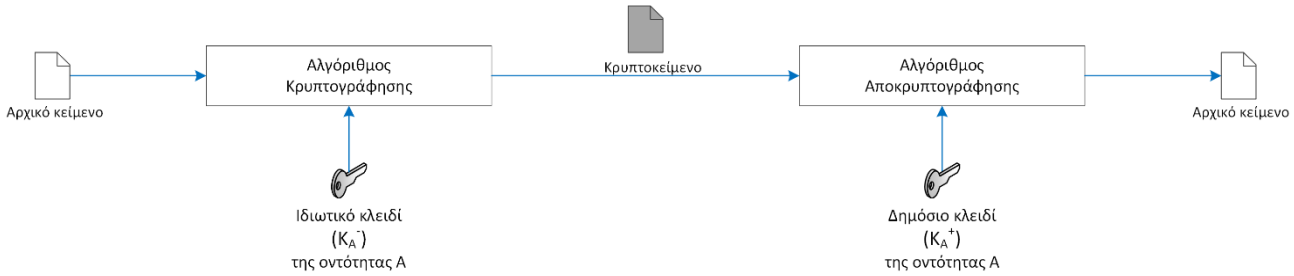
- **Αυθεντικότητα πηγής προέλευσης (origin authentication)**: Ο παραλήπτης μπορεί να είναι βέβαιος για την ταυτότητα του αποστολέα του μηνύματος.
- **Αδυναμία αποποίησης (non-repudiation)**: Ο αποστολέας δεν μπορεί να αρνηθεί εκ των υστέρων, ότι έστειλε ή υπέγραψε ένα μήνυμα.
- **Ακεραιότητα (integrity)**: Ο παραλήπτης μπορεί να εξακριβώσει μετά την παραλαβή του μηνύματος ότι αυτό δεν τροποποιήθηκε κατά τη μετάδοση του.

Υπάρχουν αρκετά σχήματα ψηφιακών υπογραφών τα οποία χρησιμοποιούνται σήμερα, με τα περισσότερα να βασίζονται στην κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography – PKC). Τα πιο διαδεδομένα από αυτά χρησιμοποιούν τους αλγόριθμους RSA, DSA/DSS και El-Gamal.

9.1.2 Σχήματα ψηφιακών υπογραφών

9.1.2.1 RSA

Σε προηγούμενο κεφάλαιο, γνωρίσαμε τον αλγόριθμο ασύμμετρης κρυπτογράφησης RSA για την παροχή υπηρεσιών ασφάλειας που αφορούν στην εμπιστευτικότητα. Όταν ο ίδιος αλγόριθμος χρησιμοποιείται για δημιουργία και επαλήθευση ψηφιακών υπογραφών, ονομάζεται μηχανισμός (σχήμα) ψηφιακής υπογραφής RSA. Στο μηχανισμό ψηφιακής υπογραφής RSA χρησιμοποιείται το ζεύγος ιδιωτικού και δημοσίου κλειδιού του αποστολέα και όχι του παραλήπτη. Γενικά, στην κρυπτογραφία δημόσιου κλειδιού η ακεραιότητα διασφαλίζεται όταν ο αποστολέας υπογράφει με το ιδιωτικό κλειδί του και ο παραλήπτης επαληθεύει με το δημόσιο κλειδί του αποστολέα, όπως φαίνεται στην Εικόνα 9.1.



Εικόνα 9.1 *Εφαρμογή κρυπτογραφίας δημοσίου κλειδιού για προστασία της ακεραιότητας.*

Όμως επειδή η κρυπτογραφία δημόσιου κλειδιού είναι αργή, δεν θα είχε κάποιο ουσιαστικό νόημα η κρυπτογράφηση του συνόλου του μηνύματος, ιδιαίτερα αν αυτό έχει απρόβλεπτα μεγάλο μέγεθος. Αντί αυτού, γνωρίζοντας ότι για κάθε διαφορετικό αρχικό κείμενο μπορεί να παραχθεί από μια συνάρτηση κατακερματισμού ένα μικρό και σταθερό σε μέγεθος μήνυμα, γνωστό ως συνόψιση, ενώ θα ικανοποιούνται οι απαιτήσεις ανθεκτικότητας της συνάρτησης κατακερματισμού (όπως είδαμε σε προηγούμενο κεφάλαιο), θα μπορούσαμε να εργαστούμε ως εξής (Εικόνα 9.2):

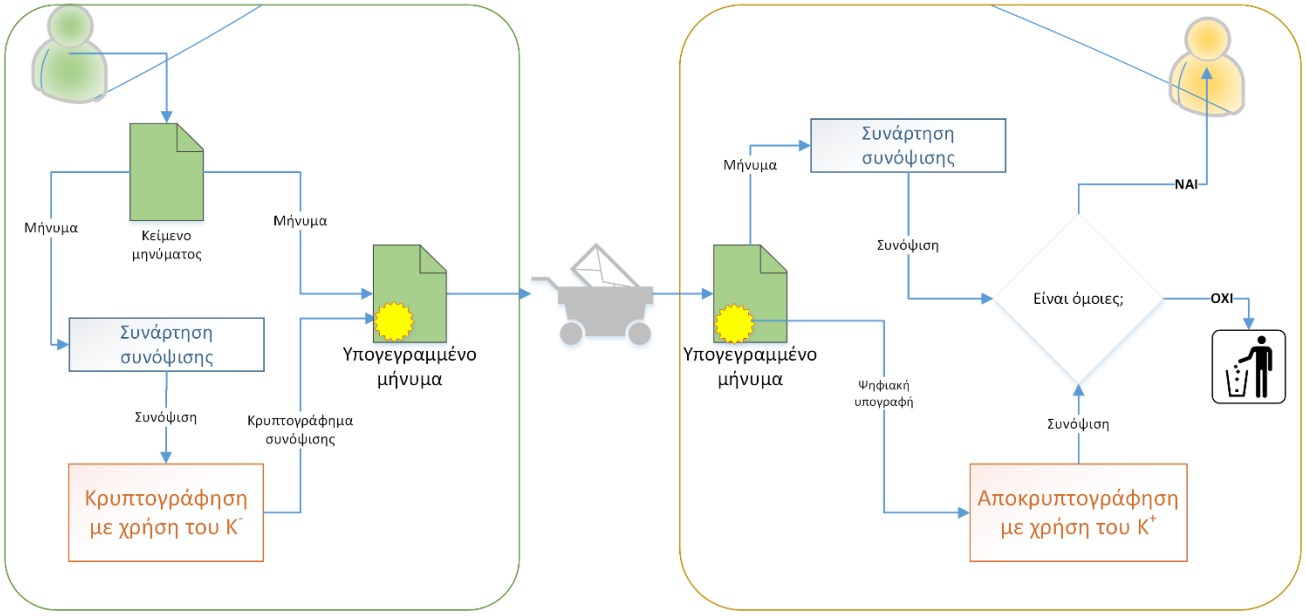
Ο αποστολέας:

- δημιουργεί τη συνόψιση του μηνύματος,
- κρυπτογραφεί τη συνόψιση με τη χρήση του ιδιωτικού του κλειδιού, δηλαδή υπογράψει ψηφιακά το μήνυμα,
- αποστέλλει το μήνυμα ως αρχικό κείμενο, συνοδευόμενο από την ψηφιακή υπογραφή του, δηλαδή το κρυπτογράφημα της συνόψισης και την ταυτότητα της συνάρτησης κατακερματισμού που χρησιμοποιήθηκε για την παραγωγή της.

Ο παραλήπτης:

- λαμβάνει το μήνυμα και παράγει εκ νέου τη συνόψισή του με τη χρήση της ίδιας συνάρτησης κατακερματισμού,
- αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα και εξάγει τη συνόψιση που είχε στείλει ο αποστολέας.
- Αν οι δύο συνοψίσεις είναι ίδιες, τότε το κείμενο δεν έχει αλλοιωθεί (διαφύλαξη της ακεραιότητας). Η επιτυχής αποκρυπτογράφηση με χρήση του δημόσιου κλειδιού επιβεβαιώνει την ταυτότητα του αποστολέα (αυθεντικοποίηση πηγής προέλευσης). Θυμηθείτε πως κάθε τι

που κρυπτογραφείται με το ένα κλειδί ενός ζεύγους κλειδιών αποκρυπτογραφείται μόνο με το άλλο κλειδί του ίδιου ζεύγους.



Εικόνα 9.2 *Σχήμα ψηφιακής υπογραφή μηνύματος με χρήση RSA.*

9.1.2.2 El-Gamal

Η παραγωγή των κλειδιών με το μηχανισμό ψηφιακής υπογραφής El-Gamal είναι όμοια με αυτή του κρυπτοσυστήματος El-Gamal, με τη διαφοροποίηση πως ο αποστολέας, όπως και στην περίπτωση του RSA, υπογράφει με το ιδιωτικό του κλειδί και ο παραλήπτης επιβεβαιώνει με το δημόσιο.

Αρχικά, υπολογίζεται ένα ζεύγος κλειδιών, επιλέγοντας έναν αρκετά μεγάλο πρώτο αριθμό q και μια πρωτογενή (generator) ρίζα του, έστω α που είναι ακέραιος ≤ q και με την ιδιότητα για κάθε αριθμό n, μεταξύ 1 και q-1, να υπάρχει μια δύναμη k τέτοια ώστε $n = \alpha^k$ **mod**q. Ο εκθέτης k (διακριτός λογάριθμος) ονομάζεται δείκτης του n για βάση α, mod q και συμβολίζεται: $k = \text{ind}_{a,q}(n)$.

Στη συνέχεια. επιλέγουμε έναν ακέραιο X_A, τέτοιον ώστε $1<X_A<q-1$. Με τη βοήθεια του ακέραιου αυτού, υπολογίζουμε το:

$$Y_A = a^{X_A} \bmod q \tag{9.1}$$

- Το ιδιωτικό κλειδί είναι ο αριθμός X_A.
- Το δημόσιο κλειδί είναι η τριάδα $\{q, \alpha, Y_A\}$.

Για την υπογραφή ενός μηνύματος, ο αποστολέας ακολουθεί τα ακόλουθα βήματα:

- Υπολογίζει τη συνόψιση h του αρχικού μηνύματος, τέτοια ώστε $0<h<q-1$.
- Επιλέγει έναν ακέραιο K, τέτοιον ώστε $0<K<q-1$ και ο K είναι σχετικά πρώτος του q-1.
- Υπολογίζει το: $S_1=\alpha^K$**mod**q.
- Υπολογίζει το: $S_2= K^{-1}(h-X_AS_1)$**mod**$(q-1)$.

- Η ψηφιακή υπογραφή που αποστέλλεται, αποτελείται από το ζευγάρι (S_1, S_2).

Ο παραλήπτης επιβεβαιώνει την υπογραφή εκτελώντας τα ακόλουθα βήματα:

- Υπολογίζει το: $V_1=\alpha^h$**mod**q, όπου h είναι η συνόψιση του μηνύματος που έλαβε και το α είναι γνωστό από το δημόσιο κλειδί.
- Υπολογίζει το $V_2=(Y_A)^{S1}(S1)^{S2}$**mod**q.
- Αν $V_1=V_2$, τότε η υπογραφή είναι έγκυρη!

Ένα παράδειγμα δημιουργίας ψηφιακής υπογραφής είναι:

- Επιλέγουμε q=11 και α=2 (το 2 είναι πρωτοβάθμια ρίζα του 11).
- Επιλέγουμε τον ακέραιο $X_A=4$ ως ιδιωτικό κλειδί.
- Υπολογίζουμε $Y_A=2^4$**mod**11=5. Το δημόσιο κλειδί είναι {11, 2, 5}.
- Έστω ότι η συνόψιση του μηνύματος έχει την τιμή 8. Επιλέγουμε K=3 που είναι σχετικά πρώτο του q-1=10.
- Υπολογίζουμε $S_1=2^3$**mod**11=8.
- Υπολογίζουμε S_2= 7(8-4(8))**mod**(10)=2.
- Άρα, η ψηφιακή υπογραφή είναι (8, 2).

Για την επιβεβαίωση της υπογραφής, ο παραλήπτης υπολογίζει:

- $V_1=2^8$**mod**11=3.
- $V_2=5^88^2$**mod**11=3.

Άρα, η ψηφιακή υπογραφή είναι έγκυρη.

9.1.2.3 DSA/DSS

Το πρότυπο Digital Signature Standard (DSS) υιοθετήθηκε από τον οργανισμό National Institute of Standards (NIST) το 1994. Ο μηχανισμός ψηφιακής υπογραφής DSS χρησιμοποιεί τον αλγόριθμο Digital Signature Algorithm (DSA), που βασίζεται στο μηχανισμό El-Gamal. Δέχτηκε επικρίσεις από την ώρα που δημοσιεύτηκε, με κυριότερο λόγο τη μυστικότητα που κάλυπτε τον σχεδιασμό του.

Ο αλγόριθμος DSA, σε αντίθεση με τον RSA, δεν χρησιμοποιείται για κρυπτογράφηση, αλλά μόνο για ψηφιακή υπογραφή, ενώ η ανθεκτικότητά του βασίζεται στο δύσκολο πρόβλημα του υπολογισμού διακριτών λογαρίθμων.

Αρχικά, παράγονται το ιδιωτικό και το δημόσιο κλειδί:

- Επιλέγεται από το χρήστη ένας πρώτος αριθμός q.
- Στη συνέχεια, πρέπει να επιλεγεί ένα πρώτος αριθμός p μήκους μεταξύ 512 και 1024 bits, τέτοιος ώστε το q να διαιρεί το (p-1).
- Επιλέγεται g=n(p - 1)/q **mod**p, όπου n ακέραιος και 1<n<(p-1)

- Επιλέγεται τυχαία ένας αριθμός x, όπου $0<x<(q-1)$. Το x είναι το ιδιωτικό κλειδί.

- Από το ιδιωτικό κλειδί x, προκύπτει το δημόσιο κλειδί (p,q,g,y), με το y να υπολογίζεται από τη σχέση $y=g^x$ **mod** p

Για τη συνόψιση h, η ψηφιακή υπογραφή αποτελείται από τους αριθμούς r και s οι οποίοι είναι:

- $r=(g^k$ **mod** p) **mod** p

- $s=(k^{-1}(h+xr)$) **mod** q, όπου k είναι μια τυχαία τιμή που είναι διαφορετική για κάθε υπογραφή.

Ο παραλήπτης, λαμβάνει τα r και s και υπολογίζει τη συνόψιση h. Στη συνέχεια, επιβεβαιώνει την υπογραφή εκτελώντας τα ακόλουθα βήματα:

- $w=s^{-1}$ **mod** q

- $u_1=(hw)$ **mod** q

- u2=rw **mod** q

- $u=(g^{u1}y^{u2}$ **mod** p) **mod** q

Η εγκυρότητα της υπογραφής επιβεβαιώνεται αν w=u.

9.2 Υποδομή Δημοσίου Κλειδιού

Η κρυπτογραφία δημοσίου κλειδιού μπορεί, όπως είδαμε, να χρησιμοποιηθεί για να υπογραφεί ένα ψηφιακό έγγραφο. Όμως, στην παρουσίαση που προηγήθηκε, δεν αναφέρθηκε ένα σημαντικό πρόβλημα που μπορεί να ανακύψει κατά τη χρήση της κρυπτογραφίας δημοσίου κλειδιού. Ο παραλήπτης λαμβάνοντας το υπογεγραμμένο μήνυμα μπορεί να επαληθεύσει πως χρησιμοποιήθηκε για την υπογραφή το ιδιωτικό κλειδί $\mathbf{K_A^-}$ της οντότητας Α, στην οποία ανήκει το δημόσιο κλειδί $\mathbf{K_A^+}$ που έχει στην κατοχή του. Δεν μπορεί όμως να γνωρίζει αν το κλειδί $\mathbf{K_A^+}$, που απέκτησε συνήθως με έναν ανασφαλή τρόπο (π.χ. μήνυμα email), είναι όντως το δημόσιο κλειδί της οντότητας Α. Θα μπορούσε, δηλαδή, κάποιος τρίτος κακόβουλος να διοχετεύσει ένα δημόσιο κλειδί $\mathbf{K'_A^+}$ με τον ισχυρισμό πως είναι το δημόσιο κλειδί της οντότητας Α. Όσοι λάβουν αυτό το ψεύτικο $\mathbf{K'_A^+}$ θα μπορούσαν να θεωρούν πως κάθε υπογεγραμμένο μήνυμα του κακόβουλου με το κλειδί $\mathbf{K'_A^-}$ προέρχεται από την οντότητα Α.

Σε ένα δεύτερο σενάριο, ο κακόβουλος θα μπορούσε να έχει υποκλέψει το ιδιωτικό κλειδί $\mathbf{K_A^-}$ και να το χρησιμοποιεί κανονικά ως ότου η οντότητα Α ενημερώσει κάθε δυνητικό παραλήπτη πως το ιδιωτικό της κλειδί έχει κλαπεί και να ζητήσει να αντικαταστήσει το δημόσιο κλειδί της με ένα νέο (από ένα καινούργιο ζεύγος κλειδιών). Τέλος, ακόμη και να μην υπήρχε ο κακόβουλος χρήστης του παραπάνω παραδείγματος, η οντότητα Α θα μπορούσε να προφασιστεί πως έχει πέσει θύμα κλοπής, ώστε να αρνηθεί πως έχει υπογράψει ψηφιακά κάποια μηνύματα. Παρατηρούμε, λοιπόν, πως θα πρέπει να καθοριστεί ένας αξιόπιστος τρόπος διανομής των δημοσίων κλειδιών, τέτοιος ώστε:

- να διασφαλίζεται η πηγή προέλευσης του δημοσίου κλειδιού,
- να διασφαλίζεται η ιδιότητα της μη-αποποίησης,
- να υπάρχει τρόπος ανάκλησης των δημοσίων κλειδιών.

Το πρόβλημα βρίσκει λύση στη χρήση **ψηφιακών πιστοποιητικών (digital certificates)** και **Υποδομών Δημοσίου Κλειδιού (Public Key Infrastructures - PKI).**

9.2.1 Ψηφιακά πιστοποιητικά

Για να κατανοήσουμε τη λειτουργία των ψηφιακών πιστοποιητικών, ας επανέλθουμε στο παράδειγμα του πραγματικού κόσμου. Σε πολλές περιπτώσεις ένας οργανισμός ή μια υπηρεσία δεν αρκείται στην υπογραφή ενός πολίτη, αλλά απαιτεί αυτή η υπογραφή να έχει θεωρηθεί / πιστοποιηθεί για το γνήσιό της από μια έμπιστη αρχή, όπως ένα αστυνομικό τμήμα. Με τον ίδιο τρόπο, στο χώρο των ΤΠΕ ένα δημόσιο κλειδί μπορεί να πιστοποιηθεί από μια τρίτη έμπιστη οντότητα. Το ψηφιακό έγγραφο που πιστοποιεί ένα δημόσιο κλειδί και το συνδέει με την ταυτότητα του ιδιοκτήτη του, αποτελεί το **ψηφιακό πιστοποιητικό.**

Το πρότυπο X.509 καθορίζει τη δομή ενός ψηφιακού πιστοποιητικού, το οποίο μεταξύ άλλων περιλαμβάνει:

- Έκδοση (version): Καθορίζει την έκδοση του πιστοποιητικού. Υπάρχουν τρεις (3) εκδόσεις, με νεότερη την έκδοση 3. Κάθε νέα έκδοση έχει προσθέσει πεδία, όπως θα φανεί στη συνέχεια.

- Αριθμός σειράς (serial number): Μια ακέραια τιμή, μοναδική για κάθε εκδότη, που χαρακτηρίζει μοναδικά το πιστοποιητικό.

- Αναγνωριστικό αλγόριθμου (Signature algorithm identifier): Περιγράφεται ο αλγόριθμος που χρησιμοποιήθηκε με τις όποιες παραμέτρους για τη δημιουργία της υπογραφής.

- Όνομα εκδότη (issuer name): Αναφέρεται το όνομα του εκδότη σύμφωνα με την τρόπο αναφοράς που περιγράφει το X.500.

- Περίοδος ισχύος (Validity date): Αποτελείται από δύο ημερομηνίες (από-έως) που καθορίζουν το διάστημα για το οποίο ισχύει το πιστοποιητικό.

- Όνομα ιδιοκτήτη (Subject name): Το όνομα του ιδιοκτήτη του δημόσιου κλειδιού που περιέχεται στο πιστοποιητικό.

- Πληροφορία δημοσίου κλειδιού ιδιοκτήτη (Subject's public key information): Περιλαμβάνεται το δημόσιο κλειδί και κάθε πληροφορία σχετική με αυτό, όπως ο αλγόριθμος κρυπτογράφησης.

Στην έκδοση 2, προστέθηκαν τα πεδία

- Μοναδικό αναγνωριστικό εκδότη (Issuer unique identifier): Αναφέρεται το όνομα του εκδότη του πιστοποιητικού, σύμφωνα με τον τρόπο αναφοράς που περιγράφει η οικογένεια προτύπων X.500, έτσι ώστε αυτός να προσδιορίζεται μονοσήμαντα.

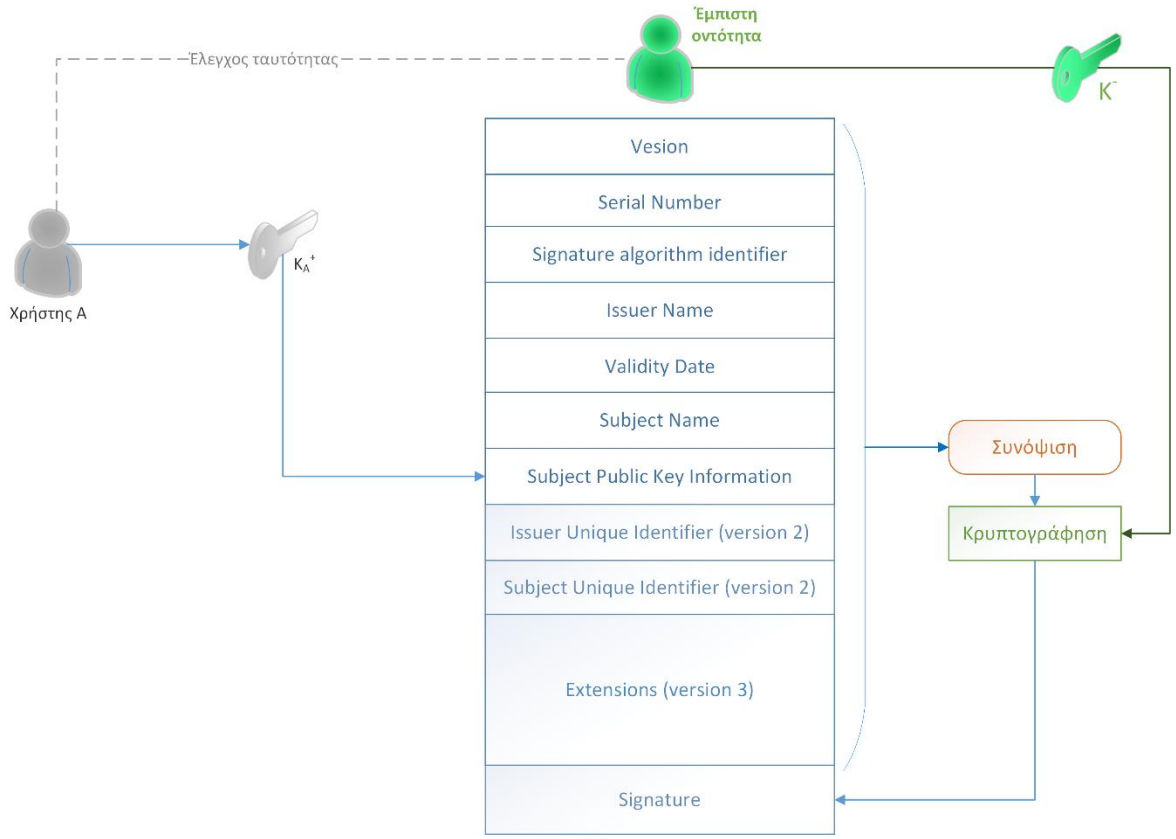
- Μοναδικό αναγνωριστικό ιδιοκτήτη (Subject unique identifier): Αναφέρεται το όνομα του ιδιοκτήτη του δημόσιου κλειδιού, σύμφωνα με τον τρόπο αναφοράς που περιγράφει το X.500, έτσι ώστε αυτός να προσδιορίζεται μονοσήμαντα.

Στην έκδοση 3, προστέθηκε πεδίο επεκτάσεων (extensions) που προσδίδει ευελιξία στον εκδότη για να προσθέσει όποια επιπρόσθετη πληροφορία επιθυμεί. Κάθε πεδίο extension αποτελείται από:

- Το όνομα της επέκτασης (extension name)
- Την κρισιμότητα της επέκτασης (criticality indicator)
- Την τιμή της επέκτασης (extension value), δηλαδή την πληροφορία που περιέχει.

Τέλος, κάθε πιστοποιητικό περιέχει την ψηφιακή υπογραφή της συνόψισής του, για την παραγωγή της οποίας γίνεται χρήση του ιδιωτικού κλειδιού της έμπιστης οντότητας που εξέδωσε το πιστοποιητικό (εκδότης). Στο πεδίο αυτό περιλαμβάνεται η συνόψιση και ο αλγόριθμος που χρησιμοποιήθηκε.

Στο τέλος του παρόντος κεφαλαίου, θα δημιουργήσουμε και θα εξετάσουμε ψηφιακά πιστοποιητικά. Η δομή και ο τρόπος δημιουργίας, φαίνεται σχηματικά στην Εικόνα 9.3



Εικόνα 9.3 *Έκδοση και περιεχόμενα ψηφιακού πιστοποιητικού X.509.*

Η χρήση του ψηφιακού πιστοποιητικού ίσως φαίνεται ότι μπορεί να λύσει το πρόβλημα της διανομής ενός δημόσιου κλειδιού, καθώς συσχετίζει πιστοποιημένα το κλειδί αυτό με τον πραγματικό ιδιοκτήτη του, με τη μεσολάβηση μιας τρίτης (από όλα τα μέρη) έμπιστης οντότητας (Trusted Third Party – TTP). Το νέο πρόβλημα που ανακύπτει αφορά ερωτήματα σχετικά με το ποια θα πρέπει να είναι η οντότητα αυτή, που θα πρέπει να βρίσκεται, πώς θα καθίσταται έμπιστη κ.ά.. Η λύση στο πρόβλημα αυτό παρέχεται με την υλοποίηση του μοντέλου Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure - PKI).

9.2.2 Αρχιτεκτονική Υποδομής Δημόσιου Κλειδιού

Σύμφωνα με το λεξιλόγιο όρων ασφάλειας ΤΠΕ του NIST η Υποδομή Δημόσιου Κλειδιού (ΥΔΚ) ορίζεται ως ένα σύνολο από πολιτικές, διεργασίες, πλατφόρμες λογισμικού και συστήματα που χρησιμοποιούνται για την έκδοση, διαχείριση και ανάκληση των ψηφιακών πιστοποιητικών.

Η ομάδα εργασίας για το PKIX (Public Key Infrastructure X.509), σχηματίστηκε από τη IETF (Internet Engineering Task Force) με σκοπό τον καθορισμό ενός λειτουργικού μοντέλου για τη διαχείριση ψηφιακών πιστοποιητικών, στο πλαίσιο του πρότυπου X.509. Σύμφωνα με το PKIX, μια ΥΔΚ αποτελείται από:

- **Οντότητες-πελάτες (End entities). Οι χρήστες της ΥΔΚ που αιτούνται και λαμβάνουν πιστοποιητικά. Μπορεί να είναι φυσικά πρόσωπα ή συσκευές.**

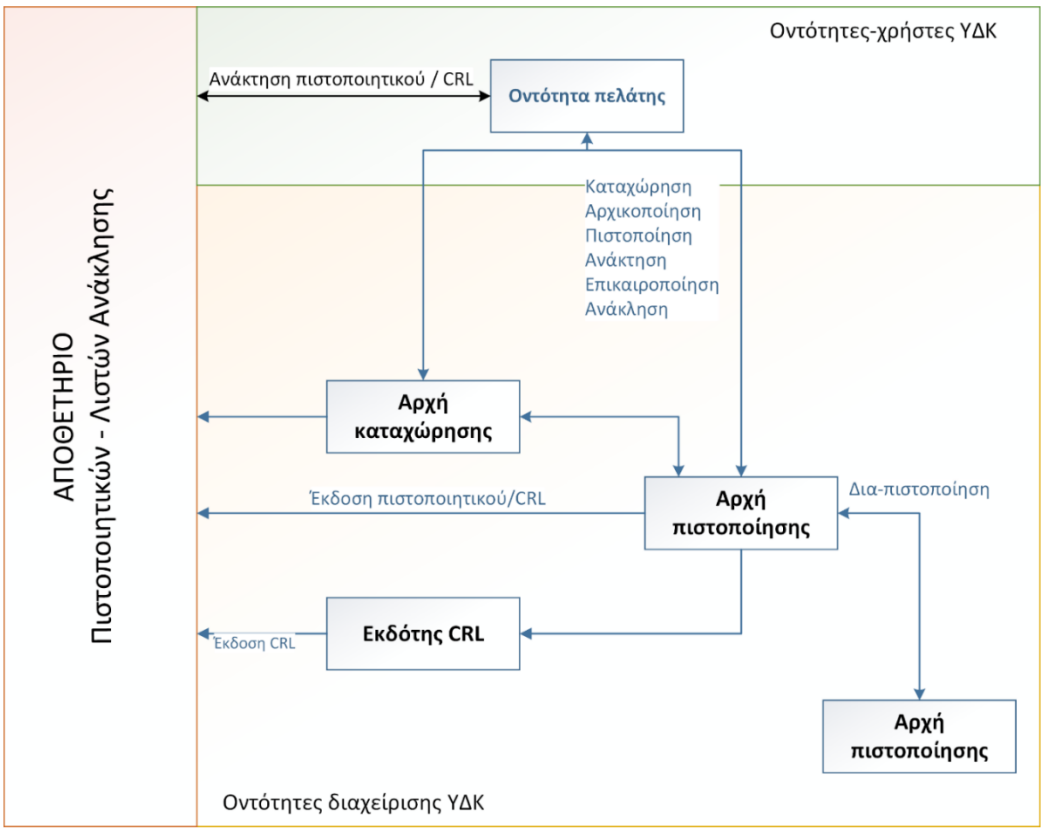
- **Αρχή Πιστοποίησης (Certificate Authority - CA)**. Είναι η έμπιστη τρίτη οντότητα, που διαχειρίζεται την έκδοση και διαχείριση των ψηφιακών πιστοποιητικών.

- **Αρχή Καταχώρησης (Registation Authority - RA)**. Διαχειρίζεται τη διαδικασία καταχώρησης των στοιχείων των τελικών οντοτήτων-πελατών και αποτελεί ενδιάμεσο στην επικοινωνία των τελευταίων με τη CA.

- **Εκδότης CRL (CRL Issuer)**. Διαχειρίζεται τη διαδικασία σύνταξης κι ενημέρωσης των λιστών ανάκλησης πιστοποιητικών (CRL).

- **Αποθετήριο (Repository)**: Το σημείο αποθήκευσης των πιστοποιητικών και των λιστών ανάκλησής τους (Certificate Revocation Lists – CRL).

Η διασύνδεση και διαλειτουργικότητα των παραπάνω δομικών στοιχείων μιας ΥΔΚ, φαίνεται στην Εικόνα 9.4.



Εικόνα 9.4 *Δομή PKIX.*

9.2.3 Λειτουργίες Υποδομής Δημόσιου Κλειδιού

Σύμφωνα με το PKIX, οι λειτουργίες μιας ΥΔΚ είναι:

- **Καταχώρηση (registration)**: Η διαδικασία με την οποία μια τελική οντότητα θα γίνει γνωστή στην Αρχή Πιστοποίησης (CA).

- **Αρχικοποίηση (initialization)**: Η διαδικασία με την οποία θα γίνεται η επικοινωνία, όπως η παροχή του δημόσιου κλειδιού προς πιστοποίηση.

- **Πιστοποίηση (certification)**: Η διαδικασία έκδοσης και διανομής ενός ψηφιακού πιστοποιητικού από την CA.

- **Ανάκτηση ζεύγους κλειδιών (key-pair recovery)**: Ανάκτηση ενός αποθηκευμένου ζεύγους κλειδιών (π.χ. για κρυπτογράφηση), σε περίπτωση απώλειας.

- **Δημιουργία κλειδιών (key generation):** Η διαδικασία δημιουργίας ζεύγους κλειδιών ή του δημόσιου κλειδιού μετά από αίτημα ενός χρήστη.

- **Επικαιροποίηση κλειδιών (key update)**: Διασφάλιση εγκυρότητας κλειδιών με ενημέρωσή τους κατά τη λήξη, ώστε να μην καθίστανται μη-έγκυρα.

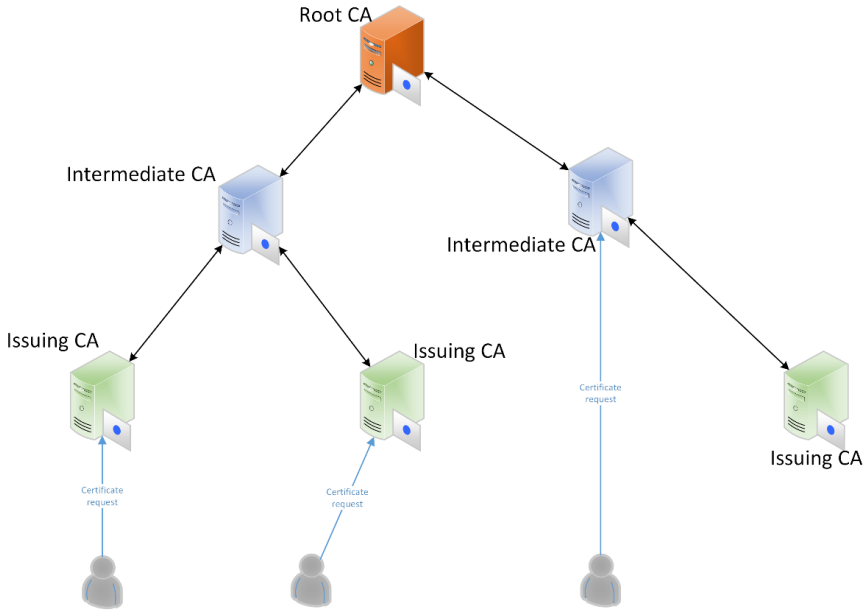
- **Διαπιστοποίηση (cross-certification)**: Η διαδικασία με την οποία δημιουργούνται αλυσίδες εμπιστοσύνης μεταξύ των CA.

- **Ανάκληση (revocation)**: Η δυνατότητα και η μέθοδος ανάκλησης ισχύος ενός πιστοποιητικού πριν την ημερομηνία λήξης του.

9.2.4 Μοντέλα Εμπιστοσύνης ΥΔΚ

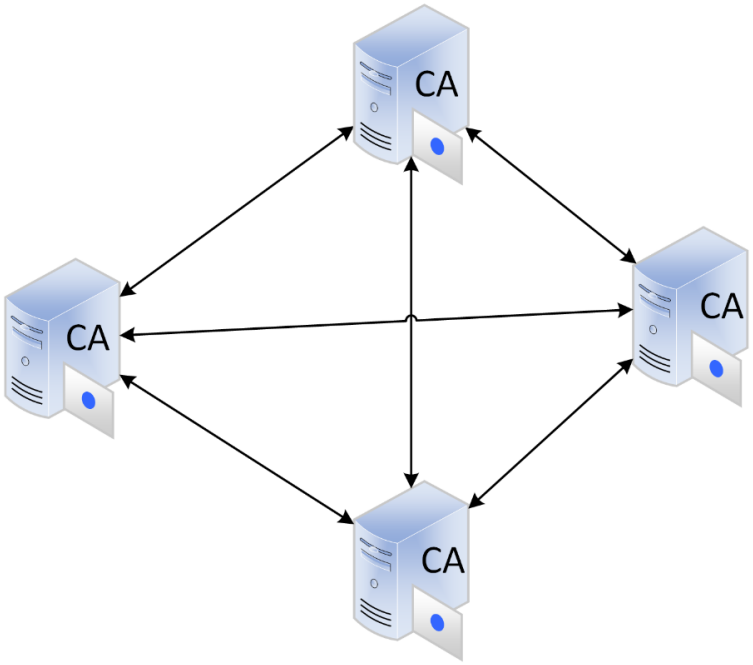
Η εμπιστοσύνη μεταξύ των CA σε μια ΥΔΚ καθορίζει τον τρόπο λειτουργίας της. Το μοντέλο εμπιστοσύνης περιγράφει αφαιρετικά τον τρόπο με τον οποίο δομείται η εμπιστοσύνη σε μια ΥΔΚ. Τρία από τα μοντέλα, που συναντώνται πιο συχνά, είναι:

- **Ιεραρχικό Μοντέλο**: Το μοντέλο αυτό αποτελεί την πλέον τυπική υλοποίηση μιας Υποδομής Δημοσίου Κλειδιού. Κάθε CA πιστοποιείται από μια έμπιστη τρίτη οντότητα, δηλαδή μια άλλη CA. Έτσι δημιουργείται μια ιεραρχία αρχών πιστοποίησης σε δενδρική μορφή, όπου η υψηλότερη στην ιεραρχία, αυτή δηλαδή που βρίσκεται στη ρίζα (Root CA), θεωρείται εξ ορισμού έμπιστη και είναι η μόνη που έχει πιστοποιήσει το δημόσιο κλειδί της (self-signed). Η Root CA δεν εκδίδει πιστοποιητικά σε χρήστες αλλά μόνο σε άλλες CA που βρίσκονται χαμηλότερα στην ιεραρχία και μπορούν να είναι ενδιάμεσες (Intermediate CA) και να εκδίδουν πιστοποιητικά για άλλες CA χαμηλότερα στην ιεραρχία ή να βρίσκονται στα φύλλα του δέντρου και να υπογράφουν μόνο πιστοποιητικά σε τελικές οντότητες-πελάτες. Κάθε πιστοποιητικό συνοδεύεται από μια αλυσίδα πιστοποίησης που οδηγεί στην έμπιστη Root CA (Εικόνα 9.5).



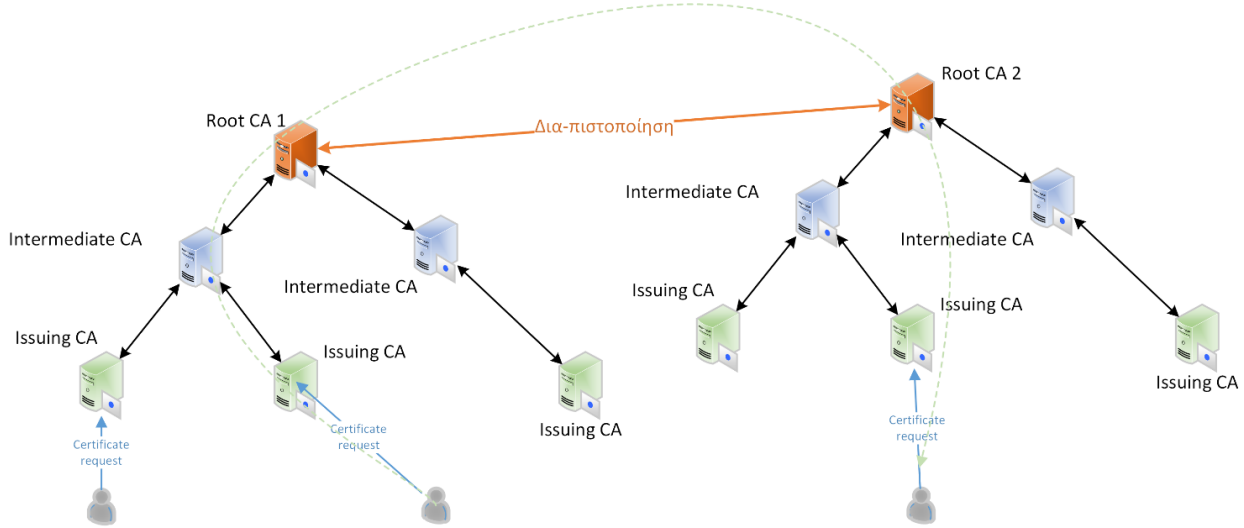
Εικόνα 9.5 *Ιεραρχικό μοντέλο ΥΔΚ.*

- **Δια-Πιστοποίηση**: Σε αντίθεση με το απόλυτα ιεραρχικό μοντέλο, στο μοντέλο δια-πιστοποίησης οι CA δημιουργούν σχέσεις εμπιστοσύνης μεταξύ τους. Ως συνέπεια, αν μια οντότητα εμπιστεύεται το πιστοποιητικό μιας CA, θα εμπιστεύεται και τα πιστοποιητικά από όλες τις δια-πιστοποιημένες αρχές (Εικόνα 9.6).



Εικόνα 9.6 *Μοντέλο Δια-Πιστοποίησης.*

- **Μικτό**: Υπάρχει δια-πιστοποίηση μεταξύ δύο δέντρων πιστοποίησης, όπως το παράδειγμα που παρουσιάζεται στην Εικόνα 9.7.



Εικόνα 9.7 *Μικτό μοντέλο.*

9.3 Πρακτική εφαρμογή

Στη συνέχεια θα αξιοποιηθεί το προϊόν λογισμικού OpenSSL σε Λ.Σ. Linux, με σκοπό την εξοικείωση με την τεχνολογία Υποδομής Δημοσίου Κλειδιού. Παρότι το παράδειγμα αναφέρεται σε Λ.Σ. Linux, μπορείτε να

εγκαταστήσετε το OpenSSL σε οποιοδήποτε λειτουργικό σύστημα και να προσαρμόσετε ανάλογα τις διάφορες δραστηριότητες παρουσιάζονται στη συνέχεια. Στόχος μας είναι να δημιουργήσουμε έναν ιστότοπο που θα υποστηρίζει ασφαλείας συνδέσεις επικοινωνίας με τους πελάτες (secure website). Για το λόγο αυτό:

- θα δημιουργήσουμε ένα ζεύγος κλειδιών (ιδιωτικό/δημόσιο),
- θα χρησιμοποιήσουμε την υπηρεσία μιας CA με σκοπό να μας υπογράψει ένα πιστοποιητικό για το δημόσιο κλειδί μας,
- θα συνδεθούμε με χρήση ενός φυλλομετρητή ιστού (browser) και αξιοποίηση της κρυπτογραφίας για ασφαλή επικοινωνία με τον ιστότοπο.

9.3.1 Δημιουργία αρχής πιστοποίησης και έκδοση πιστοποιητικού

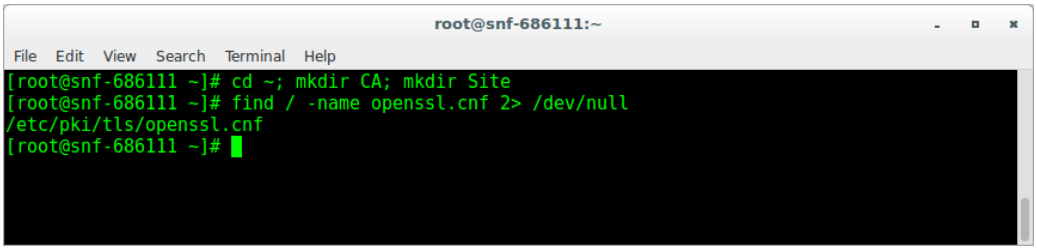
9.3.1.1 Δημιουργία RootCA

Δημιουργούμε δυο φακέλους (directories) με τις ακόλουθες εντολές:

```
cd ~; mkdir CA; mkdir Site
```

Εντοπίζουμε το αρχείο ρυθμίσεων του OpenSSL με την εντολή (Εικόνα 9.8):

```
find / -name openssl.cnf 2> /dev/null
```



Εικόνα 9.8 *Εύρεση αρχείου ρυθμίσεων του OpenSSL.*

Στην Εικόνα 9.8 παρατηρούμε ότι το αρχείο εντοπίστηκε στον κατάλογο /etc/pki/tls. Αφού εξετάσουμε τα περιεχόμενα του αρχείου, πραγματοποιούμε την αλλαγή της πολιτικής ταιριάσματος αναγνωριστικών με την εντολή:

```
sed -i "/policy = /c\policy = policy_anything" \
/etc/pki/tls/openssl.cnf
```

Στη συνέχεια, δημιουργούμε τα αρχεία που ορίζονται στο αρχείο παραμετροποίησης:

```
cd /etc/pki/CA
touch index.txt
echo 1000 > serial
```

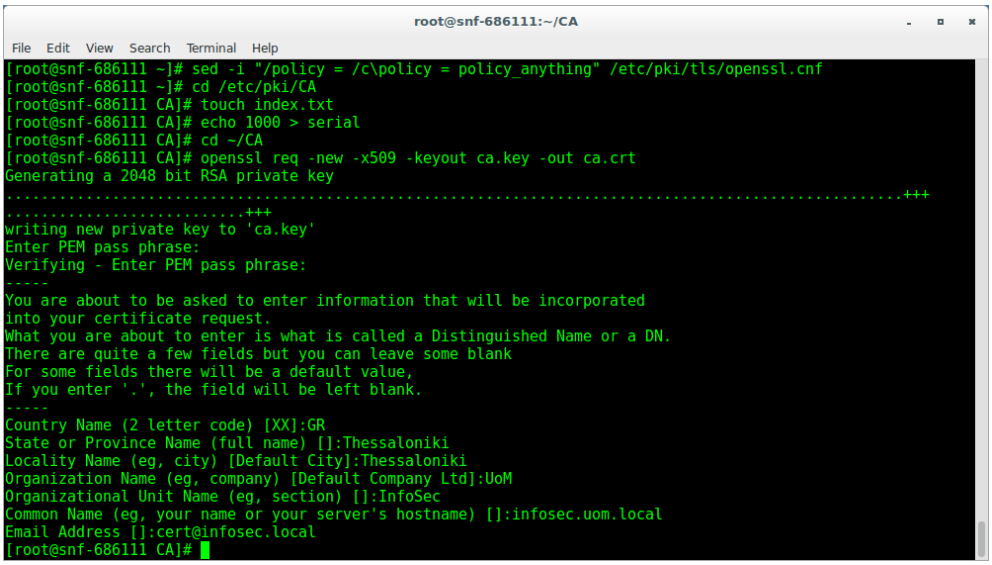
Στο σημείο αυτό έχει δημιουργηθεί μια Root CA, την οποία θα χρησιμοποιούμε για την έκδοση και υπογραφή των πιστοποιητικών.

9.3.1.2 Δημιουργία Intermediate CA

Μεταβαίνουμε στο home directory του χρήστη και δημιουργούμε ένα νέο ζεύγος κλειδιών:

```
cd ~/CA
openssl req -new -x509 -keyout ca.key -out ca.crt
```

όπου, ca.key είναι το ιδιωτικό κλειδί της CA μας και ca.crt είναι το πιστοποιητικό που περιέχει το δημόσιο κλειδί της. Το OpenSSL θα ζητήσει ένα συνθηματικό για την προστασία του ιδιωτικού κλειδιού και τα στοιχεία ταυτότητας της CA, που θα ενσωματωθούν στο πιστοποιητικό (Εικόνα 9.9).



Εικόνα 9.9 *Δημιουργία ζεύγους κλειδιών και πιστοποιητικού αρχής πιστοποίησης.*

Ελέγχουμε ότι τα αρχεία έχουν δημιουργηθεί και μελετάμε τα περιεχόμενά τους:

```
ls -la
cat ca.key
cat ca.crt
```

Σε τι μορφή είναι τα αρχεία; Γιατί χρησιμοποιήθηκε αυτός ο τρόπος αναπαράστασης των δεδομένων;

Η αρχή πιστοποίησης είναι τώρα έτοιμη να εκδώσει και να υπογράψει πιστοποιητικά. Πρώτος πελάτης η εταιρεία PKILabServer.

Ο πελάτης πρέπει πρώτα να δημιουργήσει το δικό του ζεύγος κλειδιών:

```
cd ~/Site
openssl genrsa -aes128 -out pkilabserver.key 2048
```

Εισάγουμε passphrase όταν μας ζητηθεί (π.χ. pkilabserver) και στη συνέχεια ελέγχουμε το αρχείο που δημιουργήθηκε. Τι περιέχει το αρχείο αυτό; Ποιος/οι αλγόριθμος/οι χρησιμοποιήθηκε/αν για τη δημιουργία του ζεύγους;

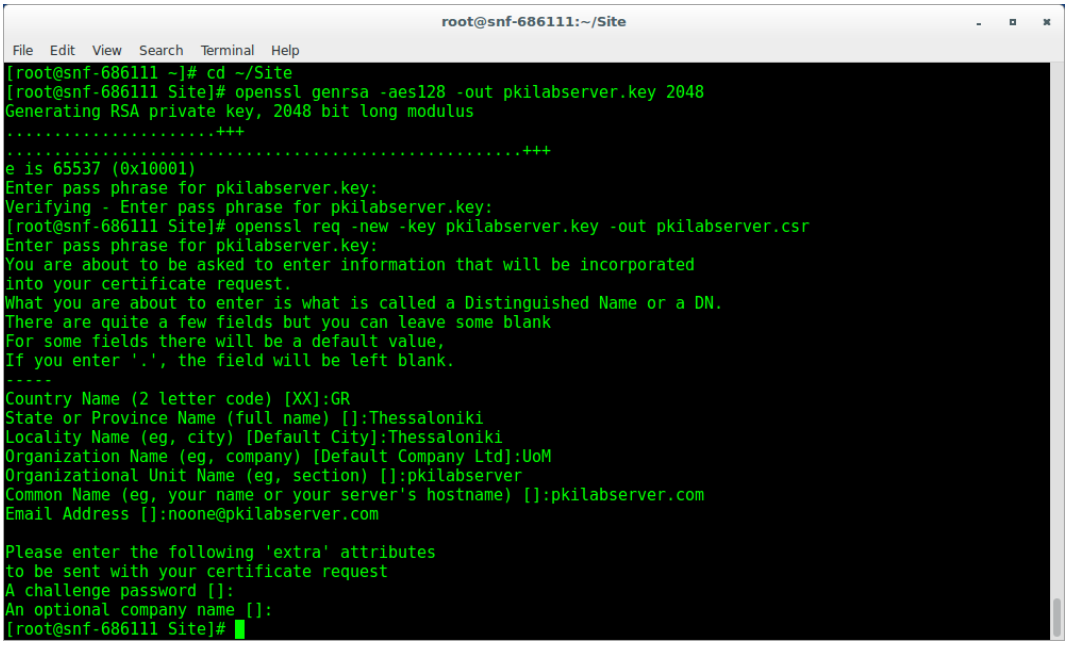
9.3.1.3 Δημιουργία αιτήματος έκδοσης πιστοποιητικού

Για να εκδοθεί ένα πιστοποιητικό από μια αρχή πιστοποίησης θα πρέπει να υποβληθεί ένα κατάλληλο αίτημα. Το αίτημα περιέχεται σε ένα αρχείο τύπου certificate request (.csr) το οποίο συμπεριλαμβάνει το δημόσιο κλειδί του αιτούντα. Άρα, ο πελάτης δημιουργεί το αίτημα, το οποίο θα υποβάλλει ώστε να λάβει ψηφιακό πιστοποιητικό υπογεγραμμένο από την CA:

```
openssl req -new -key pkilabserver.key -out pkilabserver.csr
```

Θεωρούμε ότι ο πελάτης έχει στη διάθεση του το domain: **pkilabserver.com**. Αυτό θα χρησιμοποιηθεί ως Common Name του Certificate Request. Το Common Name είναι ιδιαίτερα σημαντικό σε ένα SSL Certificate καθώς προσδιορίζει την οντότητα (hostname) για την οποία θα είναι ενεργό.

Εισάγουμε το ίδιο passphrase (δηλαδή τη λέξη που είχαμε εισάγει κατά τη δημιουργία του ζεύγους pkilabserver) και στη συνέχεια τα απαραίτητα στοιχεία για την αναγνώριση του ιδιοκτήτη του δημόσιου κλειδιού που θα περιέχει το πιστοποιητικό. Προσέξτε να εισάγετε το σωστό Common Name. Τα πεδία «challenge password» και «optional company name», τα αφήνουμε κενά (Εικόνα 9.10).



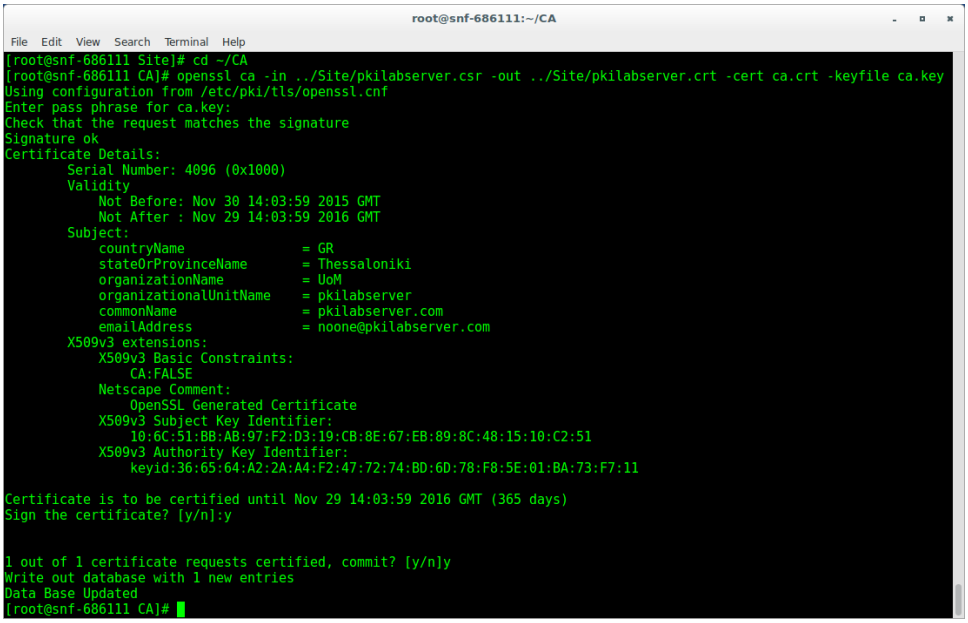
Εικόνα 9.10 *Δημιουργία ζεύγους κλειδιών και αιτήματος υπογραφής.*

Μόλις ολοκληρωθεί η διαδικασία, ελέγχουμε τα περιεχόμενα του αρχείου αιτήματος για έκδοση πιστοποιητικού (csr) που έχει δημιουργηθεί. Τι πληροφορίες μπορούμε να δούμε σε αυτό;

9.3.1.4 Έκδοση Πιστοποιητικού

Η αρχή πιστοποίησης CA παραλαμβάνει το Certificate Request και δημιουργεί ένα νέο πιστοποιητικό:

```
cd ~/CA
openssl ca -in ../Site/pkilabserver.csr -out \
../Site/pkilabserver.crt -cert ca.crt -keyfile ca.key
```



Εικόνα 9.11 *Έκδοση πιστοποιητικού.*

Όπως πάντα, ελέγχουμε τα περιεχόμενά του.

9.3.2 Ενεργοποίηση SSL

Για την εγκατάσταση του πιστοποιητικού στον OpenSSL Web server, θα πρέπει να συνενώνουμε το ιδιωτικό μας κλειδί και το πιστοποιητικό που εκδώσαμε από την αρχή πιστοποίησης, σε ένα αρχείο

```
cd ~/Site
cat pkilabserver.key pkilabserver.crt > pkilabserver.pem
```

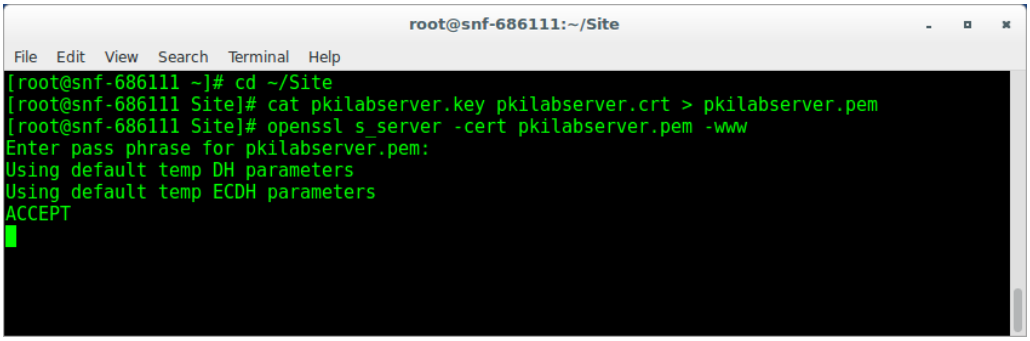
Εκκινούμε το με χρήση του ζεύγους κλειδιού-πιστοποιητικού

```
openssl s_server -cert pkilabserver.pem –www
```

Εισάγουμε το συνθηματικό που είχαμε ορίσει για τον έλεγχο πρόσβασης στο ιδιωτικό κλειδί του pkilabserver.com (pkilabserver). Ο Web server εκκινεί και «ακούει» στην πόρτα **4433**. Εναλλακτικά, μπορούμε αν τον εκκινήσουμε με χρήση διαφορετικής πόρτας εκτελώντας την εντολή:

```
openssl s_server -cert pkilabserver.pem –www -accept pNum
```

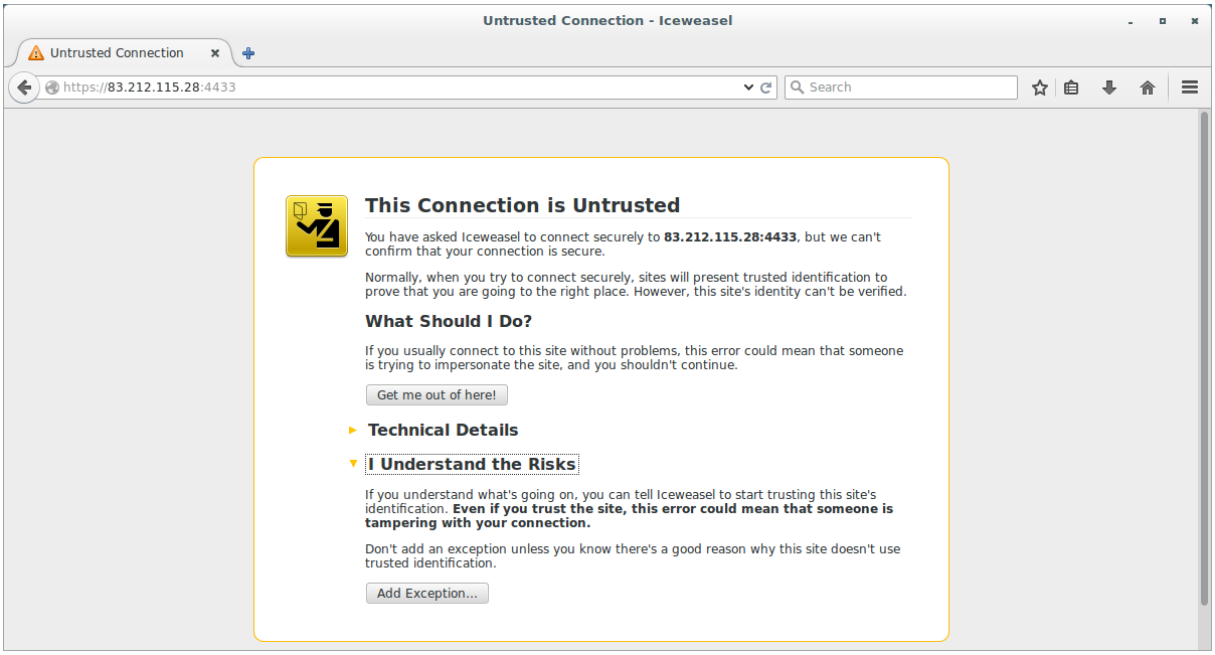
όπου pNum ο αριθμός της tcp θύρας. Θυμηθείτε πως σε περιβάλλον UNIX/Linux, ένα απλός χρήστης δε μπορεί να εκκινήσει υπηρεσίες σε θύρα με αριθμό μικρότερο του 1024.



Εικόνα 9.12 *Εκκίνηση OpenSSL Web Server.*

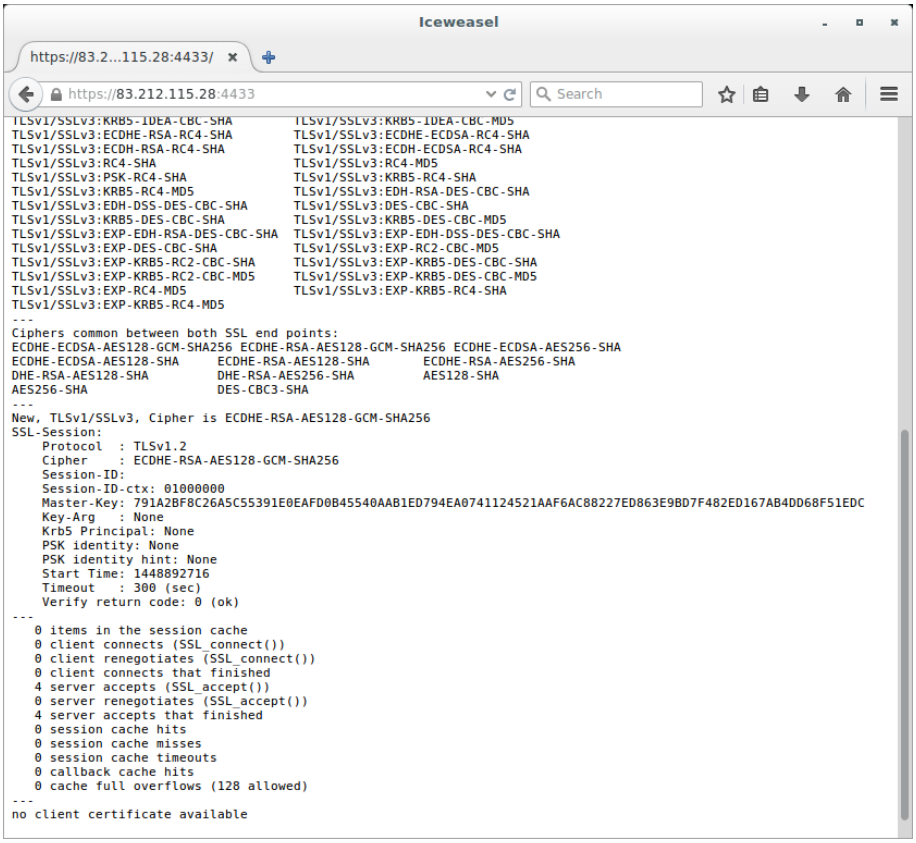
Στη συνέχεια, εκκινούμε ένα browser στην ίδια μηχανή ή σε μια μηχανή εντός του δικτύου και δίνουμε: http://<OpenSSL_Server_IP>:4433, όπου <OpenSSL_Server_IP> είναι η διεύθυνση IP του host στον οποίο εκκινήσαμε τον Web Server.

Τι παρατηρείτε; Για ποιο λόγο μας προειδοποιεί ο browser; Εντοπίστε τα προεγκατεστημένα πιστοποιητικά. Γιατί υπάρχουν εκεί;

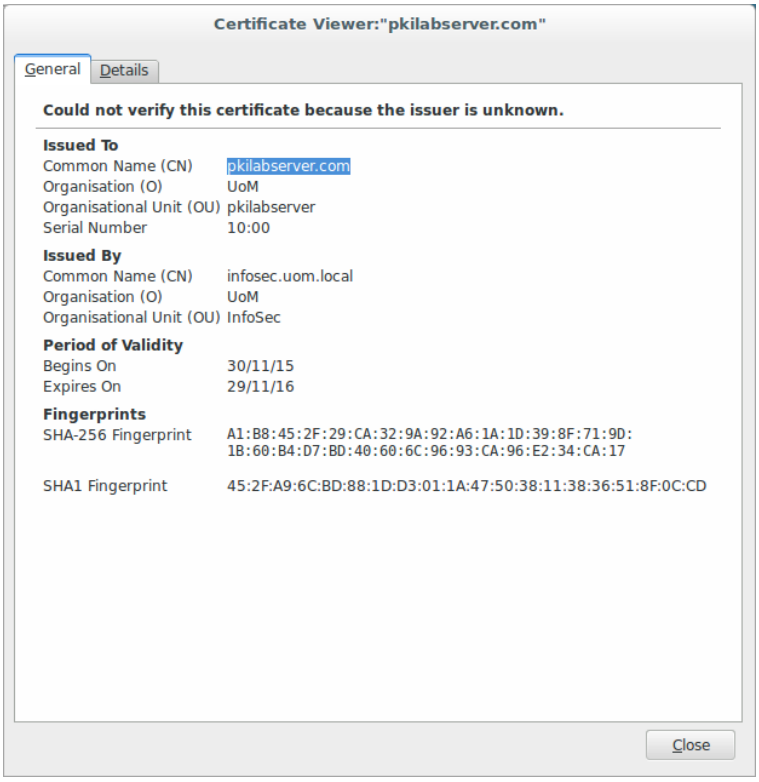


Εικόνα 9.13 *Προειδοποίηση για το πιστοποιητικό.*

Αφού υποδείξετε στο browser πως μπορεί να εμπιστευτεί και το δικό σας πιστοποιητικό, ελέγξτε ποιος αλγόριθμος χρησιμοποιείται για τη μεταφορά δεδομένων; Είναι αλγόριθμος συμμετρικής ή ασύμμετρης κρυπτογραφίας; Τι δεδομένα μπορείτε να συνάγετε για τη λειτουργία του TLS;



Εικόνα 9.14 *Πληροφορίες συνόδου.*



Εικόνα 9.15 *Προβολή πιστοποιητικού.*

9.3.4 Έλεγχος ψηφιακής υπογραφής

Ολοκληρώνοντας τη μελέτη των ΥΔΚ και των ψηφιακών υπογραφών, θα χρησιμοποιήσουμε το OpenSSL για τη δημιουργία και επιβεβαίωση ψηφιακής υπογραφής.

Δημιουργούμε το αρχείο myCal που περιέχει το ημερολόγιο του μήνα :

```
Cd ~/Site
cal > ./myCal
```

Δημιουργούμε τη συνόψιση του αρχείου myCal με χρήση του αλγορίθμου SHA256 και το υπογράφουμε με το ιδιωτικό κλειδί που είχαμε δημιουργήσει προηγουμένως:

```
openssl dgst -sha256 -sign pkilabserver.key -out \
myCal.sha256 myCal
```

Επιβεβαιώνουμε την ακεραιότητα του αρχείου με χρήση του πιστοποιητικού:

```
openssl dgst -sha256 -verify \
<(openssl x509 -in pkilabserver.crt -pubkey -noout)\
-signature myCal.sha256 ./myCal
```

Πραγματοποιούμε μια οποιαδήποτε αλλαγή στο αρχείο myCal (αρχικό κείμενο) και επαναλαμβάνουμε την επιβεβαίωση. Αντιληφθήκαμε πως το αρχείο έχει αλλοιωθεί;

Εικόνα 9.16 *Δημιουργία και έλεγχος ψηφιακής υπογραφής.*

Βιβλιογραφία

Choudhury, S., Bhatnagar, K., & Haque, W. (2002). Public key infrastructure: implementation and design. New York, NY: M&T Books.

Housley, R., & Polk, T. (2001). Planning for PKI: best practices guide for deploying public key infrastructure. New York: Wiley.

Katz, J. (2010). Digital signatures. New York: Springer.

Nash, A. (Ed.). (2001). PKI: implementing and managing E-security. New York: Osborne/McGraw-Hill.

Rhodes-Ousley, M. (2013). Information security: the complete reference (2nd. Ed). New York ;London: McGraw-Hill Education.

Stallings, W. (2014). Cryptography and network security: principles and practice (Seventh edition). Boston: Pearson.

Πάγκαλου Γ., Μαυρίδη Ι. (2002). Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων. Θεσσαλονίκη: Εκδόσεις Ανικούλα.

Κριτήρια Αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Η χρήση ψηφιακών υπογραφών διασφαλίζει:
α) Την εμπιστευτικότητα.
β) Την ακεραιότητα.
γ) Τη διαθεσιμότητα.
δ) Την αυθεντικότητα.

2. Η συνόψιση του μηνύματος:
α) Έχει μέγεθος ανάλογο με το μήνυμα.
β) Έχει πάντα μέγεθος μικρότερο από το μήνυμα.
γ) Έχει σταθερό μέγεθος.
δ) Είναι μια περίληψη με λίγα λόγια.

3. Η ψηφιακή υπογραφή περιέχει:
α) Το κρυπτογραφημένο μήνυμα.
β) Την κρυπτογραφημένη απεικόνιση υπογραφής του συντάκτη σε αρχείο εικόνας.
γ) Την κρυπτογραφημένη συνόψιση.
δ) Το ιδιωτικό κλειδί.

4. Στο σχήμα DSS:
α) Αποστέλλεται η κρυπτογραφημένη συνόψιση.
β) Δεν αποστέλλεται η κρυπτογραφημένη συνόψιση.
γ) Αποστέλλεται το ζεύγος κλειδιών.
δ) Κρυπτογραφείται το μήνυμα.

5. Ένα ψηφιακό πιστοποιητικό:
α) Περιέχει το ιδιωτικό κλειδί.
β) Περιέχει το ζεύγος κλειδιών.
γ) Περιέχει το δημόσιο κλειδί.
δ) Δεν περιέχει κλειδιά.

6. Ένα ψηφιακό πιστοποιητικό:
α) Μπορεί να ανακληθεί.
β) Δε μπορεί να ανακληθεί.
γ) Έχει συγκεκριμένη διάρκεια ισχύος.
δ) Εκδίδεται από την αστυνομία.

7. Μια Root CA:
α) Εκδίδει κάθε είδους πιστοποιητικά.
β) Δεν εκδίδει πιστοποιητικά.

γ) Πιστοποιεί μόνο άλλες CA.
δ) Πιστοποιεί τον εαυτό της υπογράφοντας τα πιστοποιητικά για την ίδια.

8. Η version 3 για τα ψηφιακά πιστοποιητικά σύμφωνα με το X.509:
α) Επιτρέπει να αποθηκεύονται σε αυτά επιπλέον ιδιότητες.
β) Αυξάνει το βαθμό ασφάλειας.
γ) Αυξάνει το μήκος της δέσμης κρυπτογράφησης.
δ) Επιτρέπει τη χρήση συμμετρικής κρυπτογραφίας.

9. Σε ένα ιεραρχικό μοντέλο ΥΔΚ, οι ενδιάμεσες αρχές (intermediate CA):
α) Δεν εκδίδουν πιστοποιητικά χρηστών.
β) Πιστοποιούν τη Root CA.
γ) Εκδίδουν πιστοποιητικά χρηστών.
δ) Πιστοποιούν άλλες CA.

10. Ο αλγόριθμος DSA:
α) Χρησιμοποιείται μόνο για ψηφιακές υπογραφές.
β) Χρησιμοποιείται μόνο για κρυπτογράφηση.
γ) Μπορεί να χρησιμοποιηθεί και για ψηφιακές υπογραφές και για κρυπτογράφηση.
δ) Κανένα από τα παραπάνω.

Δραστηριότητα

Θεωρήστε πως η σύνοψη ενός μηνύματος που θέλετε να υπογράψετε έχει δεκαδική τιμή 6. Χρησιμοποιήστε τους αλγόριθμους: RSA, El-Gamal και DSA (DSS) για να δημιουργήστε ζεύγη κλειδιών και την ψηφιακή υπογραφή. Στη συνέχεια, γίνετε ο παραλήπτης, κι επιβεβαιώστε την.

Κεφάλαιο 10. Εικονικά Ιδιωτικά Δίκτυα - VPN

Σύνοψη

Το κεφάλαιο αυτό ασχολείται με το πρόβλημα της ασφαλούς επικοινωνίας και διασύνδεσης απομακρυσμένων δικτύων. Η μελέτη του κεφαλαίου, καθώς και η μελέτη περίπτωσης που περιλαμβάνεται σε αυτό, θα δώσει στον αναγνώστη τη δυνατότητα να ολοκληρώσει τις γνώσεις που απέκτησε σε προηγούμενα κεφάλαια, προκειμένου να κατανοήσει τη χρήση τεχνολογιών και τη γενικότερη αξιοποίηση της κρυπτογραφίας στην υλοποίηση εναλλακτικών λύσεων επικοινωνίας. Ακόμη, θα τον βοηθήσει στο να αξιολογεί τις διαθέσιμες τεχνολογίες και να μπορεί να υλοποιεί αποδοτικές λύσεις.

Προαπαιτούμενη γνώση

Για την κατανόηση του κεφαλαίου πρέπει να έχει προηγηθεί η μελέτη σχεδόν όλων των προηγούμενων κεφαλαίων, καθώς θα χρησιμοποιηθούν γνώσεις και έννοιες που έχουν αναφερθεί ή αναλυθεί στα κεφάλαια αυτά.

10.1 Εισαγωγή

Στη σημερινή εποχή, ένα σημαντικό μέρος της οικονομικής και όχι μόνο δραστηριότητας βασίζεται στην ανταλλαγή δεδομένων μεταξύ πληροφοριακών συστημάτων. Συνήθως, τα Πληροφοριακά Συστήματα (ΠΣ) διαφόρων οργανισμών και εταιριών δεν περιορίζονται σε μια τοποθεσία ή ένα κτήριο, αλλά πολλές φορές εκτείνονται σε διαφορετικές πόλεις, χώρες ή ακόμη και ηπείρους.

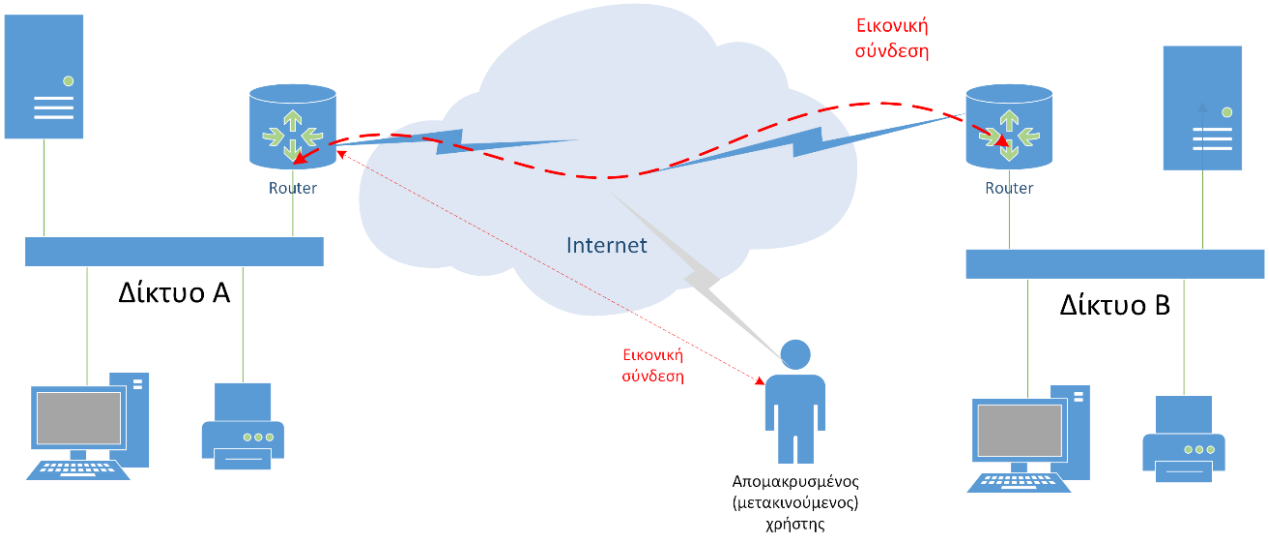
Παρόλη τη γεωγραφική διασπορά, όπου πέρα από τις επιμέρους σταθερές εγκαταστάσεις μπορεί να περιλαμβάνονται και μετακινούμενοι χρήστες (commuters), η ανάγκη για διασύνδεση των συστημάτων είναι συνεχώς αυξανόμενη. Η αρχική μέθοδος, που ακολουθήθηκε για τη διασύνδεση των συστημάτων των απομακρυσμένων τοποθεσιών ενός οργανισμού, ήταν η μίσθωση κυκλωμάτων από παρόχους τηλεπικοινωνιών. Με κάποιο τρόπο, ο πάροχος φρόντιζε να διασυνδέει τα σημεία με ένα αποκλειστικό κύκλωμα (φυσικό ή λογικό), έτσι ώστε όλα τα συμμετέχοντα μέρη να διασυνδέονται στο πλαίσιο ενός ενιαίου δικτύου που περιλάμβανε τα διάφορα υποδίκτυα του οργανισμού.

Αν και η παραπάνω υλοποίηση έδινε λύση στο επιτακτικό πρόβλημα της διασύνδεσης, παρουσίαζε τρία βασικά μειονεκτήματα:

- Υψηλό κόστος, συνήθως ανάλογο της απόστασης.
- Μεγάλο χρόνο υλοποίησης.
- Συμμετοχή του παρόχου, ως προϋπόθεση υλοποίησης κάθε αλλαγής.

Για τους παραπάνω λόγους, πολλοί οργανισμοί αδυνατούσαν να υλοποιήσουν (δια)συνδέσεις με χρήση μισθωμένων γραμμών και συνήθως κατέφευγαν σε λύσεις on-demand, όπως η χρήση dial-up συνδέσεων με μικρότερο κόστος, αλλά και σημαντικά μικρότερο εύρος διαμεταγωγής δεδομένων.

Η ανάπτυξη της ευρυζωνικότητας και η διάδοση της χρήσης σχετικών τεχνολογιών έκανε εφικτή την πρόσβαση σε ένα παγκόσμιο δημόσιο (αν και ανασφαλές) δίκτυο, το Διαδίκτυο (Internet), με μικρό κόστος αλλά αξιοπρεπείς ταχύτητες πρόσβασης. Αυτή η εξέλιξη προκάλεσε την αξιοποίηση του Διαδικτύου σε πληθώρα εφαρμογών, όπως η μεταφορά δεδομένων μεταξύ των απομακρυσμένων τοποθεσιών ενός οργανισμού διαμέσου εικονικών συνδέσεων. Με τον όρο εικονική σύνδεση (virtual connection) αναφερόμαστε σε διαδρομές δεδομένων που παρουσιάζονται ως απευθείας σύνδεση χάρη στην κατάλληλη αξιοποίηση των πόρων του φυσικού δικτύου, όπως φαίνεται στην Εικόνα 10.1. Το σύνολο τέτοιων εικονικών συνδέσεων που υλοποιούνται πάνω από ένα δημόσιας πρόσβασης δίκτυο (όπως το Διαδίκτυο), διαμορφώνει αυτό που ονομάζουμε Εικονικό Ιδιωτικό Δίκτυο - ΕΙΔ (Virtual Private Network – VPN).



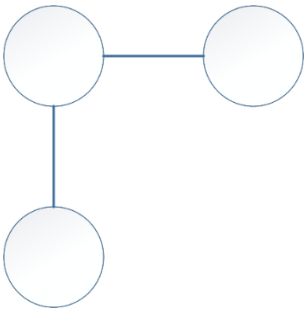
Εικόνα 10.1 *Εικονική σύνδεση μέσω του Διαδικτύου.*

Μπορούμε να κατατάξουμε τα VPN σε 3 κατηγορίες, ανάλογα με τα είδη συνδέσεων μεταξύ διαφορετικών άκρων. Συγκεκριμένα, μπορούμε να έχουμε:

- Σύνδεση κόμβου με κόμβο (Host-to-Host), όπου δημιουργούνται συνδέσεις μεταξύ κόμβων (host).
- Σύνδεση κόμβου με πύλη (Host-to-Gateway), όπου δημιουργούνται συνδέσεις μεταξύ κόμβων και πυλών δικτύων (gateway).
- Σύνδεση πύλης με πύλη (Gateway-to-Gateway), όπου δημιουργούνται συνδέσεις μεταξύ πυλών διαφορετικών δικτύων.

Συνδυάζοντας συνδέσεις από τις παραπάνω κατηγορίες, μπορούμε να δημιουργήσουμε εναλλακτικές τοπολογίες VPN, με συνηθέστερες τις:

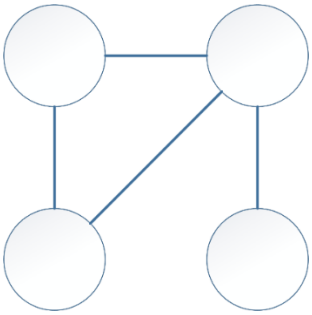
- **Hub & Spoke:** Η συνηθέστερη τοπολογία VPN είναι αυτή στην οποία σε ένα κεντρικό σημείο συνδέονται όλα τα υπόλοιπα (Εικόνα 10.2). Τα σημεία αυτά μπορεί να είναι συνεχώς συνδεδεμένα (LAN-to-LAN) ή να έχουν τη δυνατότητα να ενεργοποιούν τη σύνδεση κατ' απαίτηση (remote access).



Εικόνα 10.2 *Τοπολογία Hub & Spoke.*

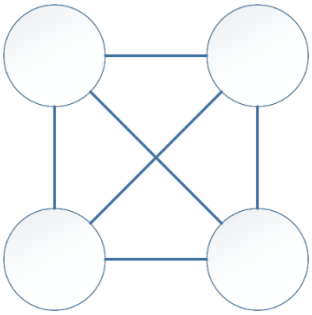
- **Partial Mesh**: Στην τοπολογία partial mesh (Εικόνα 10.3) υπάρχουν περισσότερα από δύο σημεία, κάποια εκ των οποίων συνδέονται λογικά μεταξύ τους και κάποια όχι

.



Εικόνα 10.3 *Τοπολογία Partial Mesh*.

- **Full Mesh**: Στην τοπολογία Full Mesh (Εικόνα 10.4) όλα τα σημεία συνδέονται λογικά μεταξύ τους.



Εικόνα 10.4 *Τοπολογία Full Mesh.*

Όπως αναφέρθηκε προηγουμένως, ένα VPN αποτελείται από ένα σύνολο λογικών συνδέσεων μέσω ενός δικτύου δημόσιας πρόσβασης, όπως το Διαδίκτυο. Με τον τρόπο αυτό, εξασφαλίζεται η απρόσκοπτη επικοινωνία αλλά ανακύπτει ένα βασικό πρόβλημα, που έχει να κάνει με την ανάγκη για ασφάλεια δεδομένων. Με τον όρο ασφάλεια δεδομένων, αναφερόμαστε στην προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των διακινούμενων δεδομένων. Η ανάγκη αυτή είναι τόσο σημαντική, ώστε η ασφάλεια δεδομένων να θεωρείται πρωταρχική προϋπόθεση για τη δημιουργία και λειτουργία ενός VPN. Η ικανοποίηση αυτής της ανάγκης επιτυγχάνεται κυρίως με την αξιοποίηση κρυπτογραφικών τεχνικών στο πλαίσιο κατάλληλων πρωτοκόλλων ασφάλειας.

Διαφορετικές μεθοδολογίες υλοποίησης VPN μπορούν να εφαρμοστούν με χρήση πρωτοκόλλων κάθε επίπεδου του μοντέλου του Διαδικτύου. Οι πιο γνωστές μεθοδολογίες, που θα αναλυθούν στη συνέχεια του κεφαλαίου, παρουσιάζονται στον Πίνακα 10.1.

Επίπεδο Μοντέλου Διαδικτύου	**Μεθοδολογία VPN**
Εφαρμογής (Application)	SSH Tunneling
Μεταφοράς (Transport)	SSL VPN
Διαδικτύου (Internet)	IPsec VPN
Φυσικής Ζεύξης (Data Link)	L2LP

Πίνακας 10.1 *Μεθοδολογίες VPN ανά επίπεδο του Μοντέλου Αναφοράς Διαδικτύου.*

10.1.1 Πλεονεκτήματα

Η τεχνολογική λύση των VPN παρουσιάζει διαρκή ανάπτυξη, καθώς παρέχει τα ακόλουθα βασικά πλεονεκτήματα:

- **Χαμηλό κόστος**. Η υλοποίηση ενός VPN βασίζεται στην εφαρμογή κατάλληλων τεχνικών πάνω σε ένα υπάρχον δημόσιο (κοινό) δίκτυο. Άρα δεν απαιτείται κόστος κατασκευής και/ή μίσθωσης κυκλωμάτων. Το κόστος προκύπτει από την ανάγκη εγκατάστασης κατάλληλου υλικού και λογισμικού για τα άκρα της εικονικής σύνδεσης.

- **Ευελιξία**. Ένα VPN, αποτελούμενο από εικονικές συνδέσεις, δεν απαιτεί κάποιο δεσμευμένο φυσικό μέσο πρόσβασης. Έτσι, τα άκρα μπορούν να μεταβληθούν, να μετακινηθούν ή να καταργηθούν κατά τη βούληση του διαχειριστή, με μόνη προϋπόθεση την πρόσβαση στο δημόσιο δίκτυο.

- **Ασφάλεια**. Η λειτουργία ενός VPN πάνω από ένα δημόσιο δίκτυο έχει καταστήσει την ασφάλεια ένα βασικό χαρακτηριστικό προς μελέτη. Οι κρυπτογραφικές τεχνικές που χρησιμοποιούνται μπορούν να παρέχουν εμπιστευτικότητα και ακεραιότητα στα διακινούμενα δεδομένα και αυθεντικοποίηση των άκρων.

10.1.2 Μειονεκτήματα VPN

Πέρα από τα πλεονεκτήματα που καθιστούν ιδιαίτερα ελκυστική την υλοποίηση VPN, υπάρχουν και συγκεκριμένα μειονεκτήματα τα οποία πρέπει να ληφθούν υπόψη:

- **Απαιτήσεις για πόρους:** Η διαχείριση των εικονικών συνδέσεων και κυρίως η υλοποίηση των κρυπτογραφικών τεχνικών συνήθως απαιτεί μαθηματικούς υπολογισμούς οι οποίοι δαπανούν υπολογιστικούς πόρους

- **Επιβάρυνση πακέτων:** Στην πλειονότητα των τεχνολογιών VPN το αρχικό πακέτο επιβαρύνεται με περισσότερη πληροφορία κεφαλίδας. Αυτό, πέρα από την αύξηση του μεγέθους μπορεί, να οδηγήσει σε απαίτηση κατακερματισμού, κάτι που μπορεί να επηρεάσει την απόδοση του δικτύου.

- **Δυσκολία υλοποίησης και διαχείρισης:** Η υλοποίηση ενός VPN απαιτεί εξειδικευμένες γνώσεις και ιδιαίτερη προσοχή, καθώς μπορεί να διακινούνται ευαίσθητα ή διαβαθμισμένα δεδομένα μέσα από το δημόσιο δίκτυο.

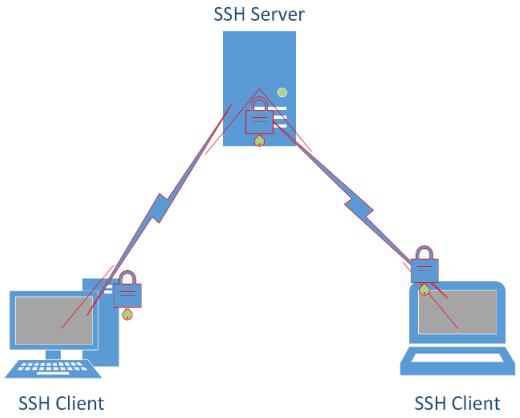
- **Διαθεσιμότητα:** Η διαθεσιμότητα των εικονικών συνδέσεων εξαρτάται απόλυτα από τη διαθεσιμότητα του δημόσιου δικτύου. Αν αυτό δεν είναι διαθέσιμο, τότε και οι εικονικές συνδέσεις καθίστανται ανενεργές.

- **Δυσκολία παροχής QoS:** Η παροχή ποιότητας υπηρεσίας (Quality of Service) είναι σημαντική για την εμπειρία των χρηστών του δικτύου. Καθώς το VPN αποτελείται από ένα σύνολο εικονικών συνδέσεων, οι παράμετροι ποιότητας είναι εξαρτώμενες από το φυσικό δίκτυο πάνω στο οποίο αυτές υλοποιούνται, το οποίο συνήθως είναι ένα δίκτυο βέλτιστης προσπάθειας (best-effort). Έτσι, χρειάζεται να εφαρμόζονται συνδυαστικά τεχνικές QoS και στο κοινό δίκτυο να παρέχει πρόβλεψη για την κίνηση δεδομένων που αφορά το VPN.

10.2 SSH Tunneling

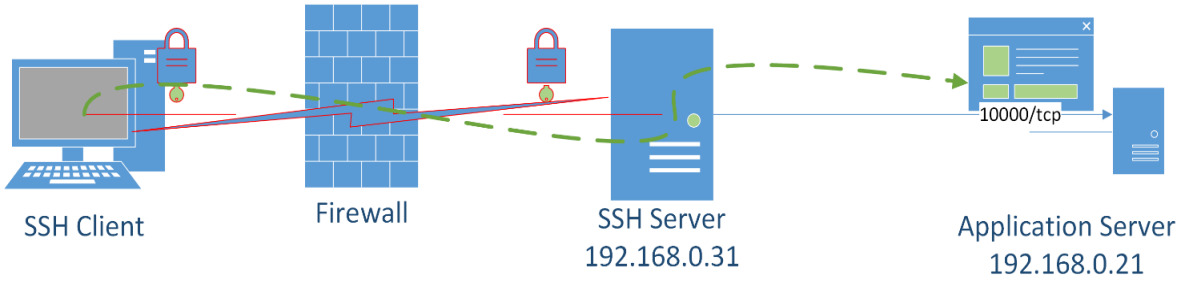
Το SSH (Secure SHell), όπως αναφέρει και το όνομά του, είναι γνωστό ως ένας τρόπος ασφαλούς σύνδεσης σε ένα κέλυφος (shell), ώστε να μπορεί ο χρήστης να εκτελεί εντολές στο απομακρυσμένο σύστημα. Το SSH είναι μια λύση Client-Server. Στην πλευρά του διακομιστή, εκτελείται ο SSH daemon, ο οποίος αναμένει συνδέσεις των πελατών (clients) σε μια TCP θύρα (συνήθως στην 22). Τα δύο μέρη (διακομιστής και πελάτης)

αυθεντικοποιούνται και, στη συνέχεια, συμφωνείται ένα κοινό κλειδί για την κρυπτογράφηση των δεδομένων (Εικόνα 10.5).



Εικόνα 10.5 *Απομακρυσμένη πρόσβαση με SSH.*

Το SSH, πέρα από τη δυνατότητα εγκατάστασης κρυπτογραφημένης συνόδου με σκοπό την απομακρυσμένη εκτέλεση εντολών, παρέχει τη δυνατότητα προώθησης θυρών (port forwarding). Μια τοπική θύρα αντιστοιχίζεται σε μια θύρα σε ένα απομακρυσμένο σύστημα. Έτσι, η κίνηση προς την τοπική θύρα προωθείται μέσω της SSH σύνδεσης και κατευθύνεται στην θύρα του απομακρυσμένου συστήματος. Η μεταφορά της κίνησης μέσω της SSH σύνδεσης, ονομάζεται SSH tunneling.



Εικόνα 10.6 *SSH Tunneling.*

Όπως φαίνεται στην Εικόνα 10.6, ο πελάτης (SSH Client) επιθυμεί να συνδεθεί με μια υπηρεσία που ακούει στην θύρα 10000/tcp του διακομιστή 192.168.0.21 στο απομακρυσμένο δίκτυο. Με χρήση του SSH tunneling, η κίνηση προς μια οποιαδήποτε θύρα του, η επιλογή της οποίας γίνεται από το χρήστη, προωθείται προς το 192.168.0.21:10000. Έτσι είναι δυνατή η επιθυμητή ανταλλαγή πληροφορίας.

Το SSH Tunneling δεν αποτελεί μια ολοκληρωμένη VPN λύση, αλλά παρουσιάζει χαμηλό κόστος και υλοποιείται άμεσα. Ένα σημαντικό πλεονέκτημα είναι πως αρκεί η δυνατότητα σύνδεσης μέσω SSH ώστε να επιτευχθεί επικοινωνία με οποιαδήποτε υπηρεσία (σημαντικό όταν υπάρχει firewall που αποτρέπει όποια άλλη κίνηση). Από την άλλη μεριά, όμως, μπορούν να εξυπηρετηθούν μόνον υπηρεσίες που βασίζονται στο TCP, ενώ προστίθεται επιπλέον επιβάρυνση (overhead) στην κίνηση και προκαλείται διαχειριστικός φόρτος, καθώς η λύση απαιτεί ρυθμίσεις που πρέπει να γίνουν από τον χρήστη.

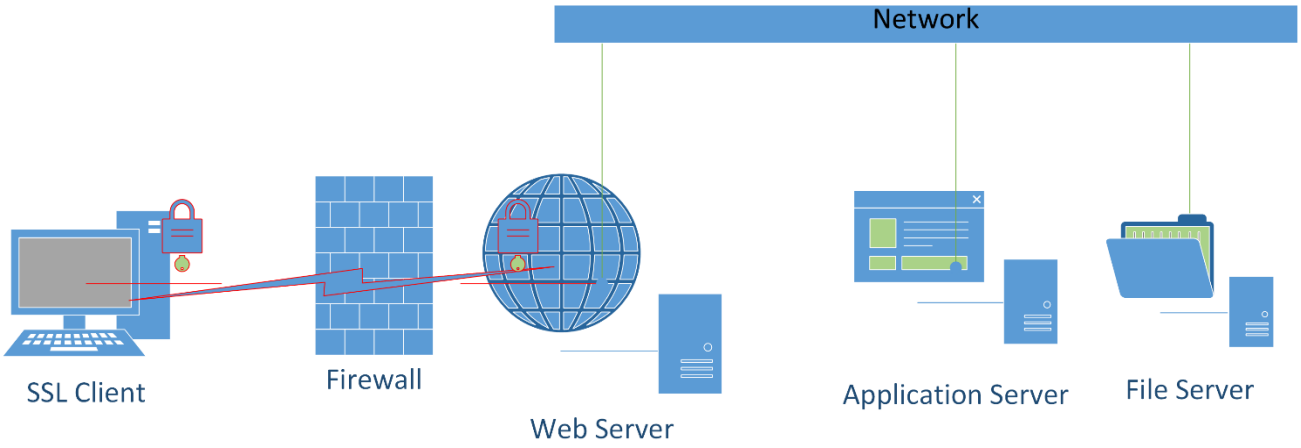
10.3. TLS/SSL VPN

Το SSL (Secure Sockets Layer), ή η νεότερη προτυποποιημένη μορφή TLS (Transport Layer Security), είναι ένα πρωτόκολλο επιπέδου μεταφοράς. Εισήχθη αρχικά από την εταιρία Netscape το 1995 στην έκδοση 2.0 και

την επόμενη χρονιά παρουσιάστηκε η βελτιωμένη έκδοση 3.0. Επίσης, παρουσιάστηκαν και άλλα αντίστοιχα πρωτόκολλα (όπως τα PCT και STLP της Microsoft). Τελικά, η IETF παρουσίασε με το RFC2246 το TLS 1.0 το οποίο βασίζεται στο SSL 3.0 (χωρίς να είναι μεταξύ τους απολύτως συμβατά).

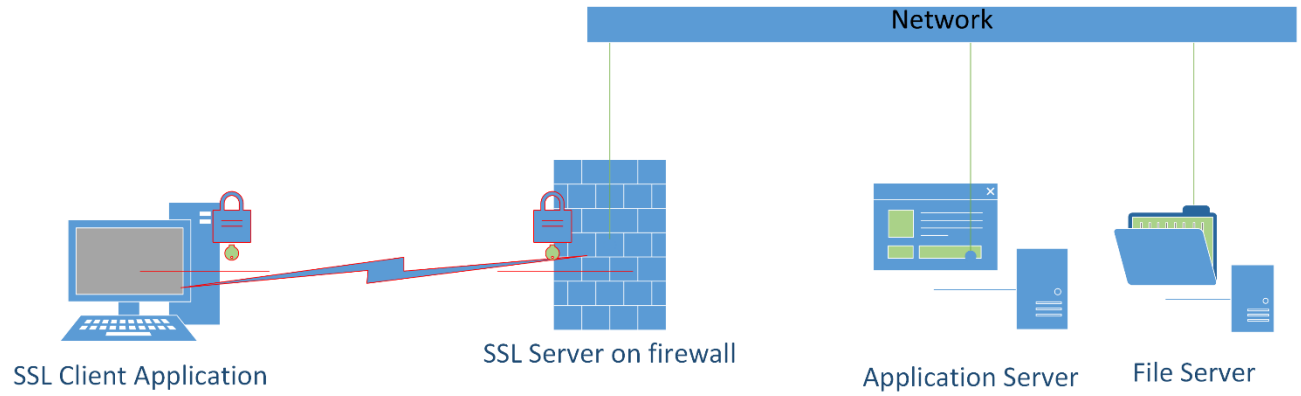
Το TLS (και το SSL), παρέχει υπηρεσίες αυθεντικοποίησης και κρυπτογράφησης στην επικοινωνία μεταξύ Web server και Web browser. Με τον ίδιο τρόπο, χρησιμοποιείται σε εφαρμογές ηλεκτρονικής αλληλογραφίας (πρωτόκολλα POP, IMAP, SMTP) ή ανταλλαγής αρχείων (FTP). Πέραν όμως από τη χρήση αυτή, παρέχει τη δυνατότητα εφαρμογής δύο βασικών τύπων VPN:

- **Portal VPN**: Το portal VPN υλοποιείται με τη χρήση ενός διακομιστή (Web server) στον οποίο συνδέεται ο πελάτης με τη χρήση ενός απλού Web browser. Στο διακομιστή αυτό φιλοξενείται ένα σύνολο ιστοσελίδων μέσω των οποίων (και πάντα με τη χρήση κλήσεων https) ο πελάτης μπορεί να έχει πρόσβαση σε υπηρεσίες που εκτελούνται σε άλλους διακομιστές του δικτύου. Το portal VPN εισάγει τον περιορισμό πως θα πρέπει όλες οι υπηρεσίες να παρουσιάζονται από τον Web Server σε μορφή Web σελίδων. Πολλές φορές κάτι τέτοιο δεν είναι δυνατό. Είναι όμως μια λύση, που δεν απαιτεί από την πλευρά του πελάτη τίποτα περισσότερο πέρα από τη χρήση ενός Web browser στον οποίο θα εισαχθεί απλά το URL μέσω του οποίου είναι προσβάσιμος ο Web Server. Στην Εικόνα 10.7 φαίνεται ο Web server ο οποίος παρέχει ως περιεχόμενο (ιστοσελίδες με κατάλληλους συνδέσμους) τις υπηρεσίες των υπόλοιπων διακομιστών (π.χ. links στον file server).



Εικόνα 10.7 *SSL Portal VPN.*

- **Tunnel VPN**: Το tunnel VPN παρέχει τη δυνατότητα δημιουργίας ενός ασφαλούς καναλιού επικοινωνίας μεταξύ ενός SSL/TLS gateway και του πελάτη με σκοπό τη διακίνηση πληροφορίας μεταξύ του τελευταίου και των κόμβων του δικτύου που βρίσκεται πίσω από το gateway (Εικόνα 10.8). Η διαφοροποίηση, όσο αφορά το portal VPN είναι πως απαιτείται η εκτέλεση ενός προγράμματος πελάτη στον client, το οποίο μπορεί να είναι μια αυτόνομη εφαρμογή ή ένα ένθετο ενός browser (java applet, activeX component κοκ). Χαρακτηριστικό παράδειγμα εφαρμογής TLS Tunnel VPN είναι η εφαρμογή OpenVPN.



Εικόνα 10.8 *SSL Tunnel VPN.*

10.4 IPsec VPN

Σκοπός του IPsec είναι η προσθήκη χαρακτηριστικών ασφάλειας στο πρωτόκολλο IP και συγκεκριμένα η διασφάλιση της αυθεντικοποίησης, της ακεραιότητας και της εμπιστευτικότητας των διακινούμενων δεδομένων. Για να επιτευχθεί ο σκοπός αυτός, το IPsec λειτουργεί στο επίπεδο δικτύου και χρησιμοποιεί ένα σύνολο πρωτοκόλλων:

- Μετα-πρωτόκολλο Internet Key Exchange (IKE)
- Πρωτόκολλα ασφάλειας
  - Encapsulating Security Payload (ESP)
  - Authentication Header (AH)

Βασικός στόχος είναι η εδραίωση συσχετίσεων ασφάλειας (Security Associations – SA) μεταξύ δύο κόμβων. Στη συνέχεια, περιγράφεται η λειτουργία κάθε πρωτοκόλλου και εξηγείται η έννοια της συσχέτισης ασφαλείας.

10.4.1 Συσχετίσεις ασφάλειας

Μια συσχέτιση ασφάλειας είναι η αποτύπωση μιας συμφωνίας μεταξύ δύο άκρων που θέλουν να επικοινωνήσουν και μπορεί να προσδιοριστεί από ένα μοναδικό αναγνωριστικό (Security Parameter Index – SPI), την IP διεύθυνση του απέναντι άκρου και τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί. Όταν επιτευχθεί μια τέτοια συμφωνία, τότε η πληροφορία καταγραφής της αποθηκεύεται σε μια βάση δεδομένων που ονομάζεται Security Association Database (SAD). Για κάθε συσχέτιση ασφάλειας καταγράφεται στη SAD:

- Η διεύθυνση του ενός άκρου.
- Η διεύθυνση του άλλου (απέναντι) άκρου.
- Ο αριθμός SPI.
- Το αναγνωριστικό του πρωτοκόλλου ασφάλειας (AH / ESP).
- Ο τρόπος λειτουργίας (transport / tunnel mode).
- Ο αλγόριθμος κρυπτογράφησης.
- Ο αλγόριθμος ακεραιότητας.
- Πληροφορίες κλειδιών.
- Ο χρόνος ζωής της συσχέτισης ασφάλειας.
- Πληροφορίες anti-replay.
- Τη ροή δεδομένων στην οποία εφαρμόζεται η συσχέτιση ασφάλειας.

Η πολιτική εφαρμογής ενεργειών (protect, bypass, discard) στην κίνηση πακέτων, περιγράφεται σε μια άλλη βάση δεδομένων, γνωστή ως SPD (Security Policy Database), όπου για τις ροές δεδομένων που προστατεύονται αναφέρονται:

- Οι IP διευθύνσεις πηγής και προορισμού.
- Το πρωτόκολλο επιπέδου μεταφοράς (TCP, UDP).
- Ο αριθμός θύρας (αν πρέπει να καθοριστεί).
- Ένας δείκτης σε συγκεκριμένη συσχέτιση ασφάλειας της SAD, αν κάτι τέτοιο απαιτείται.

Κάθε συσχέτιση ασφάλειας ισχύει για συγκεκριμένο χρόνο, μετά την παρέλευση του οποίου πρέπει να συμβεί αναδιαπραγμάτευση και εδραίωση νέας συσχέτισης ασφάλειας.

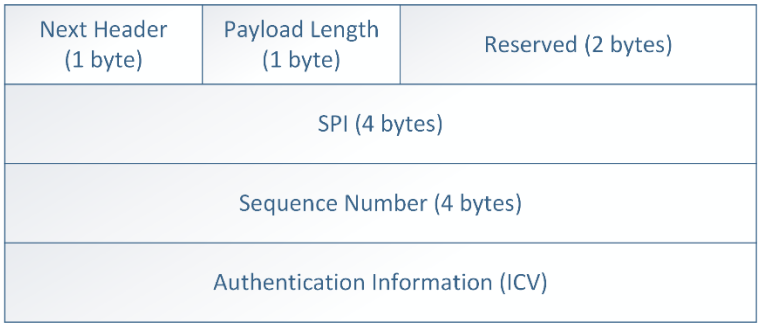
10.4.2 Πρωτόκολλα ασφάλειας

Στο IPsec υπάρχει η δυνατότητα επιλογής μεταξύ δύο διαφορετικών πρωτοκόλλων ασφάλειας. Τα δύο αυτά πρωτόκολλα είναι το AH (Authentication Headers), που προσδιορίζεται από τον αριθμό 51 στο πεδίο Protocol της κεφαλίδας IP (IP header) και περιγράφεται από το RFC4302, καθώς και το ESP (Encapsulating Security Payload), που προσδιορίζεται από τον αριθμό 50 στο πεδίο Protocol της κεφαλίδας IP και περιγράφεται από το RFC4303.

10.4.2.1 Το πρωτόκολλο AH

Το πρωτόκολλο AH (Authentication Headers) παρέχει αυθεντικοποίηση και έλεγχο ακεραιότητας των δεδομένων, αλλά δεν παρέχει εμπιστευτικότητα. Λειτουργεί προσθέτοντας μια επιπρόσθετη κεφαλίδα (header) σε κάθε IP πακέτο, μετά την πρώτη IP κεφαλίδα. Η κεφαλίδα του AH περιλαμβάνει μια σύνοψη του συνόλου των bit του πακέτου, που ονομάζεται ICV (Integrity Check Value) και διασφαλίζει πως το πακέτο δεν έχει μεταβληθεί κατά τη μεταφορά.

Η δομή της κεφαλίδας AH απεικονίζεται στην ακόλουθη Εικόνα 10.9:



Εικόνα 10.9 *Δομή της κεφαλίδας AH.*

όπου:

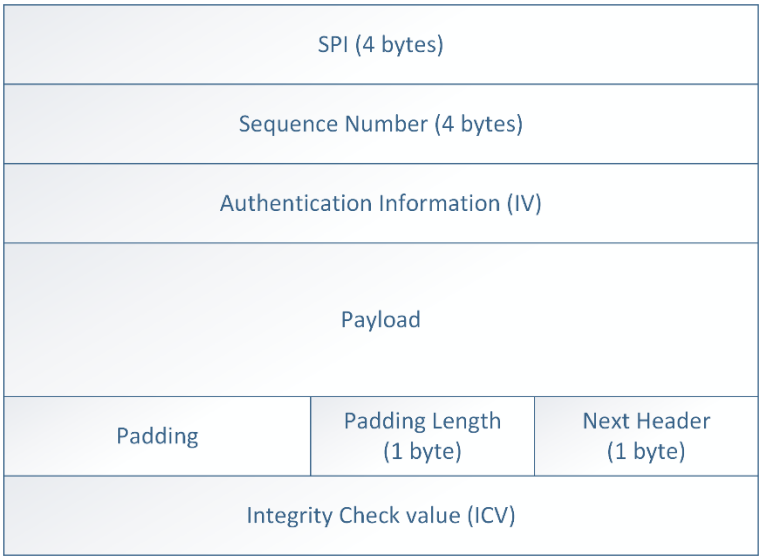
- Το Next Header περιέχει τον αριθμό πρωτοκόλλου της κεφαλίδας που ακολουθεί.
- Το Payload Length αναφέρεται στο μέγεθος του AH, σε 32bit words (4 bytes) μείον 2. Για παράδειγμα, αν το συνολικό μέγεθος είναι 192 bit, η τιμή του Payload Length θα είναι 4 (προκύπτει από το ότι τα 192 bit είναι 6word x 32bit, μείον 2).
- Το τμήμα Reserved είναι δεσμευμένο για μελλοντική χρήση με τιμή 0.
- Το αναγνωριστικό Security Parameter Index (SPI).

- Το Sequence Number είναι ο αύξων αριθμός πακέτου με σκοπό την προστασία από επιθέσεις αναπαραγωγής (replay attacks). Ο αριθμός περιέχεται και στο πεδίο authenticated data, έτσι ώστε η τροποποίηση μιας τιμής να γίνεται άμεσα αντιληπτή.

- Το Authentication Information (ή Integrity Check Value – ICV) περιέχει τη συνόψιση του πακέτου, που παράγεται από μια κατάλληλη μονόδρομη συνάρτηση. Το μέγεθός του σε bits είναι ακέραιο πολλαπλάσιο του 32.

10.4.2.2 Το πρωτόκολλο ESP

Το πρωτόκολλο ESP (Encapsulating Security Payload) παρέχει, όπως και το AH, αυθεντικοποίηση και έλεγχο ακεραιότητας, αλλά επιπρόσθετα και εμπιστευτικότητα των δεδομένων. Για το λόγο αυτό, είναι το πρωτόκολλο που συνήθως επιλέγεται στις υλοποιήσεις IPsec VPN (αν και στις αρχικές υλοποιήσεις του, το ESP παρείχε μόνο εμπιστευτικότητα, οπότε χρησιμοποιούνταν σε συνδυασμό με το AH).



Εικόνα 10.10 *Δομή της κεφαλίδας ESP.*

Το ESP προσθέτει στο IP πακέτο ένα header και ένα trailer που περικλείουν το payload του πακέτου (Εικόνα 10.10). Το header περιλαμβάνει 2 πεδία (αντίστοιχα με το AH):

- Το αναγνωριστικό Security Parameter Index (SPI).
- Τον αύξοντα αριθμό πακέτου (Sequence Number).

Στη συνέχεια, ακολουθεί ένα διάνυσμα αρχικοποίησης (Initialization Vector – IV), το οποίο γίνεται μέρος του payload. Σκοπός του είναι να παρέχει διαφορετικό κρυπτογράφημα σε δύο payload με ίδιο περιεχόμενο, προκειμένου να δυσχεραίνεται η κρυπτανάλυση.

Τέλος, το trailer περιλαμβάνει:

- Το συμπλήρωμα (padding) που αποτελεί ένα σύνολο bit με μέγεθος τέτοιο ώστε το μήκος του payload να καθίσταται κατάλληλο για καθορισμό δεσμών (blocks) κρυπτογράφησης.
- Το μήκος του συμπληρώματος (Padding Length).
- Το Next Header, όπως στο AH.
- Το Integrity Check Value, όπως στο AH.

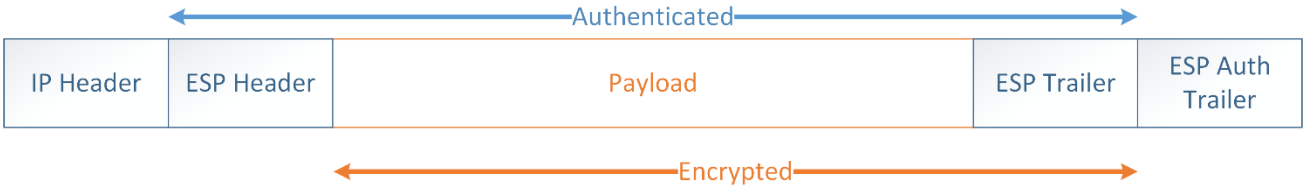
10.4.3 Τρόποι λειτουργίας του IPsec

Στο IPsec, η ασφαλής επικοινωνία μπορεί να εδραιωθεί με δύο διαφορετικούς τρόπους. Στην επικοινωνία μεταξύ δύο κόμβων, υλοποιείται το transport mode, ενώ όταν έχουμε επικοινωνία μεταξύ δύο δικτύων υλοποιείται το tunnel mode μεταξύ των gateways των δικτύων αυτών.

10.4.3.1 Transport mode

Στο transport mode, οι IP διευθύνσεις πηγής και προορισμού δε μεταβάλλονται (Εικόνα 10.11 και Εικόνα 10.12).

Εικόνα 10.11 *AH Transport Mode.*

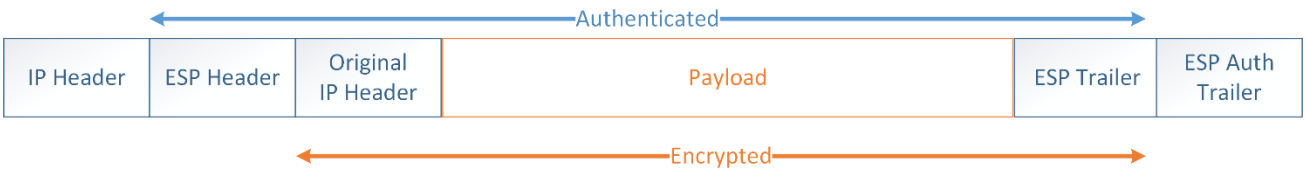


Εικόνα 10.12 *ESP Transport Mode.*

10.4.3.2 Tunnel mode

Στο tunnel mode, το αρχικό IP πακέτο ενθυλακώνεται (ως payload) μέσα σε ένα νέο πακέτο (Εικόνα 10.13 και Εικόνα 10.14).

Εικόνα 10.13 *AH Tunnel Mode.*



Εικόνα 10.14 *ESP Tunnel Mode.*

10.4.4 Μετα-πρωτόκολλο IKE

Το μετα-πρωτόκολλο Internet Key Exchange (IKE) περιγράφεται στο RFC2409 και χρησιμοποιείται για:

- Την αυθεντικοποίηση των δύο άκρων.
- Τη διαχείριση των κλειδιών συνόδου.
- Τον καθορισμό των παραμέτρων επικοινωνίας.

Χαρακτηρίζεται ως μετα-πρωτόκολλο καθώς αποτελεί το συνδυασμό χαρακτηριστικών των επιμέρους πρωτοκόλλων:

- **Internet Security Association and Key Management Protocol (ISAKMP)**: Το ISAKMP περιγράφεται στο RFC2407 και καθορίζει το πλαίσιο (framework) λειτουργίας του IKE για τη δημιουργία των συσχετίσεων ασφάλειας και τη διαχείριση των κλειδιών συνόδου.

- **Oakley**: Το Oakley περιγράφεται στο RFC2412 και χρησιμοποιείται για παραγωγή και διανομή του κλειδιού κρυπτογράφησης συνόδου, κάνοντας χρήση του αλγορίθμου Diffie-Hellman.

- **Secure Key Exchange Mechanism (SKEME)**: Το SKEME καθορίζει τη μορφή μηνυμάτων για την ανταλλαγή των κλειδιών με σκοπό την παροχή ανωνυμίας, δυνατότητας αποποίησης (repudiatability) και τον καθορισμό του τρόπου ανανέωσής τους.

Το IKE υλοποιείται σε δύο διακριτές φάσεις, οι οποίες θα περιγραφούν στις υποενότητες 4.4.2 και 4.4.3 του παρόντος κεφαλαίου.

10.4.4.1 Ο αλγόριθμος Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman προτάθηκε το 1976 από τους Whitfield Diffie και Martin Hellman και αποτελεί τον πρώτο αλγόριθμο δημοσίου κλειδιού. Ο αλγόριθμος αυτός χρησιμοποιείται με σκοπό την ασφαλή ανταλλαγή ενός μυστικού κλειδιού μέσα από ένα ανασφαλές κανάλι, όπως το Διαδίκτυο.

Αρχικά, τα δύο μέρη συμφωνούν σε δύο αριθμούς p και g. Ο p είναι ένας μεγάλος αριθμός (μεγαλύτερος από 512 bit) και ο g μια πρωτογενής ρίζα του p. Οι αριθμοί p και g είναι ορατοί σε όλους. Στη συνέχεια, τα δύο μέλη επιλέγουν το καθένα από έναν τυχαίο (μεγάλο) αριθμό n_1 και n_2, αντίστοιχα. Κατόπιν, υπολογίζουν τα:

$$y_1 = g^{n_1} \pmod{p} \tag{10.1}$$

και

$$y_2 = g^{n_2} \pmod{p} \tag{10.2}$$

Τα οποία και ανταλλάσσουν μεταξύ τους. Στη συνέχεια, τα δύο μέλη υπολογίζουν το κλειδί $K=K_1=K_2$ ως εξής:

$$K_1 = y_1^{(n_1)} \bmod p \tag{10.3}$$

και

$$K_2 = y_2^{(n_2)} \bmod p$$

(10.4)

Το κλειδί K πλέον είναι διαθέσιμο και στα δυο μέρη και μπορεί να χρησιμοποιηθεί για την κρυπτογραφημένη ανταλλαγή πληροφορίας. Για να μπορέσει κάποιος από τα γνωστά p, g, y_1 και y_2 να υπολογίσει το K θα πρέπει να λύσει:

$$K = y_i^{(\log_g n_i)} \bmod p$$

(10.5)

που αποτελεί το γνωστό ως Πρόβλημα Διακριτών Λογαρίθμων (Discrete Logarithm Problem - DLP), το οποίο ως σήμερα για μεγάλες τιμές του p δεν έχει λύση σε πεπερασμένο χρόνο.

10.4.4.2 IKE Phase 1

Η πρώτη φάση του IKE έχει ως σκοπό την αυθεντικοποίηση των επικοινωνούντων μερών (του initiator και του responder) και, στη συνέχεια, τη δημιουργία του κλειδιού και την εδραίωση μιας αμφίδρομης συσχέτισης ασφάλειας.

Η αυθεντικοποίηση μπορεί να πραγματοποιηθεί με δύο βασικούς τρόπους. Με τη χρήση προ-διαμοιρασμένων κλειδιών (pre-shared keys), που λειτουργούν ως συνθηματικά ή με τη χρήση ψηφιακών πιστοποιητικών. Η χρήση pre-shared keys είναι ο πιο απλός τρόπος υλοποίησης, αλλά παρουσιάζει ζητήματα σχετικά με το ότι πρέπει να οριστεί χειροκίνητα και να είναι κοινό τουλάχιστον ανά ζεύγος επικοινωνίας. Παρότι όμως η μέθοδος αυτή παρουσιάζει προβλήματα, κυρίως σε ότι αφορά τη μυστικότητα του προ-διαμοιρασμένου κλειδιού, εν τούτοις πολλές φορές, ιδίως εκεί όπου οι IP διευθύνσεις των επικοινωνούντων μερών δεν είναι σταθερές, η επιλογή της είναι μονόδρομος. Μετά το πέρας της αυθεντικοποίησης, πραγματοποιείται η διαπραγμάτευση των παραμέτρων επικοινωνίας και εδραιώνεται η συσχέτιση ασφάλειας (IKE SA).

Η πρώτη φάση του IKE μπορεί να υλοποιηθεί με δύο διαφορετικούς τρόπους λειτουργίας: main mode και aggressive mode. Η βασική διαφορά μεταξύ των main και aggressive mode έγκειται στο σύνολο των μηνυμάτων που ανταλλάσσονται και στην προστασία της ταυτότητας των επικοινωνούντων μερών. Συγκεκριμένα, στο main mode, που είναι και ο προεπιλεγμένος τρόπος διαπραγμάτευσης, απαιτούνται έξι (6) μηνύματα, ενώ στον aggressive mode απαιτούνται μόλις τρία (3) μηνύματα.

10.4.4.2.1 Aggressive Mode

- Ο initiator αποστέλλει όλες τις παραμέτρους που καθορίζονται από τις διαθέσιμες πολιτικές isakmp, τον αριθμό n που προκύπτει κατά την εκτέλεση του Diffie-Hellman, ένα nonce και την ταυτότητά του.

- Ο responder αποστέλλει τις παραμέτρους ασφάλειας στις οποίες συμφωνεί, το δικό του n, την ταυτότητά του, ένα nonce και το authentication payload.

- Ο initiator αποστέλλει το authentication payload

10.4.4.2.2 Main Mode

- Ο initiator αποστέλλει όλες τις παραμέτρους ασφάλειας που καθορίζονται από τις διαθέσιμες πολιτικές isakmp.

- Ο responder απαντά με την συμφωνηθείσα πολιτική.

- Ο initiator αποστέλλει το n και ένα nonce.
- Ο responder αποστέλλει το δικό του n και ένα nonce.
- Ο initiator αποστέλλει κρυπτογραφημένο (με τις συμφωνημένες παραμέτρους) το authentication message
- Ο responder αποστέλλει κρυπτογραφημένο (με τις συμφωνημένες παραμέτρους) το authentication message

Μια πολιτική ασφάλειας isakmp περιλαμβάνει:

- Μέθοδο Αυθεντικοποίησης (π.χ. Pre-Shared Key).
- Συνάρτηση κατακερματισμού (π.χ. SHA1).
- Αλγόριθμο κρυπτογράφησης (π.χ. AES).
- Αριθμό προσδιορισμού του Diffie-Hellman Group. Τα διαφορετικά group numbers, ανάλογα με το μέγεθος του modp, φαίνονται στον ακόλουθο Πίνακα10.2:

Group Number	**modp size**
1	768
2	1024
5	1536
14	2048

Πίνακας 10.2 *Προσδιοριστικοί αριθμοί για Diffie-Hellman Group*

10.4.4.3 IKE Phase 2

Η δεύτερη φάση του IKE οδηγεί στην εδραίωση δυο μονόδρομων συσχετίσεων ασφαλείας μεταξύ των δύο άκρων επικοινωνίας. Το κλειδί της συμμετρικής κρυπτογράφησης, που θα χρησιμοποιηθεί, θα παραχθεί με τη χρήση του αλγόριθμου Diffie-Hellman και μπορεί να είναι είτε το ίδιο με αυτό της αμφίδρομης συσχέτισης IKE SA, είτε ένα νέο. Σε αντίθεση με την πρώτη φάση, υπάρχει μόνον ένας τύπος λειτουργίας, το Quick Mode, με τον οποίο καθορίζονται οι παράμετροι και το πρωτόκολλο επικοινωνίας, με τις ακόλουθες ενέργειες:

- Το ένα άκρο (A) προωθεί μια πρόταση ασφάλειας (security proposal), η οποία περιλαμβάνει το πρωτόκολλο ασφάλειας (AH ή ESP), τον αλγόριθμο κρυπτογράφησης, τη συνάρτηση κατακερματισμού και το interesting traffic, δηλαδή την κίνηση (traffic) που θα προωθείται μέσω της κρυπτογραφημένης επικοινωνίας.
- Το απέναντι άκρο (B) συμφωνεί με τις προτεινόμενες παραμέτρους.
- Το άκρο A αποστέλει τα authentication payload και message digest με σκοπό την αυθεντικοποίηση και την αποφυγή αναπαραγωγής (replay).
- Το άκρο B επιβεβαιώνει.

Μια άλλη παράμετρος, κατά την εδραίωση των συσχετίσεων ασφάλειας, είναι η ενεργοποίηση ή όχι του Perfect Forward Secrecy (PFS). Το PFS διασφαλίζει πως με τη λήξη μιας συνόδου, θα υπολογιστεί ένα νέο

κλειδί συνόδου με τη χρήση του Diffie-Hellman. Με τον τρόπο αυτό, αποφεύγεται η επαναχρησιμοποίηση ενός κλειδιού που ίσως έχει αποκαλυφθεί από μια προσπάθεια κρυπτανάλυσης.

Με την επιτυχή ολοκλήρωση των δύο φάσεων, θα έχουν εδραιωθεί τρείς συσχετίσεις ασφάλειας:

- Μια αμφίδρομη ISAKMP SA, η οποία χρησιμοποιείται για την εδραίωση των IPsec SAs.
- Μια εξερχόμενη IPsec SA, η οποία χρησιμοποιείται για την προώθηση της κίνησης στο απέναντι άκρο. Το traffic αναγνωρίζεται με την προσθήκη του SPI στο header.
- Μια εισερχόμενη IPsec SA, η οποία χρησιμοποιείται για την εισερχόμενη κίνηση που, ομοίως, αναγνωρίζεται από την προσθήκη της τιμής του SPI στο IPsec header.

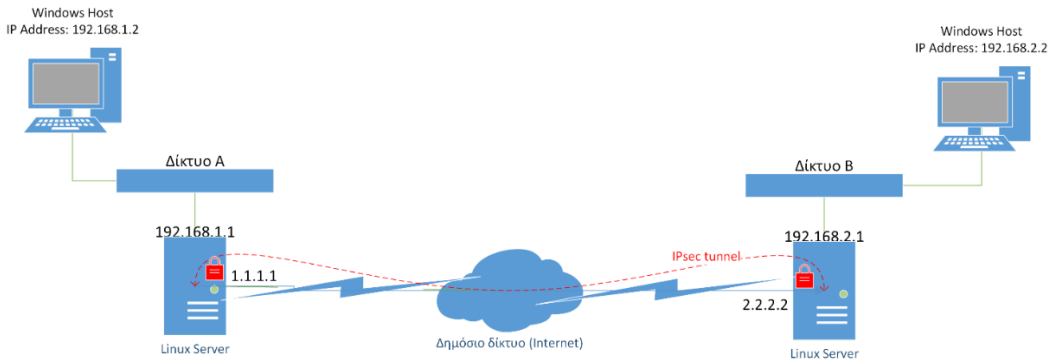
10.5 Data-Link Layer VPN

Σκοπός των τεχνολογιών VPN, που λειτουργούν στο επίπεδο Data-Link, είναι η λειτουργία πρωτοκόλλων που δεν βασίζονται στο IP. Συνήθως, οι υλοποιήσεις αυτές χρησιμοποιούν άλλα πρωτόκολλα ανώτερου επιπέδου για να παρέχουν λειτουργίες, όπως εμπιστευτικότητα ή αυθεντικοποίηση.

Ενδεικτικά Data-Link Layer VPN πρωτόκολλα είναι τα PPTP, L2F και L2TP. Τα πρωτόκολλα αυτά είναι επιρρεπή σε επιθέσεις IP spoofing και man-in-the middle (MITM). Το πλεονέκτημά τους είναι ότι, ως πρωτόκολλα που υλοποιούνται στο δεύτερο επίπεδο του μοντέλου αναφοράς του OSI, μπορούν να μεταφέρουν δεδομένα με χρήση πρωτοκόλλων εκτός του IP.

10.6 Μελέτη Περίπτωσης

Στη μελέτη περίπτωσης που ακολουθεί, απαιτείται η συνεργασία των φοιτητών σε δυάδες. Το σενάριο που καλούμαστε να υλοποιήσουμε είναι η δημιουργία συνθηκών επικοινωνίας σε IPSEC tunnel mode, μεταξύ δυο Linux υπολογιστών (hosts), ένα από κάθε διαφορετικό δίκτυο, μέσω των οποίων θα διακινείται η πληροφορία που προέρχεται από ή απευθύνεται στους υπόλοιπους hosts του κάθε δικτύου (Εικόνα 10.15).



Εικόνα 10.15 *Σενάριο μελέτης περίπτωσης.*

Προτείνεται να χρησιμοποιηθούν οι IP διευθύνσεις που φαίνονται στον ακόλουθο Πίνακα 10.3:

	Δίκτυο Α	**Δίκτυο Β**
Linux public IP / interface	1.1.1.1 / eth0	2.2.2.2 / eth0
Private Network	192.168.1.0/24	192.168.2.0/24
Linux private IP / interface	192.168.1.1 / eth1	192.168.2.1 / eth1
Windows IP	192.168.1.2	192.168.2.2

Πίνακας 10.3 *Προτεινόμενες IP διευθύνσεις.*

Αν για οποιοδήποτε λόγο, χρησιμοποιηθούν διαφορετικές IP διευθύνσεις, χρησιμοποιήστε τον παρακάτω πίνακα για να συμπληρώστε τις δικές σας διαφορετικές IP διευθύνσεις.

	Δίκτυο Α	**Δίκτυο Β**
Linux public IP / interface		
Private Network		
Linux private IP / interface		
Windows IP		

Πίνακας 10.4 *IP διευθύνσεις χρήστη*.

Αρχικά, πρέπει να βεβαιωθούμε πως έχουν εγκατασταθεί στους υπολογιστές τα IPsec-Tools. Για παράδειγμα σε διανομή τύπου RedHat (Centos, Oracle UL) εκτελούμε την εντολή:

```
yum install ipsec-tools
```

Κατόπιν, ενεργοποιούμε τη δυνατότητα προώθησης πακέτων σε κάθε Linux υπολογιστή με την εντολή:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Για τη λειτουργία της πρώτης φάσης (IKE Phase 1) και την αυθεντικοποίηση των άκρων, θα πρέπει να αντιστοιχίσουμε ένα κλειδί με κάθε απομακρυσμένο host. Φυσικά, το κλειδί που θα αντιστοιχίσουμε με την διεύθυνση IP του host, με τον οποίο θα επικοινωνήσουμε, πρέπει να είναι κοινό με εκείνο που θα αντιστοιχισθεί σε εκείνον, αντίστοιχα, από το άλλο άκρο. Έστω ότι Secret_KeY είναι το κλειδί αυτό, το οποίο θα προστεθεί στο αρχείο psk.txt, ως ακολούθως:

```
echo "2.2.2.2 Secret_KeY" >> /etc/racoon/psk.txt
```

όπου 2.2.2.2 η διεύθυνση του άλλου άκρου.

Το pre-shared key, στη συγκεκριμένη περίπτωση, χρησιμοποιείται για αυθεντικοποίηση (δεν είναι κλειδί κρυπτογράφησης). Θα μπορούσε, εναλλακτικά, να γίνει χρήση ψηφιακών πιστοποιητικών (digital certificates).

Θα πρέπει, στη συνέχεια, να βεβαιωθούμε ότι το αρχείο αυτό είναι αναγνώσιμο μόνο από εμάς (ιδιοκτήτης), με την εντολή:

```
chmod 600 /etc/racoon/psk.txt
```

Για να θέσουμε τις παραμέτρους για το SA, ανοίγουμε για επεξεργασία το αρχείο /etc/racoon/racoon.conf με τον editor vi, εκτελώντας την ακόλουθη εντολή:

```
vi /etc/racoon/racoon.conf
```

Στην τελευταία γραμμή, (με το πάτημα του πλήκτρου <o>) μπορούμε να εισάγουμε τις παρακάτω ρυθμίσεις:

```
remote 83.212.111.218 {
      exchange_mode agressive;
      proposal {
                encryption_algorithm 3des;
                hash_algorithm sha1;
                authentication_method pre_shared_key;
                dh_group modp1024;
      }
}
```

με τις οποίες επιλέγονται:

- Aggressive mode.
- Αλγόριθμος κρυπτογράφησης 3DES.
- Αλγόριθμος κατακερματισμού τον SHA1.
- Αυθεντικοποίηση με χρήση προ-διαμοιρασμένων κλειδιών.
- DH group 2.

Αποθηκεύουμε τις αλλαγές στο αρχείο, πατώντας το πλήκτρο <ESC> και αφού βεβαιωθείτε ότι όλα είναι σωστά, πατάτε:

```
:wq
```

Στη συνέχεια, πρέπει να τεθούν οι παράμετροι των SA της δεύτερης φάσης (IKE Phase 2). Για το σκοπό αυτό, ανοίγουμε για επεξεργασία το αρχείο /etc/racoon/racoon.conf:

```
vi /etc/racoon/racoon.conf
```

Έστω, ότι το δικό μας ιδιωτικό δίκτυο είναι το 192.168.1.0/24 και το απέναντι δίκτυο είναι το 192.168.2.0/24. Προσθέτουμε τις παρακάτω ρυθμίσεις:

```
sainfo address 10.13.1.0/29[any] any address 10.13.2.0/24[any]
any {
        pfs_group modp768;
        encryption_algorithm 3des;
        authentication_algorithm hmac_sha1;
        compression_algorithm deflate;
}
```

με τι οποίες ορίζονται οι παράμετροι IPsec ως εξής:

- PFS Group 1.
- Αλγόριθμος κρυπτογράφησης 3DES.
- Αλγόριθμος αυθεντικοποίησης HMAC SHA1.

Αποθηκεύουμε το ενημερωμένο αρχείο.

Τέλος, θα καθορίσουμε την «ενδιαφέρουσα κίνηση» (interesting traffic) η οποία θα διέρχεται από το tunnel. Ανοίγουμε με τον editor vi το αρχείο /etc/racoon/ipsec.conf και εισάγουμε τις παρακάτω ρυθμίσεις:

```
#!/usr/sbin/setkey -f

spdadd 192.168.1.0/24 192.168.2.0/24 any -P out ipsec
        esp/tunnel/1.1.1.1-2.2.2.2/require;

spdadd 192.168.2.0/24 192.168.1.0/24 any -P in ipsec
        esp/tunnel/2.2.2.2-1.1.1.1/require;
```

Πατάμε το πλήκτρο <ESC> και αφού βεβαιωθούμε ότι όλα είναι σωστά, πατάμε :wq

Για τον έλεγχο της επικοινωνίας, θα ελέγξουμε αν έχει εδραιωθεί το tunnel mode και αν η πληροφορία διακινείται μέσω του ασφαλούς αυτού καναλιού, ως εξής:

Αρχικά, θα πρέπει να επιτρέψουμε την κίνηση πακέτων μεταξύ των δύο hosts. Ανοίγουμε με τον editor (π.χ. vi) το αρχείο /etc/sysconfig/iptables, όπου προσθέτουμε τρείς κανόνες στα κατάλληλα σημεία.

- Ο πρώτος κανόνας ενεργοποιεί τη δυνατότητα προώθησης πακέτων μεταξύ των δικτυακών διεπαφών:

```
-A FORWARD -j ACCEPT
```

- Ο δεύτερος κανόνας επιτρέπει την αποδοχή των πακέτων τύπου ESP:

```
-A INPUT -p esp -j ACCEPT
```

- Ο τρίτος επιτρέπει τη σύνδεση στη θύρα 500 με χρήση του πρωτοκόλλου UDP:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 500 -
j ACCEPT
```

Εκκινούμε το daemon racoon με τις ακόλουθες εντολές:

```
setkey –f /etc/racoon/ipsec.conf
racoon -F
```

Στο παράθυρο που δημιουργήθηκε, εμφανίζονται όλα τα μηνύματα του IPsec daemon. Ακολούθως, ανοίγουμε ένα νέο τερματικό και εκτελούμε την εντολή:

```
ping 192.168.2.1
```

όπου 192.168.2.1 είναι η διεύθυνση IP του άλλου άκρου (απέναντι Linux host). Είναι εφικτή η επικοινωνία; Μπορείτε να ελέγξετε αν όντως τα πακέτα ενθυλακώνονται σε ESP πακέτα;

Ξεκινάμε ένα νέο SSH session και στο νέο παράθυρο εκτελούμε την εντολή:

```
tcpdump host 1.1.1.1
```

Στο προηγούμενο παράθυρο δοκιμάζουμε τις εντολές:

```
ping 2.2.2.2
ping -I 192.168.1.1 192.168.2.1
ping www.google.com
```

όπου 2.2.2.2 και 192.168.2.1 είναι οι public και local IP διευθύνσεις, αντίστοιχα, του απέναντι Linux host).

Στο προηγούμενο βήμα παρατηρήσαμε ότι, αν και έχουμε καθορίσει το interesting traffic και το tunnel έχει εδραιωθεί, δεν ήταν δυνατή η επικοινωνία. Αυτό συμβαίνει γιατί δεν έχουν δοθεί οι κατάλληλες οδηγίες δρομολόγησης.

Συνδεόμαστε με τον υπολογιστή με Λ.Σ. Windows. Σκοπός μας είναι να επικοινωνήσουμε με τον υπολογιστή Windows του συμφοιτητή που επιλέξαμε, μέσω του ασφαλούς καναλιού. Έστω ότι 192.168.1.1 είναι η local IP διεύθυνση του Linux host και 192.168.2.0/24 η διεύθυνση του απέναντι δικτύου. Ξεκινάμε ένα παράθυρο εντολών γραμμής (command prompt) και εκτελούμε την εντολή:

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.1
```

Μπορούμε τώρα να επικοινωνήσουμε; Αν και το καταφέραμε, κανονικά οι διευθύνσεις 192.168.0.0/16 δεν θα έπρεπε να δρομολογούνται μέσω του Internet. Τι συμβαίνει;

Βιβλιογραφία

Kent, S. (2005), IP Authentication Header. Retrieved 30 November 2015, from https://tools.ietf.org/html/rfc4302

Carmouche, J. H. (2007). IPsec virtual private network fundamentals. Indianapolis, Ind: Cisco Press.

Convery, S. (2004). Network security architectures. Indianapolis, IN: Cisco Press.

Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654. http://doi.org/10.1109/TIT.1976.1055638

Frankel, S. E., Hoffman, P., Orebaugh, A. D., & Park, R. (2008). SP 800-113. Guide to SSL VPNs. Gaithersburg, MD, United States: National Institute of Standards & Technology.

Krawczyk, H. (1996). SKEME: a versatile secure key exchange mechanism for Internet. In , Proceedings of the Symposium on Network and Distributed System Security, 1996 (pp. 114–127). http://doi.org/10.1109/NDSS.1996.492418

Northcutt, S. (Ed.). (2005). Inside network perimeter security (2nd ed). Indianapolis, Ind: Sams Pub.

Polk, T., McKay, K., & Chokhani, S. (2014). Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations (No. NIST SP 800-52r1). National Institute of Standards and Technology. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

RFC 4302 - IP Authentication Header. (n.d.). Retrieved 30 September 2015, from https://tools.ietf.org/html/rfc4302.

Κριτήρια αξιολόγησης

Ερωτήσεις κατανόησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Πλεονέκτημα των VPN είναι:
α) Η υψηλή ταχύτητα.
β) Το μειωμένο κόστος.
γ) Ευελιξία υλοποίησης (ευέλικτες τοπολογίες).
δ) Ευκολία υλοποίησης.

2. Στην περίπτωση που θέλετε μια γρήγορη λύση για πρόσβαση σε μία υπηρεσία ενός Linux host, όπου δεν υπάρχει εξειδικευμένος εξοπλισμός, θα επιλέγατε:
α) SSH Tunneling.
β) TLS VPN.
γ) IPsec VPN.
δ) L2F.

3. Στο IPsec, το header του IP πακέτου παραμένει αμετάβλητο:
α) στην περίπτωση του Transport Mode.
β) στην περίπτωση του Tunnel Mode.
γ) και στις δύο περιπτώσεις.
δ) σε καμία από τις δύο περιπτώσεις.

4. Στο IPsec, στην περίπτωση κατά την οποία μας ενδιαφέρει να επιβεβαιώσουμε την ταυτότητα του συναλλασσόμενου και την ακεραιότητα των δεδομένων, θα επιλέγαμε το πρωτόκολλο:
α) AH.
β) ESP.

γ) GRE.
d) OSPF.

5. Ένας δρομολογητής (router), κατά τη διακίνηση πληροφορίας
α) Δρομολογεί πακέτα (packets).
β) Προωθεί πακέτα (packets).
γ) Δρομολογεί πλαίσια (frames).
δ) Προωθεί πλαίσια (frames).

6. Η εντολή ping διακινεί πακέτα χρησιμοποιώντας το πρωτόκολλο
α) UDP.
β) TCP.
γ) ESP.
δ) IGMP.
ε) ICMP.

7. Το pre-shared κλειδί που εισάγουμε αρχικά, για τη φάση 1, θα χρησιμοποιηθεί:
α) για την πιστοποίηση του άλλου άκρου.
β) για την κρυπτογράφηση των δεδομένων.
γ) για την επιβεβαίωση των πακέτων.
δ) για όλους τους παραπάνω λόγους.

8. Ο αλγόριθμος Diffie-Hellman (DH):
α) είναι αλγόριθμος δημοσίου κλειδιού.
β) χρησιμοποιείται για την παραγωγή κλειδιών κρυπτογράφησης.
γ) χρησιμοποιείται για την κρυπτογράφηση των δεδομένων μεταξύ των δικτύων.
δ) είναι παρωχημένος (1976) και δεν χρησιμοποιείται πλέον.

9. Στην περίπτωση που θέλαμε να διασυνδέσουμε 67 κόμβους σε ένα Full Mesh Site-to-Site VPN, πόσα κλειδιά θα έπρεπε να χρησιμοποιήσουμε, με δεδομένο πως κάθε ζευγάρι κόμβων θα έπρεπε να είχε το δικό του κλειδί και χρησιμοποιείται συμμετρική κρυπτογράφηση;
α) 66
β) 67
γ) 2211
δ) 4488
ε) 4489

10. Ποιος/οι είναι ο/οι λόγος/οι που καθορίζουμε το "interesting traffic", όταν υλοποιούμε ένα IPsec tunnel;
α) Επιλέγουμε τα δεδομένα που είναι ενδιαφέροντα.
β) Μειώνουμε την ανάγκη σε επεξεργαστική ισχύ.
γ) Δεν μπορούν όλοι οι προορισμοί να αποκρυπτογραφήσουν την πληροφορία.
δ) Κανένας από τους παραπάνω.

Συγκριτική Αξιολόγηση

Συγκρίνετε τις τέσσερις υλοποιήσεις που περιεγράφηκαν στο κεφάλαιο και, μελετώντας σχετική βιβλιογραφία, εντοπίστε πλεονεκτήματα και μειονεκτήματα, και εξετάστε σε ποια περίπτωση θα προτείνατε τη χρήση κάθε μιας.

Κεφάλαιο 11. Διαχείριση Ασφάλειας

Σύνοψη
Η Ασφάλεια Πληροφοριών (Information Security) αποτελεί πλέον αντικείμενο μελέτης επιστημόνων και επαγγελματιών διαφόρων ειδικοτήτων. Επομένως, είναι απαραίτητο να οριστεί ένα πλαίσιο μέσα στο οποίο θα πραγματοποιούνται οι κατάλληλες διεργασίες ώστε να επιτυγχάνονται οι στόχοι της ασφάλειας πληροφοριών, σύμφωνα με τα όσα κάθε οργανισμός ορίζει. Συνήθως, οι διεργασίες αυτές οδηγούν στην ανάπτυξη μιας στρατηγικής ασφάλειας, η οποία περιλαμβάνει επιμέρους πολιτικές και επιπλέον εναρμονίζει τον οργανισμό με διεθνείς πρακτικές και πρότυπα. Επιπλέον, είναι απαραίτητο για την εύρυθμη λειτουργία του κάθε οργανισμού, να ορίζονται και να αξιοποιούνται μετρικές με τις οποίες μπορεί να υποστηρίζεται η ποσοτικοποίηση των μεγεθών, προκειμένου να παρέχεται με αυτόματο τρόπο η απάντηση στο βασικό ερώτημα που αφορά την επιτυχία ή την αστοχία των διεργασιών αυτών. Η διαχείριση της ασφάλειας ενσωματώνει στο αντικείμενο μελέτης της ασφάλειας πληροφοριών όλες εκείνες τις διεργασίες που πρέπει να πραγματοποιούνται ώστε να γίνεται εφικτή η απαραίτητη ποσοτικοποίηση των μεγεθών, που θα επιτρέπει κατόπιν στις διοικήσεις των οργανισμών να παίρνουν ορθές αποφάσεις και στους ειδικούς της ασφάλειας να αποτιμούν αξιόπιστα την επιτυχία ή την αποτυχία του συστήματος διαχείρισης ασφάλειας πληροφοριών που εφαρμόζουν στα πλαίσια του κάθε οργανισμού.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1).

11.1 Εισαγωγή

Το πρόβλημα της διαχείρισης της ασφάλειας πληροφοριών (information security management) αποτελεί ένα ιδιαίτερα σημαντικό ζήτημα για τα σύγχρονα πληροφοριακά συστήματα, καθώς επηρεάζει σε παγκόσμια κλίμακα το ηλεκτρονικό επιχειρείν και την ανάπτυξη εθνικών και διεθνών κρίσιμων υποδομών. Η αξιοποίηση όλο και πιο προηγμένων τεχνολογιών, όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων, τα δίκτυα και το Διαδίκτυο, προσφέρει σημαντικές δυνατότητες, αλλά αυξάνει ανάλογα και τα προβλήματα που αφορούν την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές παραμέτρους λειτουργίας (ποιότητα, απόδοση, κ.ά.), για την εξασφάλιση της εύρυθμης λειτουργίας ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα, όπου πολύ συχνά το σύνολο των παρεχόμενων υπηρεσιών ενός οργανισμού στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας). Η ικανοποίηση των απαιτήσεων για την ασφάλεια των πληροφοριών (information security) είναι, συνεπώς, μια από τις βασικές προϋποθέσεις για την αποδοτική εισαγωγή και αξιοποίηση των τεχνολογιών πληροφορίας και επικοινωνιών (ΤΠΕ).

Ως Πληροφοριακό Σύστημα εννοούμε το οργανωμένο σύνολο από ανθρώπους, λογισμικό, υλικό, διαδικασίες, εγκαταστάσεις και δεδομένα. Τα στοιχεία αυτά βρίσκονται σε μια συνεχή αλληλεπίδραση μεταξύ τους, αλλά και με το περιβάλλον, με σκοπό την παραγωγή και διαχείριση της πληροφορίας. Η πληροφορία, στο πλαίσιο ενός οργανισμού, θεωρείται αγαθό με την έννοια ότι έχει αξία. Είναι πιθανό επίσης η πληροφορία να έχει και κόστος απόκτησης.

Οι σύγχρονοι οργανισμοί εξαρτώνται από πληροφοριακά αγαθά σε ότι αφορά την αποτελεσματικότητα και τη κερδοφορία των λειτουργιών τους και για αυτό χρειάζεται να προστατεύουν αυτά τα αγαθά. Η διασφάλιση (assurance) της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών είναι σημαντική, ανεξάρτητα του κατά πόσον οι πληροφορίες αποτελούν αντικείμενο επεξεργασίας και διαχείρισης ή ανταλλάσσονται μεταξύ των συνεργαζόμενων οργανισμών. Στις μέρες μας, ο οικονομικός αλλά και εθνικός πλούτος εκφράζεται ολοένα και περισσότερο σε συνάρτηση με την πληροφορία. Η πληροφορία αποτελεί ένα σημαντικό δείκτη ανάπτυξης και επομένως είναι ανάγκη να προστατεύεται. Ακόμη, η σημασία της πληροφορίας ξεφεύγει από τα στενά οικονομικά όρια και αγγίζει το ευρύτερο κοινωνικό σύνολο. Δεν είναι λίγα τα παραδείγματα όπου η πληροφορία αποτέλεσε ένα ισχυρό όργανο κοινωνικού ελέγχου. Επομένως, υπάρχουν και κοινωνικές προεκτάσεις της απόκτησης και κατοχής πληροφορίας.

Η εμπειρία έχει δείξει ότι οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία κατά την υλοποίηση της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό:

- Η πολιτική ασφάλειας πληροφοριών, οι στόχοι και οι δραστηριότητες που αντικατοπτρίζουν τους στόχους του οργανισμού.

- Μια προσέγγιση και ένα πλαίσιο υλοποίησης, συντήρησης, επίβλεψης και βελτίωσης της ασφάλειας πληροφοριών με τρόπο συμβατό με την κουλτούρα του οργανισμού.

- Η ξεκάθαρη υποστήριξη και συμμετοχή από όλα τα επίπεδα της ιεραρχίας διοίκησης του οργανισμού.

- Μια καλή κατανόηση των απαιτήσεων ασφάλειας, με βάση τη μελέτη ανάλυσης και αποτίμησης της επικινδυνότητας.

- Η αποτελεσματική προώθηση των σκοπών της ασφάλειας πληροφοριών προς όλα τα στελέχη και τους εργαζόμενους, καθώς και τρίτα μέρη.

- Η αποκεντρωμένη καθοδήγηση σε θέματα ασφάλειας πληροφοριών και σχετικών προτύπων προς όλα τα στελέχη και τους εργαζόμενους, καθώς και τρίτα μέρη.

- Η παροχή οικονομικών πόρων για τις δραστηριότητες που αφορούν την ασφάλεια πληροφοριών.

- Η επίτευξη επαρκούς ευαισθητοποίησης και η παροχή κατάλληλης εκπαίδευσης και κατάρτισης.

- Η εφαρμογή αποτελεσματικών διαδικασιών διαχείρισης συμβάντων ασφάλειας πληροφοριών.

- Η υλοποίηση ενός συστήματος μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος διαχείρισης της ασφάλειας πληροφοριών και να προτείνει προτάσεις για βελτιώσεις.

Οι μεμονωμένες λύσεις και μηχανισμοί ασφάλειας οι οποίοι εφαρμόζονται και χρησιμοποιούνται από τους οργανισμούς, προσφέρουν λύση στο πρόβλημα της ασφάλειας αλλά μόνο σε ότι αφορά το πεδίο στο οποίο εφαρμόζονται. Για παράδειγμα, ένα ανάχωμα προστασίας (firewall) μπορεί να προσφέρει ένα πρόσθετο βαθμό ασφάλειας στη δικτυακή υποδομή ενός οργανισμού ή ένας μηχανισμός ελέγχου πρόσβασης μπορεί να προσφέρει λύση στο πρόβλημα ελέγχου πρόσβασης σε ένα επιμέρους υπολογιστικό σύστημα. Ωστόσο, μια τέτοια πρακτική από μόνη της δεν προσφέρει συνήθως τη δυνατότητα αντιμετώπισης του προβλήματος της ασφάλειας πληροφοριών στην ολότητά του. Για το λόγο αυτό, είναι επιτακτική ανάγκη για τον ορισμό ενός πλαισίου, στη βάση του οποίου να αντιμετωπίζουμε με μια ολιστική προσέγγιση το πρόβλημα της ασφάλειας πληροφοριών. Συγκεκριμένα, ο πρώτος άξονας ενός τέτοιου πλαισίου θα μπορούσε να αφορά στο υπό εξέταση πληροφοριακό σύστημα (π.χ., δημόσιας διοίκησης, επιχειρησιακό πληροφοριακό σύστημα, κλπ.) και ο δεύτερος άξονας αφορά στις δράσεις οι οποίες πρέπει να πραγματοποιούνται. Στις δράσεις αυτές συμπεριλαμβάνονται θεσμικές ρυθμίσεις, οργανωσιακές ρυθμίσεις αλλά και κοινωνικές δράσεις.

Οι θεσμικές ρυθμίσεις κατηγοριοποιούνται σε κανονιστικές και νομικές. Ένα παράδειγμα κανονιστικής ρύθμισης αποτελούν τα πρότυπα (standards). Κανονιστική ρύθμιση αποτελούν επίσης και οι κώδικες δεοντολογίας οι οποίοι συμπληρώνουν την υπάρχουσα νομοθεσία. Μια διαφορετική κατηγοριοποίηση των θεσμικών ρυθμίσεων μπορεί να γίνεται σύμφωνα με το γεωγραφικό πεδίο εφαρμογής τους. Σε μια τέτοια περίπτωση, έχουμε διεθνείς, περιφερειακές, εθνικές και τοπικές θεσμικές ρυθμίσεις. Τέλος, οι θεσμικές ρυθμίσεις μπορούν να κατηγοριοποιούνται και σύμφωνα με το τομεακό πεδίο εφαρμογής τους. Αν μία θεσμική ρύθμιση εφαρμόζεται σε παραπάνω από έναν τομέα (π.χ. υγεία, οικονομία κλπ.) τότε μιλάμε για μια οριζόντια θεσμική ρύθμιση. Αν η θεσμική ρύθμιση αφορά μόνον ένα τομέα, μιλάμε για μια κάθετη θεσμική ρύθμιση.

Οι οργανωσιακές ρυθμίσεις αφορούν εκείνα τα μέτρα οργάνωσης που κάθε επιχείρηση ή οργανισμός παίρνει προκειμένου να διασφαλίζει την ασφάλεια των πληροφοριών που διαχειρίζεται. Για παράδειγμα, μια στρατηγική και οι σχετικές πολιτικές, είναι ένα παράδειγμα οργανωσιακής ρύθμισης.

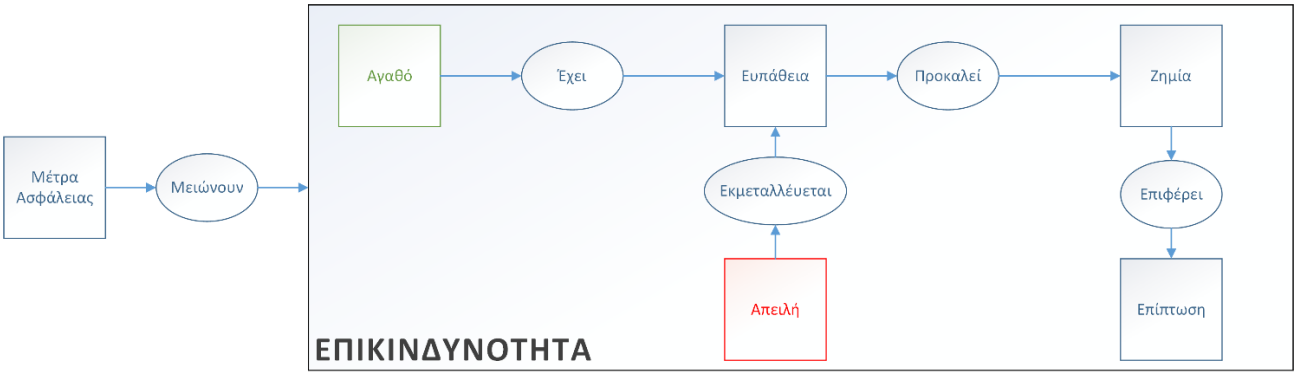
Ένα πρότυπο, όπως για παράδειγμα ένα τεχνικό πρότυπο (technical standard), είναι ένα σύνολο αποδεκτών κριτηρίων, μεθόδων και διεργασιών ή πρακτικών. Τα πρότυπα μπορεί να προκύπτουν από ενώσεις εταιρειών ή οργανισμών προτυποποίησης κατόπιν έρευνας και ευρύτερης συμφωνίας, οπότε τα de jure πρότυπα. Υπάρχουν όμως περιπτώσεις δημιουργίας προτύπων τα οποία απολαμβάνουν ευρείας αποδοχής, χωρίς να αποτελούν μέρος ενός τυπικού κανονιστικού πλαισίου. Κανείς δεν έχει τη νομική ή κανονιστική υποχρέωση να ακολουθήσει αυτά τα πρότυπα, τα οποία είναι γνωστά ως de facto πρότυπα, ενώ θεωρούνται ότι αποτελούν τα ισχυρότερα πρότυπα, καθώς επικράτησαν μετά από ανταγωνισμό στην πράξη.

Η διεργασία ανάπτυξης και υλοποίησης τεχνικών προτύπων ονομάζεται Προτυποποίηση. Συνεπώς, για να εξασφαλιστεί η συμμόρφωση ενός οργανισμού με συγκεκριμένες προδιαγραφές θα πρέπει να αυτός να αξιολογείται με σκοπό την απόκτηση του αντίστοιχου πιστοποιητικού συμμόρφωσης (πιστοποίηση). Η πιστοποίηση ορίζει τις διαδικασίες αξιολόγησης και ελέγχου ενός οργανισμού. Από τα πλέον διαδεδομένα πρότυπα ασφάλειας πληροφοριών είναι η σειρά προτύπων ISO/IEC 27000, καθώς και τα Common Criteria. Η εναρμόνιση ενός οργανισμού με κάποιο πρότυπο εξασφαλίζει την ύπαρξη συγκεκριμένων επιθυμητών χαρακτηριστικών σε προϊόντα ή υπηρεσίες. Επίσης, εξασφαλίζεται η συμβατότητα και η διαλειτουργικότητα μεταξύ διαφορετικών πληροφοριακών συστημάτων.

11.2 Εννοιολογική Θεμελίωση

Είναι αναγκαία η ύπαρξη ενός κοινού λεξιλογίου, αυστηρά καθορισμένου, έτσι ώστε να μπορέσουν δύο μέρη να επικοινωνήσουν αποτελεσματικά. Στο χώρο της Ασφάλειας Πληροφοριών, η ανάγκη αυτή είναι ακόμη επιτακτικότερη, καθώς τα μέρη τα οποία έρχονται σε επικοινωνία μπορεί να ανήκουν σε διαφορετικούς τομείς (π.χ. Πληροφορική, Οικονομικά, Διοίκηση κ.λπ.), ενώ λειτουργούν μέσα στον ίδιο οργανισμό για τον κοινό σκοπό. Έτσι, οι βασικές έννοιες που αφορούν στην Ασφάλεια Πληροφοριών (και κατ' επέκταση τη Διαχείριση της Ασφάλειας) θα πρέπει να είναι ξεκάθαρες για κάθε συμμετέχοντα στη διαδικασία λήψης αποφάσεων που αφορούν τον οργανισμό. Για το λόγο αυτό, είναι χρήσιμο να επαναλάβουμε ορισμένες βασικές έννοιες που παρουσιάσθηκαν στο πρώτο κεφάλαιο, μέσα από ένα διαφορετικό πρίσμα.

Στην παρακάτω Εικόνα 11.1, εμφανίζονται οι συσχετίσεις μεταξύ των όρων ασφάλειας πληροφοριών, οι οποίοι θα μας απασχολήσουν στη συνέχεια.



Εικόνα 11.1 *Συσχετίσεις μεταξύ όρων ασφάλειας πληροφοριών.*

Ένα αγαθό, όπως εμφανίζεται στην παραπάνω Εικόνα 11.1, έχει αξία για ένα οργανισμό και πρέπει να προστατευτεί. Αυτό είναι ιδιαίτερα σημαντικό στο διαρκώς διασυνδεόμενο επιχειρηματικό περιβάλλον, όπου οι πληροφορίες εκτίθενται σε ένα ολοένα αυξανόμενο αριθμό και με μια διερευνώμενη ποικιλία απειλών.

Η πληροφορία (ως αγαθό) μπορεί να εμφανιστεί υπό διάφορες μορφές. Μπορεί να γραφεί σε χαρτί, να αποθηκευτεί και να μεταδοθεί ηλεκτρονικά ή να αναφερθεί σε κάποια συζήτηση. Ασχέτως της μορφής ή του τρόπου αποθήκευσής της, η πληροφορία θα πρέπει πάντοτε να είναι επαρκώς προστατευμένη. Στο πλαίσιο της ασφάλειας πληροφοριών, επιδιώκεται η προστασία των πληροφοριών από μια ευρεία γκάμα απειλών, ώστε να

διασφαλιστεί η επιχειρησιακή συνέχεια, να ελαχιστοποιηθεί η συνολική εναπομείνασα επικινδυνότητα και να μεγιστοποιηθούν οι αποδόσεις των επενδύσεων και οι επιχειρησιακές ευκαιρίες.

Η μείωση της συνολικής επικινδυνότητας επιτυγχάνεται με την υλοποίηση ενός κατάλληλου συνόλου (αντι)μέτρων (controls), που περιλαμβάνουν πολιτικές, πρακτικές, διαδικασίες, τεχνικές και λειτουργίες λογισμικού και υλικού. Αυτά τα μέτρα είναι απαραίτητα προκειμένου να διασφαλιστεί ότι επιτυγχάνονται οι επιμέρους στόχοι του οργανισμού που αφορούν την ασφάλεια πληροφοριών, σε συνδυασμό με άλλες πρακτικές διαχείρισης.

Η αξία ενός αγαθού αφορά τη σημαντικότητά του για την επίτευξη των στόχων του οργανισμού και εκφράζεται είτε με χρηματικούς ή άλλους όρους. Ένα υπολογιστικό σύστημα είναι δυνατό να παρουσιάζει ευπάθειες, δηλαδή αδυναμίες τις οποίες μπορεί να εκμεταλλευτεί μια απειλή (στο πλαίσιο μια επίθεσης) και να προκαλέσει ζημία. Η απειλή μπορεί να είναι φυσική, τεχνικής φύσης, ή ανθρώπινη, εκούσια ή ακούσια. Επίσης, μια απειλή μπορεί να είναι σκόπιμη ή τυχαία. Ως ζημία, θεωρούμε την επίπτωση που προκαλεί η μείωση της αξίας του αγαθού. Η επίπτωση αποτυπώνεται ως μια αλλαγή στο δυνητικό βαθμό επίτευξης των επιχειρησιακών στόχων του οργανισμού.

Τα πέντε αυτά στοιχεία (αγαθό, ευπάθεια, ζημία, απειλή και επίπτωση) ορίζουν την έννοια της επικινδυνότητας (risk). Με βάση την κατάλληλη αποτίμηση της επικινδυνότητας θα πρέπει να γίνεται επιλογή των κατάλληλων μέτρων προστασίας, που θα μετριάζουν την επικινδυνότητα.

Ο σχεδιασμός, η υλοποίηση, η συντήρηση και η βελτίωση της ασφάλειας πληροφοριών αποτελούν ουσιαστικούς παράγοντες για την επίτευξη ανταγωνιστικών χαρακτηριστικών, κερδοφορίας, επαρκούς συμμόρφωσης με τους νόμους και διαμόρφωσης κατάλληλης φήμης. Όμως, στον αρχικό σχεδιασμό των πληροφοριακών συστημάτων συνήθως δεν συμπεριλαμβάνονται εξ αρχής τα απαραίτητα χαρακτηριστικά ασφάλειας, με αποτέλεσμα το παρεχόμενο επίπεδο ασφάλειας να είναι ανεπαρκές και να χρειάζεται μια κατάλληλη διαχείριση και υλοποίηση επιμέρους διαδικασιών. Η επιλογή των κατάλληλων μέτρων ελέγχου, προϋποθέτει προσεκτικό και λεπτομερή σχεδιασμό, ενώ η ασφάλεια των πληροφοριών γενικότερα απαιτεί τη συμμετοχή όλων των εργαζομένων του οργανισμού. Επιπλέον, μπορεί να χρειάζεται και η συμμετοχή των προμηθευτών, των πελατών ή ακόμη και η συνδρομή εξωτερικών συνεργατών, εξειδικευμένων σε θέματα ασφάλειας. Συνολικά, η Διαχείριση Ασφάλειας αποσκοπεί στη διαμόρφωση ενός οργανωμένου πλαισίου εννοιών, αρχών, πολιτικών, διαδικασιών και τεχνικών μέτρων που απαιτούνται προκειμένου να προστατευθούν τα αγαθά από σκόπιμες ή τυχαίες απειλές.

11.3 Συστήματα Διαχείρισης Ασφάλειας Πληροφοριών

Ορισμένοι βασικοί παράγοντες, στη βάση των οποίων ένας οργανισμός μπορεί να ορίζει το επιθυμητό επίπεδο ασφάλειας είναι οι εξής:

- Αποδεκτό επίπεδο ασφάλειας.
- Λειτουργικότητα του Πληροφοριακού Συστήματος που διαθέτει.
- Κόστος που επιθυμεί να επωμισθεί.

Ο σχεδιασμός της ασφάλειας πληροφοριών ενός οργανισμού είναι μια επιχειρησιακή διεργασία, η οποία αποσκοπεί στο να παρέχονται τα κατάλληλα εργαλεία λήψης αποφάσεων, προκειμένου να μπορεί η διοίκηση να ασκήσει αποτελεσματικά το ρόλο της. Υπό αυτή την έννοια, η ασφάλεια πληροφοριών δεν είναι ένα αμιγώς τεχνικό θέμα, αλλά συμπεριλαμβάνει ζητήματα και παραμέτρους από διάφορους χώρους (οικονομία, διοίκηση, κοινωνία κ.λπ.). Για να επιτευχθεί ένας αποδοτικός συντονισμός των ενεργειών προς αυτή τη κατεύθυνση, θα πρέπει να οριστούν οι στόχοι της ασφάλειας πληροφοριών, καθώς και οι διαδικασίες των οποίων η εξέλιξη αλλά και τα αποτελέσματα θα ελέγχονται διαρκώς, χρησιμοποιώντας ένα κατάλληλο σύστημα διαχείρισης της ασφάλειας. Επιπλέον, οι απαιτήσεις ασφάλειας θα πρέπει να προσδιορίζονται στη βάση μιας περιοδικά επαναλαμβανόμενης μελέτης για την ανάλυση και διαχείριση της επικινδυνότητας (Risk Management).

Ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System – ISMS) επικεντρώνεται κυρίως στις διαδικασίες που λαμβάνουν χώρα στο πλαίσιο ενός οργανισμού. Για τη διαχείριση της Ασφάλειας Πληροφοριών υπάρχουν αρκετές διαφορετικές μεθοδολογίες οι οποίες

χρησιμοποιούν ή στηρίζονται αποκλειστικά σε κάποιο από τα πολλά και διαφορετικά πρότυπα που έχουν αναπτυχθεί. Μερικές από τις γνωστότερες είναι οι παρακάτω:

- OCTAVE από τον οργανισμό CERT (Carnegie Mellon University).
- COBIT από τον οργανισμό ISACA. Βασίζεται στον κύκλο: **Govern → Direct → Control → Implement → Measure → Evaluate → Report**
- FIRM από το Information Security Forum
- Μεθοδολογία του οργανισμού NIST. Βασίζεται στον κύκλο: **System Characterization → Threat Identification → Vulnerability Identification → Control Analysis → Likelihood Determination → Impact Analysis → Risk Determination → Control Recommendations → Results Documentation**

Μια ιδιαίτερα διαδεδομένη μέθοδος για τον έλεγχο και τη βελτίωση αυτών των διαδικασιών κατά την ανάπτυξη ενός Συστήματος Διαχείρισης της Ασφάλειας Πληροφοριών (π.χ. σύμφωνα με το πρότυπο ISO/IEC 27001) είναι η μέθοδος Plan-Do-Check-Act (PDCA).

Η μέθοδος PDCA αποτελείται από τέσσερα επαναληπτικά βήματα ως εξής:

- **Σχεδιασμός (Plan):** Στο βήμα αυτό αναλύεται και μελετάται η ασφάλεια πληροφοριών στον οργανισμό, θέτονται οι στόχοι και ορίζονται οι τρόποι με τους οποίους θα επιτευχθούν οι στόχοι.
- **Υλοποίηση (Do)**: Εδώ υλοποιούνται τα μέτρα τα οποία ορίστηκαν κατά τη φάση του σχεδιασμού.
- **Έλεγχος (Check):** Πραγματοποιείται έλεγχος απόκλισης των αρχικών στόχων και των τελικών αποτελεσμάτων.
- **Δράση (Act):** Εφαρμόζονται ενέργειες διόρθωσης και βελτίωσης των μέτρων.

Μπορούμε να φανταστούμε το Σύστημα Διαχείρισης της Ασφάλειας Πληροφοριών ως μία ενιαία διεργασία η οποία δέχεται ως είσοδο τις απαιτήσεις ασφάλειας του οργανισμού και παρέχει ως έξοδο τη διαχείριση της ασφάλειας πληροφοριών.

Κατά τη φάση του σχεδιασμού, πραγματοποιείται ανάλυση και εκτίμηση της επικινδυνότητας για την ασφάλεια των πληροφοριών. Πιο συγκεκριμένα, διαμορφώνονται και πραγματοποιούνται μεταξύ άλλων τα εξής:

- Έγκριση από τη Διοίκηση του οργανισμού.
- Καθορισμός του πεδίου εφαρμογής (υπολογιστικά συστήματα, δεδομένα κλπ.).
- Μελέτη Ανάλυσης και Αποτίμησης Επικινδυνότητας.
- Καθορισμός απαιτήσεων ασφάλειας.
- Δημιουργία Πολιτικής Ασφάλειας.

Αξίζει εδώ να επισημανθεί ότι είναι πρωταρχικής σημασίας για έναν οργανισμό ο καθορισμός των απαιτήσεών του σε θέματα ασφάλειας. Μερικές βασικές πηγές άντλησης πληροφοριών για απαιτήσεις ασφάλειας είναι ο εξής:

- Η αποτίμηση της επικινδυνότητας (risk assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας, αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον, εκτιμάται η συνολική ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποιήσεών τους, καθώς και το κόστος που θα έχουν οι επιπτώσεις για τον οργανισμό από πιθανές επιθέσεις.

- Το νομικό και κανονιστικό πλαίσιο, καθώς και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.

- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες για τη λειτουργία του.

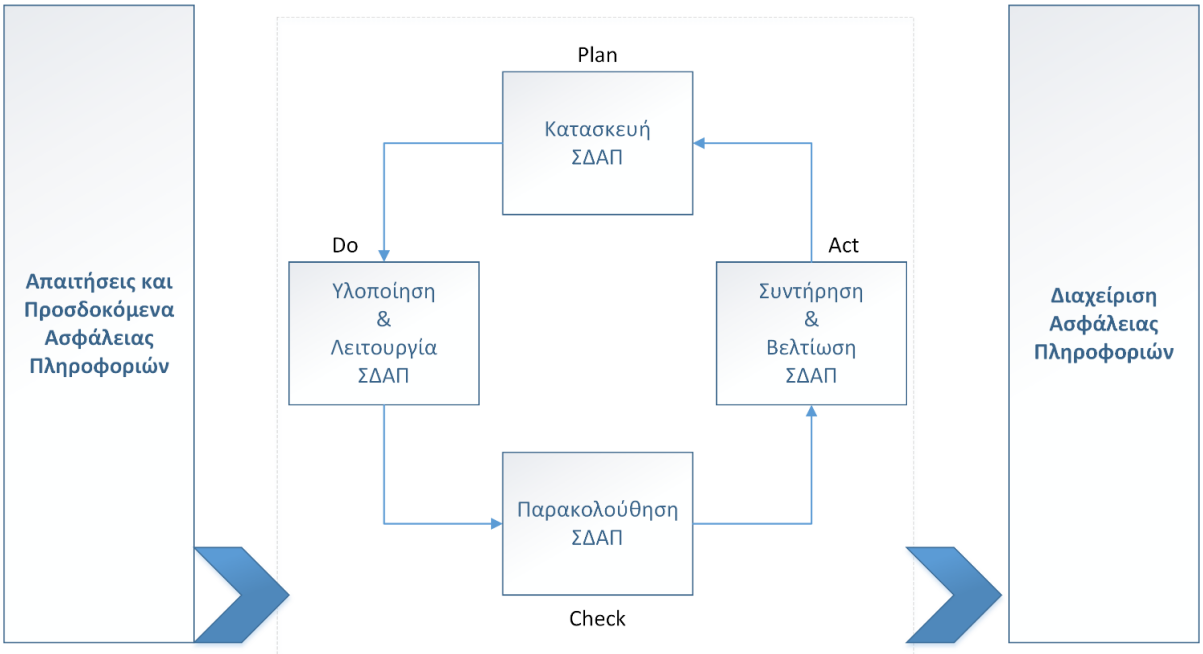
Στη φάση της υλοποίησης και με βάση τα αποτελέσματα της αποτίμησης, ακολουθεί νέα μελέτη που αποσκοπεί στη μείωση της επικινδυνότητας με την επιλογή και υλοποίηση των κατάλληλων μέτρων προστασίας. Αναλυτικότερα, διαμορφώνονται και υλοποιούνται μεταξύ άλλων τα εξής:

- Σχέδιο Διαχείρισης Επικινδυνότητας.
- Κατανομή ρόλων και αρμοδιοτήτων.
- Υλοποίηση μέτρων ασφάλειας.
- Δράσεις ενημέρωσης και κατάρτισης του προσωπικού.
- Υλοποίηση διαδικασιών έγκαιρης ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας.

Κατά τον έλεγχο, πραγματοποιείται μια αξιολόγηση των αποτελεσμάτων σε σχέση με τους αρχικούς στόχους που είχαν τεθεί και διαμορφώνεται μια αναφορά αξιολόγησης προς τη διοίκηση του οργανισμού. Η διαδικασία του ελέγχου είναι επαναληπτική και πραγματοποιείται ανά τακτά χρονικά διαστήματα, συνήθως από το αρμόδιο τμήμα εσωτερικού ελέγχου του οργανισμού.

Τέλος, στο στάδιο της δράσης εκτελούνται όλες εκείνες οι απαραίτητες ενέργειες, οι οποίες κρίθηκε ότι απαιτούνται προκειμένου να βελτιωθεί η συνολική διεργασία της διαχείρισης της ασφάλειας πληροφοριών. Πραγματοποιείται ενημέρωση της διοίκησης και παράλληλα ελέγχεται και αξιολογείται και η ίδια η διαδικασία βελτίωσης των μέτρων προστασίας.

Το πρότυπο ISO/IEC 27001, συνδυάζοντας τα τέσσερα (4) βήματα της μεθοδολογίας PDCA, ορίζει το πλαίσιο της Διαχείρισης Ασφάλειας Πληροφοριών, όπως φαίνεται στην παρακάτω Εικόνα 11.2.



Εικόνα 11.2 *Διαχείριση Ασφάλειας Πληροφοριών κατά ISO/IEC 27001.*

Το πρότυπο BS 7799-1 του Βρετανικού οργανισμού προτυποποίησης υποβλήθηκε στον οργανισμό ISO/IEC και έγινε αποδεκτό το 2000. Το έτος 2002 μετονομάστηκε σε ISO/IEC 27002 ενώ το 2005 το βρετανικό πρότυπο BS 7799-2 έγινε δεκτό και μετονομάστηκε σε ISO/IEC 27001.

Η σειρά προτύπων ISO 27K είναι ένας οδηγός βέλτιστων πρακτικών για τη διαχείριση της ασφάλειας πληροφοριών και τη διαχείριση της σχετικής επικινδυνότητας που αντιμετωπίζει ένας οργανισμός. Προτείνει μέτρα ασφάλειας, ενώ μέχρι σήμερα η οικογένεια αριθμεί 23 μέλη. Το κεντρικό πρότυπο είναι το ISO/IEC 27001 με το οποίο μπορεί ένας οργανισμός να εναρμονιστεί και να λάβει πιστοποίηση από τρίτο ανεξάρτητο φορέα. Ο φορέας πιστοποίησης με τη σειρά του μπορεί να λάβει διαπίστευση, σύμφωνα με το πρότυπο ISO/IEC 27006.

Στον ακόλουθο πίνακα παρουσιάζεται μια σύντομη περιγραφή των προτύπων της οικογένειας ISO 27000:

Όνομα	**Αντικείμενο**
ISO/IEC 27000	Εισαγωγή και λεξιλόγιο όρων
ISO/IEC 27001	Απαιτήσεις υλοποίησης και συντήρησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27002	Πρακτικές διαχείρισης της ασφάλειας και επιλογής μέτρων ασφάλειας
ISO/IEC 27003	Οδηγίες σχεδιασμού ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27004	Μετρικές εκτίμησης της αποτελεσματικότητας υλοποιημένου Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27005	Οδηγίες διαχείρισης Επικινδυνότητας
ISO/IEC 27006	Οδηγίες ελέγχου και πιστοποίησης Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27007	Οδηγίες ικανοτήτων ελεγκτών Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
ISO/IEC 27008	Οδηγίες ελέγχου της υλοποίησης Συστήματος Διαχείρισης Ασφάλειας και Πληροφοριών
ISO/IEC 27010	Οδηγίες για κοινότητες ανταλλαγής πληροφοριών
ISO/IEC 27011	Οδηγίες για τηλεπικοινωνιακούς οργανισμούς
ISO/IEC 27013	Οδηγίες υλοποίησης ISO/IEC 27001 και ISO/IEC 20000-1
ISO/IEC 27014	Έννοιες και αρχές διακυβέρνησης της ασφάλειας
ISO/IEC 27015	Οδηγίες για οργανισμούς παροχής χρηματοοικονομικών υπηρεσιών
ISO/IEC 27016	Οικονομικές επιπτώσεις αποφάσεων σχετικών με Διαχείριση Ασφάλειας Πληροφοριών
ISO/IEC 27018	Οδηγίες προστασίας Προσωπικά Αναγνωρίσιμων Πληροφοριών
ISO/IEC 27019	Οδηγίες για παρόχους Ηλεκτρικής Ενέργειας
ISO/IEC 27031	Περιγραφή εννοιών και αρχών επιχειρησιακής συνέχειας των Πληροφοριακών υποδομών
ISO/IEC 27032	Οδηγίες βελτίωσης της Κυβερνοασφάλειας
ISO/IEC 27033	Οδηγίες ασφάλειας δικτύων
ISO/IEC 27034	Οδηγίες ενσωμάτωσης των μηχανισμών ασφάλειας στις επιχειρησιακές διεργασίες
ISO/IEC 27035	Οδηγίες ανίχνευσης και αντιμετώπισης περιστατικών ασφάλειας
ISO/IEC 27036	Οδηγίες για παρόχους υπηρεσιών cloud computing
ISO/IEC 27037	Οδηγίες διαχείρισης ψηφιακών τεκμηρίων
ISO/IEC 27038	Οδηγίες επιμέλειας ψηφιακών εγγράφων
ISO/IEC 27789	Οδηγίες για συστήματα Ηλεκτρονικού Φακέλου Υγείας
ISO/IEC 27790	Οδηγίες μετάδοσης, αποθήκευσης και αξιοποίησης ψηφιακών εγγράφων για οργανισμούς υγείας
ISO/IEC 27799	Οδηγίες υλοποίησης του ISO/IEC 27002 σε οργανισμούς υγείας

Πίνακας 11.1 *Πρότυπα ασφάλειας της οικογένειας ISO 27k.*

11.4 Ανάλυση, Αποτίμηση και Διαχείριση Επικινδυνότητας

Είδαμε σε προηγούμενη ενότητα ότι κατά τη διεργασία της Διαχείρισης Ασφάλειας Πληροφοριών είναι απαραίτητη η εκπόνηση μελέτης ανάλυσης και αποτίμησης επικινδυνότητας. Μια τέτοια μελέτη είναι απαραίτητη, καθώς θα μας δώσει απαντήσεις σε ερωτήματα όπως:

- Ποια αγαθά του ΠΣ μας πρέπει να προστατέψουμε;
- Τι απειλές υπάρχουν για τα αγαθά αυτά;
- Τι μέτρα προστασίας πρέπει να χρησιμοποιηθούν;

Ένας άλλος κύριος λόγος για τον οποίο είναι απαραίτητη η μελέτη ανάλυσης και αποτίμησης επικινδυνότητας είναι γιατί με αυτό τον τρόπο μπορούμε να ποσοτικοποιήσουμε το επίπεδο ασφάλειας που

επιθυμούμε καθώς και να «μετρήσουμε» το βαθμό επίτευξης του στόχου της μείωσης επικινδυνότητας σε αποδεκτά επίπεδα. Από τη μια, οι απαιτήσεις ασφάλειας του οργανισμού προκύπτουν μετά από μια μεθοδική αποτίμηση της επικινδυνότητας που αντιμετωπίζει ο οργανισμός. Από την άλλη, το κόστος των μέτρων προστασίας θα πρέπει να εξισορροπείται από την πιθανή ζημιά στον οργανισμό σε περίπτωση που παραβιασθεί η ασφάλεια του πληροφοριακού συστήματός του. Τα αποτελέσματα της αποτίμησης επικινδυνότητας θα βοηθή0σουν στην καθοδήγηση και στη λήψη αποφάσεων για καθορισμό κατάλληλων διοικητικών ενεργειών και τον καθορισμό προτεραιοτήτων στην κατεύθυνση της διαχείρισης της ασφάλειας των πληροφοριών.

Η μελέτη ανάλυσης και αποτίμησης επικινδυνότητας είναι μια συστηματική διαδικασία και θα πρέπει να επαναλαμβάνεται σε περιοδική βάση προκειμένου να συμπεριλαμβάνονται οι οποιεσδήποτε αλλαγές στη λειτουργία του οργανισμού που πιθανώς να επηρεάζουν τα αποτελέσματα της μελέτης. Είναι απαραίτητος ο περιοδικός έλεγχος της επικινδυνότητας, όπως και της σωστής εφαρμογής των μέτρων προστασίας, προκειμένου αυτά να προσαρμόζονται στις ανάγκες και τις προτεραιότητες του οργανισμού, να επεκτείνονται για την προστασία από νέες απειλές και να επιβεβαιώνουν την ορθή και αποτελεσματική λειτουργία των υπαρχόντων μέτρων προστασίας.

Από τη στιγμή που θα καθοριστούν οι απαιτήσεις και οι απειλές ασφάλειας και θα έχουν παρθεί οι αποφάσεις για την αντιμετώπιση των απειλών, μπορεί να γίνει η επιλογή των κατάλληλων μέτρων προστασίας, τα οποία θα μειώσουν την επικινδυνότητα σε αποδεκτά επίπεδα. Τα μέτρα αυτά μπορούν να επιλεγούν από οποιοδήποτε σύνολο (π.χ. προτεινόμενο από κάποιο πρότυπο) μέτρων προστασίας είναι κατάλληλο για τον οργανισμό. Τα μέτρα θα πρέπει να επιλεγούν με κριτήριο το κόστος υλοποίησής τους σε σχέση με τις απειλές που καλούνται να αντιμετωπίσουν και το κόστος των πιθανών επιπτώσεων από πιθανές επιθέσεις στον οργανισμό. Επίσης, θα πρέπει να συμπεριληφθούν και ποιοτικοί παράγοντες, όπως η απώλεια φήμης για τον οργανισμό. Τέλος, τα μέτρα προστασίας θα πρέπει να είναι σύμφωνα με την εθνική και διεθνή νομολογία και τους κανονισμούς.

Υπάρχουν ορισμένα μέτρα προστασίας που θεωρούνται θεμελιώδη και αποτελούν τη βάση για την ασφάλεια πληροφοριών. Βασίζονται είτε σε υποχρεωτικές νομικές διατάξεις, είτε έχουν καθιερωθεί ως κοινή πρακτική στην ασφάλεια. Τέτοια μέτρα προστασίας μπορούν να αφορούν π.χ. την προστασία του προσωπικού απορρήτου, τη διαφύλαξη της ασφάλειας των δεδομένων του οργανισμού, την προστασία της πνευματικής ιδιοκτησίας, κ.ά.

Ορισμένα μέτρα προστασίας, πέρα από τα καθαρά τεχνικά, που θεωρούνται ότι αποτελούν κοινή πρακτική για την ασφάλεια πληροφοριών είναι:

- Το έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Ο επιμερισμός καθηκόντων σχετικών με την ασφάλεια πληροφοριών.
- Η ευαισθητοποίηση, η εκπαίδευση και η κατάρτιση σε θέματα ασφάλειας πληροφοριών.
- Η σωστή λειτουργία των εφαρμογών.
- Η διαχείριση των ευπαθειών.
- Η διαχείριση της επιχειρησιακής συνέχειας.
- Η διαχείριση των συμβάντων ασφάλειας και των συναφών βελτιώσεων που αφορούν την ασφάλεια πληροφοριών του οργανισμού.

Τα παραπάνω μέτρα μπορούν να χρησιμοποιηθούν σχεδόν σε κάθε οργανισμό. Ωστόσο, αν και αποτελούν βασικά βήματα εκκίνησης για την ασφάλεια πληροφοριών, δεν πρέπει σε καμιά περίπτωση να υποκαταστήσουν τη διενέργεια της μελέτης ανάλυσης και αποτίμησης επικινδυνότητας και της προσεκτικής υλοποίησης των αποτελεσμάτων της.

Η έννοια της επικινδυνότητας έχει τις ρίζες της στην Οικονομική επιστήμη, όπου στόχος είναι η μείωσή της στις επιχειρηματικές επενδύσεις. Στην επιστήμη της Πληροφορικής και ειδικότερα στο πεδίο της Ασφάλειας Πληροφοριών, η επικινδυνότητα (R) εκφράζεται ως το γινόμενο της πιθανότητας (P) να συμβεί μια παραβίαση ασφάλειας επί το κόστος (C) της ζημίας που θα προκύψει από την παραβίαση. Σύμφωνα με το

πρότυπο ISO/IEC 27005, επικινδυνότητα είναι «η επίδραση της αβεβαιότητας στους στόχους». Άρα, η επικινδυνότητα μπορεί να είναι ένα μέγεθος το οποίο μετριέται χρησιμοποιώντας τη θεωρία πιθανοτήτων (π.χ. κατά Bayes, όπου για ένα γεγονός μπορούμε να μετρήσουμε την πιθανότητα πραγματοποίησης του αν αναλύσουμε τους επιμέρους παράγοντες που το επηρεάζουν). Πιο συγκεκριμένα, η πιθανότητα να συμβεί ένα περιστατικό είναι συνάρτηση της πιθανότητας να εμφανιστεί μια απειλή και της πιθανότητας αυτή η απειλή να μπορέσει να εκμεταλλευτεί μια σχετική ευπάθεια του συστήματος.

Η ανάλυση και αποτίμηση επικινδυνότητας είναι απαραίτητο προαπαιτούμενο της διαχείρισης επικινδυνότητας. Με τη διαχείριση επικινδυνότητας στη συνέχεια επιδιώκεται:

- η μείωσή της, εφαρμόζοντας μέτρα προστασίας,
- η μεταφορά της προσλαμβάνοντας τρίτο οργανισμό π.χ. ασφαλιστικό,
- η με κάποιο τρόπο αποφυγή της,
- η αποδοχή της.

Η ανάλυση και εκτίμηση επικινδυνότητας αποτελούν τα αρχικά βήματα σε μια μεθοδολογία διαχείρισης της επικινδυνότητας. Οι οργανισμοί χρησιμοποιούν την ανάλυση και εκτίμηση επικινδυνότητας για να καθορίσουν την έκταση των πιθανών απειλών και τον κίνδυνο που σχετίζεται με ένα πληροφοριακό σύστημα. Για να μπορούμε να καθορίσουμε την πιθανότητα ενός μελλοντικού κακόβουλου γεγονότος, θα πρέπει να αναλύονται οι απειλές για ένα πληροφοριακό σύστημα σε συσχετισμό με την πιθανότητα εκμετάλλευσης ευπαθειών στο πληροφοριακό σύστημα. Η επίπτωση αναφέρεται στο μέγεθος της ζημιάς που θα μπορούσε να προκληθεί από την υλοποίηση (μέσω μιας επίθεσης) μιας απειλής, ως αποτέλεσμα της εκμετάλλευσης μιας ή περισσότερων ευπαθειών του συστήματος.

Το σχετικό πλαίσιο του οργανισμού NIST εμπεριέχει εννέα πρωτεύοντα στάδια:

- Χαρακτηρισμός Συστήματος.
- Αναγνώριση Απειλής.
- Αναγνώριση Ευπάθειας.
- Ανάλυση Μηχανισμών Ασφάλειας.
- Προσδιορισμός Πιθανότητας.
- Ανάλυση Επίπτωσης.
- Προσδιορισμός Επικινδυνότητας.
- Προτάσεις μηχανισμών Ελέγχου.
- Τεκμηρίωση Αποτελεσμάτων.

11.4.1 Χαρακτηρισμός συστήματος

Σε αυτό το βήμα, αναγνωρίζονται τα λογικά όρια του πληροφοριακού συστήματος. Οι πληροφορίες που συλλέγονται για το πληροφοριακό σύστημα αφορούν υλικό, λογισμικό, δικτυακές συνδέσεις, τα πρόσωπα που υποστηρίζουν και χρησιμοποιούν το πληροφοριακό σύστημα, την αποστολή του συστήματος καθώς και την ευαισθησία των δεδομένων του. Επίσης, συλλέγονται πληροφορίες σχετικά με τις λειτουργικές απαιτήσεις του πληροφοριακού συστήματος, τους χρήστες του, τις πολιτικές ασφαλείας, την αρχιτεκτονική του συστήματος ασφαλείας, την τρέχουσα τοπολογία δικτύου, τους διοικητικούς ελέγχους, τις ροές των πληροφοριών, τους τεχνικούς και λειτουργικούς ελέγχους, καθώς και το φυσικό περιβάλλον του πληροφοριακού συστήματος.

Για τη συλλογή των πληροφοριών χρησιμοποιούνται διάφορα εργαλεία όπως:

- Ερωτηματολόγιο, που θα πρέπει να διανέμεται στο προσωπικό που λειτουργεί ή υποστηρίζει το πληροφοριακό σύστημα. Το ερωτηματολόγιο θα μπορούσε επίσης να χρησιμοποιηθεί κατά τη διάρκεια συνεντεύξεων.

- Συνέντευξη με το διοικητικό προσωπικό.

- Εταιρικά έγγραφα, τα οποία περιγράφουν λεπτομερώς εσωτερικές διαδικασίες.

- Αυτοματοποιημένα εργαλεία συλλογής πληροφοριών.

11.4.2 Αναγνώριση απειλών

Ο σκοπός αυτού του βήματος είναι να αναγνωρίσει τις πιθανές απειλές που μπορεί να προκαλέσουν ρήγμα ασφάλειας στο πληροφοριακό μας σύστημα. Η κατηγοριοποίηση των απειλών σε φυσικές, ανθρώπινες και σκόπιμες ή τυχαίες μας βοηθάει να αντιληφθούμε το βαθμό σοβαρότητας ή το ενδεχόμενο εμφάνισης της απειλής.

11.4.3 Αναγνώριση ευπαθειών

Ο στόχος αυτού του βήματος είναι να καταγράψει μια λίστα από ευπάθειες του πληροφοριακού συστήματος, που θα μπορούσαν να γίνουν αντικείμενο εκμετάλλευσης από ενδεχόμενες απειλές. Η μεθοδολογία που θα ακολουθηθεί συνήθως ποικίλει και εξαρτάται από την φύση και κατάσταση του πληροφοριακού συστήματος. Αν το πληροφοριακό σύστημα δεν έχει σχεδιαστεί ακόμη, η αναζήτηση ευπαθειών θα πρέπει να επικεντρωθεί στις πολιτικές ασφάλειας του οργανισμού, στις σχεδιασμένες διαδικασίες ασφαλείας, καθώς και τις απαιτήσεις του συστήματος. Αν το σύστημα είναι ήδη σε λειτουργία, η αναγνώριση των ευπαθειών θα πρέπει να επεκταθεί ώστε να περιέχει περισσότερη εξειδικευμένη πληροφορία, όπως σχεδιασμένα χαρακτηριστικά ασφάλειας μέσα στα έγγραφα του σχεδίου ασφαλείας, καθώς και αποτελέσματα της αξιολόγησης της ασφάλειας του συστήματος.

11.4.4 Ανάλυση μηχανισμών ασφάλειας

Ο σκοπός αυτού του σταδίου είναι να αναλύσει τους μηχανισμούς ασφάλειας που ήδη εφαρμόζονται, ή σχεδιάζονται για εφαρμογή στον οργανισμό για να ελαττώσουν ή να εξαλείψουν την πιθανότητα εκμετάλλευσης ευπαθειών του συστήματος από διάφορες απειλές.

11.4.5 Προσδιορισμός πιθανότητας

Για τον υπολογισμό της πιθανότητας εμφάνισης ενός περιστατικού ασφάλειας, λαμβάνεται υπόψη το κίνητρο των απειλών και η ικανότητα των δυνητικά επιτιθέμενων, η φύση της ευπάθειας, η ύπαρξη και η αποτελεσματικότητα των υφιστάμενων μέτρων προστασίας.

Η πιθανότητα μπορεί να είναι:

- Υψηλή, όταν η απειλή έχει υψηλά κίνητρα, μεγάλη αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας δεν επαρκούν.
- Μεσαία, όταν η απειλή έχει υψηλά κίνητρα και μεγάλη αποτελεσματικότητα, αλλά τα υφιστάμενα μέτρα προστασίας επαρκούν.
- Χαμηλή, όταν η απειλή δεν έχει υψηλά κίνητρα, δεν έχει αποτελεσματικότητα και τα υφιστάμενα μέτρα προστασίας επαρκούν.

11.4.6 Ανάλυση επίπτωσης

Η επίπτωση ενός γεγονότος ασφάλειας (π.χ. μιας επίθεσης) μπορεί να περιγραφεί με τους όρους απώλειας ή υποβάθμισης των τριών κύριων χαρακτηριστικών της ασφάλειας: ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα.

11.4.7 Προσδιορισμός επικινδυνότητας

Ο σκοπός αυτού του βήματος είναι να εκτιμήσει το επίπεδο επικινδυνότητας του πληροφοριακού συστήματος. Η επικινδυνότητα εκφράζεται ως το γινόμενο της πιθανότητας εκδήλωσης μιας απειλής επί την επίπτωση που μπορεί αυτή να επιφέρει.

Η κλίμακα της επικινδυνότητας, με τις αξιολογήσεις της σε υψηλή, μεσαία και χαμηλή, αναπαριστά τον βαθμό του επιπέδου του κινδύνου στον οποίο ένα πληροφοριακό σύστημα, μία εγκατάσταση ή διαδικασία μπορεί να εκτεθεί αν υπάρχει μία ευπάθεια. Η κλίμακα της επικινδυνότητας, επίσης, αναπαριστά δράσεις οι οποίες πρέπει να εκτελεστούν για κάθε επίπεδο κινδύνου, ως εξής:

- Υψηλή επικινδυνότητα: Άμεση ανάγκη για διορθωτικά μέσα.
- Μεσαία επικινδυνότητα: Ανάγκη για διορθωτικά μέσα σε εύλογο χρονικό διάστημα.
- Χαμηλή επικινδυνότητα: Αποδοχή της ή διορθωτικά μέσα.

11.4.8 Προτεινόμενα μέτρα προστασίας

Κατά τη διάρκεια αυτού του σταδίου, προτείνονται εκείνα τα μέτρα προστασίας, τα οποία μπορούν να περιορίσουν τις ευπάθειες ή να τις εκμηδενίσουν. Για το σκοπό αυτό, λαμβάνονται υπόψη η αποτελεσματικότητα των προτεινόμενων επιλογών, η νομοθεσία και οι οργανωσιακοί κανονισμοί, η πολιτική, οι λειτουργικές επιπτώσεις, καθώς και η αξιοπιστία των μηχανισμών εφαρμογής των μέτρων. Τα προτεινόμενα μέτρα προστασίας είναι το αποτέλεσμα της διαδικασίας εκτίμησης της επικινδυνότητας και αποσκοπούν στο μετριασμό της επικινδυνότητας.

11.4.9 Τεκμηρίωση αποτελεσμάτων

Όταν ολοκληρωθεί η εκτίμηση της επικινδυνότητας, θα πρέπει να ακολουθήσει καταγραφή των αποτελεσμάτων σε μία ολοκληρωμένη αναφορά. Η αναφορά της εκτίμησης επικινδυνότητας βοηθά τη διοίκηση του οργανισμού στο να λάβει αποφάσεις σχετικά με την πολιτική, καθώς και τις λειτουργικές και διοικητικές αλλαγές του πληροφοριακού συστήματος που απαιτούνται. Η αναφορά της εκτίμησης επικινδυνότητας θα πρέπει να παρουσιάζεται ως μία συστηματική και αναλυτική προσέγγιση στη διαδικασία διαχείρισης της επικινδυνότητας, έτσι ώστε η διοίκηση να κατανοεί τους κινδύνους και να προβαίνει στη λήψη των κατάλληλων μέτρων προστασίας ώστε να μειώνει την επικινδυνότητα.

11.5 Σχέδιο Ασφάλειας

Η Πολιτική Ασφάλειας ανήκει ως έννοια στο οργανωσιακό πλαίσιο της Ασφάλειας Πληροφοριών. Το οργανωσιακό πλαίσιο της Ασφάλειας Πληροφοριών ενός οργανισμού περιλαμβάνει έγγραφα για πολιτικές, κανόνες, διαδικασίες και οδηγίες. Το σύνολο αυτών των εγγράφων συνηθίζεται να λέγεται Σχέδιο Ασφάλειας.

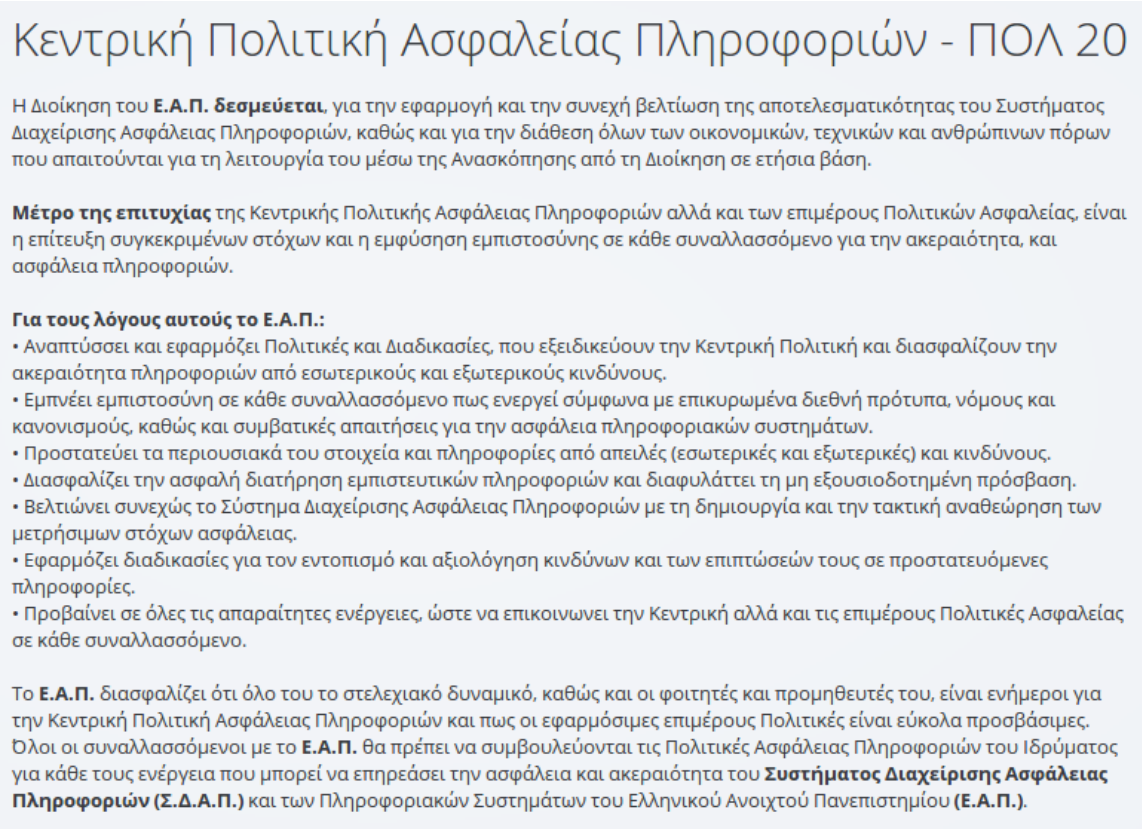
Αυτό το πλαίσιο ασφάλειας αποτελεί κεντρικό σημείο αναφοράς για την επικοινωνία μεταξύ των εμπλεκομένων, έτσι ώστε να αναπτυχθεί μια κοινή αντίληψη για την ασφάλεια και να διευκολυνθεί η συνεργασία μεταξύ των εμπλεκομένων. Το γεγονός ότι υπάρχει αυτό το πλαίσιο ασφάλειας, εξυπηρετεί ουσιαστικά στην ανάπτυξη μιας σχέσης εμπιστοσύνης του οργανισμού με τους πελάτες και τους συνεργάτες του.

Μια πολιτική (policy) είναι μια τυπική, σύντομη και υψηλού επιπέδου δήλωση, που εκφράζει τις γενικές πεποιθήσεις, τους σκοπούς, τους στόχους και τις αποδεκτές διαδικασίες ενός οργανισμού σε μια συγκεκριμένη θεματική περιοχή. Οι πολιτικές δεν ορίζουν ρητά τον τρόπο επίτευξης των στόχων, παρά μόνο ορίζουν τους στόχους. Για το λόγο αυτό, μια πολιτική συνοδεύεται από κανόνες και οδηγίες. Για έναν οργανισμό, η συμμόρφωση στην πολιτική είναι υποχρεωτική, ενώ η μη-συμμόρφωση αποτελεί πειθαρχικό παράπτωμα.

Στον επιχειρηματικό κόσμο συναντώνται διάφορα είδη πολιτικών ασφάλειας πληροφοριών. Στο υψηλότερο επίπεδο αφαίρεσης ανήκει η οργανωσιακή πολιτική ασφάλειας πληροφοριών, η οποία συνήθως περιέχει:

- Στόχους και σχέδια του οργανισμού σε σχέση με την ασφάλεια πληροφοριών.
- Ρόλους και καθήκοντα εμπλεκομένων.
- Ρητή δήλωση υποστήριξης της Διοίκησης ως προς τη συμμόρφωση με την πολιτική.
- Δέσμευση της διοίκησης για ενεργό συμμετοχή.
- Πλάνο ελέγχων των διαδικασιών.
- Πλάνο παροχής κατάλληλης κατάρτισης του προσωπικού.

Ένα παράδειγμα αυτού του πρώτου επιπέδου πολιτικής συναντάμε στο διαδικτυακό τόπο του Ελληνικού Ανοιχτού Πανεπιστημίου (http://noc.eap.gr/index.php/home/kentriki-politiki-asfaleias-pol20), που παρατίθεται στην Εικόνα 11.3.



Κεντρική Πολιτική Ασφαλείας Πληροφοριών - ΠΟΛ 20

Η Διοίκηση του **Ε.Α.Π. δεσμεύεται**, για την εφαρμογή και την συνεχή βελτίωση της αποτελεσματικότητας του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, καθώς και για την διάθεση όλων των οικονομικών, τεχνικών και ανθρώπινων πόρων που απαιτούνται για τη λειτουργία του μέσω της Ανασκόπησης από τη Διοίκηση σε ετήσια βάση.

Μέτρο της επιτυχίας της Κεντρικής Πολιτικής Ασφάλειας Πληροφοριών αλλά και των επιμέρους Πολιτικών Ασφαλείας, είναι η επίτευξη συγκεκριμένων στόχων και η εμφύσηση εμπιστοσύνης σε κάθε συναλλασσόμενο για την ακεραιότητα, και ασφάλεια πληροφοριών.

Για τους λόγους αυτούς το Ε.Α.Π.:
• Αναπτύσσει και εφαρμόζει Πολιτικές και Διαδικασίες, που εξειδικεύουν την Κεντρική Πολιτική και διασφαλίζουν την ακεραιότητα πληροφοριών από εσωτερικούς και εξωτερικούς κινδύνους.
• Εμπνέει εμπιστοσύνη σε κάθε συναλλασσόμενο πως ενεργεί σύμφωνα με επικυρωμένα διεθνή πρότυπα, νόμους και κανονισμούς, καθώς και συμβατικές απαιτήσεις για την ασφάλεια πληροφοριακών συστημάτων.
• Προστατεύει τα περιουσιακά του στοιχεία και πληροφορίες από απειλές (εσωτερικές και εξωτερικές) και κινδύνους.
• Διασφαλίζει την ασφαλή διατήρηση εμπιστευτικών πληροφοριών και διαφυλάττει τη μη εξουσιοδοτημένη πρόσβαση.
• Βελτιώνει συνεχώς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών με τη δημιουργία και την τακτική αναθεώρηση των μετρήσιμων στόχων ασφάλειας.
• Εφαρμόζει διαδικασίες για τον εντοπισμό και αξιολόγηση κινδύνων και των επιπτώσεών τους σε προστατευόμενες πληροφορίες.
• Προβαίνει σε όλες τις απαραίτητες ενέργειες, ώστε να επικοινωνεί την Κεντρική αλλά και τις επιμέρους Πολιτικές Ασφαλείας σε κάθε συναλλασσόμενο.

Το **Ε.Α.Π.** διασφαλίζει ότι όλο του το στελεχιακό δυναμικό, καθώς και οι φοιτητές και προμηθευτές του, είναι ενήμεροι για την Κεντρική Πολιτική Ασφάλειας Πληροφοριών και πως οι εφαρμόσιμες επιμέρους Πολιτικές είναι εύκολα προσβάσιμες. Όλοι οι συναλλασσόμενοι με το **Ε.Α.Π.** θα πρέπει να συμβουλεύονται τις Πολιτικές Ασφάλειας Πληροφοριών του Ιδρύματος για κάθε τους ενέργεια που μπορεί να επηρεάσει την ασφάλεια και ακεραιότητα του **Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.)** και των Πληροφοριακών Συστημάτων του Ελληνικού Ανοιχτού Πανεπιστημίου **(Ε.Α.Π.)**.

Εικόνα 11.3 *Παράδειγμα οργανωσιακής πολιτικής ασφάλειας πληροφοριών.*

Στο αμέσως χαμηλότερο (δεύτερο) επίπεδο αφαίρεσης, κάθε επιμέρους πολιτική ασφάλειας πληροφοριών στοχεύει σε συγκεκριμένες ομάδες ανθρώπων μέσα στον οργανισμό και καλύπτει συγκεκριμένες θεματικές περιοχές. Τέτοιου είδους θεματικές πολιτικές ασφάλειας μπορεί να είναι η πολιτική ελέγχου πρόσβασης, η πολιτική ασφάλειας επικοινωνιών, η πολιτική κρυπτογραφικών τεχνικών, η πολιτική χρήσης ηλεκτρονικού ταχυδρομείου κ.ά. Μια πολιτική αυτού του επιπέδου, συνήθως, αναφέρεται στο θέμα το οποίο αφορά, στους στόχους, στους όρους και στις προϋποθέσεις που θέτει, στις κατηγορίες υπαλλήλων στους οποίους απευθύνεται, στους ρόλους και στα καθήκοντα

11.6 Το πρότυπο ISO/IEC 17799

Ένας ενδεδειγμένος τρόπος για την αξιολόγηση των πολιτικών και τεχνικών ασφάλειας ενός οργανισμού, είναι αυτός που χρησιμοποιεί ως βάση τις «βέλτιστες πρακτικές» (best practices), που προτάθηκαν αρχικά (2000) με τη μορφή του διεθνώς αναγνωρισμένου προτύπου ISO/IEC 17799 (International Organization for

Standardization / International Electrotechnical Commission). Το πρότυπο ISO/IEC 17799 αποτέλεσε τον απόγονο του προτύπου BS 7799 (British Standards Institution) και είχε γίνει αποδεκτό από πολλές εθνικές αρχές προτυποποίησης, συμπεριλαμβανομένου του ΕΛΟΤ για την Ελλάδα. Το 2005 ενημερώθηκε (ISO/IEC 17799:2005) και το 2007 μετονομάσθηκε σε ISO/IEC 27002, συμμετέχοντας σε μια οικογένεια προτύπων, γνωστών ως η σειρά προτύπων ISO/IEC 27000.

Σκοπός της υιοθέτησης του προτύπου ISO/IEC 17799 από έναν οργανισμό, είναι να καθορισθεί ένας κοινός άξονας μελέτης και αντιμετώπισης των προβλημάτων ασφάλειας που αφορούν το πληροφοριακό σύστημά του. Σημαντικό πλεονέκτημα μιας τέτοιας προσέγγισης αποτελεί το γεγονός ότι τα αποτελέσματα της σχετικής μελέτης μπορούν να αποτελέσουν τη βάση για μια συνεχή και συντονισμένη προσπάθεια συμμόρφωσης (compliance) των πρακτικών και διαδικασιών ασφάλειας του οργανισμού με τα διεθνή και ευρωπαϊκά πρότυπα, προς την κατεύθυνση μιας ολιστικής διαχείρισης της ασφάλειας του πληροφοριακού συστήματος του οργανισμού.

Το πρότυπο ISO/IEC 17799 παρέχει γενικές κατευθύνσεις για τη διαχείριση της ασφάλειας πληροφοριών, στα πλαίσια βέλτιστων πρακτικών. Επιπλέον, περιγράφει μια κοινή βάση για την ανάπτυξη ασφάλειας μέσα στον οργανισμό, την αποτελεσματική διαχείριση της ασφάλειας πληροφοριών και τη δημιουργία εμπιστοσύνης κατά την πραγματοποίηση συναλλαγών με άλλους οργανισμούς. Οι προτάσεις του προτύπου θα πρέπει να υιοθετούνται και να εφαρμόζονται πάντα σε συμφωνία με την υφιστάμενη εθνική νομοθεσία.

Το πρότυπο ISO/IEC 17799 περιλαμβάνει 11 κύρια άρθρα (clauses) που συνολικά περιέχουν 39 βασικές κατηγορίες ασφάλειας (security categories), πέραν του ενός εισαγωγικού άρθρου που αφορά την αποτίμηση και μεταχείριση επικινδυνότητας. Τα κύρια άρθρα είναι τα εξής (σε παρένθεση το πλήθος των βασικών κατηγοριών ασφάλειας που περιέχονται σε καθένα από αυτά):

- Πολιτική Ασφάλειας - Security Policy.
- Οργάνωση Ασφάλειας Πληροφοριών - Organizing Information Security.
- Διαχείριση Αγαθών - Asset Management.
- Ασφάλεια Ανθρώπινων Πόρων - Human Resources Security.
- Φυσική και Περιβαλλοντική Ασφάλεια - Physical and Environmental Security.
- Διαχείριση Επικοινωνιών και Λειτουργιών - Communications and Operations Management .
- Έλεγχος Προσπέλασης - Access Control.
- Προμήθεια, Ανάπτυξη και Συντήρηση Πληροφοριακών Συστημάτων - Information Systems Acquisition, Development and Maintenance.
- Διαχείριση Συμβάντων Ασφάλειας Πληροφοριών - Information Security Incident Management.
- Διαχείριση Επιχειρησιακής Συνέχειας - Business Continuity Management.
- Συμμόρφωση – Compliance.

Η σειρά παράθεσης των παραπάνω άρθρων δεν αφορά την σπουδαιότητά τους, ενώ είναι στην ευχέρεια του κάθε οργανισμού να επιλέξει μεταξύ αυτών. Κάθε βασική κατηγορία ασφάλειας περιέχει:

- Ένα στόχο (objective), που δηλώνει το τι επιδιώκεται.
- Ένα ή περισσότερα μέτρα προστασίας (controls), που θα πρέπει να εφαρμοστούν για την επίτευξη του στόχου.

Η δομή της περιγραφής κάθε τέτοιου μέτρου είναι η ακόλουθη:

- Μέτρο (Control): μια επιμέρους δήλωση για την επίτευξη του στόχου.
- Οδηγίες υλοποίησης (Implementation guidance): περισσότερο λεπτομερής πληροφόρηση για την υποστήριξη της υλοποίησης προς την επίτευξη του στόχου.
- Άλλες πληροφορίες (Other information): επιπλέον πληροφόρηση, που πιθανώς αφορά π.χ. νομικά θέματα ή αναφορά σε άλλα πρότυπα.

11.6.1 Πολιτική ασφάλειας

Στόχος της πολιτικής ασφάλειας (security policy) πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή και ξεκάθαρη πολιτική, την οποία και θα υποστηρίζει έμπρακτα. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού. Προτεινόμενα μέτρα:

- Έγγραφο της πολιτικής ασφάλειας πληροφοριών.
- Αναθεώρηση της πολιτικής ασφάλειας πληροφοριών.

11.6.2 Οργάνωση της ασφάλειας πληροφοριών

11.6.2.1 Εσωτερική οργάνωση

Στόχος είναι η διαχείριση της ασφάλειας πληροφοριών μέσα σε έναν οργανισμό. Θα πρέπει να δημιουργηθεί ένα πλαίσιο διαχείρισης προκειμένου να ελέγχεται η υλοποίηση της ασφάλειας των πληροφοριών μέσα στον οργανισμό. Θα πρέπει να υπάρχει έμπρακτο ενδιαφέρον και υποστήριξη από τη διοίκηση του οργανισμού για τη δημιουργία της πολιτικής ασφάλειας, τον καταμερισμό καθηκόντων και τη μεθοδική εφαρμογή της τελευταίας στον οργανισμό. Αν κριθεί αναγκαίο, θα πρέπει να ζητηθεί και η βοήθεια εμπειρογνωμόνων εκτός του οργανισμού, προκειμένου να μπορούν να ληφθούν υπόψη και οι εξελίξεις στο χώρο, αλλά και να αντιμετωπίζονται διάφορα συμβάντα. Θα πρέπει να ενθαρρυνθεί μια προσέγγιση που θα βασίζεται στη συνεργασία διαφορετικών ειδικοτήτων και ομάδων, όπως οι χρήστες, οι προμηθευτές, οι ειδικοί της ασφάλειας, καθώς και η ίδια η διοίκηση του οργανισμού. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Δέσμευση της διοίκησης για ασφάλεια των πληροφοριών.
- Συντονισμός για θέματα ασφάλειας πληροφοριών.
- Κατανομή αρμοδιοτήτων για την ασφάλεια πληροφοριών.
- Διαδικασία εξουσιοδοτήσεων για τα μέσα επεξεργασίας πληροφοριών.
- Συμφωνίες εμπιστευτικότητας.
- Επικοινωνία με τις αρχές.
- Επικοινωνία με ομάδες ειδικών ενδιαφερόντων (special interest groups – SIG).
- Ανεξάρτητη επιθεώρηση της ασφάλειας πληροφοριών, π.χ. από κάποιον εξωτερικό σύμβουλο.

11.6.2.2 Εξωτερικά μέρη

Στόχος είναι η διαφύλαξη της ασφάλειας των μέσων επεξεργασίας πληροφοριών του οργανισμού, στα οποία έχουν προσπέλαση τρίτα μέρη. Η προσπέλαση από τρίτους στις εγκαταστάσεις του οργανισμού θα πρέπει να ελέγχεται. Όπου υπάρχει ανάγκη για τέτοιου είδους προσπέλαση θα πρέπει να διενεργείται αποτίμηση επικινδυνότητας προκειμένου να καθοριστούν οι επιπτώσεις στην ασφάλεια του οργανισμού και να

εγκατασταθούν τα απαραίτητα μέτρα προστασίας. Για τα μέτρα προστασίας θα πρέπει να έχει ενημερωθεί και να συμφωνεί εγγράφως κάθε τρίτο μέρος. Επίσης, θα πρέπει να προβλεφθούν και οι διαδικασίες μεταβίβασης των δικαιωμάτων προσπέλασης από τρίτα μέρη σε άλλες οντότητες. Αυτή η αντιμετώπιση θα πρέπει να αποτελεί μια βάση εφαρμογής και σε περιπτώσεις που αφορούν την εξωτερική προμήθεια (outsourcing) υπηρεσιών επεξεργασίας πληροφοριών. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Καθορισμός επικινδυνότητας λόγω προσπέλασης τρίτων μερών .
- Ικανοποίηση απαιτήσεων ασφάλειας κατά τις συναλλαγές με τρίτα μέρη.
- Ικανοποίηση απαιτήσεων ασφάλειας κατά τις συμφωνίες με τρίτα μέρη.

11.6.3 Διαχείριση αγαθών

11.6.3.1 Απόδοση ευθυνών για αγαθά

Στόχος είναι η επίτευξη και διατήρηση κατάλληλης προστασίας των αγαθών του οργανισμού. Όλα τα κύρια πληροφοριακά αγαθά του οργανισμού θα πρέπει να έχουν έναν καθορισμένο ιδιοκτήτη. Η υπευθυνότητα για τους πόρους του οργανισμού διασφαλίζει τη διατήρηση του κατάλληλου επιπέδου ασφάλειας. Θα πρέπει να καθοριστούν ιδιοκτήτες για όλα τα κύρια δεδομένα του οργανισμού, οι οποίοι θα είναι και υπεύθυνοι για την προστασία τους. Η ευθύνη της πρακτικής διασφάλισης των δεδομένων μπορεί να ανατεθεί σε κάποιον άλλον, αν και ο ιδιοκτήτης των δεδομένων έχει πάντα την τελική ευθύνη για την ασφάλειά τους. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Απογραφή των πόρων.
- Ιδιοκτησία των πόρων.
- Αποδεκτή χρήση των πόρων.

11.6.3.2 Διαβάθμιση πληροφοριών

Στόχος είναι να εξασφαλισθεί ότι όλοι οι πληροφοριακοί πόροι του οργανισμού προστατεύονται κατάλληλα. Οι πληροφορίες θα πρέπει να κατατάσσονται σε κατηγορίες προκειμένου να φαίνεται η ανάγκη, ο βαθμός και η προτεραιότητα της προστασίας που χρειάζονται. Κάποια δεδομένα μπορεί να χρειάζονται ειδική μεταχείριση και επιπλέον μέτρα προστασίας. Θα πρέπει να χρησιμοποιείται ένα σύστημα διαβάθμισης των πληροφοριών για τον καθορισμό των απαιτούμενων επιπέδων προστασίας, καθώς και για την επισήμανση τυχόν ανάγκης για ειδική μεταχείριση. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Οδηγίες διαβάθμισης.
- Σήμανση και χειρισμός των πληροφοριών.

11.6.4 Ασφάλεια ανθρώπινων πόρων

11.6.4.1 Πριν την πρόσληψη

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη κατανοούν τις ευθύνες τους και ότι είναι κατάλληλοι για τους ρόλους τους οποίους προορίζονται να αναλάβουν, καθώς επίσης και να ελαχιστοποιηθούν οι κίνδυνοι που μπορεί να προκληθούν από κλοπή, ανθρώπινο λάθος, απάτη ή κατάχρηση των εγκαταστάσεων του οργανισμού. Οι ευθύνες σχετικά με την ασφάλεια των πληροφοριών θα πρέπει να αναλύονται κατά τη διαδικασία πρόσληψης του προσωπικού. Επιπλέον θα πρέπει να αναφέρονται με σαφήνεια σε σχετικά συμβόλαια εργασίας, καθώς και να ελέγχεται η συμμόρφωση με αυτές κατά τη διάρκεια εργασίας του κάθε μέλους του προσωπικού. Οι υποψήφιοι υπάλληλοι θα πρέπει να ελέγχονται, ειδικά αυτοί που

πρόκειται να καταλάβουν ευαίσθητες θέσεις. Όλοι οι υπάλληλοι και οι συνεργάτες του οργανισμού θα πρέπει να υπογράφουν συμφωνητικό για τήρηση εχεμύθειας. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Ρόλοι και ευθύνες.
- Διαδικασία επιλογής προσωπικού.
- Όροι και συνθήκες πρόσληψης.

11.6.4.2 Μετά την πρόσληψη

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη είναι ευαισθητοποιημένοι για τους κινδύνους και τα ζητήματα που αφορούν την ασφάλεια των πληροφοριών του οργανισμού, για τις ευθύνες και τις υποχρεώσεις τους, καθώς και ότι διαθέτουν τα κατάλληλα εφόδια ώστε να υποστηρίξουν την πολιτική ασφάλειας του οργανισμού κατά τη διάρκεια της κανονικής τους εργασίας και να μειώσουν τους κινδύνους από ανθρώπινα σφάλματα. Οι ευθύνες της διοίκησης θα πρέπει να καθορίζονται ώστε να δια-σφαλίζεται ότι η ασφάλεια εφαρμόζεται σε όλο το εύρος των ανθρώπινων δραστηριοτήτων μέσα στον οργανισμό.

Θα πρέπει να παρέχεται προς όλους τους εργαζόμενους, τους εργολάβους και τους χρήστες από τρίτα μέρη ένα επαρκές επίπεδο ευαισθητοποίησης, εκπαίδευσης και κατάρτισης πάνω στις διαδικασίες ασφάλειας και τη σωστή χρήση των μέσων επεξεργασίας πληροφοριών ώστε να ελαχιστοποιούνται οι πιθανοί κίνδυνοι για την ασφάλεια. Ακόμη, θα πρέπει να εφαρμόζεται μια αυστηρά καθορισμένη πειθαρχική διαδικασία για το χειρισμό των ρηγμάτων ασφάλειας. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Υποχρεώσεις της διοίκησης.
- Ευαισθητοποίηση, εκπαίδευση και κατάρτιση πάνω στην ασφάλεια πληροφοριών.
- Πειθαρχική διαδικασία.

11.6.4.3 Τερματισμός ή αλλαγή απασχόλησης

Στόχος είναι να εξασφαλισθεί ότι οι εργαζόμενοι, οι εργολάβοι και τα τρίτα μέρη αποχωρούν ή αλλάζουν απασχόληση με έναν προβλεπόμενο τρόπο. Θα πρέπει να έχουν κατανεμηθεί οι αρμοδιότητες για να εξασφαλισθεί ότι η λύση της σύμβασης ενός εργαζόμενου ή ενός χρήστη τρίτου μέρους είναι υπό έλεγχο και ότι η επιστροφή του εξοπλισμού, καθώς και η αφαίρεση των όποιων δικαιωμάτων πρόσβαση ολοκληρώνεται. Οι αλλαγές στις υποχρεώσεις και την απασχόληση μέσα στον οργανισμό θα πρέπει να ελέγχονται παρομοίως. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Αρμοδιότητες για την περίπτωση τερματισμού απασχόλησης.
- Επιστροφή αγαθών.
- Αφαίρεση δικαιωμάτων πρόσβασης.

11.6.5 Φυσική και περιβαλλοντική ασφάλεια

11.6.5.1 Ασφαλείς περιοχές

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης φυσικής πρόσβασης, ζημιάς και παρέμβασης στις εγκαταστάσεις και το πληροφοριακό σύστημα του οργανισμού. Οι κρίσιμής σημασίας εγκαταστάσεις επεξεργασίας δεδομένων θα πρέπει να βρίσκονται σε ασφαλείς περιοχές, προστατευμένες από μια περίμετρο ασφάλειας και από τους κατάλληλους μηχανισμούς. Θα πρέπει να προστατεύονται φυσικά από μη-εξουσιοδοτημένη πρόσβαση, παρεμβολές και καταστροφή. Η παρεχόμενη προστασία θα πρέπει να είναι ανάλογη των κινδύνων. Προτεινόμενα μέτρα αποτελούν τα ακόλουθα:

- Περίμετρος φυσικής ασφάλειας.
- Μέτρα ελέγχου φυσικής πρόσβασης.
- Ασφάλεια γραφείων, δωματίων και μέσων.

- Προστασία από εξωτερικούς και περιβαλλοντικούς κινδύνους.
- Εργασία σε ασφαλείς περιοχές.
- Περιοχές φορτοεκφόρτωσης και δημόσιας πρόσβασης.

11.6.5.2 Ασφάλεια εξοπλισμού

Στόχος είναι η πρόληψη απώλειας, ζημιών, κλοπής ή διακύβευσης των αγαθών του οργανισμού και της διακοπής των επιχειρησιακών δραστηριοτήτων του. Ο εξοπλισμός θα πρέπει να προστατεύεται φυσικά από κινδύνους ασφάλειας και περιβαλλοντολογικές απειλές. Η προστασία του εξοπλισμού είναι απαραίτητη προκειμένου να ελαχιστοποιηθεί ο κίνδυνος μη-εξουσιοδοτημένης προσπέλασης των δεδομένων, όπως και η προστασία απέναντι στο ενδεχόμενο απώλειας ή καταστροφής. Θα πρέπει επίσης να ληφθούν ειδικά μέτρα προστασίας σχετικά με την υποδομή καλωδίωσης και την παροχή ρεύματος. Προτεινόμενα μέτρα:

- Τοποθέτηση και προστασία εξοπλισμού.
- Μέσα υποστήριξης.
- Ασφάλεια καλωδίωσης.
- Συντήρηση εξοπλισμού.
- Ασφάλεια εξοπλισμού εκτός των χώρων του οργανισμού.
- Ασφαλής καταστροφή ή επαναχρησιμοποίηση εξοπλισμού.
- Μετακίνηση αγαθών εκτός των χώρων του οργανισμού.

11.6.6 Διαχείριση επικοινωνιών και λειτουργιών

11.6.6.1 Λειτουργικές διαδικασίες και καθήκοντα

Στόχος είναι η σωστή και ασφαλής λειτουργία του πληροφοριακού συστήματος του οργανισμού. Τα καθήκοντα και οι διαδικασίες για τη διαχείριση και τη λειτουργία του πληροφοριακού συστήματος θα πρέπει να είναι σαφώς καθορισμένα. Επιπλέον, θα πρέπει να περιλαμβάνονται ειδικές λειτουργικές οδηγίες και διαδικασίες αντιμετώπισης συμβάντων που απειλούν την ασφάλεια του συστήματος.

Θα πρέπει να εφαρμόζεται ο διαχωρισμός των καθηκόντων, όπου αυτό είναι δυνατό, ώστε να ελαχιστοποιηθεί ο κίνδυνος κακής χρήσης του συστήματος, είτε από αμέλεια είτε από δόλο. Προτεινόμενα μέτρα:

- Τεκμηριωμένες λειτουργικές διαδικασίες.
- Διαχείριση αλλαγών.
- Διαχωρισμός καθηκόντων.
- Διαχωρισμός μεταξύ των μέσων ανάπτυξης, δοκιμής και λειτουργίας.

11.6.6.2 Διαχείριση παροχής υπηρεσιών από τρίτα μέρη

Στόχος είναι η υλοποίηση και συντήρηση ενός κατάλληλου επιπέδου ασφάλειας κατά την παροχή υπηρεσιών στο πλαίσιο συμφωνιών με τρίτα μέρη.

Ο οργανισμός θα πρέπει να ελέγχει την υλοποίηση των συμφωνιών, να επιβλέπει τη συμμόρφωση με τα συμφωνηθέντα και να διαχειρίζεται κατάλληλα τις αλλαγές ώστε να εξασφαλίζεται ότι κατά την παροχή των υπηρεσιών ικανοποιούνται όλες οι απαιτήσεις που έχουν συμφωνηθεί με τα τρίτα μέρη. Προτεινόμενα μέτρα:

- Διαδικασίες παροχής υπηρεσιών.
- Επίβλεψη και αξιολόγηση των υπηρεσιών από τρίτα μέρη.
- Διαχείριση αλλαγών των υπηρεσιών από τρίτα μέρη.

11.6.6.3 Σχεδιασμός και αποδοχή συστήματος

Στόχος είναι η ελαχιστοποίηση των κινδύνων για βλάβες του συστήματος. Ο προσεκτικός σχεδιασμός και η κατάλληλη προετοιμασία, είναι απαραίτητα στοιχεία για τη διαθεσιμότητα πόρων και χωρητικότητας του πληροφοριακού συστήματος του οργανισμού. Θα πρέπει να γίνουν προβλέψεις των μελλοντικών απαιτήσεων από το σύστημα, ώστε να μειωθεί ο κίνδυνος υπερφόρτωσής του. Τα νέα συστήματα θα πρέπει να δοκιμάζονται με βάση τις καταγεγραμμένες λειτουργικές ανάγκες του οργανισμού, πριν γίνουν αποδεκτά από τον οργανισμό και τεθούν σε παραγωγική λειτουργία. Προτεινόμενα μέτρα:

- Διαχείριση δυνατοτήτων υπαρχόντων και μελλοντικών πόρων
- Αποδοχή συστήματος

11.6.6.4 Προστασία από κακόβουλο λογισμικό

Στόχος είναι η προστασία της ακεραιότητας του λογισμικού και των πληροφοριών. Χρειάζονται προληπτικά μέτρα για τον εντοπισμό και την προστασία του πληροφοριακού συστήματος από κακόβουλο λογισμικό και μη-εξουσιοδοτημένο κινητό κώδικα. Το λογισμικό και τα μέσα επεξεργασίας πληροφοριών είναι ευάλωτα σε εισβολές κακόβουλου κώδικα, όπως ιοί, σκουλήκια, Δούρειοι Ίπποι και λογικές βόμβες.

Οι χρήστες θα πρέπει να είναι ενήμεροι για τους κινδύνους που προκαλεί το κακόβουλο λογισμικό. Η διοίκηση θα πρέπει να χρησιμοποιήσει τους κατάλληλους μηχανισμούς για τον εντοπισμό και την αποτροπή εισόδου στο σύστημα κακόβουλου κώδικα. Προτεινόμενα μέτρα:

- Μέτρα προστασίας από κακόβουλο λογισμικό.
- Μέτρα προστασίας από κινητό κώδικα.

11.6.6.5 Λήψη εφεδρικού αντιγράφου ασφαλείας

Στόχος είναι η διατήρηση της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των μέσων επεξεργασίας. Θα πρέπει να υπάρχουν διαδικασίες ρουτίνας για την καθημερινή λήψη εφεδρικών αντιγράφων του συστήματος και τη διασφάλιση της επαναφοράς τους όποτε χρειαστεί. Προτεινόμενο μέτρο:

- Λήψη εφεδρικού αντιγράφου ασφαλείας των πληροφοριών.

11.6.6.6 Διαχείριση ασφάλειας δικτύου

Στόχος είναι η ασφάλεια των πληροφοριών που υπάρχουν στο δίκτυο του οργανισμού, καθώς και της δικτυακής υποδομής. Η διαχείριση της ασφάλειας του δικτύου απαιτεί ειδική προσοχή, καθώς επηρεάζει πολλά τμήματα του οργανισμού. Θα πρέπει επίσης να εξασφαλιστεί ότι δεν αποστέλλονται ευαίσθητα δεδομένα διαμέσου δημόσιων δικτύων. Προτεινόμενα μέτρα:

- Μέτρα προστασίας δικτύου.
- Ασφάλεια των δικτυακών υπηρεσιών.

11.6.6.7 Χειρισμός αποθηκευτικών μέσων

Στόχος είναι η αποτροπή ζημιών στους πόρους του οργανισμού και παρεμβολών στις λειτουργίες του οργανισμού. Τα διάφορα αποθηκευτικά μέσα (δίσκοι, ταινίες κλπ.), τα έγγραφα, τα εγχειρίδια του συστήματος θα πρέπει να προστατεύονται κατάλληλα από καταστροφή, κλοπή ή μη-εξουσιοδοτημένη πρόσβαση. Προτεινόμενα μέτρα:

- Διαχείριση αποσπώμενων αποθηκευτικών μέσων.
- Απόσυρση αποθηκευτικών μέσων.
- Διαδικασίες χειρισμού πληροφοριών.
- Ασφάλεια τεκμηρίωσης συστήματος.

11.6.6.8 Ανταλλαγή πληροφοριών

Στόχος είναι η προστασία των πληροφοριών και του λογισμικού που ανταλλάσσονται μεταξύ του οργανισμού και μιας εξωτερικής οντότητας. Η ανταλλαγή πληροφοριών και εφαρμογών μεταξύ των οργανισμών θα πρέπει να βασίζεται σε μια αυστηρή πολιτική ανταλλαγών και να είναι σύμφωνη με τη σχετική νομοθεσία. Θα πρέπει να εφαρμόζονται διαδικασίες και πρότυπα για την προστασία των πληροφοριών και των φυσικών μέσων που περιέχουν πληροφορίες. Προτεινόμενα μέτρα:

- Διαδικασίες και πολιτικές ανταλλαγής πληροφοριών.
- Συμφωνίες ανταλλαγών.
- Ασφάλεια αποθηκευτικών μέσων κατά τη μεταφορά τους.
- Χρήση ηλεκτρονικού ταχυδρομείου.
- Επιχειρησιακά πληροφοριακά συστήματα.

11.6.6.9 Υπηρεσίες ηλεκτρονικού εμπορίου

Στόχος είναι να εξασφαλισθεί η ασφάλεια των υπηρεσιών ηλεκτρονικού εμπορίου και της χρήσης τους. Θα πρέπει να θεωρηθούν οι επιπτώσεις στην ασφάλεια, που σχετίζονται με τη χρήση των υπηρεσιών ηλεκτρονικού εμπορίου περιλαμβανομένων των άμεσων δοσοληψιών (online transactions) και των απαιτήσεων για μέτρα προστασίας. Θα πρέπει ακόμη να εξεταστεί η ακεραιότητα και η διαθεσιμότητα των ηλεκτρονικά δημοσιευόμενων πληροφοριών μέσω συστημάτων που είναι διαθέσιμα στο κοινό. Προτεινόμενα μέτρα:

- Διαδικασίες παροχής υπηρεσιών ηλεκτρονικού εμπορίου.
- Έλεγχος πρόσβασης στις δοσοληψίες,
- Έλεγχος πληροφοριών που είναι διαθέσιμες στο κοινό.

11.6.6.10 Επίβλεψη

Στόχος είναι να ανιχνευθούν δραστηριότητες μη εξουσιοδοτημένης επεξεργασίας πληροφοριών. Θα πρέπει να επιβλέπονται τα συστήματα και να καταγράφονται τα συμβάντα που αφορούν την ασφάλεια των πληροφοριών. Θα πρέπει να χρησιμοποιούνται καταγραφές λειτουργίας και σφαλμάτων για να εξασφαλισθεί ότι προσδιορίζονται τα προβλήματα που αντιμετωπίζουν τα πληροφοριακά συστήματα. Ο οργανισμός θα πρέπει να συμμορφώνεται με όλες τις εκ του νόμου απαιτήσεις που αφορούν τις ενέργειες επίβλεψης και καταγραφής. Η επίβλεψη των συστημάτων θα πρέπει να χρησιμοποιείται για να ελέγχεται η αποδοτικότητα των υιοθετημένων μέτρων και για να επιβεβαιώνεται η συμβατότητα με κάποιο μοντέλο πολιτικής πρόσβασης. Προτεινόμενα μέτρα:

- Καταγραφές ελέγχου.
- Επίβλεψη της χρήσης των συστημάτων.
- Προστασία των καταγεγραμμένων πληροφοριών.
- Καταγραφές διαχείρισης και λειτουργίας.
- Καταγραφές σφαλμάτων.
- Συγχρονισμός ρολογιών.

11.6.7 Έλεγχος πρόσβασης

11.6.7.1 Επιχειρησιακές απαιτήσεις για έλεγχο πρόσβασης

Στόχος είναι ο έλεγχος της πρόσβασης στις πληροφορίες του οργανισμού. Η πρόσβαση σε πληροφορίες και επιχειρησιακές διεργασίες θα πρέπει να ελέγχεται με βάση τις επιχειρησιακές ανάγκες και της απαιτήσεις ασφάλειας του οργανισμού, λαμβάνοντας υπόψη τις πολιτικές διάχυσης των πληροφοριών και των σχετικών εξουσιοδοτήσεων. Προτεινόμενο μέτρο:

- Πολιτική ελέγχου πρόσβασης

11.6.7.2 Διαχείριση πρόσβασης χρηστών

Στόχος είναι να εξασφαλισθεί η προσπέλαση από εξουσιοδοτημένους χρήστες και να προληφθεί η μη-εξουσιοδοτημένη πρόσβαση στα πληροφοριακά συστήματα. Θα πρέπει να υπάρχουν αυστηρές διαδικασίες για τον έλεγχο της πρόσβασης των χρηστών στα διάφορα πληροφοριακά συστήματα και τις υπηρεσίες. Οι διαδικασίες αυτές θα πρέπει να καλύπτουν ολόκληρο τον κύκλο της πρόσβασης των χρηστών, από την αρχική δήλωση του χρήστη στο σύστημα, μέχρι και τη διαγραφή του από αυτό. Ειδική προσοχή απαιτείται στον καθορισμό των δικαιωμάτων των χρηστών, ώστε να μην μπορούν να παρακάμψουν τους μηχανισμούς ασφάλειας του συστήματος. Προτεινόμενα μέτρα:

- Διαδικασία εγγραφής χρηστών.
- Διαχείριση προνομίων χρηστών.
- Διαχείριση διαπιστευτηρίων (credentials) των χρηστών.
- Επιθεώρηση προνομίων των χρηστών.

11.6.7.3 Ευθύνες χρηστών

Στόχος είναι η αποτροπή της μη-εξουσιοδοτημένης πρόσβασης χρηστών στο σύστημα και η διακύβευση των πληροφοριών και των μέσων αποθήκευσης, διακίνησης και επεξεργασίας τους. Η συνεργασία των εξουσιοδοτημένων χρηστών του συστήματος είναι απαραίτητη για τη γενικότερη ασφάλειά του. Οι χρήστες θα πρέπει να είναι ενήμεροι για τις ευθύνες τους, σχετικά με τους χρησιμοποιούμενους μηχανισμούς ασφάλειας, ειδικότερα για τη χρήση διαπιστευτηρίων (π.χ. συνθηματικών) και την ασφάλεια του εξοπλισμού. Θα πρέπει να υλοποιηθεί μια πολιτική «καθαρού γραφείου» και «καθαρής οθόνης», ώστε να μειωθούν οι κίνδυνοι για καταστροφή εγγράφων, αποθηκευτικών μέσων και μέσων επεξεργασίας πληροφοριών. Προτεινόμενα μέτρα:

- Διαδικασία χρήσης διαπιστευτηρίων.
- Καταγραφή εξοπλισμού που δεν επιβλέπεται.
- Πολιτική καθαρού γραφείου και καθαρής οθόνης.

11.6.7.4 Έλεγχος πρόσβασης δικτύου

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης πρόσβασης στις δικτυακές υπηρεσίες. Η πρόσβαση σε εσωτερικές αλλά και σε εξωτερικές δικτυακές υπηρεσίες θα πρέπει να είναι ελεγχόμενη. Αυτό είναι απαραίτητο προκειμένου να εξασφαλισθεί ότι οι χρήστες των δικτυακών υπηρεσιών δεν μπορούν να απειλήσουν την ασφάλεια αυτών των υπηρεσιών. Για αυτό θα πρέπει να εξασφαλισθεί ότι:

- Υπάρχουν οι κατάλληλες διεπαφές (interfaces) μεταξύ του δικτύου του οργανισμού και των δικτύων άλλων οργανισμών ή δημόσιων δικτύων.

- Υπάρχουν κατάλληλοι μμηχανισμοί αυθεντικοποίησης χρηστών και εξοπλισμού.

- Επιβάλλεται ελεγχόμενη πρόσβαση των χρηστών στις προσφερόμενες υπηρεσίες.

Προτεινόμενα μέτρα:

- Πολιτική χρήσης των δικτυακών υπηρεσιών.
- Αυθεντικοποίηση χρηστών για εξωτερικές συνδέσεις.
- Διαδικασία αναγνώρισης δικτυακού εξοπλισμού.
- Προστασία θυρών απομακρυσμένης διάγνωσης και διαμόρφωσης.
- Διαχωρισμός μεταξύ δικτύων.
- Έλεγχος δικτυακών συνδέσεων.
- Έλεγχος δρομολόγησης δικτύου.

11.6.7.5 Έλεγχος πρόσβασης σε λειτουργικά συστήματα

Στόχος είναι η αποτροπή μη-εξουσιοδοτημένης πρόσβασης σε λειτουργικά συστήματα. Θα πρέπει να χρησιμοποιούνται μέσα ασφάλειας για τον περιορισμό της άμεσης πρόσβασης (π.χ. στη γραμμή εντολών) του λειτουργικού συστήματος σε εξουσιοδοτημένους χρήστες. Αυτά τα μέσα θα πρέπει να είναι σε θέση να:

- Αυθεντικοποιούν τους εξουσιοδοτημένους χρήστες, με βάση την καθορισμένη πολιτική ελέγχου πρόσβασης.

- Καταγράφουν τις επιτυχείς και τις ανεπιτυχείς προσπάθειες αυθεντικοποίησης από το σύστημα.

- Καταγράφουν τη χρήση των ειδικών προνομίων συστήματος.

- Ενεργοποιούν συναγερμούς όταν παραβιάζονται οι πολιτικές ασφάλειας συστήματος.

- Παρέχουν κατάλληλα μέσα αυθεντικοποίησης.

- Περιορίζουν τους χρόνους και τόπους σύνδεσης των χρηστών, όπου αυτό κρίνεται απαραίτητο.

Προτεινόμενα μέτρα:

- Διαδικασίες ασφαλούς σύνδεσης στο σύστημα.
- Αναγνώριση και αυθεντικοποίηση χρηστών.
- Σύστημα διαχείρισης συνθηματικών.
- Χρήση εργαλείων συστήματος.
- Περιορισμός χρόνου και τόπου σύνδεσης.

11.6.7.6 Έλεγχος πρόσβασης σε πληροφορίες και εφαρμογές

Σκοπός είναι η αποτροπή της μη-εξουσιοδοτημένης πρόσβασης στις πληροφορίες που χρησιμοποιούνται από τις διάφορες εφαρμογές. Θα πρέπει να χρησιμοποιούνται ειδικά μέσα ασφάλειας για τον περιορισμό της πρόσβασης στις εφαρμογές. Η λογική πρόσβαση σε λογισμικό και πληροφορίες εφαρμογών θα πρέπει να περιορίζεται μόνο στους εξουσιοδοτημένους χρήστες. Οι εφαρμογές θα πρέπει να:

- ελέγχουν την πρόσβαση των χρηστών σε διάφορες πληροφορίες και λειτουργίες των εφαρμογών, σύμφωνα με την καθορισμένη πολιτική ελέγχου πρόσβασης του οργανισμού,

- παρέχουν προστασία από μη-εξουσιοδοτημένη προσπέλαση μέσω οποιασδήποτε υπηρεσίας, λογισμικού λειτουργικού συστήματος και κακόβουλου λογισμικού, που είναι ικανά να παρακάμψουν τα μέτρα προστασίας του συστήματος,

- μην διακυβεύουν την ασφάλεια άλλων συστημάτων, με τα οποία διαμοιράζονται πόρους.

Προτεινόμενα μέτρα:

- Περιορισμός προσπέλασης πληροφοριών.

- Απομόνωση ευαίσθητων συστημάτων.

11.6.7.7 Τηλεργασία και κινητή υπολογιστική

Σκοπός είναι η εξασφάλιση της ασφάλειας των πληροφοριών, όταν χρησιμοποιούνται μέσα κινητής υπολογιστικής και τηλεργασίας. Η απαιτούμενη προστασία θα πρέπει να είναι ανάλογη των κινδύνων που εισάγουν αυτοί οι τρόποι εργασίας. Στην περίπτωση της κινητής υπολογιστικής θα πρέπει να εξεταστούν οι κίνδυνοι λόγω εργασίας σε ένα απροστάτευτο περιβάλλον και να εφαρμοσθούν κατάλληλα μέτρα προστασίας. Στην περίπτωση της τηλεργασίας, ο οργανισμός θα πρέπει να εφαρμόσει κατάλληλα μέτρα προστασίας στην τοποθεσία από την όποια θα γίνεται τηλεργασία και να εξασφαλίσει ότι έχουν γίνει οι κατάλληλες διευθετήσεις για αυτό τον τρόπο εργασίας. Προτεινόμενα μέτρα:

- Διαδικασία κινητής υπολογιστική
- Μέτρα προστασίας των επικοινωνιών.
- Διαδικασία τηλεργασίας.

11.6.8 Προμήθεια, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

11.6.8.1 Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων

Η ασφάλεια αποτελεί αναπόσπαστο μέρος των πληροφοριακών συστημάτων. Τα πληροφοριακά συστήματα περιλαμβάνουν τα λειτουργικά συστήματα, την υποδομή, τις επιχειρησιακές εφαρμογές, τα πακέτα εφαρμογών (off-the-shelf), τις υπηρεσίες και τις εφαρμογές που αναπτύσσουν οι χρήστες. Ο σχεδιασμός και η υλοποίηση των επιχειρησιακών διεργασιών που υποστηρίζουν τις εφαρμογές ή τις υπηρεσίες του οργανισμού μπορεί να είναι ιδιαίτερα σημαντικό ζήτημα για την ασφάλεια. Οι απαιτήσεις ασφάλειας θα πρέπει να καθορίζονται και να συμφωνούνται πριν από την ανάπτυξη και την υλοποίηση των πληροφοριακών συστημάτων. Όλες οι απαιτήσεις ασφάλειας θα πρέπει να προσδιορίζονται κατά τη φάση καθορισμού των απαιτήσεων στο πλαίσιο ενός έργου, ενώ θα πρέπει επίσης να προσαρμόζονται, να συμφωνούνται και να τεκμηριώνονται στο πλαίσιο του συνολικού επιχειρησιακού σχεδίου που αφορά το πληροφοριακό σύστημα. Προτεινόμενα μέτρο:

- Ανάλυση και προδιαγραφή απαιτήσεων ασφάλειας.

11.6.8.2 Ορθή επεξεργασία από τις εφαρμογές

Σκοπός είναι η πρόληψη λαθών, απώλειας ή μη-εξουσιοδοτημένης μετατροπής των δεδομένων από τις εφαρμογές. θα πρέπει να σχεδιάζονται κατάλληλοι μηχανισμοί καταγραφής των ενεργειών στις εφαρμογές, προκειμένου να διασφαλίζεται η ορθότητα της επεξεργασίας. Θα πρέπει επίσης να περιλαμβάνουν τον έλεγχο της εγκυρότητας των προς εισαγωγή δεδομένων, την εσωτερική επεξεργασία τους. καθώς και τον έλεγχο των δεδομένων εξόδου. Επιπρόσθετα μέτρα προστασίας πιθανόν να απαιτούνται για συστήματα που επεξεργάζονται, ή προκαλούν επιπτώσεις σε ευαίσθητες ή κρίσιμες πληροφορίες. Η λήψη αυτών των μέτρων θα πρέπει να αποφασίζεται με βάση τις απαιτήσεις ασφάλειας και την εκτίμηση της επικινδυνότητας. Προτεινόμενα μέτρα:

- Επικύρωση εισαγόμενων δεδομένων.
- Έλεγχος εσωτερικής επεξεργασίας.
- Ακεραιότητα μηνυμάτων.
- Επικύρωση εξαγόμενων δεδομένων.

11.6.8.3 Κρυπτογραφικά μέτρα προστασίας

Σκοπός είναι η προστασία της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των πληροφοριών με κρυπτογραφικά μέσα. Για το σκοπό αυτό θα πρέπει να αναπτυχθεί μια πολιτική χρήσης κρυπτογραφικών μέτρων προστασίας. Ακόμη, θα πρέπει να εφαρμόζονται κατάλληλες διαδικασίες διαχείρισης κλειδιών για την υποστήριξη των διάφορων κρυπτογραφικών τεχνικών. Προτεινόμενα μέτρα:

- Πολιτική χρήσης των κρυπτογραφικών μέτρων προστασίας.
- Διαχείριση κλειδιών.

11.6.8.4 Ασφάλεια αρχείων συστήματος

Σκοπός είναι η εξασφάλιση της ασφάλειας των αρχείων συστήματος. Θα πρέπει να ελέγχεται η πρόσβαση στα αρχεία του συστήματος και στον πηγαίο κώδικα των προγραμμάτων, ενώ οι δραστηριότητες διενέργειας και υποστήριξης έργων πληροφορικής θα πρέπει να πραγματοποιούνται με ασφαλή τρόπο. Θα πρέπει επίσης να υπάρχει φροντίδα για την αποφυγή έκθεσης ευαίσθητων δεδομένων σε περιβάλλοντα δοκιμών. Προτεινόμενα μέτρα:

- Έλεγχος λογισμικού συστήματος.
- Προστασία των δεδομένων δοκιμών των συστημάτων.
- Έλεγχος πρόσβασης στον πηγαίο κώδικα προγραμμάτων.

11.6.8.5 Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης

Σκοπός είναι η διαφύλαξη της ασφάλειας του λογισμικού και των πληροφοριών των συστημάτων εφαρμογών. Τα περιβάλλοντα ανάπτυξης και υποστήριξης θα πρέπει να είναι αυστηρά ελεγχόμενα. Οι υπεύθυνοι για τα συστήματα εφαρμογών θα πρέπει να είναι υπεύθυνοι και για την ασφάλεια των περιβαλλόντων ανάπτυξης και υποστήριξής τους. Θα πρέπει να διασφαλίσουν ότι οποιαδήποτε αλλαγή στο σύστημα ελέγχεται πριν πραγματοποιηθεί και ότι δεν έχει αρνητικές επιπτώσεις στην ασφάλεια είτε του συστήματος είτε του λειτουργικού περιβάλλοντος. Προτεινόμενα μέτρα:

- Διαδικασίες ελέγχου αλλαγών.
- Τεχνική επιθεώρηση των εφαρμογών μετά από αλλαγές στο λειτουργικό σύστημα.
- Περιορισμοί στις αλλαγές των πακέτων λογισμικού.
- Διαρροή πληροφοριών.
- Ανάπτυξη λογισμικού από τρίτους (outsourced).

11.6.8.6 Διαχείριση τεχνικών ευπαθειών

Σκοπός είναι η μείωση της επικινδυνότητας που απορρέει από την αξιοποίηση δημοσίως γνωστών τεχνικών ευπαθειών. Η διαχείριση τεχνικών ευπαθειών θα πρέπει να υλοποιείται με τρόπο αποτελεσματικό, συστηματικό και επαναλαμβανόμενο, καθώς και με μετρήσεις που λαμβάνονται προκειμένου να επιβεβαιώνεται η

αποτελεσματικότητά της. Τα παραπάνω θα πρέπει να αφορούν τα λειτουργικά συστήματα και κάθε άλλη εφαρμογή σε χρήση. Προτεινόμενο μέτρο:

- Έλεγχος τεχνικών ευπαθειών

11.6.9 Συμβάντα ασφάλειας

11.6.9.1 Αναφορά συμβάντων και ευπαθειών ασφάλειας

Σκοπός είναι η διασφάλιση του ότι τα συμβάντα και οι ευπάθειες ασφάλειας πληροφοριών γνωστοποιούνται με τρόπο που επιτρέπει την έγκαιρη λήψη κατάλληλων ενεργειών. Για αυτό, θα πρέπει να έχουν καθορισθεί και εφαρμοσθεί επίσημες διαδικασίες αναφοράς συμβάντων και κλιμάκωσης ενεργειών. Όλοι οι εργαζόμενοι, οι συμβαλλόμενοι και οι χρήστες τρίτων μερών θα πρέπει να προσδίδουν την απαραίτητη προσοχή στις διαδικασίες αναφοράς διαφόρων τύπων συμβάντων και ευπαθειών που πιθανώς να έχουν επίπτωση στην ασφάλεια των αγαθών του οργανισμού. Επιπλέον, θα πρέπει να είναι υποχρεωμένοι να αναφέρουν οποιαδήποτε συμβάντα και ευπάθειες για την ασφάλεια πληροφοριών το συντομότερο δυνατόν στο προκαθορισμένο σημείο επικοινωνίας. Προτεινόμενα μέτρα:

- Αναφορά συμβάντων ασφάλειας.
- Αναφορά ευπαθειών ασφάλειας.

11.6.9.2 Διαχείριση συμβάντων ασφάλειας

Σκοπός είναι η διασφάλιση της εφαρμογής μιας συνεπούς και αποτελεσματικής προσέγγισης για τη διαχείριση των συμβάντων ασφάλειας πληροφοριών. Θα πρέπει να έχουν καθορισθεί και να εφαρμόζονται κατάλληλες αρμοδιότητες και διαδικασίες διαχείρισης συμβάντων ασφάλειας πληροφοριών, κατά τρόπο αποτελεσματικό, από τη στιγμή της αναφοράς τους. Θα πρέπει να εφαρμόζεται μια διαδικασία συνεχούς βελτίωσης ως αποτέλεσμα της επιθεώρησης, εκτίμησης και συνολικής διαχείρισης των συμβάντων ασφάλειας πληροφοριών. Όπου απαιτείται, θα πρέπει να συλλέγονται αποδείξεις για να διασφαλίζεται η συμμόρφωση με τις απαιτήσεις του νόμου. Προτεινόμενα μέτρα:

- Αρμοδιότητες και διαδικασίες.
- Μαθαίνοντας από τα συμβάντα ασφάλειας πληροφοριών.
- Συλλογή αποδείξεων (forensics).

11.6.10 Διαχείριση επιχειρησιακής συνέχειας

Σκοπός είναι η αντίδραση σε περίπτωση διακοπών στις επιχειρησιακές δραστηριότητες του οργανισμού και η προστασία των κρίσιμων διαδικασιών από τις επιπτώσεις σημαντικών αστοχιών των πληροφοριακών συστημάτων ή καταστροφών και η διασφάλιση της έγκαιρης ανάκτησής τους.

Θα πρέπει να έχει υλοποιηθεί μια διαδικασία διαχείρισης της επιχειρησιακής συνέχειας (business continuity management) του οργανισμού προκειμένου να μειωθούν οι επιπτώσεις στον οργανισμό και να ανακτηθούν τα απολεσθέντα αγαθά του οργανισμού (π.χ. ως αποτέλεσμα φυσικών καταστροφών, δυστυχημάτων, αστοχιών εξοπλισμού και εσκεμμένων πράξεων) σε ένα ανεκτό επίπεδο, μέσω συνδυασμένων μέτρων πρόληψης και ανάκτησης. Σε αυτή τη διαδικασία θα πρέπει να ορίζονται οι κρίσιμες επιχειρησιακές διαδικασίες και να ενοποιούνται οι απαιτήσεις διαχείρισης ασφάλειας πληροφοριών με άλλες απαιτήσεις συνέχειας που αφορούν λειτουργίες, προσωπικό, υλικά, μεταφορές και υπηρεσίες.

Οι συνέπειες των καταστροφών, αστοχιών ασφάλειας, απωλειών υπηρεσιών και διαθεσιμότητας υπηρεσιών θα πρέπει να γίνουν αντικείμενο μιας ανάλυσης επιχειρησιακών επιπτώσεων (business impact analysis – BIA). Ακόμη, θα πρέπει να αναπτυχθούν και να υλοποιηθούν σχέδια επιχειρησιακής συνέχειας (business continuity plans) προκειμένου να διασφαλισθεί η έγκαιρη ανάκτηση των βασικών λειτουργιών. Η

ασφάλεια πληροφοριών θα πρέπει να αποτελεί αναπόσπαστο μέρος της συνολικής διαδικασίας επιχειρησιακής συνέχειας, καθώς και άλλων διαδικασιών διαχείρισης μέσα στον οργανισμό. Η διαχείριση της επιχειρησιακής συνέχειας θα πρέπει να περιλαμβάνει μέτρα για τον καθορισμό και τη μείωση επικινδυνότητας, πέραν της γενικής διαδικασίας εκτίμησης επικινδυνότητας, για τον περιορισμό των συνεπειών από καταστροφικά συμβάντα και για τη διασφάλιση της άμεσης διαθεσιμότητας των πληροφοριών που είναι απαραίτητες για τις επιχειρησιακές λειτουργίες. Προτεινόμενα μέτρα:

- Εισαγωγή της ασφάλειας πληροφοριών στη διαδικασία διαχείρισης επιχειρησιακής συνέχειας.
- Σχεδιασμός επιχειρησιακής συνέχειας και εκτίμηση επικινδυνότητας.
- Υλοποίηση σχεδίων επιχειρησιακής συνέχειας σε συνδυασμό με τη διαχείριση ασφάλειας των πληροφοριών.
- Δοκιμή, συντήρηση και επανεκτίμηση των σχεδίων επιχειρησιακής συνέχειας.

11.6.11 Συμμόρφωση

11.6.11.1 Συμμόρφωση με τις απαιτήσεις του νόμου

Σκοπός είναι η αποφυγή παραβιάσεων οποιουδήποτε νόμου, ρυθμίσεων, κανονισμών ή συμβατικών υποχρεώσεων, καθώς και κάθε είδους απαιτήσεων ασφάλειας. Ο σχεδιασμός, η λειτουργία, η χρήση και η διαχείριση πληροφοριακών συστημάτων είναι πιθανό να υπόκειται σε κάποιας μορφής νόμους, ρυθμίσεις, κανονισμούς ή συμβατικές υποχρεώσεις ασφάλειας. Το νομικό τμήμα του οργανισμού θα πρέπει να παρέχει συμβουλές για τη συμμόρφωση με τους διάφορους νόμους και ρυθμίσεις. Ιδιαίτερη προσοχή χρειάζεται όταν εμπλέκονται νομοθεσίες διαφορετικών χωρών (π.χ. κατά τη μεταφορά δεδομένων ανάμεσα σε χώρες). Προτεινόμενα μέτρα:

- Καθορισμός της εφαρμοζόμενης νομοθεσίας.
- Δικαιώματα πνευματικής ιδιοκτησίας.
- Προστασία των αρχείων δεδομένων του οργανισμού.
- Προστασία του απόρρητου των προσωπικών πληροφοριών.
- Πρόληψη κακής χρήσης των μέσων αποθήκευσης, διακίνησης και επεξεργασίας πληροφοριών.
- Νομοταγής χρήση των κρυπτογραφικών μέσων.

11.6.11.2 Συμμόρφωση με πολιτικές ασφάλειας, πρότυπα και τεχνικές

Σκοπός είναι η διασφάλιση της συμμόρφωσης των συστημάτων με πολιτικές ασφάλειας του οργανισμού και πρότυπα. Θα πρέπει να εξετάζεται σε τακτικά χρονικά διαστήματα η ασφάλεια των πληροφοριακών συστημάτων. Οι εξετάσεις αυτές θα πρέπει να γίνονται σε αντιπαράθεση με τις κατάλληλες πολιτικές ασφάλειας. Ακόμη, τα πληροφοριακά συστήματα θα πρέπει να επιθεωρούνται για να ελέγχεται η συμμόρφωσή τους με εφαρμοζόμενα πρότυπα υλοποίησης μηχανισμών ασφάλειας και τεκμηριωμένα μέτρα προστασίας. Προτεινόμενα μέτρα:

- Συμμόρφωση με πολιτικές ασφάλειας και πρότυπα.
- Έλεγχος τεχνικής συμμόρφωσης.
- Καθορισμός της εφαρμοζόμενης νομοθεσίας.

11.6.11.3 Ζητήματα επιθεώρησης πληροφοριακών συστημάτων

Σκοπός είναι η μεγιστοποίηση της αποτελεσματικότητας της διαδικασίας επιθεώρησης, καθώς και η ελαχιστοποίηση των παρεμβολών που μπορεί να προκαλέσει στη λειτουργία των πληροφοριακών συστημάτων.

Θα πρέπει να λαμβάνονται μέτρα προστασίας για την προφύλαξη των παραγωγικών συστημάτων και των εργαλείων επιθεώρησης κατά τη διάρκεια των επιθεωρήσεων πληροφοριακών συστημάτων. Επιπλέον, απαιτείται κατάλληλη προστασία για την προφύλαξη της ακεραιότητας και την αποφυγή κατάχρησης των εργαλείων επιθεώρησης. Προτεινόμενα μέτρα:

- Μέτρα επιθεώρησης πληροφοριακών συστημάτων.
- Προστασία των εργαλείων επιθεώρησης πληροφοριακών συστημάτων.
- Συμμόρφωση με πολιτικές ασφάλειας και πρότυπα.

11.7 Διακυβέρνηση – Επικινδυνότητα - Συμμόρφωση

Στις μέρες μας έχει γίνει κατανοητό από τους οργανισμούς ότι οι άξονες Διακυβέρνηση – Επικινδυνότητα – Συμμόρφωση αλληλοσυμπληρώνονται και πρέπει να αντιμετωπίζονται ενιαία. Στη διεθνή βιβλιογραφία αυτοί οι τρεις άξονες αναφέρονται με το ακρωνύμιο GRC (Governance – Risk – Compliance).

Η αντιμετώπιση των εννοιών της εταιρικής διακυβέρνησης, της διαχείρισης επικινδυνότητας και της κανονιστικής συμμόρφωσης ως ένα ενιαίο σύνολο, αποτελεί πλέον απαίτηση στο σύγχρονο επιχειρηματικό περιβάλλον. Οι Racz, Weippl και Seufert διατύπωσαν τον ακόλουθο ορισμό για το τρίπτυχο GRC: «είναι μία ολοκληρωμένη, ολιστική προσέγγιση σε επίπεδο εταιρικής διακυβέρνησης, επικινδυνότητας και συμμόρφωσης που εξασφαλίζει ότι ολόκληρος ο οργανισμός δρα ηθικά και σύμφωνα με το αποδεκτό επίπεδο ανάληψης επικινδυνότητας, τις εσωτερικές πολιτικές και τους εξωτερικούς κανονισμούς, δια μέσου της ευθυγράμμισης των στρατηγικών, των διαδικασιών, της τεχνολογίας και των ανθρώπων, βελτιώνοντας έτσι την αποδοτικότητα και την αποτελεσματικότητα της επιχείρησης.». Από τον παραπάνω ορισμό προκύπτει το πλαίσιο αναφοράς ενιαίας διαχείρισης GRC, που αποτυπώνεται στην ακόλουθη Εικόνα 11.4.

Εικόνα 11.4 *Πλαίσιο αναφοράς GRC.*

Υπάρχουν ολοκληρωμένες λύσεις και εξειδικευμένο λογισμικό GRC, που ικανοποιεί την ανάγκη αυτοματοποίησης των σχετικών ελέγχων. Η αυτοματοποίηση των διαδικασιών διευκολύνει τη συμμόρφωση των σύγχρονων επιχειρήσεων με το εκάστοτε ρυθμιστικό πλαίσιο, τη διενέργεια εσωτερικών ελέγχων, την αποτελεσματικότητα των ελέγχων, ενώ ταυτόχρονα καθιστά ευκολότερο τον εντοπισμό των απειλών.

Βιβλιογραφία

Blyth, M. (2008). Risk and security management: protecting people and sites worldwide. Hoboken, N.J: John Wiley & Sons.

Dhillon, G. (Ed.). (2001). Information security management: global challenges in the new millennium. Hershey, PA: Idea Group Pub.

Fay, J. (2011). Contemporary security management (3rd ed). Burlington, MA: Butterworth-Heinemann.

Initiative, J. T. F. T. (2011). SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg, MD, United States: National Institute of Standards & Technology.

ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management. (n.d.). Retrieved 30 September 2015, from

NIST Computer Security Resource Center. (n.d.). Retrieved 30 September 2015, from http://csrc.nist.gov/

Ortmeier, P. J. (2002). Security management: an introduction. Upper Saddle River, NJ: Prentice Hall.

Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in Computing (3rd ed.). Prentice Hall Professional Technical Reference.

Racz, N., Panitz, J., Amberg, M., Weippl, E., & Seufert, A. (2010). Governance, risk & compliance (grc) status quo and software use: Results from a survey among large enterprises. Governance, 1, 1–2010.

Sennewald, C. A. (2011). Effective security management (5th ed). Burlington, MA: Butterworth-Heinemann.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). SP 800-30. Risk Management Guide for Information Technology Systems. Gaithersburg, MD, United States: National Institute of Standards & Technology.

Tarantino, A. (Ed.). (2008). Governance, risk, and compliance handbook: technology, finance, environmental, and international guidance and best practices. Hoboken, N.J: John Wiley & Sons.

Tipton, H. F., & Nozaki, M. K. (Eds.). (2007). Information security management handbook (6th ed). Boca Raton: Auerbach Publications.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποιο από τα παρακάτω ανήκει σε ένα Πληροφοριακό Σύστημα:
α) άνθρωποι
β) λογισμικό
γ) υλικό
δ) όλα τα παραπάνω

2. Μια απειλή:
α) προκαλεί πάντα επιπτώσεις.
β) μπορεί να εκμεταλλευτεί μια ευπάθεια.
γ) προκαλεί πάντα ζημιά.
δ) ανιχνεύεται σε ένα αγαθό.

3. Η ονομασία PDCA σημαίνει:

α) Plan - Do - Check -Act
β) Plan - Design - Check - Act
γ) People - Do - Check - Act
δ) Plan - Direct - Computer - Action

4. Η οικογένεια προτύπων ISO/IEC 27K στηρίχτηκε στη συλλογή προτύπων:
α) DIN.
β) BSI.
γ) BS.
δ) IEC.

5. Ποιο είναι το κεντρικό πρότυπο της οικογένειας προτύπων 27K;
α) 27000
β) 27001
γ) 27100
δ) 27010

6. Τι σημαίνουν τα αρχικά ΣΔΑΠ;
α) Σωστή Διαχείριση Ασφάλειας Πληροφοριών
β) Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
γ) Σωστή Διαχείριση Ασφάλειας Πληροφορικής
δ) κανένα από τα παραπάνω

7. Ποια από τις παρακάτω είναι μεθοδολογία εκτίμησης επικινδυνότητας;
α) COBIT
β) OCTAVE
γ) FRIM
δ) FIRM

8. Πόσα στάδια έχει η μεθοδολογία NIST;
α) 6
β) 7
γ) 8
δ) 9

9. Ποιος όρος δεν ανήκει στο GRC;
α) Governance
β) Government
γ) Risk
δ) Compliance

10. Ποιο πρότυπο της οικογένειας ISO/IEC 27K χρησιμοποιείται κατά τη διαδικασία διαπίστευσης;
α) 27001
β) 27006
γ) 27600
δ) κανένα από τα παραπάνω

Κεφάλαιο 12. Απόκριση σε Συμβάντα Ασφάλειας & Digital Forensics

Σύνοψη
*Στο χώρο των τεχνολογιών πληροφορίας και επικοινωνιών (ΤΠΕ) εκδηλώνονται καθημερινά συμβάντα (αν)ασφάλειας, συνήθως από μη εξουσιοδοτημένους χρήστες, οι οποίοι αποκτούν πρόσβαση σε πόρους πληροφοριακών συστημάτων, παραβιάζοντας με αυτό τον τρόπο τα θεμελιώδη χαρακτηριστικά της ασφάλειας πληροφοριών: την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Μια τέτοια ακολουθία γεγονότων, από την πλευρά του ερευνητή της ασφάλειας πληροφοριών, ξεκινάει με την ανίχνευση της εισβολής. Στη συνέχεια, ο ερευνητής πρέπει να διαχειριστεί το συμβάν ασφάλειας με κατάλληλες ενέργειες. Οι ενέργειες αυτές, οι γενικότερες πρακτικές που ακολουθούνται, καθώς και οι σχετικές μέθοδοι και τεχνικές, ορίζουν το γνωστικό πεδίο που ονομάζεται Απόκριση σε Συμβάντα Ασφάλειας (*Incident Response*). Το επόμενο βήμα σε αυτή την αλληλουχία ενεργειών του ερευνητή ασφάλειας, εφόσον ορίζεται στο Σχέδιο Ασφάλειας του οργανισμού, είναι η μετέπειτα και σε βάθος διερεύνηση του συμβάντος με σκοπό τη συλλογή και επεξεργασία πληροφοριών έτσι ώστε να εντοπιστούν τα απαραίτητα πειστήρια (αποδείξεις) τα οποία θα τον βοηθήσουν να καταλήξει σε συμπεράσματα σχετικά με τον επιτιθέμενο, τη ζημία που δημιουργήθηκε καθώς και το αντίκτυπο της επίθεσης. Αυτό το τελευταίο στάδιο ορίζει το πεδίο της Ψηφιακής Εγκληματολογίας (*Digital Forensics*).*

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1), γνώση εννοιών ασφαλούς διασύνδεσης (Κεφ. 3) καθώς και γνώση βασικών εννοιών κρυπτογραφίας (Κεφ. 6)

12.1 Συμβάντα Ασφάλειας

12.1.1 Εισαγωγή

Το Διαδίκτυο έχει γίνει ένα από τα περισσότερο ευρέως διαθέσιμα δίκτυα επικοινωνιών, με αποτέλεσμα την ολοένα και μεγαλύτερη εξάπλωση της χρήσης του σε καθημερινές αλλά και κρίσιμες εφαρμογές. Κυβερνήσεις, επιχειρήσεις, τράπεζες, και πανεπιστήμια πραγματοποιούν καθημερινά μεγάλο όγκο των δραστηριοτήτων τους μέσω του Διαδικτύου. Με μια τέτοια ευρεία χρήση, τα δεδομένα που διακινούνται μέσω του Διαδικτύου ποικίλλουν, από προσωπική αλληλογραφία, τραπεζικές και χρηματιστηριακές συναλλαγές, ιατρικά αρχεία μέχρι και δεδομένα βιομηχανικής παραγωγής.

Η πρόσβαση στο Διαδίκτυο είναι εύκολη και ευρέως διαθέσιμη. Ωστόσο, τα υπολογιστικά συστήματα (προσωπικοί υπολογιστές, υπολογιστές χειρός κ.ά.) που συνδέονται σε αυτό, απαιτείται να διαθέτουν ορθή παραμετροποίηση της λειτουργίας τους, κάτι το οποίο εισάγει επιπλέον πολυπλοκότητα στη διαχείριση των παραμέτρων ασφαλείας τους. Ως αποτέλεσμα, τα πλεονεκτήματα του Διαδικτύου μπορεί σε ορισμένες περιπτώσεις να μετατρέπονται σε μειονεκτήματα, καθώς επιτρέπεται η πρόσβαση σε πληροφοριακούς πόρους χωρίς καν να απαιτείται η φυσική παρουσία των χρηστών στο χώρο του κάθε υπολογιστικού συστήματος. Επιπλέον, αρκετά από τα υποκείμενα πρωτόκολλα δικτύου, που υποστηρίζουν την επικοινωνία στο Διαδίκτυο, δεν είναι ασφαλή, ενώ λίγες εφαρμογές κάνουν σωστή χρήση των μηχανισμών προστασίας που είναι σήμερα διαθέσιμοι. Ο συνδυασμός της διαθεσιμότητας υπολογιστικών πόρων μέσω του Διαδικτύου, σε συνδυασμό με τις δυσκολίες στην παραμετροποίηση των μηχανισμών προστασίας τους, δημιουργούν τις προϋποθέσεις για ευάλωτα πληροφοριακά συστήματα που αποτελούν στόχους διαδικτυακών επιθέσεων. Οι αυτοματοποιημένες λύσεις ασφάλειας δεν επαρκούν και σε καμία περίπτωση δεν μπορούν να υποκαταστήσουν την ανθρώπινη παρουσία και νοημοσύνη. Για το λόγο αυτό, ομάδες ειδικών επιστημόνων στον τομέα της ασφάλειας πληροφοριών συγκροτούνται με σκοπό την πρόληψη και προστασία των κρίσιμων τεχνολογικών υποδομών των οργανισμών ή ολόκληρων κρατών.

Όπως είδαμε σε προηγούμενο κεφάλαιο, η εισβολή ενός μη εξουσιοδοτημένου χρήστη μπορεί να εκδηλωθεί, είτε σε κάποιο κόμβο ενός δικτύου (υπολογιστικό σύστημα), επηρεάζοντας τη λειτουργία των υπηρεσιών που προσφέρει, είτε σε ένα ολόκληρο δίκτυο υπολογιστικών συστημάτων. Η εισβολή στο δίκτυο

επηρεάζει υπηρεσίες οι οποίες προσφέρονται δικτυακά μεταξύ των κόμβων του δικτύου (π.χ. διαμοιρασμός αρχείων, υπηρεσίες ιστού κ.ά.).

Μια πρώτη γραμμή άμυνας ενός οργανισμού αποτελούν οι μηχανισμοί ελέγχου πρόσβασης (π.χ. firewalls, ACL, κ.ά.), καθώς και τα συστήματα ανίχνευσης εισβολών (όπως αυτά έχουν περιγραφεί σε προηγούμενο κεφάλαιο). Ωστόσο, η προστασία των αγαθών δεν είναι πάντα εξασφαλισμένη και αργά ή γρήγορα μπορεί να παρουσιαστεί κάποιο ρήγμα ασφάλειας. Σε μια τέτοια περίπτωση, ο οργανισμός είναι υποχρεωμένος να αντιμετωπίσει το ενδεχόμενο συμβάν ασφάλειας, μετά την ανίχνευσή του. Η αντιμετώπιση των συμβάντων ασφάλειας, συνήθως αποτελεί το αντικείμενο εργασίας και έρευνας μιας ειδικής ομάδας, που είναι αφοσιωμένη στο σκοπό αυτό και ονομάζεται CSIRT (Computer Security Incident Response Team) ή εναλλακτικά, CERT (Computer Emergency Response Team).

Η συστηματική διερεύνηση υπολογιστών με ασφαλή ανάκτηση και ανάλυση ψηφιακών δεδομένων ή ψηφιακή εγκληματολογία, όπως είναι επίσης γνωστή, είναι ένας σύγχρονος τομέας που εξελίσσεται ταχύτατα και σχετίζεται άμεσα με τον τομέα της ασφάλειας πληροφοριών. Στη διεθνή βιβλιογραφία συναντάται με τους όρους Computer Forensics, Digital Forensics, κ.ά. Αντικείμενό της είναι η έρευνα και ανάλυση των ψηφιακών δεδομένων ενός υπολογιστικού συστήματος ή δικτύου με σκοπό την εξαγωγή αδιαμφισβήτητων, αδιάβλητων και έγκυρων νομικά αποδεικτικών στοιχείων. Σε αυτό περιλαμβάνεται και η μελέτη ειδικών προβλημάτων ασφάλειας, όπως οι τεχνικές ανάκτησης και ανάλυσης πληροφοριακών στοιχείων από οποιοδήποτε μέσο αποθήκευσης, διακίνησης και επεξεργασίας δεδομένων, καθώς επίσης η αναλυτική διερεύνηση των ενεργειών που πραγματοποιούνται στο υπολογιστικό σύστημα. Η διαδικασία αναλυτικής διερεύνησης (ανάκτησης και ανάλυσης) ψηφιακών δεδομένων μπορεί, συνεπώς, να οριστεί ως μια συστηματική διαδικασία συλλογής, επεξεργασίας και αναλυτικής διερεύνησης αποδεικτικών στοιχείων, βασισμένη στα ψηφιακά δεδομένα που βρίσκονται σε υπολογιστές, στο Διαδίκτυο, καθώς και σε άλλο σχετικό τεχνικό εξοπλισμό και συσκευές. Η ανάκτηση και ανάλυση των αποδεικτικών στοιχείων γίνεται με βάση αυστηρούς κανόνες και πραγματοποιείται με την βοήθεια ειδικού εξοπλισμού (hardware) και λογισμικού (software).

Η ραγδαία εξάπλωση της χρήσης των υπολογιστών σε όλο και περισσότερους τομείς της σημερινής κοινωνικής και οικονομικής ζωής, αναδεικνύει ολοένα και περισσότερο τη σημασία αυτής της επιστημονικής περιοχής, ενώ η ανάγκη ύπαρξης και βελτίωσής της γίνεται ολοένα και πιο αισθητή. Η χρησιμότητά της δεν περιορίζεται όμως μόνο στην εξαγωγή αδιαμφισβήτητων, αδιάβλητων και έγκυρων νομικά αποδεικτικών στοιχείων. Οι σχετικές τεχνικές ανάκτησης δεδομένων διευκολύνουν επίσης την επίλυση καθημερινών ζητημάτων που ολοένα και περισσότερο επηρεάζουν την καθημερινή ζωή των χρηστών, όπως η εύρεση χαμένων συνθηματικών ή η αποκατάσταση κατεστραμμένων σκληρών δίσκων ή άλλων μέσων αποθήκευσης δεδομένων. Όσο πιο πολύ λοιπόν εξελίσσεται και ενδυναμώνεται η επιστήμη αυτή απέναντι στις νέες απειλές, τα νέα προβλήματα, αλλά και τις νέες μεθόδους των κακόβουλων χρηστών, τόσο πιο ήσυχος νιώθει ο κάθε νόμιμος χρήστης.

12.1.2 CSIRT

12.1.2.1 Υφιστάμενη κατάσταση

Οι Ομάδες Αντιμετώπισης Συμβάντων Ασφάλειας (ΟΑΣΑ) αποτελούν κρίσιμο παράγοντα στον τομέα της ασφάλειας πληροφοριακών συστημάτων και για το λόγο αυτό έχουν ιδρυθεί οργανισμοί σε ευρωπαϊκό αλλά και παγκόσμιο επίπεδο οι οποίοι προσφέρουν υποστήριξη στο έργο τους.

Το 2004 με Ευρωπαϊκό Κανονισμό (ΕΚ 460/2004) δημιουργήθηκε ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA, European Union for Network and Information Security) με σκοπούς:

- Να υποστηρίζει τις διάφορες κοινότητες ασφάλειας στην Ευρώπη (CSIRT/CERT, WARP κτλ.).
- Να παρέχει συμβουλές στα κράτη μέλη της ΕΕ σε ζητήματα ασφάλειας.
- Να υποστηρίζει τη δημιουργία νέων ομάδων CSIRT.

Ο οργανισμός FIRST (Forum of Incident Response and Security Teams) υποστηρίζει τις ομάδες CSIRT αλλά και τις ομάδες ασφάλειας σε ολόκληρο τον κόσμο. Ο οργανισμός FIRST περιλαμβάνει σήμερα περισσότερα από 200 μέλη σε 40 και πλέον χώρες. Ταυτόχρονα, υπάρχουν ερευνητικά και εκπαιδευτικά δίκτυα συνεργασίας τα οποία προωθούν το αντικείμενο μελέτης της αντιμετώπισης συμβάντων ασφάλειας. Ο Πανευρωπαϊκός Σύνδεσμος Συνεργασίας Ερευνητικών και Εκπαιδευτικών Ιδρυμάτων (TERENA – Trans-European Research and Education Networking Association) προσφέρει ένα φόρουμ συνεργασίας, καινοτομίας και διαμοιρασμού των γνώσεων των διαφόρων ιδρυμάτων, με σκοπό να προωθήσει την ανάπτυξη της τεχνολογίας του Διαδικτύου, καθώς και να υποστηρίξει τις σχετικές υποδομές και υπηρεσίες που χρησιμοποιούνται από την ερευνητική και εκπαιδευτική κοινότητα. Η υπηρεσία Trusted Introducer (TI) - ιδρύθηκε από την ευρωπαϊκή κοινότητα CERT το 2000 για την αντιμετώπιση των κοινών αναγκών και για την οικοδόμηση μιας υποδομής υπηρεσιών που θα παρέχει ζωτικής σημασίας υποστήριξη προς όλες τις ομάδες αντιμετώπισης συμβάντων ασφάλειας. Η υπηρεσία Trusted Introducer αποτελεί μια αξιόπιστη ραχοκοκαλιά των υπηρεσιών υποδομής και λειτουργεί ως κέντρο πληροφόρησης για όλες τις ομάδες αντιμετώπισης συμβάντων ασφάλειας. Ακόμη, διατηρεί κατάλογο αναγνωρισμένων ομάδων, ενώ ελέγχει και πιστοποιεί διαρκώς τις ομάδες αυτές καταδεικνύοντας το επίπεδο ωριμότητάς τους. Οι ομάδες CSIRT κατηγοριοποιούνται σε 3 κατηγορίες ανάλογα με το επίπεδο ωριμότητάς τους. Οι κατηγορίες αυτές είναι:

- Καταχωρημένη (Listed).
- Διαπιστευμένη (Accredited).
- Certified (Πιστοποιημένη).

12.1.2.2 Ομάδες CSIRT

Μια ομάδα CSIRT (Computer Security Incident Response Team) είναι μία ομάδα ειδικών στην ασφάλεια πληροφοριών, η κύρια δραστηριότητα των οποίων είναι να αντιμετωπίζουν συμβάντα ασφάλειας σε πληροφοριακά συστήματα. Μια ομάδα CSIRT παρέχει:

- Μια οργανωμένη και δομημένη προσέγγιση για την αντιμετώπιση συμβάντων ασφάλειας πληροφοριακών συστημάτων.

- Τις απαραίτητες υπηρεσίες για την αντιμετώπισή τους, καθώς και την υποστήριξη των μελών της κοινότητας αποδεκτών (χρηστών) ώστε να ξεπερνούν τις διάφορες παραβιάσεις ασφάλειας.

- Προληπτικές υπηρεσίες ασφάλειας, όπως συναγερμούς.

- Συμβουλές ασφάλειας και εκπαίδευση (έκδοση συμβουλευτικών αναφορών για αδυναμίες λογισμικού, κενά ασφάλειας, εμφάνιση ιών κτλ.).

- Υπηρεσίες διαχείρισης ασφάλειας πληροφοριών.

Η ομάδα CSIRT συνεπικουρείται από συστήματα (εξοπλισμό και λογισμικό) ειδικού σκοπού, με τα οποία πραγματοποιείται η συλλογή και επεξεργασία των απαραίτητων δεδομένων. Στα οφέλη, από την ύπαρξη μιας ομάδας CSIRT στο πλαίσιο ενός οργανισμού, συμπεριλαμβάνονται μεταξύ άλλων:

- Η μείωση των πιθανών επιπτώσεων και η προστασία πολύτιμων πόρων πληροφοριακών συστημάτων.

- Η ύπαρξη κεντρικού συντονισμού για ζητήματα ασφάλειας πληροφοριακών συστημάτων εντός του οργανισμού (Point of Contact, PoC).

- Η κεντρική και εξειδικευμένη αντιμετώπιση και απόκριση σε συμβάντα ασφάλειας πληροφοριακών συστημάτων.

- Η ύπαρξη διαθέσιμων ειδικών για την υποστήριξη και την υποβοήθηση των μελών της κοινότητας αποδεκτών (χρηστών) ώστε να ανακάμπτουν γρήγορα μετά από συμβάντα ασφάλειας.

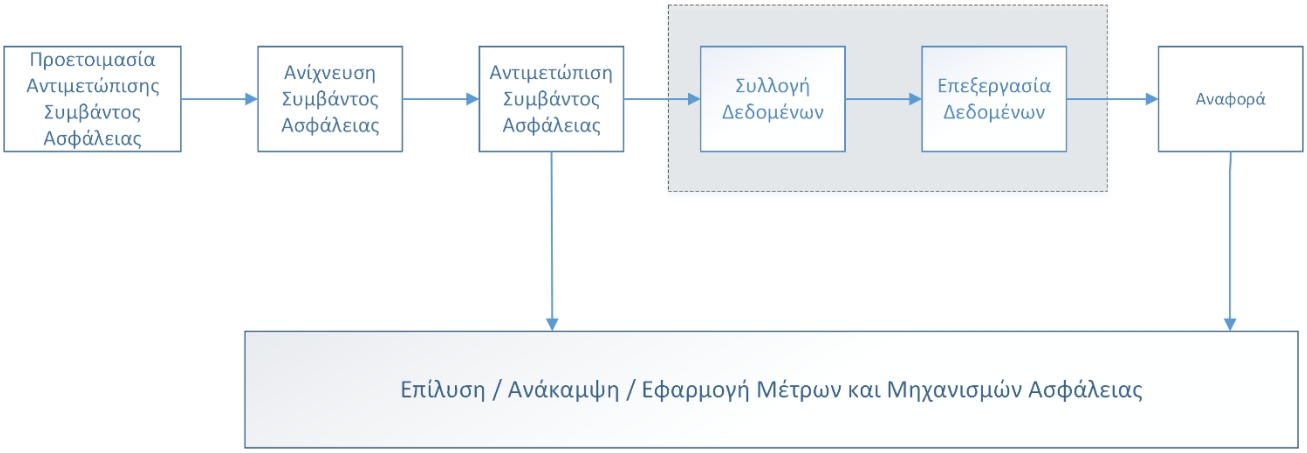
- Η παροχή αποδεικτικών στοιχείων σε περίπτωση δικαστικών ενεργειών.

- Η παρακολούθηση εξελίξεων στον τομέα της ασφάλειας πληροφοριών.

- Η τόνωση της συνεργασίας μεταξύ των μελών της κοινότητας αποδεκτών για θέματα ασφάλειας πληροφοριών (ενίσχυση ευαισθητοποίησης).

12.1.3 Μεθοδολογία αντιμετώπισης συμβάντων ασφάλειας

Μια ομάδα αντιμετώπισης συμβάντων ασφάλειας μελετάει διαρκώς και για αυτό γνωρίζει την πληροφοριακή υποδομή του οργανισμού τον οποίο υποστηρίζει. Επιπλέον, έχοντας ως δεδομένο ότι θα συμβεί αργά ή γρήγορα κάποιο συμβάν ασφάλειας, έχει στη διάθεση της το χρόνο και τις γνώσεις για να υλοποιήσει έγκαιρα ένα σχέδιο στη βάση του οποίου θα πραγματοποιηθούν οι κατάλληλες ενέργειες, εάν και όταν παραστεί η ανάγκη αντιμετώπισης ενός συμβάντος ασφάλειας. Οι ενέργειες αυτές διαφέρουν από οργανισμό σε οργανισμό, καθώς οι παράγοντες που καθορίζουν την αντιμετώπιση σχετίζονται με λεπτομέρειες που αφορούν τόσο την πληροφοριακή υποδομή του, όσο και τις προσφερόμενες υπηρεσίες. Ωστόσο, μπορούμε να περιγράψουμε μια γενική μεθοδολογία η οποία περικλείει τα βασικά στάδια στα οποία διαχωρίζονται οι ενέργειες αντιμετώπισης συμβάντων ασφάλειας. Τα στάδια μιας τέτοιας μεθοδολογίας παρουσιάζονται στην ακόλουθη Εικόνα 12.1, όπου τα σκιασμένα στάδια αφορούν το πεδίο της Ψηφιακής Εγκληματολογίας.



Εικόνα 12.1 *Μεθοδολογία Αντιμετώπισης Συμβάντων Ασφάλειας.*

12.1.3.1 Προετοιμασία αντιμετώπισης συμβάντος ασφάλειας

Προφανώς, είναι απαραίτητες οι ενέργειες προετοιμασίας και διαμόρφωσης των συνθηκών για «κατάλληλη υποδοχή» του πιθανού εισβολέα και για αποφυγή ή κατά το δυνατό μείωση του αντίκτυπου των κακόβουλων πράξεών του. Η προετοιμασία εξαρτάται από την πληροφοριακή υποδομή που υποστηρίζει η ομάδα CSIRT και είναι πιθανό να ποικίλουν οι ενέργειες που θα επιλεγούν.

Αρχικά, θα πρέπει να εγκατασταθεί κατάλληλο λογισμικό το οποίο θα προστατεύει το λειτουργικό σύστημα (π.χ. Antivirus, Antimalware), όσο και λογισμικό το οποίο θα προστατεύει τις δικτυακές συνδέσεις του υπολογιστικού συστήματος (π.χ. Firewall). Με τη βοήθεια παρόμοιου λογισμικού θα πραγματοποιηθεί σε επόμενο στάδιο η συλλογή των στοιχείων, τα οποία θα μας οδηγήσουν σε ασφαλή συμπεράσματα σχετικά με την παραβίαση που εκδηλώθηκε.

Η εγκατάσταση ενός συστήματος ανίχνευσης εισβολών (Intrusion Detection System, IDS) θεωρείται απαραίτητη προκειμένου να προειδοποιήσει έγκαιρα (όσο είναι εφικτό και αναλόγως της τεχνολογίας

ανίχνευσης) και να δώσει μια καλή εικόνα για τη δικτυακή δραστηριότητα που λαμβάνει χώρα στο δίκτυο του οργανισμού. Το σύστημα ανίχνευσης εισβολών είναι καλό να ακολουθεί την αρχιτεκτονική πελάτη/εξυπηρετητή (client/server), ώστε κάθε υπολογιστικός κόμβος να αποτελεί αισθητήρα (sensor) του συνολικού συστήματος ανίχνευσης.

Μια ακόμη καλή πρακτική προς την κατεύθυνση της σωστής και ολοκληρωμένης προετοιμασίας, είναι η ενημέρωση και εκπαίδευση των χρηστών των υπολογιστικών συστημάτων. Η σύνταξη μιας πολιτικής η οποία θα αποτελεί μέρος του γενικότερου σχεδίου ασφάλειας του οργανισμού και η οποία θα περιγράφει λεπτομερώς τις ενέργειες των χρηστών στην περίπτωση που αντιληφθούν παραβίαση της ασφάλειας του πληροφοριακού συστήματος, καθιστά ενεργούς τους χρήστες, πολλαπλασιάζοντας έτσι την ισχύ της ομάδας CSIRT.

Στα πλαίσια μιας ανάλογης πολιτικής θα πρέπει να ανήκει και ο περιοδικός έλεγχος ευπαθειών (vulnerability assessment), ώστε να ελαχιστοποιούνται τα περιθώρια που θα μπορούσε να εκμεταλλευτεί ένας κακόβουλος χρήστης για να προκαλέσει ρήγματα ασφάλειας. Η ενημέρωση των σχετικών αναβαθμίσεων του λογισμικού των υπολογιστικών συστημάτων, καθώς και μία συντονισμένη πολιτική δημιουργίας και συντήρησης αντιγράφων ασφαλείας (backups) βοηθάει ώστε να έχουμε κατάλληλα προετοιμασμένα τα υπολογιστικά συστήματα, ενώ ταυτόχρονα θα μπορούμε σε μικρό χρονικό διάστημα να τα επαναφέρουμε σε λειτουργία, σε περίπτωση περιορισμένης ζημιάς ή καταστροφής των δεδομένων που είναι αποθηκευμένα σε αυτά.

12.1.3.2 Ανίχνευση συμβάντος ασφάλειας

Η ανίχνευση αποτελεί το δεύτερο κατά σειρά ουσιαστικό βήμα στη συνολική αντιμετώπιση συμβάντων ασφάλειας. Οι μηχανισμοί ανίχνευσης περιλαμβάνουν εξοπλισμό, λογισμικό αλλά και ανθρώπινο δυναμικό. Η σπουδαιότητα των τριών αυτών μερών διαφέρει ανάλογα με το είδος του εξοπλισμού που διαθέτουμε, τις λειτουργίες του λογισμικού αλλά και τις ικανότητες και την εκπαίδευση του ανθρώπινου δυναμικού.

Στη «φαρέτρα» των ομάδων αντιμετώπισης συμβάντων ασφάλειας συναντάμε, συνήθως, συστήματα ανίχνευσης/αποτροπής εισβολών (IDS/IPS), ειδικό εξοπλισμό προστασίας (όπως firewall κ.ά.), εκπαιδευμένους τελικούς χρήστες και διαχειριστές συστημάτων (administrators) αλλά και λογισμικό εποπτείας και καταγραφής. Στις πληροφορίες, που συνηθίζεται να συλλέγονται στο στάδιο της ανίχνευσης συμβάντος ασφάλειας, συμπεριλαμβάνονται και οι παρακάτω:

- Ώρα και ημέρα εκδήλωσης του συμβάντος.
- Ποιος κατέγραψε το συμβάν.
- Τι κατέγραψε.
- Κατηγορία συμβάντος (π.χ. δικτυακό, υπολογιστικό κ.ά.).
- Εξοπλισμός ή λογισμικό που εμπλέκεται, κ.ά.

12.1.3.3 Αντιμετώπιση συμβάντος ασφάλειας

Το στάδιο της αντιμετώπισης συμβάντος ασφάλειας ποικίλει ανάλογα με τον οργανισμό στον οποίο εκδηλώθηκε το συμβάν και εξαρτάται από το σχέδιο ασφάλειας που ακολουθείται. Αρκετοί οργανισμοί διαχωρίζουν το στάδιο αυτό σε δύο μικρότερα υποστάδια: αρχική αντιμετώπιση και κυρίως αντιμετώπιση. Στην αρχική αντιμετώπιση, πραγματοποιούνται άμεσα ενέργειες οι οποίες έχουν ως στόχο να ανακόψουν την εισβολή (αν αυτή συνεχίζει να βρίσκεται σε εξέλιξη). Κατά την κύρια αντιμετώπιση αντιμετωπίζεται το συμβάν με «χρονική άνεση», με στόχο την εξακρίβωση των αιτίων εκδήλωσης και την αποτροπή μελλοντικής επανάληψης παρόμοιου συμβάντος.

Στο στάδιο της αντιμετώπισης είναι συνηθισμένη η πρακτική της συνέντευξης με το διαχειριστή συστημάτων, ο οποίος διαθέτει γνώσεις με τις απαραίτητες τεχνικές λεπτομέρειες, ή/και με τον τελικό χρήστη στου οποίου το υπολογιστικό σύστημα εκδηλώθηκε το συμβάν. Σε συνεργασία με τους διαχειριστές δικτύου, αναλύεται επίσης η τοπολογία της δικτυακής υποδομής και μελετώνται τα σχετικά αρχεία καταγραφής που έχουν δημιουργηθεί από τους εμπλεκόμενους μηχανισμούς ασφάλειας. Είναι σημαντικό να επιβεβαιωθεί ότι πραγματικά έχει εκδηλωθεί συμβάν ασφάλειας και δεν έχουμε περίπτωση ψευδούς συναγερμού (false alarm), έτσι ώστε να ανακοπεί άμεσα και η διαδικασία αντιμετώπισης. Κάθε επιμέρους περίπτωση ψευδούς

συναγερμού μπορεί να ενσωματώνεται σε μια γνωσιακή βάση, προκειμένου να μην επαναλαμβάνεται το φαινόμενο.

12.1.3.4 Συλλογή δεδομένων

Το στάδιο της συλλογής δεδομένων καθώς και το επόμενο στάδιο της επεξεργασίας δεδομένων αποτελούν τον κεντρικό άξονα του Digital Forensics, όπως θα δούμε στη συνέχεια. Μια ομάδα αντιμετώπισης συμβάντων ασφάλειας εφαρμόζει τα δύο αυτά στάδια ακόμη και στην περίπτωση που δεν υπάρχει αξιόποινη πράξη, με σκοπό να προστατεύσει τα αγαθά του οργανισμού που εξυπηρετεί.

Το στάδιο της συλλογής των δεδομένων είναι ιδιαίτερα σημαντικό, καθώς σε αυτά θα στηρίξουμε την προσπάθεια εξαγωγής συμπερασμάτων, στη συνέχεια. Αποτελούν στην ουσία, ένα «παράθυρο στο παρελθόν» και μας δίνουν τη δυνατότητα, εικονικά, να μεταφερθούμε στο χρόνο και να πληροφορηθούμε για την αλληλουχία των δραστηριοτήτων που έλαβαν χώρα. Η συλλογή των δεδομένων πρέπει να πραγματοποιείται με τέτοιο τρόπο ώστε τα δεδομένα να αποτελούν εργαλείο προς την κατεύθυνση της εξαγωγής συμπερασμάτων. Δεν είναι όλα τα αρχεία καταγραφής συμβάντων ικανά να μας δώσουν πληροφορίες. Στα περισσότερα λογισμικά υπάρχει δυνατότητα παραμετροποίησης του τρόπου συλλογής των δεδομένων και κάθε ομάδα αντιμετώπισης συμβάντων ακολουθεί το δικό της πρότυπο / τρόπο.

Η ποσότητα των πληροφοριών που συλλέγονται αποτελεί έναν επιπλέον σημαντικό παράγοντα. Στις μέρες μας το φαινόμενο των Μεγάλων Δεδομένων (Big Data) αποτελεί γεγονός, με την έννοια ότι έχουμε στη διάθεσή μας πολύ μεγάλες ποσότητες δεδομένων που ορισμένες φορές η επεξεργασία τους υπερβαίνει τις ικανότητες του εξοπλισμού μας. Σε αυτή την περίπτωση, εφαρμόζονται τεχνικές στατιστικής ανάλυσης έτσι ώστε να ελαχιστοποιείται το απαραίτητο δείγμα μελέτης και να γίνεται εφικτή η επεξεργασία των δεδομένων με πιο αποδοτικές μεθόδους.

Οι πηγές από τις οποίες γίνεται άντληση δεδομένων είναι συνήθως οι παρακάτω:

- Αρχεία καταγραφής IDS/IPS, router, firewall.
- Συστήματα Επίβλεψης Δικτύου (Network Monitoring Systems).
- Αρχεία καταγραφής κεντρικού συστήματος (π.χ. syslog).
- Εξυπηρετητές αυθεντικοποίησης (authentication servers)

Οι πληροφορίες που συλλέγονται περιλαμβάνουν, μεταξύ άλλων, τα ακόλουθα:

- Ημερομηνία και ώρα δραστηριότητας.
- Εφαρμογές που εκτελούνταν.
- Ενεργές δικτυακές συνδέσεις.
- Ανοιχτές θύρες (ports).
- Εφαρμογές που βρίσκονταν σε κατάσταση ακρόασης.
- Κατάσταση δικτυακής διεπαφής σε «αδιάκριτη» λειτουργία (promiscuous mode), κ.ά.

12.1.3.5 Επεξεργασία δεδομένων

Με την επεξεργασία των δεδομένων οδηγούμαστε στην εξαγωγή συμπερασμάτων για το συμβάν ασφάλειας που εκδηλώθηκε. Οι τεχνικές που ακολουθούνται είναι πολλές, αλλά όλες μας βοηθούν ώστε να επιβεβαιώσουμε, καταρχήν, αν πραγματικά πρόκειται για συμβάν ασφάλειας. Μπορούμε, επίσης, να σχηματίσουμε εικόνα σχετικά με την έκταση της παραβίασης (π.χ. πόσα υπολογιστικά συστήματα παραβιάστηκαν ή ποιες ζώνες της δικτυακής τοπολογίας μας επηρεάστηκαν).

Η συνδυαστική ανάλυση με ταυτόχρονη χρήση εξειδικευμένων στατιστικών τεχνικών μπορεί να μας βοηθήσει ώστε να εξακριβώσουμε το είδος της επίθεσης, το πλήθος των επιτιθέμενων, τη γεωγραφική τους τοποθεσία, την ώρα της επίθεσης, καθώς και λεπτομέρειες σχετικά με την μεθοδολογία της επίθεσης (στάδια κλπ.). Επίσης μπορούμε να γνωρίσουμε αρκετές φορές ποια συγκεκριμένα εργαλεία λογισμικού χρησιμοποιήθηκαν προκειμένου να εκμεταλλευτούν οι εισβολείς τις ευπάθειες των υπολογιστικών μας συστημάτων ή της ευρύτερης δικτυακής μας υποδομής. Με προσεκτικότερο έλεγχο μπορούμε ακόμη να

εντοπίσουμε ποια σημεία του σχεδίου ασφάλειας ή συγκεκριμένων πολιτικών μας δεν απέδωσαν ή παραβιάστηκαν, ώστε στο μέλλον να προβούμε σε κατάλληλες βελτιώσεις.

12.1.3.6 Δημιουργία αναφοράς

Το στάδιο της δημιουργίας αναφοράς είναι ιδιαίτερα σημαντικό, καθώς παράγονται έγγραφα που περιγράφουν το συμβάν με τεχνικές λεπτομέρειες και στο μέλλον αποτελούν ένα σημαντικό γνωσιακό πλεονέκτημα για την ασφάλεια πληροφοριών του οργανισμού.

Η σχετική αναφορά πρέπει να είναι ακριβής και λεπτομερής και να μπορεί να υποστηρίξει ακόμη και νομικές διαδικασίες, εφόσον το επιθυμεί ο οργανισμός ή δικαιολογείται από το αξιόποινο των πράξεων των εισβολέων. Ο χρόνος συγγραφής της αναφοράς δεν πρέπει να απέχει χρονικά από την πραγματοποίηση καθενός από τα στάδια της μεθοδολογίας, έτσι ώστε να μην παραληφθεί οποιαδήποτε λεπτομέρεια θα μπορούσε να φανεί χρήσιμη στο μέλλον. Με τον τρόπο αυτό, γίνεται ευκολότερη η επικοινωνία και η πληροφόρηση τρίτων στην περίπτωση που θελήσουμε να ζητήσουμε βοήθεια.

Ο τρόπος συγγραφής πρέπει να είναι ξεκάθαρος χωρίς μεγάλες προτάσεις και να εστιάζει την ουσία των γεγονότων, των ευρημάτων και των ενεργειών μας. Συνηθίζεται να ακολουθείται κάποιο πρότυπο-έντυπο στο οποίο συμπληρώνονται στοιχεία έτσι ώστε να είναι συγκεκριμένη η δομή της καταγραφής και ευκολότερη η ανάγνωση και επεξεργασία του κειμένου.

12.1.3.7 Επίλυση συμβάντος

Όλα τα προηγούμενα στάδια έχουν ως στόχο να φτάσουμε σε ένα σημείο όπου θα μπορέσουμε να επαναφέρουμε το πληροφοριακό σύστημα σε πλήρη λειτουργία και να το προστατέψουμε από άλλη παρόμοια εισβολή. Το έργο της ομάδας αντιμετώπισης συμβάντος είναι κυρίως συμβουλευτικό, καθώς θα πρέπει να προτείνει ένα σύνολο οδηγιών και συμβουλών, οι οποίες στη συνέχεια θα υλοποιηθούν από τα αντίστοιχα τμήματα κατόπιν έγκρισης από τη διοίκηση του οργανισμού.

Το σχέδιο ασφάλειας του οργανισμού θα πρέπει να ορίζει τις προτεραιότητες των ενεργειών σε περίπτωση εκδήλωσης συμβάντος ασφάλειας, ανάμεσα στη γρήγορη ανάκαμψη των υπολογιστικών συστημάτων σε πλήρη λειτουργία, τη συλλογή δεδομένων, τη μείωση του αντίκτυπου, την αποφυγή δημοσιοποίησης της παραβίασης κλπ. Με γνώμονα τις προτεραιότητες του οργανισμού, η ομάδα αντιμετώπισης συμβάντων ασφάλειας οδηγείται στη δημιουργία κατάλληλων προτάσεων επίλυσης των ζητημάτων που προκύπτουν.

Γενικότερα, στο τελικό κείμενο συμπεριλαμβάνονται μεταξύ άλλων τα ακόλουθα:

- Αιτιολόγηση της παραβίασης και προτάσεις μείωσης των ευπαθειών που επέτρεψαν το ρήγμα.
- Προτάσεις νέων πολιτικών ή προσθήκης νέων στοιχείων σε υπάρχουσες.
- Προτάσεις τρόπου επαναφοράς των υπολογιστικών συστημάτων σε πλήρη λειτουργική κατάσταση.
- Δημιουργία κατάλληλων μηχανισμών ελέγχου πρόσβασης (π.χ. Λιστών Ελέγχου Πρόσβασης
- Access Control Lists, ACLs) στους δικτυακούς και υπολογιστικούς πόρους.
- Καταμερισμός ευθυνών σε ανθρώπινο δυναμικό (αν υπάρχουν λόγοι).
- Καταμερισμός απαραίτητων εργασιών σε επιμέρους τμήματα του οργανισμού.
- Τρόποι παρακολούθησης της εξέλιξης των προτάσεων και των εργασιών υλοποίησης.
- Τρόποι επαλήθευσης και επιβεβαίωσης της ορθότητας των προτάσεων επίλυσης.

12.1.4 Εργαλεία αντιμετώπισης συμβάντων ασφάλειας

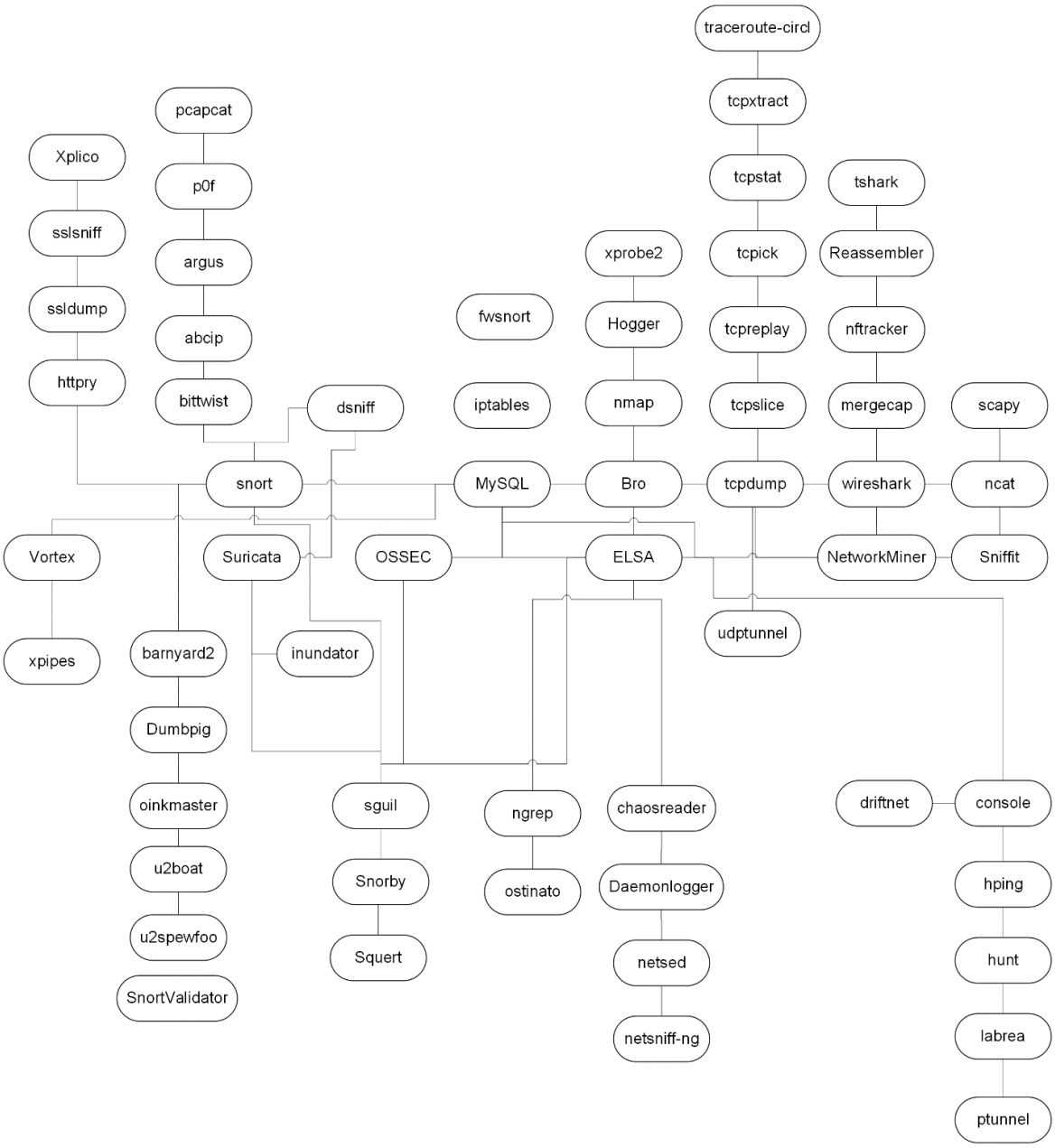
Σε κάθε στάδιο της μεθοδολογίας, μια ομάδα αντιμετώπισης συμβάντων ασφάλειας μπορεί να χρησιμοποιήσει αρκετά εργαλεία λογισμικού προκειμένου να φέρει σε πέρας τις εργασίες της. Η ομάδα μπορεί επίσης να χρησιμοποιήσει έτοιμα προϊόντα λογισμικού ή να συγγράψει κώδικα δημιουργώντας τα δικά της εξειδικευμένα εργαλεία. Στον Πίνακα 12.1, που ακολουθεί, αναφέρονται μερικά τέτοια ενδεικτικά εργαλεία, καθώς και το στάδιο στο οποίο μπορούν να χρησιμοποιηθούν.

Εργαλείο	**Σκοπός**	**Στάδιο**
Συνάρτηση κατακερματισμού.	Δημιουργία συνοψίσεων για κρίσιμα αρχεία του υπολογιστικού συστήματος με σκοπό τη διαφύλαξη της ακεραιότητάς τους.	Προετοιμασία
Audit Logging.	Ενεργοποίηση μηχανισμών καταγραφής μητρώου.	Προετοιμασία
Λογισμικό παρακολούθησης δικτυακής δραστηριότητας.	Εντοπισμός ανωμαλιών συμπεριφοράς δικτυακών κόμβων και υπηρεσιών.	Ανίχνευση
Υπηρεσία σύννεφου με γνωσιακό περιεχόμενο και υπογραφές γνωστών επιθέσεων.	Χρήση πρότερης γνώσης η οποία έχει συσσωρευτεί από περιπτώσεις εκδήλωσης συμβάντων ασφάλειας σε τρίτους παρόμοιους οργανισμούς.	Ανίχνευση
Κανόνες Τείχους Προστασίας.	Βίαιη διακοπή λειτουργίας δικτυακής διεπαφής με σκοπό την προστασία των αγαθών της δικτυακής υποδομής.	Αντιμετώπιση
Λογισμικό δημιουργίας αντιγράφων σκληρών δίσκων.	Δημιουργία αντιγράφου του προσβεβλημένου σκληρού δίσκου με ταυτόχρονη προστασία του αυθεντικού υλικού.	Αντιμετώπιση
Εξυπηρετητής Ιστού και Βάση Δεδομένων.	Αποθήκευση δεδομένων με σκοπό την επεξεργασία τους.	Συλλογή
Υπηρεσία σύννεφου με γνωσιακό περιεχόμενο.	Χρήση πρότερης γνώσης η οποία έχει συσσωρευτεί από περιπτώσεις εκδήλωσης συμβάντων ασφάλειας σε τρίτους παρόμοιους οργανισμούς.	Επεξεργασία
Λογισμικό Στατιστικής Ανάλυσης και δημιουργίας γραφημάτων.	Εξαγωγή συμπερασμάτων για το συμβάν ασφάλειας.	Επεξεργασία
Λογισμικό χρήσης αλγορίθμων τεχνητής νοημοσύνης.	Συνδυαστική ανάλυση των δεδομένων και εξαγωγή συμπερασμάτων στη βάση κατάλληλα επιλεγμένου δείγματος πληροφοριών.	Επεξεργασία
Λογισμικό αυτόματης εξαγωγής στοιχείων και αναφορών.	Γρήγορη εξαγωγή αποτελεσμάτων σε συνεπτυγμένη μορφή με σκοπό τον εμπλουτισμό με λεπτομέρειες από την ομάδα αντιμετώπισης του συμβάντος.	Αναφορά
Λογισμικό εξαγωγής αναφορών σε διαφορετικές μορφές.	Ευελιξία στην ανταλλαγή των δεδομένων και τη δημιουργία αναφορών μεταξύ των τμημάτων	Αναφορά & Επεξεργασία

	του οργανισμού, καθώς και ευκολία στην εισαγωγή τους σε λογισμικό τρίτων κατασκευαστών με σκοπό την παραπέρα επεξεργασία τους.	

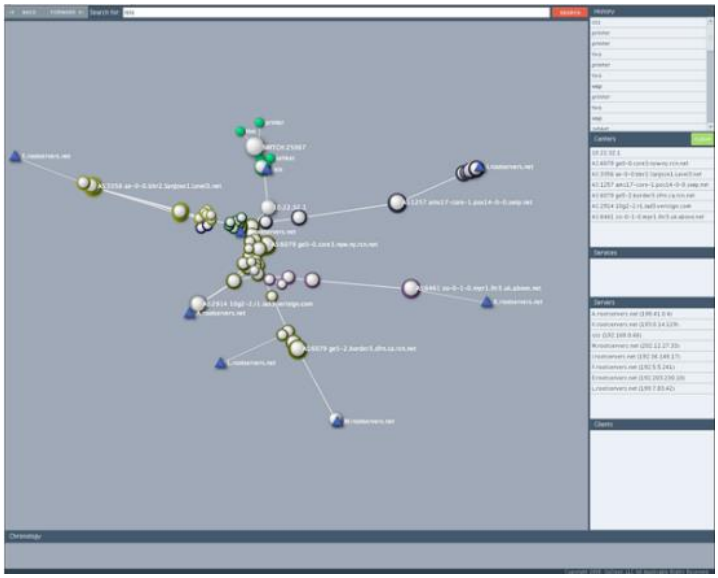
Πίνακας 12.1 *Εργαλεία ομάδας αντιμετώπισης συμβάντων ασφάλειας.*

Στην παρακάτω Εικόνα 12.2, εμφανίζονται προϊόντα λογισμικού ανοιχτού κώδικα, τα οποία αποτελούν ένα μικρό δείγμα, που θεωρείται όμως ως ένα απαραίτητο σετ εργαλείων για μια ομάδα αντιμετώπισης συμβάντος ασφάλειας.

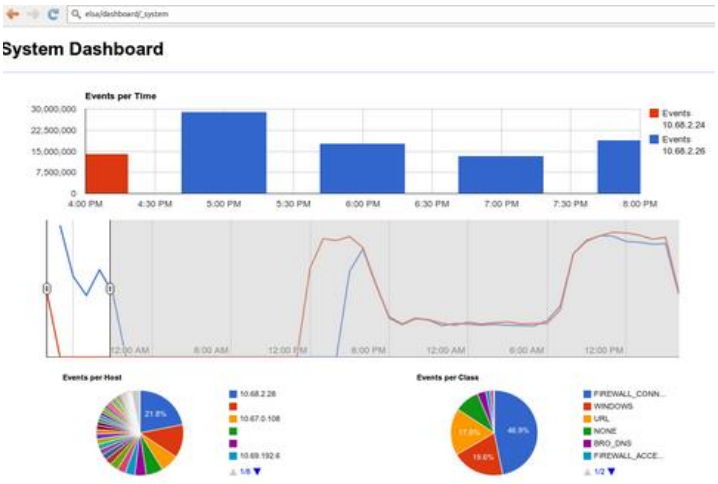


Εικόνα 12.2 *Ελάχιστο απαραίτητο λογισμικό ομάδας CSIRT.*

Στις παρακάτω εικόνες 12.3 έως 12.8 εμφανίζονται δείγματα διεπαφής από μερικά από τα εργαλεία που αναφέρθηκαν παραπάνω:



Εικόνα 12.3 *Argus.*



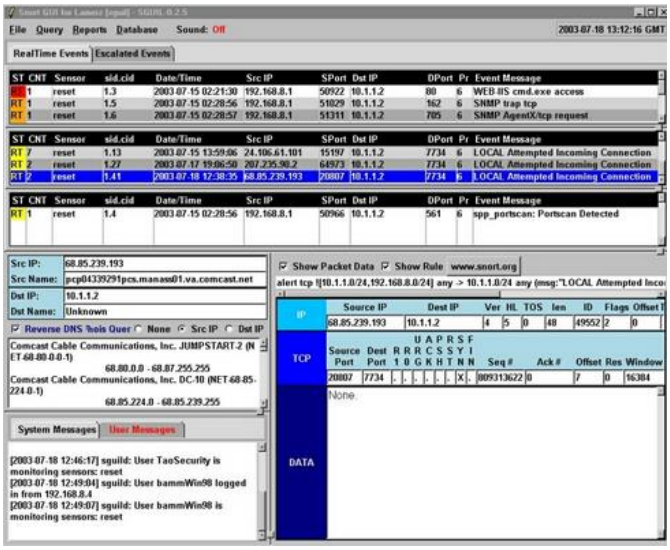
Εικόνα 12.4 *Bro IDS.*

TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• as_html
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• as_html
3.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1367 <-> 192.77.84.99:80	web	374 bytes	• as_html
4.	Sun Nov 16 20:38:24 2003	22 s	192.168.1.3:1369 <-> 192.168.1.1:23	telnet	2047 bytes	• as_html • session_0004.telnet.replay 22 seconds
5.	Sun Nov 16 20:38:28 2003	21 s	192.168.1.3:1364 <-> 192.77.84.99:80	web	361 bytes	• as_html
6.	Sun Nov 16 20:38:48 2003	62 s	192.168.1.3:1370 <-> 192.77.84.99:80	web	13285 bytes	• as_html • session_0006.part_01.html 12610 bytes
7.	Sun Nov 16 20:38:51 2003	61 s	192.168.1.3:1371 <-> 192.77.84.99:80	web	951 bytes	• as_html • session_0007.part_01.gif 258 bytes
8.	Sun Nov 16 20:38:51 2003	61 s	192.168.1.3:1372 <-> 192.77.84.99:80	web	4136 bytes	• as_html • session_0008.part_01.jpeg 3448 bytes
9.	Sun Nov 16 20:38:51 2003	64 s	192.168.1.3:1373 <-> 192.77.84.99:80	web	19442 bytes	• as_html • session_0009.part_01.gif 18746 bytes
10.	Sun Nov 16 20:39:02 2003	16 s	192.168.1.3:1374 <-> 192.168.1.1:21	ftp	1091 bytes	• as_html
11.	Sun Nov 16 20:39:07 2003	0 s	192.168.1.3:1375 <-> 192.168.1.1:20	ftp-data	99 bytes	• session_0011.part_01.ftp-data.data 99 bytes
12.	Sun Nov 16 20:39:08 2003	0 s	192.168.1.3:1376 <-> 192.168.1.1:20	ftp-data	854 bytes	• session_0012.part_01.ftp-data.data 854 bytes
13.	Sun Nov 16 20:39:13 2003	0 s	192.168.1.3:1377 <-> 192.168.1.1:20	ftp-data	11096 bytes	• session_0013.part_01.ftp-data.jpeg 11096 bytes
14.	Sun Nov 16 20:39:16 2003	0 s	192.168.1.3:1378 <-> 192.168.1.1:20	ftp-data	12155 bytes	• session_0014.part_01.ftp-data.gz 12155 bytes
15.	Sun Nov 16 20:39:18 2003	0 s	192.168.1.3:1379 <-> 192.168.1.1:20	ftp-data	516 bytes	• session_0015.part_01.ftp-data.data 516 bytes
16.	Sun Nov 16 20:39:20 2003	0 s	192.168.1.3 -> 192.168.1.1	ICMP	32 bytes	Echo
17.	Sun Nov 16 20:39:20 2003	0 s	192.168.1.1 -> 192.168.1.3	ICMP	32 bytes	Echo Reply

Εικόνα 12.5 *Chaosreader.*

Εικόνα 12.6 *OSSEC.*



Εικόνα 12.7 *Squill.*

Εικόνα 12.8 *Snorby.*

12.2 Digital Forensics

12.2.1 Εισαγωγή

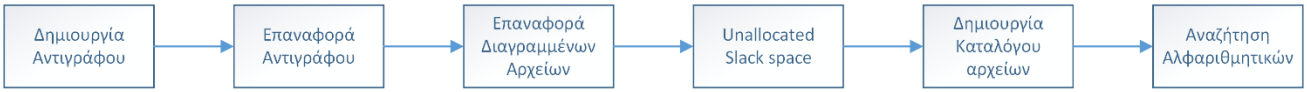
Η ηλεκτρονική εγκληματολογία (digital forensics) είναι ένας αναπτυσσόμενος κλάδος της Πληροφορικής, ο οποίος εντάσσεται στο γενικότερο πλαίσιο της ασφάλειας πληροφοριών και ειδικότερα σχετίζεται μέσω κοινών πρακτικών και εργαλείων με την απόκριση σε συμβάντα ασφάλειας. Ωστόσο, η ειδοποιός διαφορά είναι η πρόσθετη ανάγκη για χρήση των εντοπισμένων πειστηρίων προς νομική υπεράσπιση του οργανισμού ο οποίος υπέστη την εισβολή. Δηλαδή, η έμφαση δίνεται στην προσεκτική άντληση των στοιχείων χωρίς να αλλοιωθεί το πρωτογενές υλικό και στη λεπτομερή ανάλυσή τους, προκειμένου να τεκμηριωθούν τα συμπεράσματα με ακλόνητες αποδείξεις που δεν επιτρέπουν διφορούμενες ερμηνείες.

Πολλοί οργανισμοί δηλώνουν ακόμη και σήμερα άγνοια για το κατά πόσον τα πληροφοριακά τους συστήματα έχουν αποτελέσει αντικείμενο μη εξουσιοδοτημένης χρήσης. Αυτό σημαίνει ότι υπάρχει σημαντική ανάγκη συλλογής και ανάλυσης στοιχείων, ώστε να μπορεί να επιβεβαιωθεί ο ορθός τρόπος χρήσης των συστημάτων, ή με βάση αυτά τα στοιχεία να είναι δυνατή η στοιχειοθέτηση πιθανών δικαστικών διαδικασιών. Μια διαδικασία digital forensics αρχίζει συνήθως στη βάση μιας συγκεκριμένης κατηγορίας για τέλεση αδικήματος. Αυτή η κατηγορία ορίζει, θα λέγαμε, τα όρια της έρευνας που πρόκειται να πραγματοποιηθεί στη συνέχεια. Στην ουσία ορίζει ακόμη και τα επιμέρους βήματα που θα ακολουθηθούν, καθώς και το είδος των αρχείων που θα εξεταστούν. Τα εργαλεία, που μπορούν να χρησιμοποιηθούν, αποτελούνται από μεμονωμένα προϊόντα ή ολοκληρωμένες σουίτες λογισμικού, που είναι αφοσιωμένες στο σκοπό αυτό. Επίσης, αρκετές φορές χρησιμοποιείται εξοπλισμός με τον οποίο γίνεται προσπάθεια επαναφοράς (ανάκτησης) δεδομένων από συσκευές (π.χ. σκληρούς δίσκους) οι οποίες έχουν μερικώς ή ολικώς καταστραφεί (εσκεμμένα ή όχι). Η διαδικασία του digital forensics επιβάλει ορισμένες φορές την παρουσία ενός τουλάχιστον μάρτυρα κατά τη διάρκεια των εργασιών που πραγματοποιούνται ώστε να διασφαλίζεται η νομιμότητα και η εγκυρότητα των στοιχείων που συλλέγονται και πρόκειται να επεξεργαστούν κατόπιν.

Η διαδικασία της ασφαλούς ανάκτησης και ανάλυσης στοιχείων περιλαμβάνει συνήθως δυο φάσεις: την φάση της ανάκτησης (συλλογής), και την φάση της ανάλυσης (έρευνας) των στοιχείων. Για παράδειγμα, μπορεί να περιλαμβάνει διεργασίες όπως:

- Η ασφαλής συλλογή στοιχείων από το πληροφοριακό σύστημα και από διάφορες on-line πηγές στο Internet.
- Η ανάκτηση δεδομένων που σβήστηκαν ή που αλλοιώθηκαν.
- Η ανάκτηση των συνθηματικών (passwords) που χρησιμοποιήθηκαν από μη εξουσιοδοτημένους χρήστες για να πραγματοποιήσουν αλλά και να αποκρύψουν τις πράξεις τους.
- Η τεκμηρίωση πράξεων και λειτουργιών από μη εξουσιοδοτημένους χρήστες.
- Η αναλυτική επεξεργασία αποδεικτικών στοιχείων που συγκεντρώθηκαν.
- Η σύνταξη λεπτομερούς ανάλυσης των στοιχείων της ερευνητικής διαδικασίας ως βάση πορισμάτων για τον αρμόδιο πραγματογνώμονα, κλπ.

Μια τυπική ακολουθία βημάτων, η οποία ακολουθείται συνήθως σε μια διαδικασία digital forensics, εμφανίζεται στην ακόλουθη Εικόνα 12.9. Τα βήματα αυτά περιγράφονται στις ακόλουθες υποενότητες.



Εικόνα 12.9 *Ακολουθία βημάτων digital forensics.*

12.2.2 Δημιουργία αντιγράφου

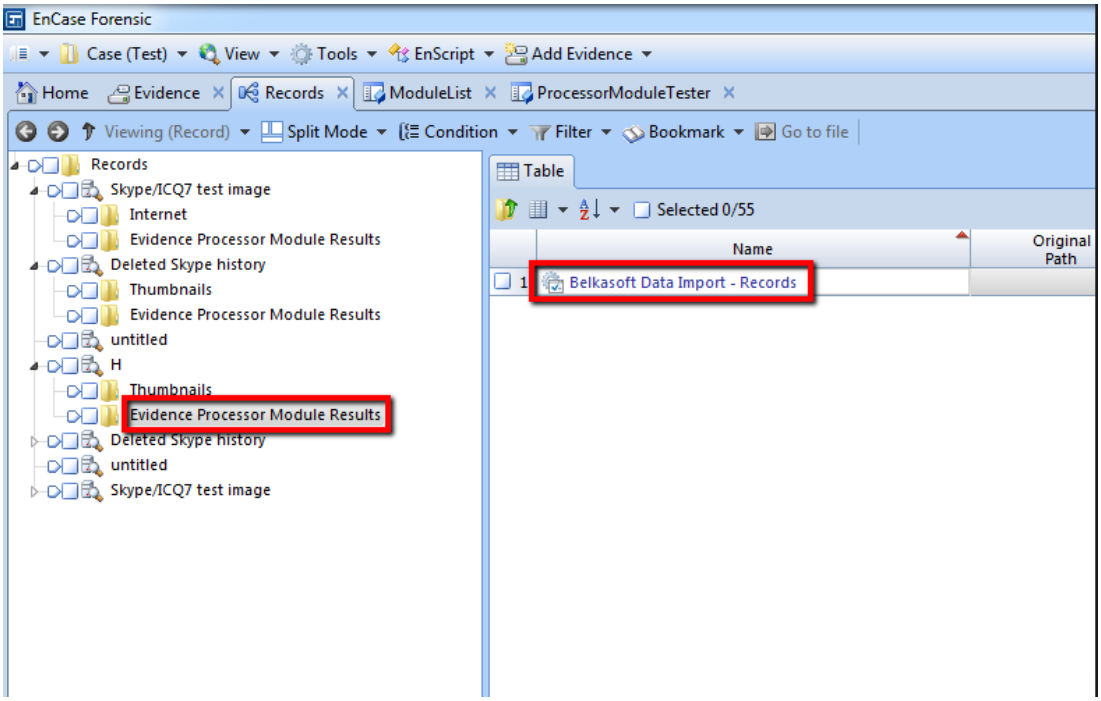
Το πρώτο βήμα είναι από τα σημαντικότερα καθώς πρέπει με προσεκτικό τρόπο να δημιουργηθεί ένα αντίγραφο του μέσου αποθήκευσης, το οποίο περιέχει πιθανά στοιχεία προς εξακρίβωση. Ωστόσο, δεν πρέπει αυτό το μέσο να χρησιμοποιηθεί άμεσα από τον ερευνητή, γιατί κάτι τέτοιο ενέχει τον κίνδυνο καταστροφής του μέσου ή του συστήματος αρχείων που αυτό περιέχει και να χαθεί οριστικά η ευκαιρία ανάκτησης πληροφοριών.

Συνηθίζεται να χρησιμοποιείται ένα δεύτερο μέσο, ίδιας ή μεγαλύτερης χωρητικότητας, για τη δημιουργία αντιγράφου του αρχικού μέσου (π.χ. σκληρός δίσκος). Είναι καλή πρακτική να χρησιμοποιηθεί μέσο του ίδιου κατασκευαστή με το αρχικό μέσο αποθήκευσης, καθώς διαφορές σε τεχνικές λεπτομέρειες κατασκευής μπορεί να οδηγήσουν σε αποτυχία επαναφοράς του αντιγράφου.

Ο ερευνητής μπορεί να χρησιμοποιήσει ένα λειτουργικό σύστημα το οποίο είναι εγκατεστημένο σε CD/DVD ή σε USB stick και να εκκινήσει το σύστημα αφήνοντας με αυτό τον τρόπο μηδενικό αποτύπωμα στο υπό εξέταση υπολογιστικό σύστημα. Η διακοπή της δικτυακής λειτουργίας, επίσης, ελαττώνει τον κίνδυνο να τροποποιηθούν δεδομένα στο σκληρό δίσκο, παρά τη θέληση του ερευνητή.

Το αντίγραφο που δημιουργείται με αυτό τον τρόπο αποκαλείται Αρχείο Αποδεικτικών Στοιχείων (Evidence File) και είναι αυτό το οποίο στη συνέχεια θα επαναφέρει ο ερευνητής σε άλλο αποθηκευτικό μέσο προκειμένου να το διερευνήσει ή θα το εισάγει ως αρχείο εισόδου σε μια εξειδικευμένη σουίτα λογισμικού με εργαλεία εγκληματολογικού ελέγχου.

Στην παρακάτω Εικόνα 12.10, απεικονίζεται ένα Evidence File το οποίο έχει εισαχθεί στο EnCase Forensic, το οποίο αποτελεί μια από τις γνωστότερες σουίτες για digital forensics.



Εικόνα 12.10 *Εισαγωγή Evidence File στο EnCase Forensic.*

Στη συνέχεια, παραθέτουμε τμήμα εντολών για τη χρήση του εργαλείου ddrescue, το οποίο δημιουργεί ακριβές αντίγραφο του δίσκου sda στον δίσκο sdb (όπου sda και sdb τα ονόματα συσκευών των δίσκων στο Linux):

```
## Δημιουργία αντιγράφου ##
ddrescue -f -n /dev/sda /dev/sdb logfile
ddrescue -d -f -r3 /dev/sda /dev/sdb logfile

## Λίστα διαμερισμάτων (partitions) στον sdb ##
fdisk /dev/sdb
```

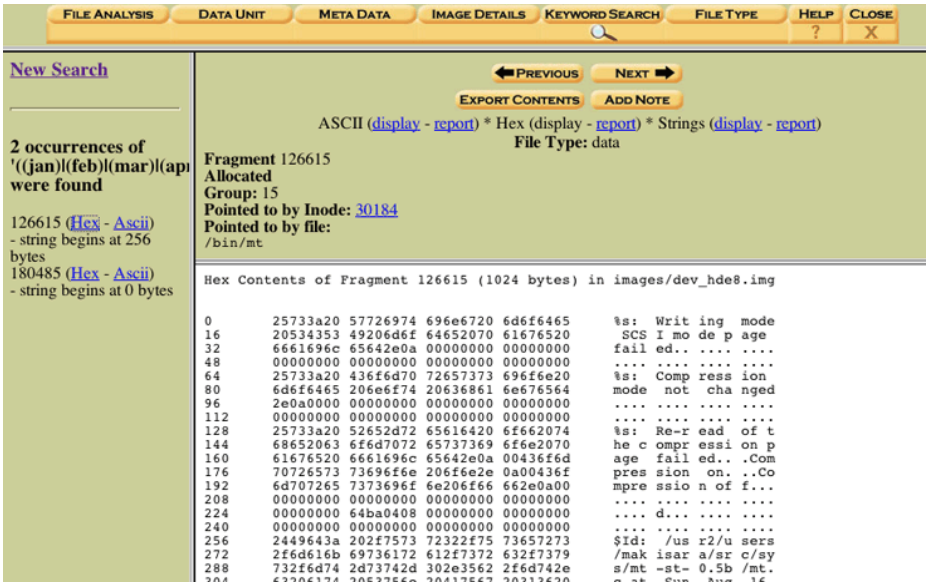
```
## Έλεγχος για λάθη σε κάθε ένα από τα partitions του νέου
δίσκου ##
fsck -v -f /dev/sdb1
fsck -v -f /dev/sdb2
```

12.2.3 Επαναφορά αντιγράφου

Η επαναφορά διαγραμμένων αρχείων διαφέρει ανάλογα με το λειτουργικό σύστημα και το σύστημα αρχείων που χρησιμοποιεί το υπολογιστικό σύστημα που ερευνούμε. Υπάρχουν αρκετά λειτουργικά συστήματα και δεκάδες συστήματα αρχείων, οπότε οι πιθανοί συνδυασμοί είναι πολλαπλάσιοι και πρέπει ο ερευνητής να είναι σε θέση να αναγνωρίζει το υπό χρήση σύστημα αρχείων προκειμένου να αξιοποιήσει με τον καλύτερο τρόπο τα εργαλεία του.

Το λειτουργικό σύστημα Linux είναι σε θέση να αναγνωρίσει τα περισσότερα συστήματα αρχείων (file systems) από κάθε άλλο λειτουργικό σύστημα και για το λόγο αυτό αποτελεί μια από τις συνηθέστερες επιλογές των ερευνητών ηλεκτρονικής εγκληματολογίας. Ενδεικτικά, αναφέρουμε την αναγνώριση των συστημάτων αρχείων FAT12, FAT16, FAT32, NTFS, HPFS, Macintosh, OS/2/, EXT2, EXT3, EXT4, UFS, ReiserFS κ.ά.

Το εργαλείο Autopsy είναι ένα από τα συνηθέστερα εργαλεία ανοιχτού κώδικα που χρησιμοποιείται και για αυτό το σκοπό (Εικόνα 12.11).



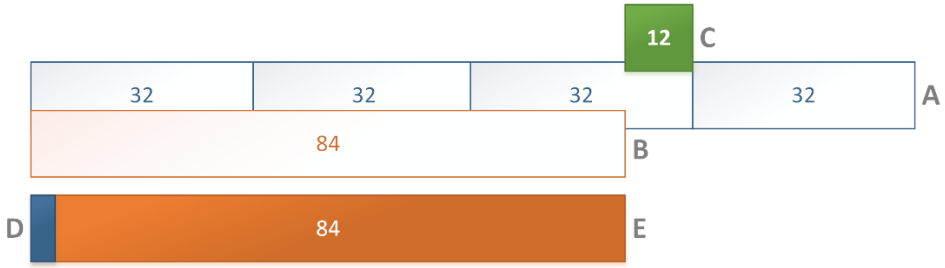
Εικόνα 12.11 *Επαναφορά διαγραμμένου αρχείου με το εργαλείο Autopsy.*

12.2.4 Επαναφορά διαγραμμένων αρχείων

Το μαγνητικό μέσο αποθήκευσης ενός υπολογιστή, χρησιμοποιεί ένα σύστημα αρχείων προκειμένου να ταξινομεί και να διαχειρίζεται τα δεδομένα μας. Τα δεδομένα αυτά αποθηκεύονται στο σκληρό δίσκο με τη μορφή αρχείων. Ολόκληρο το μαγνητικό μέσο, κατά τη διαμόρφωσή του σύμφωνα με το σύστημα αρχείων που θα αναλάβει τη διαχείριση των δεδομένων, έχει τμηματοποιηθεί σε μονάδες δέσμευσης χώρου (allocation unit), γνωστές ως τμήματα (cluster).

Ας υποθέσουμε ότι έχουμε ένα μαγνητικό μέσο με χωρητικότητα (σύμφωνα με το σύστημα αρχείων του) 128KB, ενώ τα τμήματα έχουν μέγεθος 32KB. Έστω ότι θέλουμε να αποθηκεύσουμε ένα αρχείο μεγέθους 84KB. Σε αυτή την περίπτωση, το σύστημα αρχείων θα χρησιμοποιήσει 3 clusters (3 x 32), δεσμεύοντας συνολικά 96KB. Η διαφορά 96 - 84 = 12KB είναι το λεγόμενο slack space (αδιάθετος χώρος). Η παραπάνω υπόθεση χρησιμοποιείται για να γίνει κατανοητή η έννοια του slack space. Αν τώρα επιλέξουμε να διαγράψουμε αυτό το αρχείο των 84KB, τότε το σύστημα αρχείων απλά διαγράφει τα πρώτα bytes του αρχείου στα οποία περιέχονται πληροφορίες του αρχείου (όνομα, μέγεθος, τύπος κλπ.) και στη συνέχεια θεωρεί τον χώρο αυτό

unallocated (ότι είναι διαθέσιμος προς χρήση, πιθανόν για να αποθηκευτεί εκεί ένα αρχείο που θα δημιουργηθεί κατόπιν). Ωστόσο, μέχρι να επανεγγραφεί το σημείο εκείνο του σκληρού δίσκου, το σύστημα αρχείων τον θεωρεί «άδειο χώρο», αλλά στην ουσία διατηρούνται στο μαγνητικό μέσο σχεδόν όλα τα δεδομένα που είχαν αποθηκευτεί στο αρχείο. Στην παρακάτω Εικόνα 12.12, απεικονίζονται τα τμήματα στα οποία αναφερθήκαμε:



Εικόνα 12.12 *Αδέσμευτος (unallocated) και αδιάθετος (slack) χώρος.*

όπου

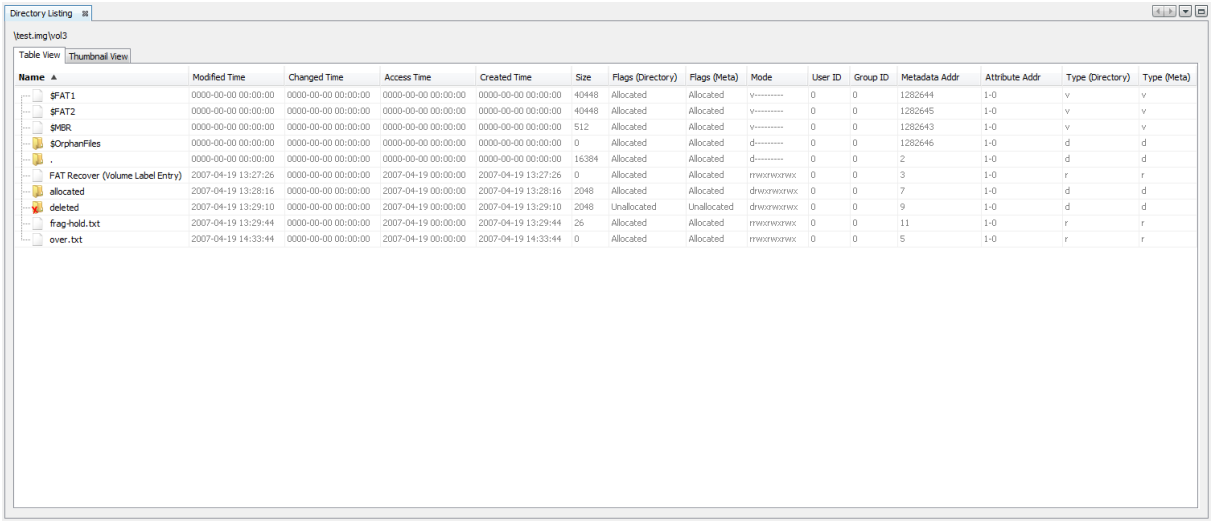
- Τμήμα A: σκληρός δίσκος (εμφανίζονται 128K).
- Τμήμα B: αρχείο 84K.
- Τμήμα C: αδιάθετος χώρος (slack space).
- Τμήμα D: διαγραμμένη κεφαλίδα αρχείου.
- Τμήμα E: μέρος αρχείου που παραμένει στον αδέσμευτο χώρο (unallocated space).

Από τα παραπάνω αντιλαμβανόμαστε ότι είναι ιδιαίτερα σημαντική η εξέταση του unallocated και του slack space, καθώς εκεί μπορεί να «κρύβονται» ενοχοποιητικά στοιχεία τα οποία πιθανόν ο εισβολέας / θύτης να ήθελε να διαγράψει. Για το σκοπό αυτό, υπάρχουν αρκετά εργαλεία τα οποία είναι σε θέση να επαναφέρουν τα δεδομένα των χώρων αυτών αλλά και να αναγνωρίσουν τον τύπο του αρχείου που είναι αποθηκευμένα εκεί. Η αναγνώριση του τύπου ενός αρχείου είναι επίσης σημαντική γιατί μπορούμε άμεσα να δούμε τα περιεχόμενα του αρχείου ως πληροφορίες με την κατάλληλη εφαρμογή.

12.2.5 Δημιουργία καταλόγου αρχείων

Το επόμενο βήμα περιλαμβάνει την εργασία δημιουργίας καταλόγου αρχείων ο οποίος βασίζεται στα ευρήματα των προηγούμενων βημάτων. Η αναγνώριση των τύπων των αρχείων βασίζεται συνήθως στη χρήση αυτοματοποιημένων εργαλείων τα οποία χρησιμοποιούν γνωστά μοτίβα. Η ονοματολογία διαμορφώνεται είτε από τα κανονικά ονόματα των αρχείων, σε όσα αυτό είναι εφικτό, ή από μια αυτόματη ονομασία (ένα πρόθεμα μαζί με έναν αύξοντα αριθμό) για όσα αρχεία ανακτήθηκαν από unallocated ή slack space. Συνηθίζεται να χρησιμοποιούνται γενικές εφαρμογές (π.χ. hexdump), όπου στην ίδια διεπαφή ο ερευνητής έχει τη δυνατότητα να διαβάσει το περιεχόμενο των αρχείων σε δεκαεξαδική ή σε ASCII μορφή. Επίσης, ο ερευνητής μπορεί να ορίσει ρητά τον τύπο ενός αρχείου που έχει ανακτηθεί, εφόσον έχει καλύτερη εκτίμηση από αυτή ενός αυτοματοποιημένου εργαλείου.

Στην παρακάτω Εικόνα 12.13, εμφανίζεται η δημιουργία καταλόγου αρχείων από το λογισμικό Autopsy:



Εικόνα 12.13 *Δημιουργία καταλόγου αρχείων με το Autopsy.*

12.2.6 Αναζήτηση αλφαριθμητικών

Στο στάδιο αυτό ο ερευνητής αναζητά κάτι συγκεκριμένο (μια ορισμένη σειρά χαρακτήρων) ή δοκιμάζει με κάτι που πιστεύει ότι θα τον οδηγήσει σε συμπεράσματα ή πρόσθετες πληροφορίες για το συμβάν. Θα πρέπει να είναι δυνατή η χρήση regular expressions, ώστε να οριστεί όσο το δυνατόν με περισσότερες παραλλαγές το είδος της πληροφορίας που αναζητείται. Το λογισμικό που χρησιμοποιεί ο ερευνητής μπορεί να του αναφέρει το αρχείο στο οποίο βρίσκεται το αλφαριθμητικό που αναζητά και να του δώσει τη δυνατότητα να βρει άλλα σχετιζόμενα με αυτό αρχεία (π.χ. χρονική συσχέτιση).

Στην παρακάτω Εικόνα 12.14, χρησιμοποιείται εργαλείο γραμμένο σε γλώσσα προγραμματισμού Python, προκειμένου να αναζητηθεί η διεύθυνση IP 192.168.56.1.

```
root@SIFT-Workstation: /$ export VOLATILITY_PROFILE=LinuxDebian5_26x86
root@SIFT-Workstation: /$ voldev.py -f hnet2011.img linux_yarascan -Y "192.168.56.1"
Volatile Systems Volatility Framework 2.3_beta
Task: rsyslogd pid 1661 rule r1 addr 0x8e614c6
0x08e614c6  31 39 32 2e 31 36 38 2e 35 36 2e 31 20 70 6f 72   192.168.56.1.por
0x08e614d6  74 20 34 34 36 31 36 20 73 73 68 32 00 39 11 00   t.44616.ssh2.9..
0x08e614e6  00 00 b8 c4 e5 08 98 a1 72 b7 80 00 00 00 20 00   ........r.......
0x08e614f6  00 00 00 00 00 00 20 36 20 31 35 3a 32 30 3a 35   ......6.15:20:5

 ..SNIP..

Task: bash pid 2042 rule r1 addr 0x8983dd0
0x08983dd0  31 39 32 2e 31 36 38 2e 35 36 2e 31 3a 2f 68 6f   192.168.56.1:/ho
0x08983de0  6d 65 2f 79 6f 6d 2f 74 65 6d 70 6f 72 61 72 79   me/yom/temporary
0x08983df0  2f 65 78 69 6d 34 2f 2a 20 2e 00 33 00 00 00 00   /exim4/*...3....
0x08983e00  f7 04 55 55 42 00 00 00 50 41 54 48 3d 2f 75 73   ..UUB...PATH=/us

 ..SNIP..

Task: bash pid 2042 rule r1 addr 0x89a2895
0x089a2895  31 39 32 2e 31 36 38 2e 35 36 2e 31 20 38 38 38   192.168.56.1.888
0x089a28a5  38 0a 00 20 00 00 00 cf cf cf cf 28 00 00 00 00   8..........(....
0x089a28b5  00 00 00 00 00 00 00 00 00 00 00 f7 03 55 55 1f   .............UU.
0x089a28c5  00 00 00 6d 65 6d 64 75 6d 70 20 7c 20 6e 63 20   ...memdump.|.nc.
```

Εικόνα 12.14 *Αναζήτηση αλφαριθμητικού.*

Το συγκεκριμένο εργαλείο συμπεριλαμβάνεται στην εξειδικευμένη εικονική μηχανή SIFT του οργανισμού SANS, η οποία είναι αφοσιωμένη για digital forensics και περιλαμβάνει εκατοντάδες εργαλεία.

Βιβλιογραφία

Bidgoli, H. (Ed.). (2006). Handbook of information security. Hoboken, N.J: John Wiley.

EC-Council Press (Ed.). (2010). Computer forensics: investigation procedures and response. Clifton Park, NY: Course Technology Cengage Learning.

ENISA. (n.d.). [Plone Site]. Retrieved 1 December 2015, from https://www.enisa.europa.eu/

FIRST.org / FIRST - Improving security together. (n.d.). Retrieved 30 September 2015, from http://www.first.org/

Molino, L. N. (2006). Emergency incident management systems: fundamentals and applications. Hoboken, N.J: J. Wiley & Sons, Inc.

Pepe, M., Luttgens, J. T., Kazanciyan, R., & Mandia, K. (2014). Incident response & computer forensics (Third edition). New York: McGraw-Hill Education.

SANS Information Security Training | Cyber Certifications | Research. (n.d.). Retrieved 30 September2015, from https://www.sans.org/

Santos, O. (2008). End-to-end network security: defense-in-depth. Indianapolis, Ind: Cisco Press.

TERENA. (n.d.). Retrieved 1 December 2015, from https://www.terena.org/

Wang, J., & Ishisoko, K. C. (2012, September). Analysis of CSIRT/SOC Incidents and Continuous Monitoring of Threats. Retrieved from http://ntrs.nasa.gov/search.jsp?R=20120016686

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Η ονομασία CSIRT σημαίνει:
α) Computer Emergency Response Team.
β) Cluster Security Response Team.
γ) Computer Security Incident Response Team.
δ) κανένα από τα παραπάνω.

2. Ο οργανισμός ENISA είναι:
α) Ελληνικός.
β) Παγκόσμιος
γ) Αμερικανικός.
δ) Ευρωπαϊκός.

3. Η μεθοδολογία της Αντιμετώπισης Συμβάντων αρχίζει με το στάδιο της:
α) Ανίχνευσης.
β) Προετοιμασίας.
γ) Αντιμετώπισης.
δ) Συλλογής.

4. Το υποστάδιο της Αρχικής Αντιμετώπισης χρησιμοποιείται για να
α) προετοιμαστούμε καλύτερα.
β) ανακόψουμε άμεσα την εισβολή.

γ) επαναφέρουμε σε λειτουργία τα υπολογιστικά συστήματα.
δ) όλα τα παραπάνω.

5. Κατά την αντιμετώπισης συμβάντων ασφάλειας, για τη συλλογή δεδομένων χρησιμοποιούνται:
α) όλοι οι εξυπηρετητές.
β) ο δικτυακός εξοπλισμός.
γ) τα αρχεία καταγραφής IDS/IPS.
δ) όλα τα παραπάνω.

6. Το τελευταίο στάδιο της μεθοδολογίας ηλεκτρονικής εγκληματολογίας είναι η:
α) δημιουργία αντιγράφου.
β) επαναφορά αντιγράφου.
γ) επαναφορά αρχείων.
δ) αναζήτηση αλφαριθμητικών.

7. Ποιο λειτουργικό σύστημα αναγνωρίζει τα περισσότερα συστήματα αρχείων;
α) Linux
β) Solaris
γ) OS/2
δ) Macintosh

8. Το slack space μπορεί να είναι μεγαλύτερο από ένα αρχείο;
α) Όχι.
β) Ναι.
γ) Είναι ίσο.
δ) Κανένα από τα παραπάνω.

9. Το unallocated space είναι:
α) πάντα άδειο.
β) πάντα γεμάτο πληροφορία.
γ) άδειο ή γεμάτο, αναλόγως του τρόπου διαγραφής.
δ) κανένα από τα παραπάνω.

10. Οι σουίτες λογισμικού για digital forensics εγκαθίστανται σε:
α) Linux.
β) MS Windows.
γ) Mac OS X.
δ) Όλα τα παραπάνω.

Κεφάλαιο 13. Ιδιωτικότητα στο Διαδίκτυο και Κυβερνοέγκλημα

Σύνοψη
Η χρήση της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ) έχει αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί η σύγχρονη κοινωνία. Όλες οι μορφές της ανθρώπινης δραστηριότητας έχουν επηρεαστεί από την υιοθέτηση των νέων τεχνολογικών εργαλείων και μέσων που προσφέρονται και οδηγούν στην επέκταση της ανθρώπινης συμπεριφοράς με νέες μορφές διάδρασης. Όμως, άλλοτε ο άνθρωπος χρησιμοποιεί την τεχνολογία για καλό σκοπό και άλλοτε για κακό σκοπό. Το σύνολο της παραβατικής ανθρώπινης συμπεριφοράς, το οποίο περιλαμβάνει σε κάποιο στάδιο χρήση τεχνολογικών εργαλείων και μέσων, ονομάζεται ηλεκτρονικό έγκλημα. Από την εκδήλωση των πρώτων φαινομένων ηλεκτρονικού εγκλήματος έχει ενεργοποιηθεί η παγκόσμια κοινότητα με στόχο να ανακόψει ή να αποτρέψει αυτού του είδους την παραβατική συμπεριφορά. Για το σκοπό αυτό, έχουν θεσπιστεί νομικά και κανονιστικά πλαίσια σε περιφερειακό ή εθνικό επίπεδο τα οποία εξετάζουν τους τρόπους ηλεκτρονικού εγκλήματος και οδηγούν στην επιβολή κυρώσεων στους παραβάτες.Τα πλαίσια αυτά βρίσκονται σε συμφωνία με τα αντίστοιχα Ευρωπαϊκά και διεθνή νομικά και κανονιστικά πλαίσια. Η εξέλιξη του ηλεκτρονικού εγκλήματος στο Διαδίκτυο, είναι γνωστή ως Κυβερνοέγκλημα.

Προαπαιτούμενη γνώση
Για την κατανόηση του παρόντος κεφαλαίου απαιτείται γνώση των βασικών εννοιών και ζητημάτων ασφάλειας (Κεφ. 1).

13.1 Εισαγωγή

Οι τεχνολογίες πληροφορίας και επικοινωνιών (ΤΠΕ) κατέστησαν δυνατή τη διάπραξη ενός μεγάλου αριθμού εγκληματικών πράξεων, οι οποίες προϋποθέτουν εξειδίκευση και τεχνολογική κατάρτιση. Ο όρος «Ηλεκτρονικό Έγκλημα» περιλαμβάνει όλες εκείνες τις αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση υπολογιστών και δικτύων επικοινωνίας. Οι πράξεις αυτές τιμωρούνται με συγκεκριμένες ποινές από την ελληνική και τη διεθνή νομοθεσία. Λόγω της πολυπλοκότητας των ΤΠΕ, αλλά και των πολλών διαφορετικών τεχνολογιών που εμπλέκονται, είναι δύσκολο να κατηγοριοποιήσουμε το ηλεκτρονικό έγκλημα σε σχέση με την τεχνολογία που χρησιμοποιείται. Συνηθίζεται, ωστόσο, μια κατηγοριοποίηση σε σχέση με τον τρόπο τέλεσης των παραβατικών πράξεων. Έτσι έχουμε εγκλήματα τα οποία διαπράττονται με τη χρήση υπολογιστών (computer crime) χωρίς τη χρήση του διαδικτύου και εγκλήματα τα οποία διαπράττονται μέσω διαδικτύου, τα οποία είναι γνωστότερα ως Κυβερνοεγκλήματα (cyber crimes). Επίσης, ανάλογα με το περιεχόμενο της επίθεσης, τα εγκλήματα διακρίνονται σε

- Εγκλήματα κατά της προσωπικότητας και της ιδιωτικότητας.
- Εγκλήματα κατά της περιουσίας.
- Διακίνηση παράνομου και αθέμιτου / επιβλαβούς περιεχομένου.

Η διαδικτύωση έδωσε ένα παγκόσμιο χαρακτήρα στο ηλεκτρονικό έγκλημα, το οποίο δεν θα μπορούσε σε καμία περίπτωση να αντιμετωπιστεί μόνο σε εθνικό ή τοπικό επίπεδο. Η ανάγκη σχηματισμού ενός κοινού μετώπου οδήγησε σε μια διακρατική συνεννόηση και στην εκπόνηση μιας αποτελεσματικής στρατηγικής. Το 2001, οι υπουργοί 26 ευρωπαϊκών κρατών, καθώς επίσης και 4 χωρών – παρατηρητών (Καναδάς, Ιαπωνία, Νότιος Αφρική και ΗΠΑ), υπέγραψαν τη Συνθήκη της Βουδαπέστης (Convention on Cybercrime). Η σύμβαση της Βουδαπέστης έχει ως σκοπό να εναρμονίσει τις εθνικές ποινικές νομοθεσίες των κρατών στον τομέα της εγκληματικότητας στον κυβερνοχώρο. Στη συνθήκη αυτή υπάρχουν επεξηγήσεις και ρυθμίσεις για όλες τις μορφές ηλεκτρονικού εγκλήματος, ενώ θεσπίζονται γρήγοροι και αποτελεσματικοί κανόνες στον τομέα της διεθνούς συνεργασίας.

Η οικονομία, η διοίκηση αλλά και γενικότερα η κοινωνία εξαρτάται από την αποτελεσματικότητα, την αξιοπιστία και την ασφάλεια των πληροφοριακών συστημάτων, και των δικτύων. Το γεγονός αυτό καθιστά την αντιμετώπιση του ηλεκτρονικού εγκλήματος μία καθημερινή μάχη. Σε διαφορετική περίπτωση, ο σύγχρονος

άνθρωπος θα βρεθεί στο μέσο μιας κοινωνίας γεμάτης κινδύνους, όπου θα λείπει η εμπιστοσύνη, ενώ η τεχνολογία θα αποτελεί έναν ανασταλτικό παράγοντα για την κοινωνική ανάπτυξη.

Υπάρχουν διάφοροι τρόποι με τους οποίους είναι δυνατό να εμπλακούν οι ΤΠΕ στο ηλεκτρονικό έγκλημα. Μπορεί, δηλαδή, να αποτελούν στόχο ή εργαλείο του εγκλήματος. Ένας σημαντικός παράγοντας που αυξάνει τη συχνότητα των ηλεκτρονικών εγκλημάτων είναι η ανωνυμία. Η ανωνυμία ενθαρρύνει τον κακόβουλο χρήστη στο να προχωρήσει σε παραβατική συμπεριφορά χωρίς φόβο. Έχουν αναπτυχθεί αρκετοί μηχανισμοί ασφάλειας οι οποίοι μας επιτρέπουν να συλλέξουμε πληροφορίες για κάθε δικτυακό κόμβο, άρα και για κάθε κακόβουλο χρήστη. Ωστόσο, αυτή η προσέγγιση δίνει αποτελέσματα μόνον εφόσον αυτοί οι μηχανισμοί είναι έγκαιρα ενεργοποιημένοι, στο πλαίσιο μιας συντονισμένης προσπάθειας πρόληψης των εγκληματικών πράξεων.

Ταυτόχρονα, η Ηλεκτρονική Εγκληματολογία (Digital Forensics), όπως είδαμε στο κεφάλαιο 12, απαιτεί αρκετές εργατοώρες και τεχνογνωσία προκειμένου να διαλευκάνει ένα ηλεκτρονικό έγκλημα. Ακόμη όμως και αν συμβεί αυτό, οι σχετικές εργασίες δεν εκτελούνται σε πραγματικό χρόνο, οπότε υπάρχει πάντα το ενδεχόμενο ο εισβολέας / θύτης να έχει καλύψει αρκετά από τα ίχνη του.

Ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος συνοδεύεται από ακόμη ένα χαρακτηριστικό το οποίο διαφοροποιεί το ηλεκτρονικό έγκλημα από το έγκλημα με την συμβατική του έννοια. Η γνώση και η τεχνική κατάρτιση που απαιτείται για τα ηλεκτρονικά εγκλήματα είναι αυξημένη, ωστόσο τα τελευταία χρόνια υπάρχει πληθώρα αυτοματοποιημένων εργαλείων, τα οποία δίνουν τη δυνατότητα ακόμη και σε ένα μέσο χρήστη ηλεκτρονικού υπολογιστή να πάρει μέρος σε μία παράνομη δραστηριότητα, εφόσον το επιθυμεί. Κάτι τέτοιο καθιστά δυνητικό εγκληματία κάθε άνθρωπο που διαθέτει υπολογιστή.

13.2 Νομικό Πλαίσιο

Το νομικό πλαίσιο και οι σχετικοί κανόνες μπορούν να κατηγοριοποιηθούν σε τέσσερις ενότητες, που αφορούν τα ακόλουθα:

- Προστασία της προσωπικότητας / ιδιωτικότητας.
- Καταστολή του οικονομικού ηλεκτρονικού εγκλήματος.
- Προστασία της πνευματικής ιδιοκτησίας.
- Προστασία από παράνομο και αθέμιτο περιεχόμενο.

Για να στοιχειοθετηθεί ένα ηλεκτρονικό έγκλημα απαιτείται καταρχήν μία περιγραφή της πράξης ή της παράλειψης που τελέστηκε η οποία συνιστά ποινικά κολάσιμη συμπεριφορά. Χρειάζεται να γνωρίζουμε τον χρόνο και τον τόπο τέλεσης, καθώς και τα εμπλεκόμενα πρόσωπα (π.χ. ποιος είναι ο θύτης και ποιος το θύμα).

Ο τόπος τέλεσης ενός ηλεκτρονικού εγκλήματος είναι ιδιαίτερα σημαντικός για να προσδιοριστεί το εφαρμοστέο δίκαιο και τα αρμόδια δικαστήρια. Στην περίπτωση κυβερνοεγκλήματος, υπάρχει διαχωρισμός του τόπου εκδήλωσης της αξιόποινης συμπεριφοράς και του τόπου επιβολής των αποτελεσμάτων της αξιόποινης συμπεριφοράς. Γίνεται φανερό ότι υπάρχει μια δυσχέρεια στον προσδιορισμό του τόπου, ειδικότερα στα κυβερνοεγκλήματα, καθώς κανείς μπορεί από κάθε τόπο να αποκτήσει πρόσβαση στα δεδομένα ενός υπολογιστή που είναι συνδεμένος στο Διαδίκτυο. Επίσης, τις περισσότερες φορές γίνεται χρήση διαφορετικών ενδιάμεσων σταθμών οι οποίοι μεσολαβούν μέχρι να τελεστεί η αξιόποινη πράξη, λόγω του ότι ένας υπολογιστής συνδέεται με κάποιον άλλο χρησιμοποιώντας αρκετούς ενδιάμεσους κόμβους του Διαδικτύου, με εναλλακτικές διαδρομές εφόσον χρειαστεί.

Η Ελληνική νομοθεσία διαθέτει αρκετές νομοθετικές ρυθμίσεις για θέματα ηλεκτρονικού εγκλήματος. Αποσπασματικά αναφέρονται οι Νόμοι 370 και 370^{A} του Ποινικού Κώδικα περί ποινικής προστασίας του απορρήτου, που μεταξύ άλλων αφορούν:

- Αθέμιτη εισχώρηση σε ξένα απόρρητα γραπτά (ανάγνωση – αντιγραφή – αποτύπωση με οποιοδήποτε τρόπο), που τιμωρείται με φυλάκιση μέχρι 1 έτος.

- Αθέμιτη παγίδευση ή παρέμβαση σε συσκευή, σύνδεση ή δίκτυο – υλικό – λογισμικό με σκοπό γνώση – αποτύπωση επικοινωνίας - δεδομένων κίνησης, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

- Αθέμιτη παρακολούθηση με ειδικά τεχνικά μέσα – αποτύπωση συνομιλίας ή μη δημόσιας πράξης άλλου, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

- Χρήση πληροφορίας/υλικού φορέα, που τιμωρείται με κάθειρξη μέχρι 10 έτη.

Επίσης, ο Νόμος 292^{A} μεταξύ άλλων αφορά:

- Χωρίς δικαίωμα πρόσβαση σε σύνδεση ή δίκτυο παροχής υπηρεσιών τηλεφωνίας, που τιμωρείται με φυλάκιση τουλάχιστον 1 έτους και χρηματική ποινή (20.000-50.000 ευρώ).

- Παραβίαση διάταξης Κανονισμού ΑΔΑΕ ή Γενικής Άδειας ΕΕΤΤ, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (100.000 - 500.000 ευρώ).

- Παράλειψη αποτροπής παράνομης πρόσβασης, που τιμωρείται με φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή (20.000 - 50.000 ευρώ).

Στη συνέχεια, αναφέρονται Νόμοι της Ελληνικής Νομοθεσίας, Προεδρικά Διατάγματα και Άρθρα Ποινικού Κώδικα, που είναι σχετικά με το ηλεκτρονικό έγκλημα και το κυβερνοέγκλημα:

Ν.2225/1994	«Προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας»
Ν. 2246/1994	«Οργάνωση και λειτουργία του τομέα τηλεπικοινωνιών»
Ν.2472/1997	«Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»
Ν. 2672/1998	«Διακίνηση εγγράφων με ηλεκτρονικά μέσα»
Ν.2774/1999	«Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα»
Ν.2867/2000	«Οργάνωση και λειτουργία των τηλεπικοινωνιών»
Ν .3115/2003	«Αρχή διασφάλισης του απορρήτου των επικοινωνιών»
Ν.3431/2006	«Περί ηλεκτρονικών επικοινωνιών»
Ν. 3471/2006	«Προστασία Δεδομένων Προσωπικού Χαρακτήρα»

Πίνακας 13.1 *Νόμοι για το ηλεκτρονικό έγκλημα.*

Π.Δ. 150/2001	«Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».
Π.Δ. 342/2002	«Διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο»
Π.Δ. 131/2003	«Προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά»
Π.Δ.47/2005	«Διαδικασίες για την Άρση του Απορρήτου των Επικοινωνιών»

Πίνακας 13.2 *Προεδρικά Διατάγματα για το ηλεκτρονικό έγκλημα.*

Άρθρο 3 48Α ΠΚ	Πορνογραφία ανηλίκων
Άρθρο 370Α	Παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας
Άρθρο 370 Β	Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα
Άρθρο 370Γ	Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών
Άρθρο 386Α	Απάτη με υπολογιστή

Πίνακας 13.3 *Άρθρα Ποινικού Κώδικα για το ηλεκτρονικό έγκλημα.*

Οδηγία 87/102/ΕΟΚ	Προσέγγιση των νομοθετικών, κανονιστικών και διοικητικών διατάξεων των κρατών μελών που διέπουν την καταναλωτική πίστη (τροποποιείται με την Οδηγία 90/88/ΕΟΚ).
Οδηγία 90/387/ΕΟΚ	Δημιουργία της εσωτερικής αγοράς στον τομέα των τηλεπικοινωνιακών υπηρεσιών μέσω της εφαρμογής της παροχής ανοικτού δικτύου (Open Network Provision - ONP).

Οδηγία 91/250/ΕΟΚ	Νομική προστασία των προγραμμάτων ηλεκτρονικών υπολογιστών
Οδηγία 96/9/ΕΟΚ	Νομική προστασία των βάσεων δεδομένων.
Οδηγία 97/7/ΕΚ	Προστασία των καταναλωτών κατά τις εξ' αποστάσεως συμβάσεις.
Οδηγία 1999/93/ΕΚ	Κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.
Οδηγία 2000/31/ΕΚ	Νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά
Οδηγία 2002/19/ΕΚ	Πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες, καθώς και με τη διασύνδεσή τους
Οδηγία 2002/20/ΕΚ	Αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών
Οδηγία 2002/21/ΕΚ	Κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/22/ΕΚ	Καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών
Οδηγία 2002/58/ΕΚ	Επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών
Οδηγία 2002/77/ΕΚ	Ανταγωνισμός στις αγορές δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

Πίνακας 13.4 *Ευρωπαϊκή νομοθεσία για το ηλεκτρονικό έγκλημα.*

Ιδιαίτερο ρόλο στο Κυβερνοέγκλημα διαδραματίζουν οι πάροχοι υπηρεσιών Διαδικτύου, καθώς οι ίδιοι αποτελούν το όχημα πρόσβασης και περιήγησης των χρηστών σε αυτό. Όταν η υπηρεσία που παρέχει ένας πάροχος αφορά στην απλή μετάδοση δεδομένων ή ακόμη και στην αποθήκευση των δεδομένων για μικρό χρονικό διάστημα (caching), τότε ο πάροχος δεν φέρει ευθύνη για το περιεχόμενο των δεδομένων.

Η αυτόματη ενδιάμεση και προσωρινή αποθήκευση των δεδομένων πραγματοποιείται από την πλευρά των παρόχων για να καταστεί αποτελεσματικότερη η μεταγενέστερη μετάδοσή τους και απαλλάσσει τους παρόχους από κάθε ευθύνη. Ο πάροχος επίσης δεν πρέπει να τροποποιεί ή να παρεμβαίνει με οποιονδήποτε τρόπο στα διακινούμενα δεδομένα. Αν ο πάροχος αντιληφθεί ότι τα δεδομένα έχουν αποσυρθεί από το σημείο αφετηρίας της μετάδοσής τους (π.χ. ιστοσελίδα), τότε έχει την υποχρέωση να αποσύρει άμεσα ή να καταστήσει αδύνατη την πρόσβαση σε αυτά τα δεδομένα που αποθήκευσε. Για την υπηρεσία φιλοξενίας ιστοσελίδας ο πάροχος δεν φέρει καμία ευθύνη εφόσον δεν γνωρίζει πραγματικά το τυχόν παράνομο περιεχόμενο της δραστηριότητας ή της πληροφορίας.

13.3 Κατηγορίες Ηλεκτρονικού Εγκλήματος

Η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων ποικίλει σε μεγάλο βαθμό και εξαρτάται κυρίως από την οπτική με την οποία τη δημιουργεί κανείς. Ένας διαχωρισμός ο οποίος χρησιμοποιείται αρκετά προέρχεται από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα το οποίο από την ίδρυση του, στις αρχές της δεκαετίας του 1980, διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του ηλεκτρονικού εγκλήματος σε δημόσιο και ιδιωτικό τομέα. Στις κατηγορίες αυτές, μεταξύ άλλων, συμπεριλαμβάνονται τα ακόλουθα:

- Απάτη: αλλοίωση δεδομένων για προσωπικό όφελος.
- Κλοπή: δεδομένων ή λογισμικού.
- Χρήση λογισμικού χωρίς άδεια (π.χ. παράνομα αντίγραφα λογισμικού).
- Μη εγκεκριμένη χρήση των δυνατοτήτων του υπολογιστή για ίδιον όφελος.
- Κακή χρήση προσωπικών δεδομένων.
- Hacking.
- Σαμποτάζ: πρόκληση ζημιάς σε λογισμικό ή υλικό.
- Εισαγωγή πορνογραφικού υλικού στο Διαδίκτυο.

Σε αυτές τις γενικές κατηγορίες ή σε άλλες παρόμοιες ανήκουν διάφορες εκφάνσεις του ηλεκτρονικού εγκλήματος οι οποίες χαρακτηρίζονται από τα ιδιαίτερα εργαλεία λογισμικού που χρησιμοποιούνται σε κάθε περίπτωση. Είναι βέβαιο ότι εφόσον η τεχνολογία υλικού συνεχίζει να αλλάζει, το ίδιο θα συμβαίνει και με τις μεθόδους που θα χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου. Στη συνέχεια, παρουσιάζονται αναλυτικότερα οι συνηθέστερες κατηγορίες

13.3.1 Αλίευση

Η επίθεση αλίευσης (phishing attack), περιλαμβάνει εκείνες τις περιπτώσεις όπου ο θύτης χρησιμοποιεί συνδυασμό μηνυμάτων email και πλαστών ιστοσελίδων προκειμένου να παραπλανήσει τον ανυποψίαστο χρήστη. Είναι ιδιαίτερα συνηθισμένη η περίπτωση όπου ο ανυποψίαστος χρήστης δέχεται μήνυμα ηλεκτρονικής αλληλογραφίας το οποίο εμφανίζεται μεταμφιεσμένο ώστε να δείχνει ότι προέρχεται από τραπεζικό ίδρυμα (πιθανόν από κάποιο τραπεζικό ίδρυμα με το οποίο και ο ίδιος έχει συναλλαγές) και του ζητά να εισέλθει στο πληροφοριακό σύστημα προκειμένου να αλλάξει κάποια στοιχεία επικοινωνίας του. Αν η επίθεση αυτού του τύπου πετύχει, τότε μόλις ο χρήστης εισάγει τα στοιχεία του (ιδιαίτερα το αναγνωριστικό και το συνθηματικό για τη σύνδεσή του με το πληροφοριακό σύστημα της τράπεζας) τότε αυτά αποστέλλονται μέσω του Διαδικτύου στο θύτη.

Οι μέθοδοι που χρησιμοποιούνται για αυτό τον τύπο εγκλήματος είναι συνήθως η ηλεκτρονική αλληλογραφία (email), η οποία μοιάζει να προέρχεται από έμπιστη πηγή. Ακόμη, χρησιμοποιούνται παραπλανητικού τύπου σύνδεσμοι (hyperlinks) με ονομασίες δημοφιλών διαδικτυακών τόπων ή παραπλανητικά γραφικά και διαφημιστικές πινακίδες με σκοπό να δελεάσουν τον ανυποψίαστο χρήστη. Ακόμη, μπορεί να συναντήσουμε χρήση παραθύρων pop-up για την ενσωμάτωση κακόβουλου κώδικα σε μια ιστοσελίδα. Ο κακόβουλος κώδικας εκμεταλλεύεται μια ευπάθεια του φυλλομετρητή ή του εξυπηρετητή (Web server) για να παρασύρει τον επισκέπτη σε λανθασμένες ενέργειες.

13.3.2 Παιδική πορνογραφία

Με την κατηγορία της κατοχής ή διακίνησης παιδικής πορνογραφίας κατηγορείται όποιος με πρόθεση παράγει, προσφέρει, πουλάει ή με οποιοδήποτε τρόπο διανέμει, διαβιβάζει, αγοράζει, προμηθεύεται ή κατέχει υλικό παιδικής πορνογραφίας. Η χρήση ηλεκτρονικού υπολογιστή ή του Διαδικτύου εντάσσει το έγκλημα αυτό στις κατηγορίες ηλεκτρονικού εγκλήματος και κυβερνοεγκλήματος, αντίστοιχα. Η τιμωρία της κατοχής ή διακίνησης παιδικής πορνογραφίας αφορά φυλάκιση τουλάχιστον 2 ετών και χρηματική ποινή τουλάχιστον 50.000 ευρώ.

Σύμφωνα με το «Προαιρετικό Πρωτόκολλο στη Σύμβαση για τα Δικαιώματα του Παιδιού σχετικά με την εμπορία παιδιών, την παιδική πορνεία και παιδική πορνογραφία», ο όρος *'παιδική πορνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσομοιωμένες ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς'*. Το φαινόμενο αυτό δεν είναι απόρροια της χρήσης του Διαδικτύου, αλλά το Διαδίκτυο ώθησε ακόμη μεγαλύτερη μερίδα ανθρώπων στην παρανομία, καθώς:

- Θεωρείται ευκολότερη η μυστικότητα και η ανωνυμία.
- Διευκολύνεται η άμεση ανταλλαγή του παράνομου υλικού.

Με βάση το άρθρο 348^{A} του Ποινικού Κώδικα, οι τρόποι εγκληματικής δράσης είναι:

- Κατασκευή υλικού πορνογραφίας.
- Κατοχή πορνογραφικού υλικού.
- Προμήθεια και αγορά υλικού πορνογραφίας.
- Μεταφορά πορνογραφικού υλικού.
- Κυκλοφορία πορνογραφικού υλικού.

13.3.3 Αθέμιτη υποκλοπή

Η αθέμιτη υποκλοπή περιγράφει εκείνο το ηλεκτρονικό έγκλημα κατά το οποίο διαπράττεται εκ προθέσεως υποκλοπή δεδομένων από, προς ή μέσα σε ένα σύστημα υπολογιστών και η οποία γίνεται με χρήση ηλεκτρονικών ή άλλων τεχνικών μέσων.

13.3.4 Παράνομη πρόσβαση

Ως παράνομη πρόσβαση χαρακτηρίζεται η εκ προθέσεως και χωρίς εξουσιοδότηση πρόσβαση σε ένα πληροφοριακό σύστημα. Η δραστηριότητα αυτή είναι γνωστότερη ως hacking ή cracking.

Hacking είναι η μη εξουσιοδοτημένη πρόσβαση μέσω διείσδυσης (δηλαδή ηθελημένης παραβίασης των μηχανισμών ελέγχου πρόσβασης) σε υπολογιστικά συστήματα, σκοπός της οποίας καταρχήν δεν είναι η δολιοφθορά, η καταστροφή ή η αποκόμιση οικονομικού οφέλους, αλλά η προσωπική ικανοποίηση από την παράκαμψη των συστημάτων ασφαλείας και η επιβεβαίωση των τεχνολογικών γνώσεων και δεξιοτήτων μέσω της εισβολής σε ένα ξένο υπολογιστικό σύστημα.

Η έννοια του hacking είναι ευρεία. Μπορεί να αφορά μια σειρά προγραμματιστικών δραστηριοτήτων που απαιτούν αυξημένες ικανότητες, ορισμένες από τις οποίες μπορούν να χαρακτηριστούν ως παράνομες ή και εγκληματικές. Η εισβολή σε ένα τρίτο σύστημα ακόμα και αν δεν είναι κακόβουλη, ενέχει παράνομο χαρακτήρα. Ο επιτιθέμενος, διεισδύοντας σε ένα τρίτο σύστημα αποκτά γνώσεις για το επίπεδο ασφάλειας του, εντοπίζει τα αδύνατα σημεία του και στη συνέχεια μπορεί να διαπράξει κακόβουλη επίθεση ή ακόμα και να δημοσιοποιήσει τις πληροφορίες που έχει συγκεντρώσει σε κάποιον τρίτο που θα προχωρήσει αργότερα σε μια ή περισσότερες επιθέσεις.

13.3.5 Επέμβαση σε δεδομένα

Επέμβαση σε δεδομένα θεωρείται η εκ προθέσεως καταστροφή, διαγραφή, μεταβολή ή απόκρυψη δεδομένων χωρίς προηγούμενη εξουσιοδότηση. Σε αυτή την περίπτωση, προστατευόμενο έννομο αγαθό είναι η ακεραιότητα και η κανονική χρήση των αποθηκευμένων δεδομένων ή των προγραμμάτων ηλεκτρονικών υπολογιστών.

13.3.6 Διασπορά κακόβουλου λογισμικού

Ως κακόβουλο λογισμικό (malware) θεωρούμε εφαρμογές οι οποίες έχουν ως στόχο την παραβίαση της ασφάλειας των υπολογιστών (host) στους οποίους εκτελούνται, με σκοπό να προκαλέσουν φθορές, υποβάθμιση ή διακοπή λειτουργίας, καθώς και να υποκλέψουν προσωπικά στοιχεία. Υπάρχουν αρκετοί τρόποι διασποράς κακόβουλου λογισμικού με τους γνωστότερους να είναι οι ιοί (virus), τα σκουλήκια (worms) και οι Δούρειοι Ίπποι (Trojan Horses).

Τα είδη του κακόβουλου λογισμικού διαρκώς πολλαπλασιάζονται, καθώς η εξέλιξη της τεχνολογίας λειτουργεί ευεργετικά και για τους κακόβουλους χρήστες. Δεν είναι σπάνια η εμφάνιση κακόβουλου λογισμικού με εξειδίκευση στη στόχευση αλλά και στον τρόπο λειτουργίας του. Χαρακτηριστικό παράδειγμα είναι η κατηγορία ransomware, όπου το κακόβουλο λογισμικό κάνει χρήση της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) και της κρυπτογραφίας ελλειπτικών καμπυλών προκειμένου να κρυπτογραφήσει όλα τα αρχεία κειμένου του ανυποψίαστου χρήστη και στη συνέχεια να απαιτήσει λύτρα (χρηματικό ποσό), προκειμένου να αποστείλει στον χρήστη το απαραίτητο ιδιωτικό κλειδί για να αποκρυπτογραφήσει τα αρχεία του υπολογιστή του. Οι συγγραφείς τέτοιων ransomware εφαρμογών εκμεταλλεύονται τεχνικές ανωνυμίας, κυρίως μέσω του δικτύου Tor ώστε να εισέλθουν στο λεγόμενο darknet και να εγκαταστήσουν εκεί τους εξυπηρετητές οι οποίοι είναι απαραίτητοι για να επιτελέσουν τους σκοπούς και να εξαπολύσουν «εκ τους ασφαλούς» τις επιθέσεις τους.

13.4 Εξιχνίαση

Η έρευνα για την εξιχνίαση των ηλεκτρονικών εγκλημάτων είναι μια αρκετά δύσκολη και ιδιαίτερα χρονοβόρος διαδικασία με σκοπό τον εντοπισμό των «ηλεκτρονικών ιχνών». Οι κακόβουλοι χρήστες έχουν στη διάθεσή τους και χρησιμοποιούν αρκετά μέτρα προστασίας τα οποία δυσχεραίνουν τη διαδικασία της εξιχνίασης και πολλές φορές την καθιστούν αδύνατη. Ορισμένες χώρες, κράτη-μέλη της Ευρωπαϊκής ένωσης ή και εκτός αυτής, στηρίζουν με την νομοθεσία τους την ανωνυμία μέσω υπηρεσιών Ιδεατών Ιδιωτικών Δικτύων (VPN) και με τον τρόπο αυτό βοηθούν τους θύτες να καλύψουν τα ίχνη τους. Ο λόγος χρήσης των VPN αφορά την

υποστήριξη του δικαιώματος της ιδιωτικότητας του κάθε ανθρώπου. Ωστόσο, αυτό ακριβώς εκμεταλλεύονται και οι ηλεκτρονικοί εγκληματίες.

Σε όλες τις περιπτώσεις όπου διεξάγεται διαδικτυακή έρευνα γίνεται προσπάθεια να εντοπιστεί το «ηλεκτρονικό ίχνος» του δράστη. Το ηλεκτρονικό ίχνος κάθε χρήστη του διαδικτύου είναι μοναδικό και αποτελεί ένα από τα σημαντικότερα στοιχεία για την αποδεικτική διαδικασία στο δικαστήριο. Η λεγομένη ηλεκτρονική απόδειξη (electronic evidence) δεν ταυτίζεται με τα παραδοσιακά αποδεικτικά μέσα. Τα τελευταία, έχουν κατά κανόνα υλική υπόσταση και μπορούν να εντοπιστούν σε συγκεκριμένο τόπο και χρόνο. Αντίθετα, τα ηλεκτρονικά αποδεικτικά μέσα είναι ψηφιακά και μπορεί να διατηρούνται για μεγάλα χρονικά διαστήματα.

Ειδικότερα, στα χαρακτηριστικά γνωρίσματα του εγκλήματος στον Κυβερνοχώρο συμπεριλαμβάνονται και τα ακόλουθα

- Το έγκλημα στον Κυβερνοχώρο είναι τις περισσότερες φορές γρήγορο, διαπράττεται σε ελάχιστο χρόνο και συνήθως δεν γίνεται αντιληπτό ούτε από το ίδιο το θύμα.

- Η διάπραξη του είναι εύκολη , για όσους κατέχουν τις ιδιαίτερες ικανότητες που απαιτούνται, ενώ τα ηλεκτρονικά ίχνη που αφήνει είναι ψηφιακά.

- Για την τέλεσή του απαιτούνται συνήθως ιδιαίτερα εξειδικευμένες γνώσεις.

- Ο δράστης μπορεί να διαπράξει το ηλεκτρονικό έγκλημα χωρίς να μετακινηθεί, από το σπίτι ή το γραφείο του, μέσω του υπολογιστή του.

- Δίνει τη δυνατότητα στους θύτες, όπως οι παιδόφιλοι, να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα, ανέξοδα, να βρίσκονται πολλοί μαζί στις ίδιες ομάδες συζητήσεως (news groups) ή μέσα σε chat rooms που χρησιμοποιούνται για άλλους σκοπούς.

- Τις περισσότερες φορές οι κυβερνοεγκληματίες επικοινωνούν χρησιμοποιώντας ψευδείς ταυτότητες, τις οποίες χρησιμοποιούν για να αποστείλουν ηλεκτρονικά μηνύματα

- Το ηλεκτρονικό έγκλημα συνήθως διασχίζει τα εθνικά σύνορα και οι επιπτώσεις του επηρεάζουν ταυτόχρονα πολλούς τόπους.

- Είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσής του και επίσης είναι αρκετά δύσκολη η διερεύνηση και ο εντοπισμός του δράστη. Υπάρχει ενδεχόμενο ο δράστης να εντοπισθεί σε μια χώρα και τα αποδεικτικά στοιχεία να βρίσκονται σε μια άλλη, απομακρυσμένη χώρα ή και να βρίσκονται ταυτόχρονα σε πολλές διαφορετικές χώρες.

- Είναι συνηθισμένη η συνεργασία δύο ή περισσότερων κρατών κατά την διερεύνηση ενός ηλεκτρονικού εγκλήματος. Περιπτώσεις εγκληματικής συμπεριφοράς στα όρια ενός μόνον κράτους είναι λιγοστές.

13.5 Ιδιωτικότητα

Η ραγδαία αύξηση του όγκου των πληροφοριών και των επικοινωνιακών ροών είναι γεγονός το οποίο γίνεται άμεσα αντιληπτό από το καθένα μας. Η πληροφορία αφορά κάθε ανθρώπινη δραστηριότητα αλλά και τον ίδιο τον άνθρωπο. Στοιχεία που αφορούν τον καθέναν από μας υπάρχουν πλέον ως δεδομένα σε πολλά και διαφορετικά πληροφοριακά συστήματα. Ταυτόχρονα, γνωρίζουμε ήδη ότι ο κυβερνοχώρος είναι ένα πεδίο στο οποίο μαίνονται «μάχες» ανάμεσα σε κυβερνοεγκληματίες και κυβερνοφύλακες. Κανείς δεν μπορεί να νιώθει ήσυχος σε μια τέτοια κατάσταση. Τα προσωπικά δεδομένα ή δεδομένα προσωπικού χαρακτήρα, δηλαδή αυτά που αφορούν / χαρακτηρίζουν ένα πρόσωπο και συνδέονται με την ταυτότητά του, θα πρέπει να διασφαλίζονται με τέτοιο τρόπο ώστε να μην υπάρχει ο κίνδυνος έκθεσής τους σε τρίτους.

Η ανάγκη για τη συνταγματική κατοχύρωση της ιδιωτικότητας (privacy) εμφανίζεται, για πρώτη φορά στη νεότερη ιστορία, το 1890 οπότε η έννοια της ιδιωτικότητας συνδέθηκε με το δικαίωμα να μείνει κανείς μόνος (the right to be left alone). Το 1950 η ευρωπαϊκή επιτροπή των ανθρώπινων δικαιωμάτων θέσπισε το δικαίωμα σεβασμού της ιδιωτικής ζωής των πολιτών της.

Η έννοια της ιδιωτικότητας προσδιορίζεται ανάλογα με το πλαίσιο στο οποίο αυτή εξετάζεται. Έτσι, έχουμε τις ακόλουθες παραλλαγές της:

- Πληροφοριακή Ιδιωτικότητα: σχετίζεται με τη συγκέντρωση, την αποθήκευση, την επεξεργασία και τη διάδοση των πληροφοριών που αποτελούν προσωπικά δεδομένα ενός ανθρώπου (προσώπου).

- Χωρική Ιδιωτικότητα: σχετίζεται με την προστασία της φυσικής περιοχής στην οποία βρίσκεται ένα πρόσωπο (π.χ. οικία, εργασιακός χώρος κλπ.).

- Σωματική Ιδιωτικότητα: σχετίζεται με την προστασία ενός του σώματος ενός προσώπου από αδικαιολόγητη παρέμβαση (π.χ. σωματικός έλεγχος κλπ.).

- Επικοινωνιακή Ιδιωτικότητα: σχετίζεται με την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.

Ο πιο κοινά αποδεκτός ορισμός της Πληροφοριακής Ιδιωτικότητας προτάθηκε το 1967 από τον Alan F. Westin και αναφέρει ότι: «Ιδιωτικότητα είναι η αξίωση των ατόμων, των ομάδων και των ιδρυμάτων να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που αφορούν αυτούς, θα διαβιβάζονται σε άλλους». Το σημαντικό στον παραπάνω ορισμό είναι ο διαχωρισμός της πληροφορίας σε δημόσια ή ιδιωτική. Συνήθως, ο διαχωρισμός αυτός βασίζεται στο ισχύον νομικό και κανονιστικό πλαίσιο.

Η έννοια της Πληροφοριακής Ιδιωτικότητας καθίσταται εξαιρετικά σημαντική στη διαχείριση και λειτουργία των πληροφοριακών συστημάτων, κυρίως εξαιτίας τόσο του χαρακτήρα των εργασιών που επιτελούνται, όσο και του σημαντικού όγκου δεδομένων που συλλέγονται, επεξεργάζονται και αποθηκεύονται σε αυτά. Για την προστασία δεδομένων, η Ευρωπαϊκή Οδηγία 1995/46/ΕΚ ορίζει τις αρχές της νομιμότητας και της δικαιοσύνης, την αρχή του καθορισμού του σκοπού της συλλογής των δεδομένων και της επεξεργασίας αυτών για το σκοπό που συλλέχθηκαν, την αρχή της αναγκαιότητας της συλλογής και επεξεργασίας των δεδομένων, την αρχή της παροχής πληροφόρησης, ενημέρωσης και πρόσβασης στους κατόχους των δεδομένων, την αρχή της ασφάλειας και της ακεραιότητας, καθώς και την αρχή της εποπτείας και επικύρωσης. Είναι σημαντικό να τονίσουμε ότι μια επίθεση σε ένα πληροφοριακό σύστημα δεν προσβάλει απαραίτητα το απόρρητο της επεξεργασίας προσωπικών δεδομένων. Τα αντίμετρα προστασίας τα οποία χρησιμοποιεί ένα πληροφοριακό σύστημα πολλές φορές δεν καλύπτουν τις ανάγκες προστασίας και ενίσχυσης της ιδιωτικότητας.

Η προστασία της ιδιωτικότητας είναι ένα ζήτημα το οποίο πολλές φορές μπορεί να έρθει σε σύγκρουση με τη χρήση άλλων μηχανισμών ασφάλειας. Για παράδειγμα, σε ένα εργασιακό χώρο είναι πιθανό η εταιρική πολιτική να ορίζει τη χρήση κάμερας για επιτήρηση ενός χώρου, κάτι όμως το οποίο παραβιάζει την ιδιωτικότητα των εργαζομένων. Άλλη παρόμοια περίπτωση συμβαίνει με την αξιοποίηση της τεχνολογίας DRM (digital rights management), όπου μπορεί να γίνεται αξιοποίηση μηχανισμών προσδιορισμού ταυτότητας, καταγραφής ηλεκτρονικών ιχνών και κατά συνέπεια εντοπισμού των χρηστών. Η επιβολή της απαραίτητης ισορροπίας είναι μια δύσκολη υπόθεση, καθώς η πληροφορία αποτελεί ένα σημαντικό παράγοντα ανάπτυξης και εδραίωσης για κάθε οργανισμό ή κράτος. Σε κάθε περίπτωση, οι μηχανισμοί ασφάλειας που υλοποιούνται θα πρέπει να είναι συμβατοί με τις βασικές αρχές μιας δημοκρατικής κοινωνίας, όπως ορίζεται από τον ΟΟΣΑ: «Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency»

Βιβλιογραφία

Maniotis, D., Marinos, M.-T., Anthimos, A., Iglezakis, I., & Nouskalis, G. (2011). Cyber law in Greece. Alphen aan den Rijn, The Netherlands: Kluwer Law International.

Moore, A. D. (2010). Privacy rights: moral and legal foundations. University Park, Pa: Pennsylvania State University Press.

Nissenbaum, H. F. (2010). Privacy in context: technology, policy, and the integrity of social life. Stanford, Calif: Stanford Law Books.

Pedneault, S., & Davia, H. R. (2009). Fraud 101: techniques and strategies for understanding fraud (3rd ed., Fully rev). Hoboken, N.J: John Wiley & Sons.

Regan, P. M. (2009). Legislating privacy: technology, social values and public policy. Chapel Hill, NC: The Univ. of North Carolina Press.

Αρμαμέντος, Π., & Σωτηρόπουλος, Β. (2005). Προσωπικά δεδομένα - Ερμηνεία Ν. 2472/1997, Εκδόσεις Σάκκουλα.

Ηλεκτρονικό Έγκλημα - Υπ. Εσωτερικών και Διοικητικής Ανασυγκρότησης - Ελληνική Αστυνομία. (n.d.). Retrieved 30 September 2015, from http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=1414.

Λίλιαν Μήτρου.Προστασία Προσωπικών Δεδομένων [open]. Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD117/

Λίλιαν Μήτρου.Κανονιστικές και Κοινωνικές Διαστάσεις της Κοινωνίας της Πληροφορίας [open].Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD118/

Λίλιαν Μήτρου.Ειδικά Θέματα Δικαίου της Πληροφορίας [open].Retrieved 30 September 2015 from https://eclass.aegean.gr/courses/ICSD119/.

Κριτήρια αξιολόγησης

Απαντήστε στις ακόλουθες ερωτήσεις. Η κάθε ερώτηση μπορεί να έχει μοναδική ή περισσότερες απαντήσεις.

1. Ποιες από τις παρακάτω κατηγορίες θεωρούνται Κυβερνοεγκλήματα;
α) Εγκλήματα κατά της προσωπικότητας και της ιδιωτικότητας.
β) Εγκλήματα κατά της περιουσίας.
γ) Διακίνηση παράνομου και αθέμιτου / επιβλαβούς περιεχομένου.
δ) Όλα τα παραπάνω.

2. Ποιοι Νόμοι του Ποινικού Κώδικα αφορούν την προστασία του απορρήτου;
α) 360
β) 370
γ) 370Α
δ) 380

3. Η «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» καθορίζεται από το νόμο:
α) Ν.2472/1997
β) Ν.2774/1999
γ) Ν .3115/2003

δ) Ν.3431/2006

4. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα και η προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών αναφέρεται στην Ευρωπαϊκή Οδηγία:
α) 2002/58/ΕΚ
β) 2002/20/ΕΚ
γ) 2000/31/ΕΚ
δ) 2002/77/ΕΚ

5. Τι σημαίνει ο όρος DRM;
α) Digital Recording Management
β) Digital Rights Manager
γ) Digital Recording Manager
δ) Digital Rights Management

6. Αν ο πάροχος αντιληφθεί ότι τα δεδομένα έχουν αποσυρθεί από το σημείο αφετηρίας της μετάδοσής τους οφείλει:
α) να συνεχίσει να προσφέρει πρόσβαση.
β) να ενημερώσει τον ιδιοκτήτη της πληροφορίας.
γ) να αποσύρει άμεσα ή να καταστήσει αδύνατη την πρόσβαση σε αυτά τα δεδομένα που αποθήκευσε.
δ) να μην κάνει κάτι από τα παραπάνω.

7.Ποιες από τις παρακάτω είναι κατηγορίες Ηλεκτρονικού Εγκλήματος;
α) Σαμποτάζ.
β) Καμουφλάζ.
γ) Απάτη.
δ) Αλίευση.

8. Ο όρος Hacking είναι συνώνυμος του Cracking;
α) Ναι.
β) Όχι.
γ) Ναι, τις περισσότερες φορές.
δ) Όχι, τις περισσότερες φορές.

9. Ποιες από τις παρακάτω έννοιες αφορούν την Ιδιωτικότητα;
α) Πληροφοριακή Ιδιωτικότητα.
β) Χωρική Ιδιωτικότητα.
γ) Σωματική Ιδιωτικότητα.
δ) Όλες οι παραπάνω.

10. Η Επικοινωνιακή Ιδιωτικότητα σχετίζεται με:
α) την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας πολλών προσώπων με ένα πρόσωπο.
β) την προστασία από εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.
γ) την προστασία από μη εξουσιοδοτημένη παρακολούθηση της επικοινωνίας ενός προσώπου με άλλα πρόσωπα.
δ) κανένα από τα παραπάνω

Λίστα μαθησιακών αντικειμένων

Αντιστοίχιση Ελληνικών - ξενόγλωσσων όρων

Access point	Σημείο πρόσβασης
Active tapping	Ενεργή Παρακολούθηση
Address translation	Μετάφραση διεύθυνσης
Application-level Gateways	Πύλες εφαρμογών
Asset	Αγαθό
Attack	Επίθεση
Authentication	Αυθεντικοποίηση
Authorization	Εξουσιοδότηση
Availability	Διαθεσιμότητα
Block	Δέσμης
Brute-Force Attack	Επίθεση Ωμής Βίας
Buffer overflow	Υπερχείλιση ενταμιευτή
Channel Capacity	Χωρητικότητα Καναλιού
Ciphertext	Κρυπτογράφημα
Circuit-level Gateways	Πύλες κυκλώματος
Collision resistance	Αντοχή σε συγκρούσεις
Communication Security	Προστασία Επικοινωνιών
Computationally infeasible	Υπολογιστικά ανέφικτη
Computer Security	Προστασία Υπολογιστικών Συστημάτων
Confidentiality	Εμπιστευτικότητα
Congestion control	Έλεγχος συμφόρησης
Connectionless	Ασυνδεσμική
Correlation attack	Επίθεση αυτοσυσχέτισης
Cost	Κόστος
Countermeasure	Αντίμετρο
Cryptanalysis	Κρυπτανάλυση
Cryptography	Κρυπτογραφία
cybercriminals	Κυβερνο-εγκληματίες
cyberterrorists	Κυβερνο-τρομοκράτες
Cyclic Redundancy Check	Κυκλικός Έλεγχος Πλεονασμού
Danger	Κίνδυνος
Datagram	Δεδομενόγραμμα
Decoder	Αποκωδικοποιητής
Decryption/Decipherment	Αποκρυπτογράφηση
Denial of service	Άρνηση Εξυπηρέτησης
Destination address	Διεύθυνση προορισμού
Destination port	Θύρα προορισμού
Digital Fingerprinting	Ψηφιακά Αποτυπώματα
Digital Forensics	Ψηφιακής Εγκληματολογίας
Digital Watermarking	Ψηφιακή Υδατογράφηση
Encoder	Κωδικοποιητής
Exception handling	Χειρισμός εξαίρεσης
Fabrication	Πλαστογραφία
Firewall	Τείχος προστασίας
Flow control	Έλεγχος ροής
Forensics	Συλλογή αποδείξεων
Frame	Πλαίσιο
Grant	Εκχώρηση
Harm	Ζημιά
Hashing function	Συνάρτηση κατακερματισμού
Heap	Σωρός
Host	Κόμβος
Identification	Αναγνώριση
Identity provider	Πάροχος ταυτοτήτων

Information and Communication Technologies	Τεχνολογίες Πληροφορίας και Επικοινωνιών
Information Security	Ασφάλεια Πληροφοριών
Information Security Management System	Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
Information Theory	Θεωρία Πληροφορίας
Initial Permutation	Αρχική μετάθεση
Initialization vector	Διάνυσμα αρχικοποίησης
Integrity	Ακεραιότητα
Interception	Υποκλοπή
Internet of Things	Διαδίκτυο των Πραγμάτων
Interruption	Διακοπή
Intrusion detection	Ανίχνευση εισβολών
Invalidated input	Μη επικυρωμένη είσοδος
Local Area Networks	Δίκτυα Τοπικής Περιοχής
Malware	Κακόβουλο Λογισμικό
Man-in-the-middle attack	Επίθεση ενδιάμεσου
Masquerading	Πλαστοπροσωπία
Media	Μέσο
Message Detection Code	Κώδικας Ανίχνευσης Μετατροπών
Message digest	Συνόψιση μηνύματος
Metropolitan Area Networks	Μητροπολιτικά Δίκτυα
Mobility	Κινητικότητα
Modification	Μεταβολή
Nor-repudiation	Αδυναμία Αποποίησης
Packet Filters	Φιλτράρισμα πακέτων
Parity bit	Ψηφίο Ισοτιμίας
Passive tapping	Παθητική Παρακολούθηση
Personal Area Networks	Δίκτυα Προσωπικής Περιοχής
Personal Digital Assistant	Προσωπικός Ψηφιακός Βοηθός
Preimage resistance	Αντοχή προαπεικόνισης
Privilege	Προνόμιο
Protocol field	Πρωτόκολλο επικοινωνίας
Race conditions	Συνθήκες ανταγωνισμού
Replay	Επανεκπομπή μηνυμάτων
Repudiation	Αποποίηση
Routing	Δρομολόγηση
Slack space	Αδιάθετος χώρος
Software	Λογισμικό
Source address	Διεύθυνση προέλευσης
Source port	Θύρα προέλευσης
Stack	Στοίβα
Statistical Analysis Attack	Επίθεση Στατιστικής Ανάλυσης
Steganography	Στεγανογραφίας
Stream	Ροή
Switch	Μεταγωγέας
Threads	Νήματα
Threat	Απειλή
Ubiquitous / Pervasive Computing	Συστήματα Διάχυτου Υπολογισμού
User	Χρήστης
Vulnerability	Ευπάθεια
Web Application	Διαδικτυακή Εφαρμογή
Wide Area Networks	Δίκτυα Ευρείας Περιοχής