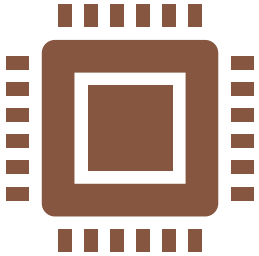
Ασφάλεια Πληροφοριακών Συστημάτων

Κώστας Σαΐδης

Περιεχόμενα

- Βασικές έννοιες
- Τύποι απειλών
- Ευπάθειες, Απειλές, Έλεγχοι
- Επιτιθέμενοι
- Μέθοδοι άμυνας
- Κρυπτογραφία
- Ψηφιακές υπογραφές
- Ψηφιακά πιστοποιητικά
- Αρχές ασφαλείας



Computer Security:

Διαφύλαξη υπολογιστικών πόρων από μη εξουσιοδοτημένη χρήση

Προστασία πληροφορίας από ακούσια ή σκόπιμη βλάβη, αποκάλυψη ή τροποποίησή της

Communication Security:

Προστασία δεδομένων κατά τη μετάδοση σε δίκτυα και κατανεμημένα συστήματα

Απόλυτη ασφάλεια δεν είναι δυνατόν να υπάρξει

Βασικές έννοιες

Αγαθό (asset)

Αγαθό (asset) είναι κάθε αντικείμενο (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, είτε από το διαχειριστή του συστήματος.

Κίνδυνοι και Ζημίες

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).**

Απειλές, Επιθέσεις & Αντίμετρα

- Απειλή (Threat): Οντότητα που μπορεί να προκαλέσει ζημιά ή παραβίαση σε τμήμα ή στο σύνολο του δικτύου
  - Κλίμακα: local, shared, national
  - Είδη: φυσική, εκούσια, ακούσια
- Επίθεση (Attack): Είναι η εκμετάλλευση μιας αδυναμίας ή ευπάθειες (vulnerability) από εισβολέα για την πραγματοποίηση απειλής (Exploit = επιτυχής επίθεση)
  - Είδη ευπαθειών: human (insider), software, hardware, media, communication, physical, natural
  - Οι επιθέσεις έχουν επιπτώσεις (impact) και προκαλούν ζημίες
- Αντίμετρα (Countermeasures): Μηχανισμός ή διαδικασία με στόχο τον περιορισμό ή την εξάλειψη επιπτώσεων απειλής
  - Συνεπάγονται πρόσθετο κόστος

Ασφάλεια Πληροφοριών

Εμπιστευτικότητα (Confidentiality)

Ακεραιότητα (Integrity)

Διαθεσιμότητα (Availability)

Ασφάλεια Πληροφοριών

Επίσης

- Πιστοποίηση Ταυτότητας (Authentication)
- Εξουσιοδότηση (Authorization)
- Μη-αποποίηση (Non-repudiation)
- Λογιστική καταγραφή (Accounting)

Αλληλεξάρτηση

- Παράδειγμα 1
  - Αποσυνδέουμε τους υπολογιστές από το Διαδίκτυο ώστε να αυξήσουμε την εμπιστευτικότητα
  - Δημιουργούμε πρόβλημα στη διαθεσιμότητα και πιθανώς στην ακεραιότητα (lost updates)
- Παράδειγμα 2
  - Ενεργοποιούμε πολλαπλούς ελέγχους (άνθρωποι / μηχανές) για να αυξήσουμε την ακεραιότητα
  - Προκαλούμε πρόβλημα στην εμπιστευτικότητα μιας και η πληροφορία γίνεται διαθέσιμη σε περισσότερες οντότητες
  - Ομοίως στη διαθεσιμότητα μιας και οι περισσότεροι έλεγχοι (μέχρις ότου ολοκληρωθούν) απαγορεύουν την πρόσβαση στα δεδομένα

Εμπιστευτικότητα

- Εγγυάται ότι τα δεδομένα **δεν** αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες
- Εμπιστευτικότητας μη Εγκατεστημένης Σύνδεσης (Connectionless Confidentiality Service). Παρέχει εμπιστευτικότητα μεμονωμένων τμημάτων δεδομένων
- Εμπιστευτικότητα σύνδεσης (Connection Confidentiality Service). Παρέχει εμπιστευτικότητα στα προς μετάδοση δεδομένα

Εμπιστευτικότητα

- Υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου (Selected Field Confidentiality Service). Παρέχει εμπιστευτικότητα συγκεκριμένων πεδίων στα δεδομένα μιας σύνδεσης ή σε μεμονωμένα τμήματά τους

- Υπηρεσία Εμπιστευτικότητας Ροής Κίνησης (Traffic Flow Confidentiality Service). Παρέχει προστασία από επιθέσεις τύπου ανάλυσης κυκλοφορίας

Ακεραιότητα Δεδομένων

- Εξασφαλίζει τη **μη τροποποίηση** των δεδομένων από μη-εξουσιοδοτημένους χρήστες. Π.χ. για την ασφάλεια επικοινωνιών διακρίνουμε σε:
  - Υπηρεσία Ακεραιότητας Σύνδεσης με αποκατάσταση (Connection Integrity Service With Recovery). Εξασφαλίζει ακεραιότητα και παρέχει παράλληλα δυνατότητα ανάκτησης
  - Υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery). Παρέχει μόνον ακεραιότητα δεδομένων

Αυθεντικοποίηση / Πιστοποίηση ταυτότητας

- Στοχεύει να αποδεικνύει την ταυτότητα οντότητας και να εξασφαλίζει τη γνησιότητα μηνυμάτων που ανταλλάσσονται σε μια επικοινωνία. Διακρίνουμε σε:
  - Αυθεντικοποίηση Ομότιμης Οντότητας (Peer Entity Authentication). Μία οντότητα δεν μπορεί να προσποιηθεί ότι είναι μία άλλη
  - Αυθεντικοποίηση Προέλευσης δεδομένων (Data Origin Authentication). Η πηγή προέλευσης μηνύματος είναι αυτή που ισχυρίζεται.

Τεχνικές υλοποίησης

- Τύπος I: Κάτι που το λογικό υποκείμενο γνωρίζει (πχ. ένα συνθηματικό ή ένα PIN)
- Τύπος II: Κάτι που το λογικό υποκείμενο κατέχει (μαγνητική συσκευή αναγνώρισης π.χ. έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)
- Τύπος III: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του (συστήματα βιομετρικής τεχνολογίας, π.χ. εφαρμογές δακτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού)
- Τύπος IV: Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο (π.χ. διεύθυνση IP).

Προστατευόμενος πόρος	**Κάτι που γνωρίζεις**	**Κάτι που έχεις**	**Κάτι που είσαι**	**Γεωγραφική θέση**
Πλατφόρμα, Host	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Αναγνωριστικό υπολογιστή ή IP διεύθυνση
Σύστημα Διαχείρισης Δικτύου (σύστημα αρχείων και εκτυπώσεων)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα - Ψηφιακό πιστοποιητικό	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Έλεγχος χρονικής στιγμής ή θέση του Η/Υ από τον οποίο γίνεται η πρόσβαση
Υπηρεσία Δικτύου (Web, FTP, Telnet)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα		Διεύθυνση IP
Σύστημα Διαχείρισης Βάσεων Δεδομένων	Όνομα χρήστη/ συνθηματικό			Διεύθυνση IP

Σχήματα αυθεντικοποίησης προστατευόμενων πόρων

Εξουσιοδότηση /Έλεγχος προσπέλασης

- Παρέχει προστασία χρήσης πόρων του συστήματος, από μη εξουσιοδοτημένες οντότητες.
- Συνεργάζεται με τις υπηρεσίες αυθεντικοποίησης.

(Μη) Αποποίηση

- Π.χ. για την ασφάλεια επικοινωνιών
  - Μη αποποίηση με Απόδειξη Προελεύσεως (Non-Repudiation With Proof Of Origin). Παρέχει πιστοποίηση προέλευσης των ληφθέντων μηνυμάτων
  - Μη αποποίηση με Απόδειξη Παραδόσεως (Non-Repudiation With Proof Of Delivery). Παρέχει πιστοποίηση παράδοσης μηνυμάτων στον αποστολέα

Είδη απειλών

- Interception
  - Μη εξουσιοδοτημένη οντότητα καταφέρνει να προσπελάσει κάποιο πόρο
- Interruption
  - Ένας πόρος καταστρέφεται, ή δεν είναι προσπελάσιμος
- Modification
  - Μη εξουσιοδοτημένη οντότητα μεταβάλλει την κατάσταση ενός πόρου
- Fabrication
  - Μη εξουσιοδοτημένη οντότητα φαλκιδεύει έναν πόρο

Είδη Απειλών

- Για τους πόρους (resources)
- Για τα δεδομένα (data)
- Για το λογισμικό (s/w)
- Για το υλικό (h/w)

Είδη Απειλών για το Υλικό

- Εγκατάσταση / αφαίρεση μιας συσκευής
  - Π.χ.: Snooping, wiretapping
  - Π.χ.: Modification, alteration
- Φυσικές απειλές/επιθέσεις στο h/w
  - Αθέλητες ή εσκεμμένες
  - Κλοπή / Καταστροφή
    - Πρόκληση ζημιάς στη μηχανή
    - Κλοπή
- Απαιτούνται αντίμετρα: φύλακες, κλειδαριές, επιτήρηση χώρου

Είδη Απειλών για το Λογισμικό

- Κατά λάθος διαγραφή
  - Version management
  - Version control
- Modification
  - Trojan Horses
  - Viruses
  - Logic Bombs
  - Trapdoors
- Theft

Bacterium (rabbit programs)

A specialized form of virus which does not attach to a specific file. A type of malware that create many instances of themselves or run many times simultaneously in order to consume large amounts of system resources.

Logic bomb

Malicious [program] logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources.

Trapdoor

A hidden computer flaw known to an intruder, or a hidden computer mechanism (usually software) installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms.

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virus

A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Worm

A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Είδη Απειλών για τα Δεδομένα

- Πόσο πολύτιμα είναι τα δεδομένα; Αριθμός πιστωτικής κάρτας vs. Αριθμός τηλεφώνου
  - Πηγαίος κώδικας
  - “4798” ->πρόθεμα τηλεφωνικού αριθμού ή τμήμα Α.Φ.Μ.?
- Επαρκής προστασία
  - Κρυπτογραφία
  - Χρονικοί περιορισμοί (αναθεώρηση)

Είδη Απειλών στο Διαδίκτυο

Πλαστοπροσωπία (masquerading)

Συμβαίνει όταν ένας μη εξουσιοδοτημένος χρήστης προσπαθεί μέσω αντιποίησης ταυτότητας να εγελάσει το σύστημα ελέγχου πρόσβασης και να χρησιμοποιήσει πόρους του συστήματος ως να ήταν κάποιος άλλος νόμιμα εξουσιοδοτημένος χρήστης

Είδη Απειλών στο Διαδίκτυο

Παθητική παρακολούθηση (passive tapping)

Συμβαίνει όταν ο επιτιθέμενος αποκτά πρόσβαση στη διακίνηση δεδομένων και τα καταγράφει, π.χ. με σκοπό τη μετέπειτα ανάλυσή τους.

Είδη Απειλών στο Διαδίκτυο

Ενεργή παρακολούθηση (active tapping)

Συμβαίνει όταν ο επιτιθέμενος αποκτά πρόσβαση στη διακίνηση δεδομένων και είτε τα τροποποιεί είτε εισάγει δικά του πλαστά δεδομένα.

Είδη Απειλών στο Διαδίκτυο

Αποποίηση (repudiation)

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

Είδη Απειλών στο Διαδίκτυο

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

Είδη Απειλών στο Διαδίκτυο

Επανεκπομπή μηνυμάτων (replay)

Συμβαίνει όταν ο επιτιθέμενος συνδυάζει παθητική παρακολούθηση με καταγραφή μηνυμάτων και μεταγενέστερη επανεκπομπή (playback) τους.

Είδη Απειλών στο Διαδίκτυο

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.

Είδη Απειλών στο Διαδίκτυο

Κακόβουλο λογισμικό

Λογισμικό του οποίου ο επιτιθέμενος επιδιώκει την εκτέλεση από νόμιμα εξουσιοδοτημένες οντότητες με σκοπό την εξαπόλυση πρόσθετων επιμέρους επιθέσεων (trojan horse, virus, κλπ. Βλ. παραπάνω).

Επιθέσεις & Συνέπειές τους

Αποκάλυψη (Disclosure)

Επίθεση κατά της εμπιστευτικότητας

Tapping / snooping

Επιθέσεις & Συνέπειές τους

Μη-εξουσιοδοτημένη μεταβολή (modification) ή εξαπάτηση (deception)

Π.χ., παροχή εσφαλμένων δεδομένων (επίθεση κατά της ακεραιότητας)

Modification: salami attack

Π.χ., από κάθε λογαριασμό καταθέσεων μιας τράπεζας αποκόπτω λεπτά του € και τα καταθέτω στο δικό μου λογαριασμό

Fabrication: replay data

Κάνω την ίδια κατάθεση στο λογαριασμό μου δύο ή περισσότερες φορές

Επιθέσεις & Συνέπειές τους

Παρεμπόδιση (Disruption)
Επίθεση κατά της διαθεσιμότητας

Latency/delay

DoS (non-responsiveness / downtime)

Επιθέσεις & Συνέπειές τους

Σφετερισμός (Usurpation)

Μη-εξουσιοδοτημένη χρήση υπηρεσιών (επίθεση κατά της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας)

Ποτέ δεν το έστειλα

Ποτέ δεν το έλαβα

Ευπάθειες

Network vulnerabilities

Οφείλονται σε πολυπλοκότητα

Δίνουν στους επιτιθέμενους τη δυνατότητα συνεργασίας

Ασύρματα δίκτυα

Access vulnerabilities

Κλοπή κύκλων επεξεργαστή, εύρους ζώνης

Κακόβουλη φυσική πρόσβαση

DoS στους εξουσιοδοτημένους χρήστες

People vulnerabilities

Πολύ συχνά το πιο αδύναμο σημείο ασφάλειας

Δυσαρεστημένοι υπάλληλοι

Social engineering

Social Engineering

Phishing
Baiting
Quid pro quo
Virus hoaxes
Dumpster diving
Reverse social engineering
Pretexting

Επιτιθέμενοι

Χρειάζονται ΜΟΜ

Μέθοδο (Method)
Skill, knowledge, tools …

Ευκαιρία (Opportunity)
χρόνο και πρόσβαση

Κίνητρο (Motive)
Χρήματα, ανταγωνισμός, …

Μέθοδοι άμυνας

Prevent attack

Εμπόδισε την επίθεση / διόρθωσε την αδυναμία

Deter attack

Δυσκόλεψε την επίθεση

Deflect attack

Κάνε κάποιο άλλο στόχο ελκυστικότερο

Detect attack

Κατά τη διάρκεια ή μετά

Recover from attack

Μηχανισμοί ελέγχου

Κρυπτογραφία
Έλεγχοι S/W
Έλεγχοι H/W
Πολιτικές και διαδικασίες
Φυσικοί έλεγχοι

Πολιτικές & Διαδικασίες

Πολιτική (policy) vs. Διαδικασία (procedure)

Policy: τι ακριβώς επιτρέπεται/απαγορεύεται

Procedure: το πώς επιβάλλεται η πολιτική

Κάθε πολιτική πρέπει να λαμβάνει υπόψη:

- Τις ισχύουσες νομικές και ηθικές νόρμες
- Ευχρηστία υλοποίησης
- Περιοδικοί έλεγχοι / αναθεώρηση

Εμπιστοσύνη

- “Μία οντότητα Α θεωρείται ότι εμπιστεύεται μία δεύτερη οντότητα Β όταν η οντότητα Α αποδέχεται ότι η οντότητα Β θα συμπεριφερθεί ακριβώς όπως αναμένεται και απαιτείται”.
- Εμπιστοσύνη βασισμένη στο λογισμό: εκτίμηση του βαθμού εξάρτησης από τις άλλες οντότητες, το προσδοκώμενο όφελος και τους ενδεχόμενους κινδύνους
- Εμπιστοσύνη βασισμένη στην πληροφορία: μείωση της αίσθησης αβεβαιότητας και ελαχιστοποίηση των ενδεχόμενων κινδύνων
- Μεταβατική εμπιστοσύνη: τυφλή εμπιστοσύνη προς τις οντότητες που υποδεικνύονται από μια ήδη έμπιστη τρίτη οντότητα

Κρυπτογραφία

Συμμετρική (Κλασική) Κρυπτογραφία

- Το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση δεδομένων
- Τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί
- Η προστασία και διανομή του κλειδιού αποτελεί κρίσιμο πρόβλημα

Ασύμμετρη (Δημόσιου Κλειδιού) Κρυπτογραφία

- Χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα ιδιωτικό και ένα δημόσιο, τα οποία σχετίζονται μεταξύ τους με μονόδρομες συναρτήσεις (one-way functions)
- Τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται αποκλειστικά με το άλλο
- Μόνο μία φυσική οντότητα γνωρίζει το ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί είναι εύκολα διαθέσιμο στο κοινό

Κρυπτογραφία Δημόσιου κλειδιού και Ψηφιακά Πιστοποιητικά

- Πώς επαληθεύεται η ταυτότητα του κατόχου ενός ζεύγους κλειδιών;
- Πώς διασφαλίζεται η μυστικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία και τη χρήση τους;
- Πώς διανέμονται στο κοινό τα δημόσια κλειδιά, έτσι ώστε να διασφαλίζεται η αντιστοίχησή τους με μία φυσική οντότητα;
- Πώς ολοκληρώνεται ο κύκλος ζωής τους, όταν αυτό κριθεί αναγκαίο;
- Διαφαίνεται η ανάγκη ύπαρξης μίας **«Έμπιστης Τρίτης Οντότητας»** που διαχειρίζεται **«Ψηφιακά Πιστοποιητικά»**.

Ψηφιακό Πιστοποιητικό

- Ψηφιακό Πιστοποιητικό είναι μία ψηφιακά υπογεγραμμένη δομή δεδομένων, η οποία αντιστοιχίζει μία ή περισσότερες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει
- Το πιστοποιητικό είναι υπογεγραμμένο από μία Τρίτη Οντότητα, η οποία είναι Έμπιστη και Αναγνωρισμένη να δρα ως «Πάροχος Υπηρεσιών Πιστοποίησης» (Trusted Third Party – TTP & Certification Services Provider – CSP)
- Διασφαλίζει με τεχνικά, αλλά και νομικά, μέσα ότι ένα δημόσιο κλειδί ανήκει σε μία και μόνο συγκεκριμένη οντότητα και συνεπώς ότι η οντότητα αυτή είναι ο νόμιμος κάτοχος του αντίστοιχου ιδιωτικού κλειδιού

Είδη Ψηφιακών Πιστοποιητικών

- Προσωπικό πιστοποιητικό: Το υποκείμενο είναι φυσικό πρόσωπο
- Πιστοποιητικό Συσκευής ή Εξυπηρετητή (Server or Device certificate): Π.χ. Δρομολογητής ή Web server
- Πιστοποιητικό Ρόλου (Role-based certificate): Το υποκείμενο δεν είναι φυσικό πρόσωπο και ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αλλάζει
- Πιστοποιητικό Οργανισμού (Organisational certificate): Π.χ. “Microsoft Corp” για την υπογραφή λογισμικού
- Πιστοποιητικό Αντιπροσώπου ή Προσωρινό (Proxy certificate): Παράγεται από το ίδιο το υποκείμενο, έχει διάρκεια ισχύος λίγων ωρών, π.χ. μηχανισμοί single sign-on

Ηλεκτρονική Υπογραφή

- Η Ηλεκτρονική Υπογραφή (electronic signature) είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητάς του
- Χαρακτηριστικά:
  - Είναι μονοσήμαντα συνδεδεμένη με τον υπογράφοντα
  - Παρέχει τη δυνατότητα αναγνώρισης του υπογράφοντα
  - Δημιουργείται με μέσα που βρίσκονται στον αποκλειστικό έλεγχο του υπογράφοντα
  - Είναι μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο, με τρόπο ώστε να διασφαλίζεται η ακεραιότητά του

Νομικό Πλαίσιο

- Διεθνής αναγνώριση των ψηφιακών υπογραφών ως ισότιμες με τις ιδιόχειρες
- Η Ευρωπαϊκή οδηγία ΕC/93/1999 για τις ηλεκτρονικές υπογραφές έχει ήδη υιοθετηθεί από όλα τα κράτη-μέλη
- Στην Ελλάδα υιοθετήθηκε με το Π.Δ. 150/2001
- Η ΕΕΤΤ με την απόφαση 248/71 (ΦΕΚ 603/Β'/16-5-2002) ρυθμίζει τη διαπίστευση των παρόχων υπηρεσιών ταυτοποίησης και την έκδοση αναγνωρισμένων πιστοποιητικών

Αρχές Ασφαλείας

Η αρχή της ευκολότερης διείσδυσης (Principle of Easiest Penetration)

Ο επιτιθέμενος αναμένεται να χρησιμοποιήσει οποιοδήποτε πρόσφορο μέσο για να διεισδύσει σε ένα σύστημα

Αρχές Ασφαλείας

Η αρχή της επαρκούς προστασίας
(Principle of Adequate Protection)

Οι πόροι πρέπει να προστατεύονται στο βαθμό που το δικαιούνται και μόνο για το χρονικό διάστημα που έχουν κάποια αξία

Αρχές Ασφαλείας

Η αρχή της αποτελεσματικότητας (Principle of Effectiveness)

Κάθε μηχανισμός ελέγχου πρέπει να χρησιμοποιείται σωστά ώστε να είναι αποτελεσματικός.

Αρχές Ασφαλείας

Η αρχή του πιο αδύναμου συνδέσμου (Principle of Weakest Link)

Η ασφάλεια είναι τόσο ισχυρή όσο η πιο αδύναμη συνιστώσα της

Αρχές Ασφαλείας

Μην επικοινωνείς με αγνώστους -και μην τους εμπιστεύεσαι!

Μην αποδέχεσαι τίποτα χωρίς εγγυήσεις (αυθεντικότητας)

Όλοι πρέπει να αντιμετωπίζονται ως δυνητικά εχθροί / κακόβουλοι μέχρις αποδείξεως του εναντίου

Μην εμπιστεύεσαι κανέναν και τίποτα για μεγάλο χρονικό διάστημα

Πάντοτε να χρησιμοποιείς βέλτιστες, καλά δοκιμασμένες διεθνώς, αποτελεσματικές λύσεις και πρακτικές

Να είσαι πάντοτε σε επιφυλακή