ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ

- Η προστασία πόρων (δεδομένων και προγραμμάτων) από συμπτωματική ή κακόβουλη τροποποίηση, καταστροφή ή διαρροή
  - Ακεραιότητα
  - Αυθεντικότητα
  - Εγκυρότητα
  - Εμπιστευτικότητα
  - Διαθεσιμότητα

Γενικές έννοιες (1)

- Αγαθό
  - οτιδήποτε χρήζει προστασίας, υλικό ή λογισμικό
- Ιδιοκτήτης
  - ο νόμιμος κάτοχος ενός αγαθού
- Εξουσιοδότηση
  - παροχή δικαιώματος χρήσης από τον ιδιοκτήτη σε φυσικό πρόσωπο ή διαδικασία
- Χρήστης (εξουσιοδοτημένος ή μη)
  - αυτός που χρησιμοποιεί το αγαθό
- Αξία
  - μέτρο έκφρασης της σπουδαιότητας του αγαθού
- Επίπτωση
  - οι συνέπειες που μπορεί να έχει η απώλεια ή βλάβη του αγαθού

Γενικές έννοιες (2)

- Ρήγμα ασφάλειας (breach) ή παραβίαση (violation)
  - συμβάν κατά το οποίο το αγαθό υφίσταται ζημιά
- Αδυναμία (vulnerability)
  - χαρακτηριστικό που είναι δυνατόν να επιτρέψει μια παραβίαση
- Απειλή (threat)
  - παράγων που μπορεί να προξενήσει ζημιά
- Μέσο προστασίας (safeguard)
  - ενέργειες και μηχανισμοί για τον περιορισμό των κινδύνων
- Πρόληψη, ανίχνευση, επανόρθωση
  - εφαρμογή μέσων προστασίας για να μη συμβεί παραβίαση
- Ανίχνευση
  - εντοπισμός του ότι έγινε παραβίαση
- Επανόρθωση
  - αποκατάσταση των επιπτώσεων της παραβίασης
- Κόστος
  - Σε χρήμα, υποβάθμιση απόδοσης, δυσαρέσκεια

Γενικές έννοιες

- για να προστατεύσουμε κάποια **αγαθά** που έχουν συγκεκριμένη **αξία** και να μην υποστούμε τις **επιπτώσεις** που θα έχει μία **παραβίαση** που θα τα αφορά, θα πρέπει να χρησιμοποιήσουμε κάποια **μέσα προστασίας** που έχουν κάποιο **κόστος**
- Πιθανόν να **επιλέξει** ο ιδιοκτήτης ενός πληροφοριακού συστήματος να μην εφαρμόσει κάποια μέσα προστασίας, διότι εκτιμά ότι το κόστος τους είναι υπερβολικό, σε σχέση με την αξία τους και τους κινδύνους που διατρέχουν

ΑΣΦΑΛΕΙΑ Ή ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΩΝ;

- Υπάρχει ασφαλές σύστημα;
  - Η εφαρμογή μέσων προστασίας έχει κόστος
  - Τα αγαθά έχουν αξία
  - Το κόστος προστασίας οφείλει να είναι ανάλογο της προστατευόμενης αξίας
  - Το κόστος παραβίασης πρέπει να είναι υψηλότερο του οφέλους του εισβολέα από την παραβίαση

ΕΠΙΣΚΟΠΗΣΗ

- Παραδείγματα συνηθισμένων απειλών
- Κατηγοριοποίηση των απειλών
- Μηχανισμοί προστασίας
- Τεχνικές διασφάλισης της ασφάλειας των συστημάτων
- Ασφάλεια δικτύων

Συνηθισμένες απειλές (1)

- Αποκάλυψη συνθηματικών
  - Εξαντλητική αναζήτηση
  - Λίστες συχνά χρησιμοποιούμενων συνθηματικών
  - Προκαθορισμένα συνθηματικά
- Οι «κακοί» διευκολύνονται από τους γρήγορους υπολογιστές και τα δίκτυα

Συνηθισμένες απειλές (2)

- Πλοήγηση
  - Μετά την επιτυχία της πρώτης εισβολής, συλλέγονται δεδομένα και πληροφορίες για επίθεση ευρύτερης κλίμακας
  - Αναζήτηση σε σελίδες μνήμης ή σε μπλοκ δίσκου για χρήσιμες πληροφορίες

Συνηθισμένες απειλές

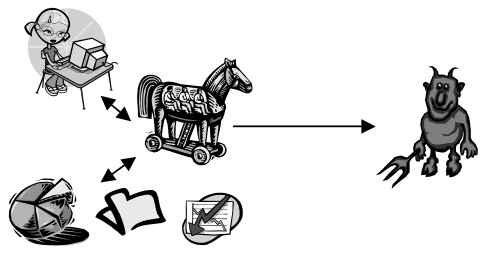
- Αντιποίηση (spoofing): Ο χρήστης πιστεύει ότι αλληλεπιδρά με το σύστημα ή τον προτιθέμενο δικτυακό τόπο
  - Υποκλοπείς συνθηματικών
  - Παραφθαρμένα ονόματα δικτυακών τόπων
    - » https://www.amason.com/online-shop/cart?item=20
  - Πλαστές δικτυακές διευθύνσεις

Συνηθισμένες απειλές

- Δούρειοι Ίπποι
  - Προγράμματα με «περισσότερη λειτουργικότητα» απ' ό,τι υπόσχονται
    - » Κειμενογράφοι που θέτουν τα αρχεία να είναι αναγνώσιμα-εγγράψιμα από όλους
    - » Προγράμματα υποκλοπής διευθύνσεων, συνθηματικών, στοιχείων του υπολογιστή
    - » Κάθε πρόγραμμα είναι τόσο «ύποπτο» όσο ο συγγραφέας του ή το δίκτυο διανομής του

Συνηθισμένες απειλές

- Δούρειοι ίπποι



Συνηθισμένες απειλές

- Παραπόρτια (trapdoors)
  - Τροποποιήσεις συστημάτων που εγκαθίστανται από εισβολείς και που δίνουν πρόσβαση στους εισβολείς
    - » Προγράμματα login που δίνουν δικαιώματα υπερχρήστη για συγκεκριμένα ονόματα σύνδεσης
    - » Back Orifice
  - Ενίοτε εγκαθίστανται από τους κατασκευαστές

Συνηθισμένες απειλές

- Ιοί
  - Προγράμματα που «μολύνουν» άλλα προγράμματα, ενσωματώνοντας σ' αυτά -πιθανώς εξελιγμένα- αντίγραφα του εαυτού τους
    - » Βλάβες: διαγραφή/αλλοίωση αρχείων, υποβάθμιση απόδοσης, κατανάλωση χώρου, ενόχληση
    - » Βασικοί τρόποι διάδοσης: τομείς εκκίνησης, εκτέλεση μολυσμένου προγράμματος, εκτέλεση δικτυακής εφαρμογής, άνοιγμα «παραλλαγμένου» συνημμένου αρχείου, χρήση διαμοιρασμένου πόρου

Συνηθισμένες απειλές

- Διαρροή πληροφοριών
  - Διεργασίες που είναι εξουσιοδοτημένες να προσπελαύνουν δεδομένα τα αποκαλύπτουν σε χρήστες που δεν είναι εξουσιοδοτημένοι
- Συμπερασμός δεδομένων
  - Η συσχέτιση φαινομενικά άσχετων δεδομένων οδηγεί σε εξαγωγή πληροφοριών

Στατιστικές βάσεις δεδομένων

- Οι στατιστικές βάσεις δεδομένων δίνουν πληροφορίες για ομάδες πληθυσμού, αλλά όχι για μεμονωμένα άτομα
  - Με κατάλληλες ερωτήσεις είναι δυνατόν να εξαχθούν ατομικές πληροφορίες

«Πλήθος και μέσος μισθός των ανδρών με ηλικία μικρότερη των 35 ετών» → (10, 2000)

«Πλήθος και μέσος μισθός των ανδρών με ηλικία μικρότερη των 34 ετών» → (9, 1800)

Συνηθισμένες απειλές

- Πλαστογράφηση
  - Η μη εξουσιοδοτημένη τροποποίηση δεδομένων
    - » Αποθηκευμένα δεδομένα
    - » Μεταδιδόμενα δεδομένα
- Παρεμπόδιση παροχής υπηρεσιών
  - Υποβάθμιση απόδοσης ή ολική αποτροπή της πρόσβασης των εξουσιοδοτημένων χρηστών
- Μη ηθελημένη καταστροφή
  - Εξουσιοδοτημένοι χρήστες πραγματοποιούν ατυχείς ενέργειες

Προβλήματα στην ασφάλεια δεν αναφέρονται

- Η αναφορά ενός προβλήματος δίνει ιδέες σε άλλους επίδοξους εισβολείς
- Η αρνητική δημοσιότητα διώχνει πελάτες και δυσαρεστεί τους μετόχους
- Πολλές φορές η σημασία ενός συμβάντος υποβαθμίζεται

Διαστάσεις της ασφάλειας (1)

- *Εμπιστευτικότητα*: οι πληροφορίες είναι προσπελάσιμες μόνο από εξουσιοδοτημένους χρήστες
- *Ακεραιότητα*: τα δεδομένα και τα προγράμματα τροποποιούνται και καταστρέφονται μόνο με καλά καθορισμένους τρόπους και με κατάλληλη εξουσιοδότηση
- *Διαθεσιμότητα*: Οι εξουσιοδοτημένοι χρήστες θα μπορούν να χρησιμοποιήσουν δεδομένα, προγράμματα και υπηρεσίες όταν το επιθυμήσουν

Διαστάσεις της ασφάλειας (2)

- *Αυθεντικότητα*: εξασφάλιση ότι τα δεδομένα είναι απαλλαγμένα ατελειών και ανακριβειών κατά τις εξουσιοδοτημένες τροποποιήσεις
- *Εγκυρότητα*: εξασφάλιση ότι τα δεδομένα είναι ακριβή και πλήρη

Ασφάλεια σε δικτυακό περιβάλλον

- Δίκτυο: ένα σύνολο διασυνδεδεμένων υπολογιστών
- Οι υπολογιστές παρέχουν υπηρεσίες και αποθηκεύουν πληροφορίες
- Οι χρήστες προσπελαύνουν υπηρεσίες και ανταλλάσσουν ή/και αποθηκεύουν πληροφορίες
- Απαίτηση: Να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα

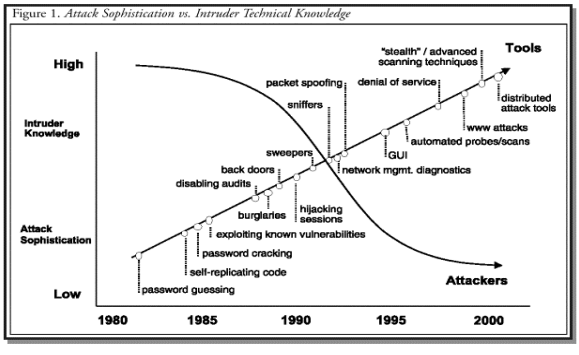
Ασφάλεια σε δικτυακό περιβάλλον - Προσεγγίσεις

- Ισχυρή διακρίβωση ταυτότητας των ενεχόμενων μερών (χρηστών-συστημάτων)
- Αξιόπιστοι μηχανισμοί ελέγχου εξουσιοδότησης/προσπέλασης
- Αποτελεσματικοί έλεγχοι κατάχρησης δικαιωμάτων
- Άψογα πρωτόκολλα, λειτουργικά συστήματα, εφαρμογές
- Τέλειες πολιτικές, απαράβατη εφαρμογή τους
- Κάθε χρήστης είναι ειδικός στην ασφάλεια

Δικτυακή ασφάλεια – η πραγματικότητα

- Δεν εφαρμόζονται αποτελεσματικοί μέθοδοι προστασίας
- Δεν εγκαθίστανται οι επιδιορθώσεις που παρέχονται από τους κατασκευαστές λογισμικού
- Η δικτυακή πρόσβαση δεν απαιτεί επαρκή πιστοποίηση, η πρόσβαση στους «εσωτερικούς» υπολογιστές δεν παρακολουθείται και δεν ελέγχεται
- Δεν διατίθεται προσωπικό για ζητήματα ασφάλειας
- Δεν εφαρμόζονται πολιτικές
- «Ωχ αδελφέ, δεν θα το βρουν»

Ποιοι και πώς επιτίθενται



Προσεγγίσεις στην ασφάλεια

- Ορισμός ασφαλών διαδικασιών
- Μηχανισμοί για επιβολή των μέτρων ασφαλείας
- Διασφάλιση μέσω ανάλυσης-επαλήθευσης

Μηχανισμοί προστασίας

- Διακρίβωση ταυτότητας
- Έλεγχος προσπέλασης

Διακρίβωση ταυτότητας

- Το σύστημα προσπαθεί να εξακριβώσει με ποιον συνδιαλλάσσεται εξετάζοντας:
  - αν ο χρήστης *γνωρίζει κάτι* (κάποιο μυστικό, συνθηματικό, προσωπικό αριθμό αναγνώρισης κ.λπ.)
  - αν ο χρήστης *κατέχει κάτι* (έξυπνη κάρτα, κάρτα αυτόματων συναλλαγών κ.ά.)
  - αν ο χρήστης *έχει κάποιο βιομετρικό χαρακτηριστικό* (*δακτυλικά αποτυπώματα, ίριδα ματιού κ.ο.κ.)*

Διακρίβωση ταυτότητας μέσω στοιχείων που ο χρήστης γνωρίζει

- Συνήθως ζητάται κάποια *ταυτότητα* και κάποιο *συνθηματικό*
  - Στη γενική περίπτωση οι ταυτότητες είναι δημόσια γνωστές, τα συνθηματικά όχι
- Το συνθηματικό συγκρίνεται με αυτό που έχει το σύστημα αποθηκευμένο στο αρχείο συνθηματικών

Αξιολόγηση προσέγγισης

- Θετικά
  - Δοκιμασμένη τεχνική
  - Εύκολα κατανοητή από τους χρήστες
  - Ενσωματωμένη στα περισσότερα λειτουργικά συστήματα
- Αρνητικά
  - Τα συνθηματικά μπορεί να «μαντευθούν»
  - Οι χρήστες μπορεί να διαμοιράζονται τα συνθηματικά
  - Τα συνθηματικά μπορεί να υποκλαπούν
  - Μπορεί να εξαχθούν πληροφορίες από το αρχείο συνθηματικών

Αποφυγή μαντέματος συνθηματικών

- Είναι σκόπιμο να αποφεύγονται:
  - Κενά συνθηματικά
  - Ονόματα, επώνυμα, ημερομηνίες γέννησης, αριθμοί ταυτότητας, τηλέφωνα, διευθύνσεις
  - Το όνομα χρήστη
  - Τα παραπάνω γραμμένα ανάποδα, ή με μείγματα πεζών-κεφαλαίων χαρακτήρων
  - Ονόματα οδών, πόλεων, «υπαρκτές» λέξεις
- Είναι σκόπιμο να:
  - χρησιμοποιούνται συνθηματικά με μεγάλο πλήθος χαρακτήρων
    - » Δυνατοί συνδυασμοί: $96^{\text{πλήθος χαρακτήρων}}$
  - Να αλλάζουν σε τακτά χρονικά διαστήματα
- Αρκετοί κανόνες είναι δυνατόν να εφαρμόζονται από το σύστημα

Αποφυγή διαμοιρασμού

- Δεν αποκαλύπτουμε το συνθηματικό σε συναδέλφους, φίλους κ.λπ., ούτε σε άτομα που δηλώνουν «υπεύθυνοι ασφάλειας»
- Δεν γράφουμε το συνθηματικό, ειδικότερα σε προφανή σημεία

Αποφυγή υποκλοπής

- Τα συνθηματικά υποκλέπτονται:
  - σε κανάλια επικοινωνίας
    - » ασφαλή κανάλια
    - » «κρυπτογράφηση μίας φοράς»
  - όταν ο χρήστης τα εισάγει σε προγράμματα που αναπαράγουν τη διεπαφή του συστήματος
    - » Πλήκτρα ενεργοποίησης διαδικασίας σύνδεσης
      - Αποτρέπει προσπάθειες αντιποίησης
      - Εγγυάται ασφαλή πρόσβαση στο σύστημα
      - Ο χρήστης πρέπει να τα χρησιμοποιήσει

Αποφυγή διαρροής του αρχείου συνθηματικών

- Απλοϊκή προσέγγιση
  - Αποθηκεύω το συνθηματικό σε προστατευμένο αρχείο, συγκρίνω με αυτό που δίνει ο χρήστης
- Καλύτερη προσέγγιση
  - Κρυπτογραφώ το συνθηματικό με *μονόδρομη συνάρτηση*, το αποθηκεύω σε προσβάσιμο αρχείο. Κρυπτογραφώ και αυτό που δίνει ο χρήστης και συγκρίνω
  - Επιθέσεις με λεξικά ή «ωμή βία»
- Ακόμη καλύτερη προσέγγιση
  - Όπως στη δεύτερη περίπτωση, αλλά το αρχείο αποθήκευσης συνθηματικών είναι προστατευμένο

Διακρίβωση ταυτότητας μέσω στοιχείων που ο χρήστης κατέχει

- Ο χρήστης πρέπει να έχει στην κατοχή του ένα *διακριτικό* (token), το οποίο παρουσιάζει στο σύστημα
- Συνήθως συνδυάζεται με κάτι που ο χρήστης *γνωρίζει* (προσωπικός αριθμός αναγνώρισης)
- Δύο τύποι:
  - διακριτικά μνήμης
  - έξυπνα διακριτικά

Διακριτικά μνήμης

- Συνήθως κάρτες με μαγνητική ταινία όπου αποθηκεύεται η ταυτότητα του χρήστη
- Στη γενική περίπτωση ζητάται κάτι που ο χρήστης γνωρίζει, εκτός από συστήματα ελέγχου φυσικής πρόσβασης
- Γράφονται και διαβάζονται από εξειδικευμένες συσκευές
  - για τη χρήση του απαιτείται μόνο συσκευή ανάγνωσης

Αξιολόγηση διακριτικών μνήμης

- ✓ Πιο ασφαλή από το συνδυασμό *ταυτότητα-συνθηματικό*
- ✓ Διευκολύνουν την παραγωγή αρχείων καταγραφής
- ✓ Αν χρησιμοποιείται το ίδιο διακριτικό για φυσική πρόσβαση και πρόσβαση στον υπολογιστή, αποκλείεται να αφήσει κάποιος χρήστης τον υπολογιστή του όντας συνδεδεμένος
- × Απαιτούν εξειδικευμένες συσκευές ανάγνωσης
- × Διαχειριστικό και οικονομικό κόστος, καθώς και απώλεια πρόσβασης όταν χάνεται το διακριτικό
- × Οι χρήστες δεν το αποδέχονται πάντα

Έξυπνα διακριτικά

- Ένα έξυπνο διακριτικό αποτελείται από:
  - ένα διακριτικό μνήμης
  - ολοκληρωμένα κυκλώματα επεξεργασίας
  - διεπαφή για επικοινωνία με ανθρώπους ή μηχανές

Έξυπνα διακριτικά – Τρόπος λειτουργίας

- Ο χρήστης *πιστοποιεί τον εαυτό του* στο έξυπνο διακριτικό, εισάγοντας ένα συνθηματικό ή έναν προσωπικό αριθμό αναγνώρισης
- Το υπολογιστικό σύστημα ανταλλάσσει ταυτότητες με το διακριτικό και στέλνει στο διακριτικό έναν κωδικό, τον οποίο το διακριτικό επεξεργάζεται και επιστρέφει την απάντηση στο σύστημα
- Το σύστημα ελέγχει αν πρόκειται για παραδεκτή απάντηση από το συγκεκριμένο διακριτικό. Αν ναι, η ταυτότητα του χρήστη έχει διακριβωθεί
- Είναι πιθανόν κάποια τμήματα να γίνονται από τον ίδιο τον χρήστη

Αξιολόγηση έξυπνων διακριτικών

✓ Μεγαλύτερη ασφάλεια σε σχέση με τα διακριτικά μνήμης
  ✓ Συνθηματικά μίας χρήσης
  ✓ ελαττωμένος κίνδυνος παραχάραξης
    ✓ η μνήμη διαβάζεται μόνο αν έχει πιστοποιηθεί ο χρήστης στο διακριτικό
    ✓ πολύπλοκα κυκλώματα = δύσκολη κατασκευή πλαστών διακριτικών
✓ Μεγαλύτερη ευελιξία
  ✓ Χρήση με πολλά υπολογιστικά συστήματα – το διακριτικό περιέχει τη λογική συνδιαλλαγής με το καθένα, ο χρήστης πιστοποιεί τον εαυτό του στο διακριτικό
× Αυξημένο διαχειριστικό και οικονομικό κόστος, καθώς και απώλεια πρόσβασης όταν χάνεται το διακριτικό
× Οι χρήστες δεν το αποδέχονται πάντα, ειδικότερα όταν πρέπει να πληκτρολογούν εκτενείς συμβολοσειρές

Διακρίβωση ταυτότητας βάσει βιομετρικών χαρακτηριστικών

- Ανάγνωση βιομετρικών χαρακτηριστικών του ανθρώπου που είναι μοναδικά
  - δακτυλικά αποτυπώματα
  - ίριδα ματιού
  - χροιά φωνής
- Σύγκριση του χαρακτηριστικού με το πρότυπο που εγνωσμένα ανήκει στον χρήστη
× Όχι ώριμη τεχνολογία πιθανά σφάλματα (π.χ. η χροιά της φωνής αλλάζει λόγω κρυολογήματος)
× Μεγάλο κόστος
× Σημαντικά προβλήματα αποδοχής από τους χρήστες
✓ Αν δουλέψει, παρέχει πολύ καλή ασφάλεια

Έλεγχος προσπέλασης

- Ο περιορισμός της πρόσβασης του χρήστη μόνο στα αντικείμενα που δικαιούται
- Έννοιες
  - *Υποκείμενα*: Οι ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)
  - *Αντικείμενα*: Οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)
  - *Τρόπος προσπέλασης*: ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών
- *Ελέγχουμε αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο*

Είδη ελέγχου προσπέλασης

- Κατ' επιλογήν
  - Ο ιδιοκτήτης του κάθε αντικειμένου αποφασίζει ποιο υποκείμενο έχει δικαίωμα να το προσπελάσει και πώς
- Υποχρεωτικός
  - Το σύστημα αποφασίζει ποιο υποκείμενο να προσπελάσει κάθε αντικείμενο και τους επιτρεπτούς τρόπους
  - Η απόφαση βασίζεται στα ιδιοχαρακτηριστικά του χρήστη και του πόρου

Παραδείγματα κατ' επιλογήν ελέγχου προσπέλασης

- Συνθηματικά για πρόσβαση αρχείων
- Bits RWX του Unix για ιδιοκτήτη, ομάδα, λοιπούς
- Πίνακες ελέγχου προσπέλασης με μορφή:
  - λιστών ελέγχου προσπέλασης
  - λιστών προσδιοριστών δικαιωμάτων

Bits RWX

R	W	X	R	W	X	R	W	X
Ιδιοκτήτης			Ομάδα			Λοιποί		

- Εύκολη υλοποίηση από άποψης συστήματος
- Σχετικά κατανοητό από τους χρήστες
- Δύσκαμπτο για λεπτομερή ανάθεση δικαιωμάτων

Πίνακες ελέγχου πρόσβασης

Υποκείμενα \ Αντικείμενα	A1	A2	A3	A4	A5
Y1			R	RWD	R
Y2	R	X		R	
Y3		RXD	W	X	
Y4	RW		R	XD	

Λίστες ελέγχου προσπέλασης & προσδιοριστών δικαιωμάτων

	A1	A2	A3	A4	A5
Y1					
Y2		X			
Y3		RXD	W	X	
Y3					

Λίστα προσδιοριστών δικαιωμάτων

Λίστα ελέγχου προσπέλασης

Υποχρεωτικός Έλεγχος Προσπέλασης

- Κάθε υποκείμενο έχει ένα επίπεδο ασφάλειας
- Κάθε αντικείμενο έχει ένα επίπεδο ασφάλειας
- Το κάθε επίπεδο ασφάλειας αποτελείται από μια *διαβάθμιση* και ένα *σύνολο κατηγοριών*
- Στην πρόσβαση συγκρίνονται τα επίπεδα ασφάλειας
  - ίσο, μεγαλύτερο, μικρότερο, *μη συγκρίσιμο*

Υποχρεωτικός Έλεγχος Προσπέλασης - Παράδειγμα

- Τρία επίπεδα ασφάλειας
  - αδιαβάθμητο, εμπιστευτικό, απόρρητο
- Τρεις κατηγορίες ασφάλειας
  - προμήθειες, λογιστήριο, διοίκηση

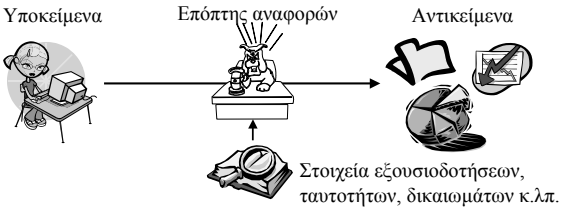
εμπιστευτικό/(προμήθειες) = εμπιστευτικό/(προμήθειες)
απόρρητο/(προμήθειες) > εμπιστευτικό/(προμήθειες)
εμπιστευτικό/(προμήθειες) < εμπιστευτικό(προμήθειες, λογιστήριο)
απόρρητο(προμήθειες) ***μη συγκρίσιμο*** απόρρητο(λογιστήριο)

Υποχρεωτικός Έλεγχος Προσπέλασης - Εφαρμογή

- Η ανάγνωση επιτρέπεται αν το υποκείμενο έχει μεγαλύτερο ή ίσο επίπεδο ασφάλειας από το αντικείμενο (no read-up)
- Η εγγραφή επιτρέπεται αν το υποκείμενο έχει μικρότερο ή ίσο επίπεδο ασφάλειας από το αντικείμενο (no write-down)

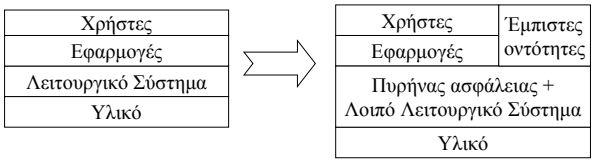
Επόπτης αναφορών

- Ελέγχει όλες τις αναφορές για να εγγυηθεί ότι εφαρμόζονται οι κανόνες



- Πρέπει να μην μπορεί να παρακαμφθεί, να ξεγελαστεί, να έχει δυνατότητα καταγραφής και να μπορεί να αποδειχθεί η ορθότητά του

Πυρήνας ασφάλειας



- Υπεύθυνος για την υλοποίηση όλων των μηχανισμών ασφάλειας του Λ.Σ. και σε όλα τα επίπεδα (υλικό, εφαρμογές, χρήστες κ.λπ.)
  - Υπέρ: Διαχωρισμός, ενοποίηση, συντηρησιμότητα, επαλήθευση
  - Κατά: Υποβάθμιση απόδοσης, μέγεθος, δυσκολία ενσωμάτωσης σε υπάρχοντα λειτουργικά συστήματα (άλλη δομή)
- Οι έμπιστες οντότητες επιτρέπεται να εκτελέσουν ενέργειες πέρα από τις δικαιοδοσίες τους ΑΛΛΑ πρέπει να μπορούν να παρακολουθηθούν/επαληθευθούν