



Πολιτικές ασφάλειας



Δρ. Χρήστος Ηλιούδης



Ασφαλές ή Έμπιστο υπολογιστικό σύστημα;

- Υπάρχει διαφορά στο χαρακτηρισμό ενός ΠΣ ως ασφαλούς και ως έμπιστου.
- Οι ειδικοί της ασφάλειας προτιμούν να μιλούν για
 - **έμπιστα συστήματα,**παρά για
 - **ασφαλή συστήματα,**υπονοώντας ότι αυτά ικανοποιούν τις επιδιωκόμενες απαιτήσεις ασφάλειας και έχουν αρκετά υψηλή και βεβαιωμένη ποιότητα.



Ασφαλές ή Έμπιστο υπολογιστικό σύστημα;

ΑΣΦΑΛΕΣ	ΕΜΠΙΣΤΟ
Είναι ή δεν είναι ασφαλές	Υπάρχουν βαθμίδες εμπιστοσύνης
Βεβαιούμενο στη βάση χαρακτηριστικών του προϊόντος	Κρινόμενο στη βάση γεγονότων και αναλύσεων
Απόλυτο: χωρίς επιφυλάξεις για το πώς, που, πότε και από ποιον χρησιμοποιείται	Σχετικό: θεωρείται στο πλαίσιο της χρήσης
Σκοπός	Χαρακτηριστικό



Πολιτικές Ασφάλειας

- Για να μπορούμε να γνωρίζουμε κατά πόσον ένα υπολογιστικό σύστημα παρέχει την αναμενόμενη ασφάλεια, πρέπει να μπορούμε να διατυπώσουμε το **τι είναι** αυτή η ασφάλεια.
- Οι απαιτήσεις ασφάλειας ενός υπολογιστικού συστήματος προσδιορίζονται διαμέσου μιας πολιτικής ασφάλειας (security policy).



Πολιτικές Ασφάλειας

- Η πολιτική ασφάλειας ενός υπολογιστικού συστήματος είναι ένα σύνολο:
 - από αρχές (principles) και
 - οδηγίες υψηλού επιπέδου (high level guidelines) που αφορούν τη σχεδίαση και διαχείριση συστημάτων ελέγχου προσπάθειας.
- Μια πολιτική ασφάλειας εκφράζεται με κανόνες προσπάθειας που ρυθμίζουν:
 - πως ελέγχονται οι προσπελάσεις και
 - πως λαμβάνονται οι αποφάσεις για προσπάθεια.



Μηχανισμοί Ασφάλειας

- Οι πολιτικές ασφάλειας συνήθως επιβάλλονται από διάφορους μηχανισμούς ασφάλειας, οι οποίοι μπορούν να ταξινομηθούν στις παρακάτω κατηγορίες:
 - αναγνώριση (identification),
 - αυθεντικοποίηση (authentication),
 - εξουσιοδότηση (authorization),
 - έλεγχος προσπέλασης (access control),
 - ακεραιότητα (integrity),
 - συνέπεια (consistency),
 - επίβλεψη (auditing).

Μηχανισμοί Ασφάλειας

- ... είναι χαμηλού επιπέδου λειτουργίες λογισμικού και υλικού που διαμορφώνονται κατάλληλα για την υλοποίηση μιας πολιτικής ασφάλειας.



Το TCSEC λεξιλόγιο

- Το TCSEC λεξιλόγιο ορίζει μια πολιτική ασφάλειας ως :
"το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως ένας οργανισμός διαχειρίζεται, προστατεύει και κατανέμει ευαίσθητες πληροφορίες".



Το ITSEC λεξιλόγιο

- Ομοίως, το ITSEC λεξιλόγιο ορίζει τον όρο πολιτική ασφάλειας ως:

"το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν με ποιο τρόπο τα στοιχεία διαχειρίζονται, προστατεύονται και κατανέμονται μέσα σε έναν οργανισμό χρηστών".



Υποκείμενα και Αντικείμενα

- Μια πολιτική ασφάλειας ορίζεται τυπικά στη βάση των όρων «υποκείμενα» και «αντικείμενα».
- Ένα υποκείμενο (subject) είναι κάτι ενεργό στο σύστημα,
 - Π.χ. οι χρήστες (users), οι διεργασίες (processes) και τα προγράμματα (programs).
- Αντικείμενο (object) είναι κάτι στο οποίο ενεργεί το υποκείμενο.
 - Π.χ. αρχεία (files), οι κατάλογοι (directories), οι συσκευές (devices), οι υποδοχές (sockets) και τα παράθυρα (windows).