ΕΝΟΤΗΤΑ 9

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ

Περιεχόμενα

1. Ασφάλεια vs Προστασία

- Με τον όρο *ασφάλεια* (security) αναφερόμαστε στο ολικό πρόβλημα της προστασίας των πληροφοριών σε ένα σύστημα από άτομα μη εξουσιοδοτημένα για να τις διαβάσουν ή και να τις τροποποιήσουν. Με τον όρο *μηχανισμοί προστασίας* (protection mechanisms) αναφερόμαστε στους συγκεκριμένους μηχανισμούς που προσφέρει ένα Λ.Σ. για να προστατεύσει τις πληροφορίες σε ένα σύστημα.

2. Ασφάλεια

- Η ασφάλεια έχει δύο όψεις:

  Απώλεια δεδομένων:

  — Φυσικές καταστροφές.
  — Σφάλματα υλικού ή λογισμικού.
  — Ανθρώπινα λάθη.

  Τα περισσότερα από αυτά μπορούν να αντιμετωπισθούν με τη χρήση εφεδρικών αρχείων, κατά προτίμηση σε μακρινή απόσταση από τα πρωτογενή δεδομένα.

  Εισβολείς:

  — Περίεργοι.
  — Εσωτερικοί εισβολείς (π.χ. υφιστάμενοι στα αρχεία προϊσταμένων τους).
  — Εξωτερικοί εισβολείς (π.χ. πρόσβαση σε λογαριασμούς τραπεζών).
  — Κατασκοπία (εμπορική, στρατιωτική).

3. Προϋποθέσεις για ύπαρξη ασφάλειας

- Μυστικότητα: Η προσπέλαση στις πληροφορίες πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα για αποφυγή π.χ. αντιγραφής λογισμικού με copyright, ή διάβασμα αρχείων με απόρρητες πληροφορίες.

- Πιστότητα: Η τροποποίηση των πληροφοριών πρέπει να επιτρέπεται μόνο από εξουσιοδοτημένα άτομα για αποφυγή π.χ. τροποποίησης λογισμικού έτσι ώστε να μην τρέχει σωστά κάτω από κάποιες συνθήκες ή μετά από αλλαγές κάποιων δεδομένων.

- Διαθεσιμότητα: Δυνατότητα χρήσης των οντοτήτων που βρίσκονται στο σύστημα (αρχεία, συσκευές, κλπ.) από τα εξουσιοδοτημένα σε κάθε περίπτωση άτομα. Αποφυγή δηλαδή κλοπής συσκευών, σβήσιμο αρχείων και λογισμικού, κλπ.

4. Είδη απειλών

- Διακοπή δυνατότητας χρήσης κάποιας οντότητας (interruption), π.χ. καταστροφή συσκευής, σβήσιμο αρχείου, κλπ. Απειλεί τη διαθεσιμότητα.

- Αναχαίτηση (interception) οντοτήτων, π.χ. αντιγραφή απαγορευμένων πληροφοριών. Απειλεί τη μυστικότητα.

- Μετατροπή, χωρίς εξουσιοδότηση, κάποιων πληροφοριών. Απειλεί την πιστότητα.

- Πηγές απειλών: i) “πόρτες-παγίδα” (trap doors), όπου ο προγραμματιστής κρύβει στο πρόγραμμα κάποια ρουτίνα που θα εκτελεσθεί μόνο αν στο πρόγραμμα δοθούν συγκεκριμένα δεδομένα, ii) “σκουλήκια” (worms) και ιοί (viruses) που αναπαραγάγονται σε ένα σύστημα, iii) αλλαγή σε ένα πρόγραμμα κοινής χρήσης (π.χ. κειμενογράφο) έτσι ώστε να κάνει κανονικά τη δουλειά του αλλά και να κλέβει λ.χ. αρχεία (δούρειος ίππος).

5. Σχεδιαστικές αρχές για ασφάλεια

- Για τον σχεδιασμό ενός ασφαλούς συστήματος, οι Saltzer και Schroeder (1975) διατύπωσαν τις εξής γενικές αρχές:

  Το σύστημα πρέπει να είναι ανοικτό (open design), δηλαδή η ασφάλειά του να μην βασίζεται στο να κρατήσει μυστικό τον σχεδιασμό του ή τους μηχανισμούς χρήσης του.

  Κάθε οντότητα στο σύστημα (χρήστης, πρόγραμμα, κλπ.) θα πρέπει να έχει τα ελάχιστα δυνατά δικαιώματα που θα του επιτρέπουν να επιτελεί την εργασία του.

  Οι μηχανισμοί προστασίας πρέπει να είναι όσο το δυνατόν πιο απλοί, ομοιόμορφοι και ενσωματωμένοι στα χαμηλότερα επίπεδα του συστήματος. Πρέπει να θεωρείται σχεδόν πάντα αποτυχημένη η προσπάθεια των εκ των υστέρων πρόσθεσης μηχανισμών ασφάλειας σε σύστημα που είναι ανασφαλές.

  Το επιλεγμένο σχήμα προστασίας πρέπει να είναι ψυχολογικά αποδεκτό. Οι χρήστες δεν πρέπει να αισθάνονται ότι η χρήση των διαθέσιμων μηχανισμών προστασίας απαιτεί πολύ δουλειά.

  Κάθε προσπάθεια προσπέλασης στο σύστημα (επιτυχημένη ή αποτυχημένη) πρέπει να καταγράφεται και να αναφέρεται στον σχετικό χρήστη.

  Οι εξουσιοδοτήσεις πρέπει να ελέγχονται περιοδικά για να διαπιστωθεί αν παραμένουν οι ίδιες.

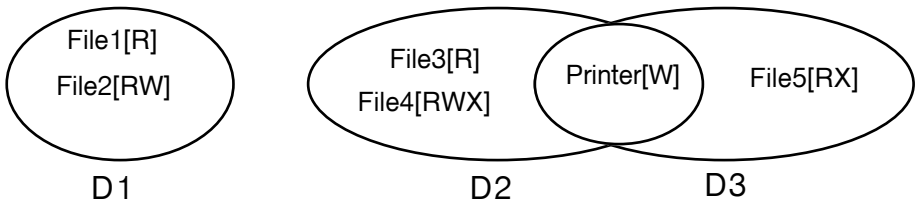
6. Μηχανισμοί προστασίας

- Τοποθέτηση των εξυπηρετητών σε ειδικά δωμάτια όπου πρόσβαση επιτρέπεται μόνο στο προσωπικό που ελέγχει τη λειτουργία τους.

- Χρήση *τεχνικών πιστοποίησης* (authentication) της ταυτότητας του χρήστη, π.χ. συνθηματικών λέξεων (passwords) όταν γίνεται σύνδεση με το σύστημα (login), μαγνητικές κάρτες ή εξακρίβωση δακτυλικών αποτυπωμάτων. Πληροφόρηση του χρήστη πότε ήταν η τελευταία φορά που επιχείρησε σύνδεση και αν ήταν επιτυχημένη.

- Παροχή δυνατοτήτων κρυπτογράφησης και αποκρυπτογράφησης αρχείων (όπως του αρχείου στο οποίο βρίσκονται καταχωρημένες οι συνθηματικές λέξεις των χρηστών).

- Χρήση *περιοχών προστασίας* (protection domains). Κάθε διεργασία βρίσκεται σε κάποια περιοχή που καθορίζει τα δικαιώματα που έχει για διάβασμα, γράψιμο ή εκτέλεση των αντικειμένων (και μόνο αυτών) που βρίσκονται στην περιοχή. Είναι σύνηθες κάποιες περιοχές να έχουν κοινά τμήματα.



- Χρήση *πινάκων προστασίας* (access tables) που ουσιαστικά υλοποιούν το ανωτέρω μοντέλο.

Περιοχή	File1	File2	File3	File4	File5	Printer
D1	R	RW				
D2			R	RWX		W
D3					RX	W

6. Μηχανισμοί προστασίας (συνέχεια)

- Το πρόβλημα είναι ότι οι περισσότερες από τις θέσεις του πίνακα είναι άδειες και ο πίνακας είναι μεγάλος και αραιός. Έτσι σπάνια υλοποιείται ο πίνακας καθ' εαυτός αλλά διασπάται σε σειρές ή στήλες.

- Αν αποθηκευθεί σε στήλες τότε έχουμε μία λίστα για κάθε αντικείμενο που δείχνει τους διαφορετικούς τρόπους που μπορεί να προσπελασθεί από κάθε περιοχή. Αυτή η λίστα λέγεται *λίστα ελέγχου προσπέλασης* (access control list, ACL). Π.χ. για το ανωτέρω παράδειγμα, η λίστα ελέγχου για το File4 είναι ACL_File4:D2(RWX). Η λίστα ελέγχου ενός αρχείου μπορεί να αποθηκευθεί σε ένα ξεχωριστό μπλοκ του δίσκου από αυτά που έχουν δοθεί στο αρχείο για την αποθήκευσή του.

- Αν αποθηκευθεί σε γραμμές τότε έχουμε μία λίστα από αντικείμενα για κάθε διεργασία που δείχνει για το ποιες πράξεις επιτρέπονται πάνω στο καθένα από αυτά, με άλλα λόγια την περιοχή του. Αυτή η λίστα λέγεται *λίστα προσδιοριστών δικαιωμάτων* (capability list) και κάθε στοιχείο της λέγεται *προσδιοριστής δικαιωμάτων* (capability). Π.χ. η λίστα προσδιοριστών δικαιωμάτων για την περιοχή D2 είναι CL_D2:File3(R), File4(RWX), Printer(W). Μία τέτοια λίστα συσχετίζεται με κάθε διεργασία που "βρίσκεται" στην περιοχή D2.

- Εκτός από τα συγκεκριμένα δικαιώματα (read, write, execute) τα οποία εξαρτώνται από τα αντικείμενα, οι προσδιοριστές δικαιωμάτων έχουν συνήθως και γενικευμένα δικαιώματα όπως:
  - δημιουργία νέου προσδιοριστή δικαιωμάτων για κάποιο αντικείμενο,
  - δημιουργία νέου αντικειμένου με νέο προσδιοριστή δικαιωμάτων,
  - διαγραφή δικαιώματος από τον προσδιοριστή κάποιου αντικειμένου,
  - διαγραφή αντικειμένου και του προσδιοριστή του.

6. Μηχανισμοί προστασίας (συνέχεια)

- Ο πίνακας προστασίας δεν παραμένει στατικός αν επιτρέπεται να αλλάζουν δυναμικά τα δικαιώματα των αντικειμένων. Κατ' αρχήν μπορεί να επιτρέπεται σε μία διεργασία να αλλάζει περιοχή. Αυτό επιτυγχάνεται με την απεικόνηση στον πίνακα κάθε περιοχής σαν αντικείμενο και την τοποθέτηση ενός συμβόλου (π.χ. της λέξης switch) στα μέρη εκείνα του πίνακα που δείχνουν μετάβαση από μία περιοχή σε άλλη. Στο κατωτέρω σχήμα οι διεργασίες που είναι στην περιοχή D3 μπορούν να μεταβούν στην D2 και αυτές που είναι στην D1 να μεταβούν στην D3.

Περιοχή	File1	File2	File3	File4	File5	Printer	D1	D2	D3
D1	R	RW							switch
D2			R	RWX		W			
D3					RX			switch	

- Επιπλέον, μπορεί να δοθεί η δυνατότητα μεταφοράς ή αντιγραφής ενός δικαιώματος από μία περιοχή σε κάποια άλλη. Αυτό πάλι παριστάνεται στον πίνακα με ένα κατάλληλο σύμβολο (π.χ. έναν αστερίσκο). Στην κατωτέρω παραλλαγή του πίνακα το δικαίωμα του αντικειμένου File3 να διαβαστεί από κάποια διεργασία που βρίσκεται στην περιοχή D2 μπορεί να μεταφερθεί σε κάποια άλλη διεργασία που βρίσκεται σε διαφορετική περιοχή. Κάτι ανάλογο μπορεί να συμβεί (και συνέβη) με τον εκτυπωτή. Τέτοιου είδους αλλαγές στα δικαιώματα μπορούν να γίνουν με τρεις παραλλαγές: i) μεταφορά, ii) αντιγραφή, και iii) περιορισμένη αντιγραφή.

Περιοχή	File1	File2	File3	File4	File5	Printer	D1	D2	D3
D1	R	RW							switch
D2			R*	RWX		W*			
D3					RX	W		switch	