ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 1: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

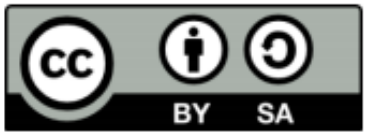
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 1

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

Σκοποί ενότητας

Ασφάλεια Δικτύων

Ασφάλεια δικτύων

- Στα χαμηλά επίπεδα: να φτάσουν τα πακέτα στον παραλήπτη χωρίς σφάλματα
- Σε ανώτερο επίπεδο: να προστατευθεί η διακινούμενη πληροφορία έτσι ώστε:
  - Να μην μπορεί να διαβαστεί από μη εξουσιοδοτημένα πρόσωπα ή συσκευές
  - Να μη μπορεί να τροποποιηθεί από μη εξουσιοδοτημένα άτομα
  - Να μην επιτρέπεται η πρόσβαση σε υπολογιστικούς και δικτυακούς πόρους από μη εξουσιοδοτημένα άτομα
  - Να ταυτοποιείται το πρόσωπο που στέλνει το μήνυμα
  - Να ταυτοποιείται ένα μήνυμα και ο αποστολέας του

Οι παραβιάσεις ασφάλειας γίνονται από άτομα που προσπαθούν …

- Να προσποριστούν κέρδος
- Να προκαλέσουν την προσοχή
- Να εκδικηθούν ή να βλάψουν κάποιον
- Να διασκεδάσουν
- Να κερδίσουν στρατηγικό πλεονέκτημα

- Ένα μεγάλο ποσοστό προβλημάτων ασφαλείας προκαλούνται από εσωτερικούς χρήστες, υπαλλήλους, κ.λ.π.

Σκέψεις σχετικές με την ασφάλεια

- Στην ασφάλεια η θεωρία και η πράξη είναι έννοιες συμβιωτικές
- Η ασφάλεια και η κρυπτογραφία δεν είναι έννοιες ταυτόσημες
- Η ασφάλεια δεν είναι μόνο επιστήμη αλλά και τέχνη

Τέσσερις κύριες Έννοιες

- Εμπιστευτικότητα (Confidentiality ή secrecy): η πληροφορία να πηγαίνει μόνο στα χέρια του ενδιαφερομένου
  - Ιδιωτικότητα (privacy)
  - Μυστικότητα (secrecy)
- Ακεραιότητα (Integrity): ότι το μήνυμα δεν έχει αλλοιωθεί. Προστασία από μετατροπή, διαγραφή ή/ και δημιουργία.
- Αυθεντικοποίηση (Authentication): Να ξέρεις σίγουρα ότι αυτός με τον οποίον μιλάς είναι αυτός που ισχυρίζεται. → επέκταση στα μηνύματα που ανταλλάσσεις μαζί του
- Μη απάρνηση (non-repudiation): η δυνατότητα να αποδείξουμε ότι κάποιος έστειλε ένα μήνυμα και όχι κάποιος άλλος. Δηλ., ο αποστολέας του μηνύματος (ή ο δημιουργός ενός ψηφιακού εγγράφου) δεν μπορεί να αρνηθεί ότι το έστειλε. Επίσης, μπορεί να χρησιμοποιηθεί για να αποδείξουμε ότι ένα ηλεκτρονικό μήνυμα (e-mail) έχει ανοιχτεί.

Εμπιστευτικότητα

- Δεν αφορά μόνο στην προστασία των πληροφοριών αλλά και στην προστασία των πόρων
- Υποστηρίζεται μέσω μηχανισμών ελέγχου πρόσβασης (access control)
- Η εμπιστευτικότητα μπορεί να αφορά και στην απλή γνώση για την ύπαρξη των δεδομένων ή στην απόκρυψη χρήσης κάποιων πόρων

Ακεραιότητα (integrity)

1. *Data integrity*
2. *Origin integrity*
   - Ακεραιότητα της πηγής των δεδομένων
   - authentication
- Μηχανισμοί διαφύλαξης της ακεραιότητας

Ανίχνευση (detection):
αναφέρουν ότι δεν μπορούμε πλέον να εμπιστευτούμε την ακεραιότητα των δεδομένων

Πρόληψη (prevention):
στόχος είναι να αποτρέψω μη εξουσιοδοτημένες προσπάθειες αλλαγής των δεδομένων, όπως και αλλαγή των δεδομένων με μη εξουσιοδοτημένο τρόπο. (είναι άλλο να μπεις στα λογιστικά βιβλία μιας εταιρείας και να αλλάξεις δεδομένα και άλλο ο λογιστής να παραποιήσει δεδομένα προς όφελός του)

Προσοχή!

Η ακεραιότητα προϋποθέτει ότι η πηγή των δεδομένων είναι έμπιστη και ότι τα δεδομένα ήταν ακέραια όταν συλλέχθηκαν ή όταν ήρθαν στην κατοχή μας (δηλαδή, πριν την ανάλυσή της προηγείται μια υπόθεση) .

Αντίθετα, για την εμπιστευτικότητα χρειάζεται απλά να διαπιστώσουμε αν κάποιος παρεισέφρησε στα δεδομένα μας ή όχι.

Διαθεσιμότητα

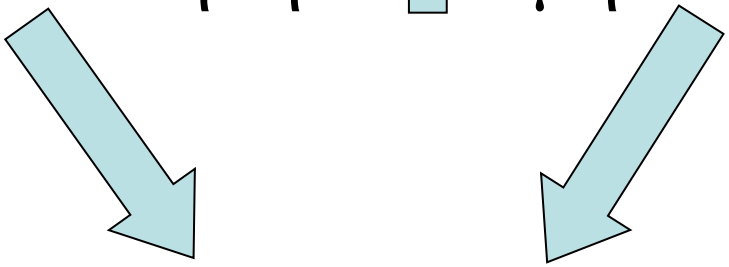
- Διαθεσιμότητα (availability): κρίσιμη έννοια που δεν συνδέεται όμως στενά με την έννοια της ασφάλειας. Με αυτήν ασχολείται ο κλάδος που ονομάζεται fault tolerant computing.
- Αναφέρεται στη δυνατότητα που έχω να χρησιμοποιήσω την πληροφορία ή τον πόρο του συστήματος που επιθυμώ (εφόσον βέβαια έχω τη δικαιοδοσία)
- Η σχέση της με την ασφάλεια έγκειται στο ότι κάποιος μπορεί επίτηδες να στερήσει την πρόσβαση κάποιου άλλου σε δεδομένα ή σε υπηρεσία καθιστώντας την μη-διαθέσιμη

Διαθεσιμότητα

- Οι ενέργειες κατά της διαθεσιμότητας εντάσσουν τους κακόβουλους χρήστες στην κατηγορία των επιτιθέμενων στην ασφάλεια του συστήματος επειδή παρακωλύουν την απρόσκοπτη πρόσβαση των νόμιμων χρηστών στο σύστημα.
- Τέτοιες ενέργειες ονομάζονται *επιθέσεις άρνησης υπηρεσίας* (denial of service attacks) και γενικά είναι πολύ δύσκολο να ανιχνευθούν.
- Ο λόγος είναι ότι η ανίχνευσή τους βασίζεται σε στατιστικά μοντέλα για τα οποία μια μη αναμενόμενη συμπεριφορά μπορεί απλά να ερμηνευθεί ως στατιστικό ακρότατο ή ακόμη και να μην ανιχνευθεί καθόλου.

Συνεπαγόμενες έννοιες

Αυθεντικοποίηση ✚ μη-απάρνηση



Απόδοση ευθυνών (accountability) + χρέωση (billing)

Άλλες έννοιες

- Έκθεση σε κίνδυνο (exposure): μια μορφή πιθανής απώλειας (loss) ή ζημιάς (harm).
- Ευπάθεια (vulnerability): αδυναμία ή ευάλωτο σημείο
- Επίθεση (attack)
- Απειλή (threat): καταστάσεις όπου υπάρχει το ενδεχόμενο απωλειών ή ζημιών. Ανθρώπινες, φυσικές καταστροφές, ακούσια λάθη, ατέλειες
- Έλεγχος (control): προστατευτικό μέσο: πράξη, συσκευή, διαδικασία, τεχνική που μειώνει την ευπάθεια

Ευπάθειες

- Φυσικές (αφορούν το χώρο εγκατάστασης)
- Εκ φύσεως (πλημμύρες, πυρκαγιές, …)
- Υλικού και λογισμικού
- Μέσων (π.χ. μαγνητικά μέσα)
- Εκπομπών
- Επικοινωνιών
- Ανθρώπινες

ΑΠΕΙΛΕΣ

- Απειλή είναι μια πιθανή παραβίαση της ασφάλειας
- Η απειλή υπάρχει και χωρίς να υπάρξει παραβίαση της ασφάλειας
- Η ενέργεια κάποιου να παραβιάσει την ασφάλεια ενός συστήματος λέγεται επίθεση και αυτός που τη διαπράττει επιτιθέμενος

Απειλές

Ο Shirey (1994) κατατάσσει τις απειλές σε 4 κατηγορίες:

1. *Disclosure* (αποκάλυψη, γνωστοποίηση): μη-εξουσιοδοτημένη πρόσβαση σε πληροφορία
2. *Deception* (εξαπάτηση): η αποδοχή-διανομή παραποιημένων-ψευδών δεδομένων
3. *Disruption* (διατάραξη, διακοπή): η διακοπή ή αποτροπή της ορθής λειτουργία
4. *Usurpation* (σφετερισμός): μη-εξουσιοδοτημένος έλεγχος κάποιου μέρους του συστήματος

Είδη απειλών σε σχέση με το κανάλι επικοινωνίας

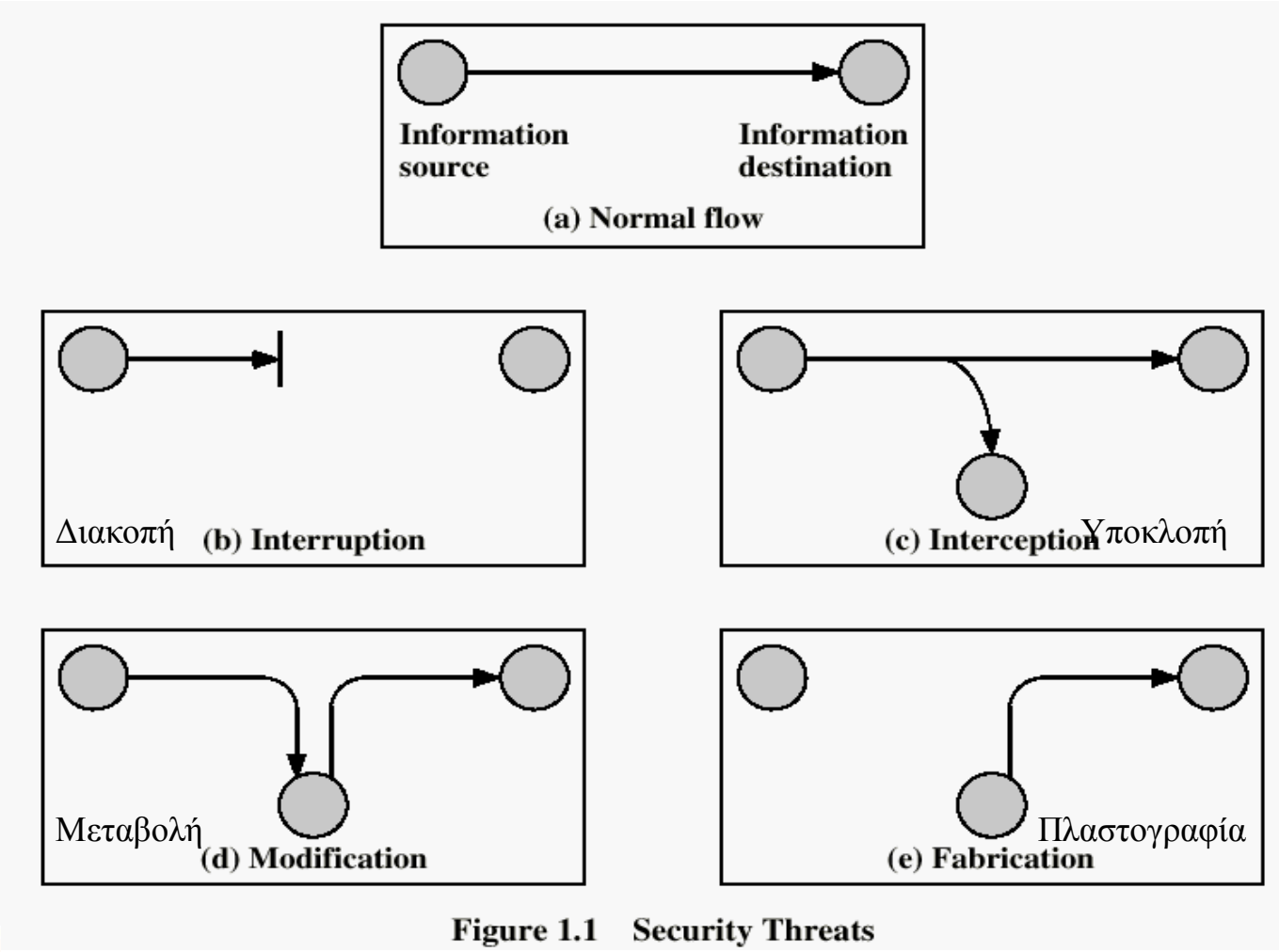


Figure 1.1 Security Threats

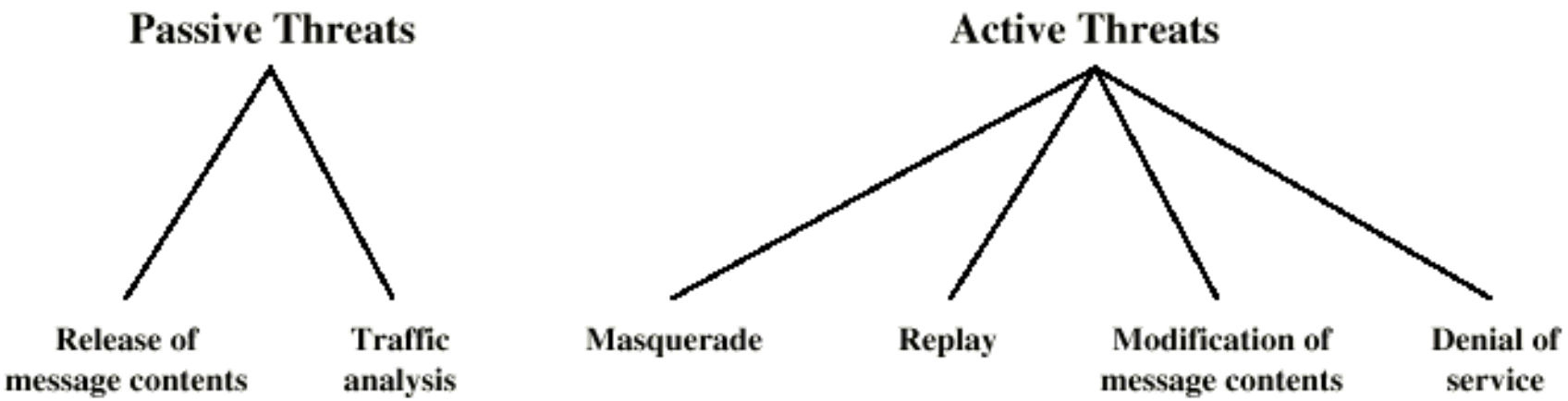
Παθητικές επιθέσεις

- Παρακολούθηση επικοινωνιών
- Για την απόκτηση πληροφορίας
- Ανίχνευση περιεχομένου μηνυμάτων
- Ανάλυση κίνησης
  - Υπάρχει δυνατότητα εύρεσης του τύπου της επικοινωνίας από τη συχνότητα και το μέγεθος των μηνυμάτων.
- Δύσκολη ανίχνευση
- Μπορεί να αποφευχθεί

Ενεργητικές επιθέσεις

- Μασκάρεμα
  - Ο επιτιθέμενος προσποιείται ότι είναι διαφορετική οντότητα
- Επανάληψη (Replay)
- Παραποίηση μηνυμάτων
- Άρνηση υπηρεσίας (Denial of service)
- Εύκολη ανίχνευση
  - Η ανίχνευση μπορεί να οδηγήσει σε τιμωρία
- Δύσκολη αντιμετώπιση

Απειλές για την ασφάλεια



Απειλές για την ασφάλεια

- Κλοπή ή απώλεια δεδομένων (SOS φορητές συσκευές)
- Κλοπή προσωπικών δεδομένων (πελατών, προσωπικού, οικονομικά ή επιχειρηματικά σχέδια) → Πρόστιμα
- Ασύρματα δίκτυα (ασθενής ή ανύπαρκτη προστασία)
- Εσωτερικοί κίνδυνοι (απρόσεκτοι ή δυσαρεστημένοι υπάλληλοι)

Απειλές

- Υποκλοπή (*snooping*): είναι παθητική επίθεση κατά της εμπιστευτικότητας (*wiretapping*)
- Αλλοίωση (*modification*, *alteration*): ενεργητική επίθεση, συνήθως κατά της ακεραιότητας των δεδομένων
  - man-in-the-middle attack
- Πλαστοπροσωπία (*masquerading* ή *spoofing*): είναι επίθεση κατά της αυθεντικοποίησης (*origin integrity*)
  - ταυτόχρονη πράξη εξαπάτησης και σφετερισμού
  - μπορεί να είναι τόσο ενεργητική όσο και παθητική
  - Το «*μασκάρεμα*» ενδέχεται να είναι και επιθυμητή ενέργεια σε ένα δίκτυο. Η περίπτωση της *εκπροσώπησης* (*delegation*) αναφέρεται στην περίπτωση που μια οντότητα εξουσιοδοτεί μια άλλη να ενεργήσει εκ μέρους της.

Απειλές

- Απάρνηση (*repudiation of origin*): είναι ψευδής άρνηση ότι μια οντότητα απέστειλε ή δημιούργησε κάτι (πληροφορία, μήνυμα, ενέργεια, …)
  - η προστασία από την απάρνηση είναι αρμοδιότητα των μηχανισμών ακεραιότητας
- Άρνηση παραλαβής (*denial of receipt*): η ψευδής άρνηση ότι μια οντότητα παρέλαβε πληροφορία ή μήνυμα
  - η προστασία είναι αρμοδιότητα των μηχανισμών ακεραιότητας και διαθεσιμότητας

Απειλές

- Καθυστέρηση (*delay*): η προσωρινή παρακώλυση μιας υπηρεσίας.
  - Αποτελεί μια μορφή σφετερισμού επειδή η επίτευξή της προϋποθέτει τον έλεγχο συσκευών του δικτύου.
  - Χρησιμοποιείται όμως σαν εργαλείο εξαπάτησης.
  - Είναι αρμοδιότητα των μηχανισμών διαθεσιμότητας
- Άρνηση υπηρεσίας (*denial of service*): η μακροχρόνια παρακώλυση μιας υπηρεσίας.
  - Ισχύουν τα ίδια με την καθυστέρηση

Μέτρα Προστασίας Πληροφοριακών Συστημάτων

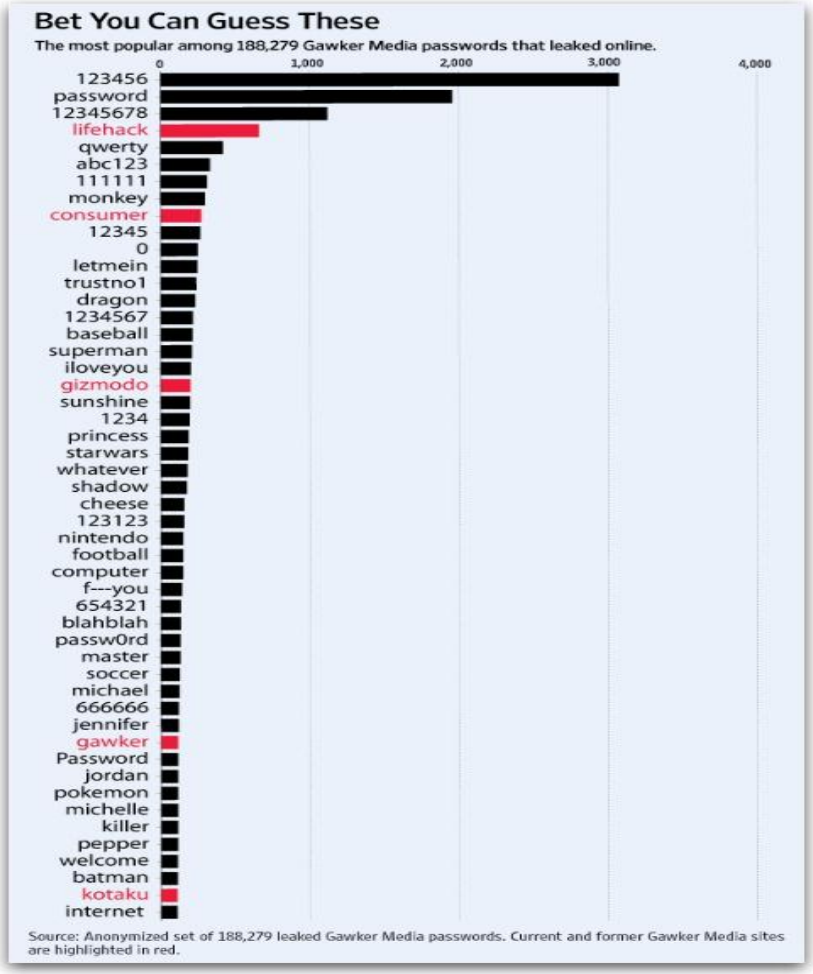
- Φυσική ασφάλεια
- Ασφάλεια υπολογιστικού συστήματος (computer security): ποιος δικαιούται προσπέλαση
- Ασφάλεια βάσεων δεδομένων
- Ασφάλεια Δικτύων

Τρόποι άμυνας

- Έλεγχος προσπέλασης στο σύστημα
- Έλεγχος προσπέλασης στα δεδομένα
- Διαχείριση συστήματος και ασφάλειας
- Σχεδιασμός συστήματος (αξιοποίηση δυνατοτήτων ασφάλειας)

Τύποι μέτρων προστασίας

- Κρυπτογράφηση: Η κύρια μέθοδος προστασίας των δεδομένων κατά τη μετάδοσή τους
- Μέτρα λογισμικού:
  - χρήση προτύπων, λειτουργικό σύστημα, μέτρα στα προγράμματα (π.χ. pswd στις ΒΔ)
- Μέτρα υλικού
  - συσκευές κρυπτογράφησης ή βιομετρικής αναγνώρισης χρηστών (ίριδα, δακτυλικά απ., hasp, κάρτες πρόσβασης κ.α.)
- Φυσικά μέτρα υλικού
  - κλειδαριές, back up, UPS, κλιματισμός, …
- Πολιτικές ασφάλειας.
  - π.χ. συχνή αλλαγή συνθηματικών!
  - Απαραίτητες σε μεγάλους οργανισμούς



Πηγή: Sophos Labs
http://nakedsecurity.sophos.com/2010/12/15/the-top-50-passwords-you-should-never-use/

Προβλήματα κατά ή για την εισαγωγή ασφάλειας

- Δεν σχεδιάζεται / περιλαμβάνεται από την αρχή αλλά προστίθεται μετά
- Κοστίζει, συνήθως, αρκετά.
- Μεγάλη πολυπλοκότητα (κυρίως στα λογισμικά)
- Το κύριο πρόβλημα ασφάλειας είναι οι χρήστες

Πολιτικές και μηχανισμοί ασφάλειας

- Η πολιτική ασφάλειας είναι μια δήλωση του τι επιτρέπεται και τι όχι
- Ένας μηχανισμός ασφάλειας είναι μια μέθοδος, εργαλείο ή διαδικασία για την επιβολή μιας πολιτικής ασφάλειας
  - π.χ. στο εργαστήριο απαγορεύεται η αντιγραφή αρχείων των συμφοιτητών σας [*Πολιτική*]
  - Η δημιουργία χρηστών και φακέλων με δικαιώματα πρόσβασης είναι ο *μηχανισμός*
  - Αν δω τα αρχεία κάποιου χωρίς να τα αντιγράψω είναι παραβίαση ασφαλείας; Αν κάποιος δεν προστάτεψε επαρκώς τα αρχεία του, είναι υπεύθυνος για την απώλειά τους ή για άλλη ενέργεια; Πώς τεκμηριώνω ότι οι χρήστες αποδέχονται τους όρους χρήσης;

Ερώτημα: πώς περιγράφω επαρκώς με χρήση φυσικής γλώσσας τις τεχνικές απαιτήσεις μιας πολιτικής ασφάλειας;

Στόχοι της ασφάλειας (δια των μηχανισμών της)

- Η αποτροπή (*prevention*) των επιθέσεων
- Η ανίχνευση (*detection*) των επιθέσεων
- Η ανάνηψη (*recovery*) των συστημάτων μετά την επίθεση
  - περιλαμβάνει και την *αναχαίτιση* της επίθεσης
- Η «αντεπίθεση»
  - Forensics analysis (δικανική ανάλυση)

Υποθέσεις και εμπιστοσύνη

Έστω ότι έχω ένα κλειδί για να ανοίγω την κλειδαριά του γραφείου μου

Υπόθεση 1η: Η κλειδαριά είναι απαραβίαστη

Υπόθεση 2η: Κανένας έμπειρος μη-έμπιστος κλειδαράς δεν θα ενδιαφερθεί για το περιεχόμενο του γραφείου μου

Αν μια τουλάχιστον από τις υποθέσεις μου είναι ψευδής τότε ο μηχανισμός ασφάλειας είναι αναξιόπιστος

Υποθέσεις και εμπιστοσύνη

Όποιος σχεδιάζει πολιτικές ασφαλείας κάνει δύο υποθέσεις:

1ον : *η πολιτική διχοτομεί σωστά και χωρίς αμφιβολία τις καταστάσεις του συστήματος* σε «ασφαλείς» και «μη-ασφαλείς»

π.χ. η πολιτική μιας τράπεζας να επιτρέπει τη μεταφορά χρημάτων μεταξύ λογαριασμών από το προσωπικό της, είναι σωστή πολιτική;

2ον : *οι μηχανισμοί ασφάλειας απαγορεύουν το σύστημα να εισέλθει σε μη ασφαλή κατάσταση* (άρα είναι επαρκείς και μπορούν να επιβάλουν την πολιτική)

Αν μια από τις δύο δεν ισχύει, τότε έχουμε ένα μη ασφαλές σύστημα

Μηχανισμοί ασφαλείας (ασφαλείς, ακριβείς και ευρείς)

Έστω P το σύνολο όλων των πιθανών καταστάσεων του συστήματος

Q το σύνολο όλων των ασφαλών καταστάσεων (όπως ορίζονται στην πολιτική ασφάλειας του συστήματος)

Έστω ότι οι μηχανισμοί ασφάλειας περιορίζουν το σύστημα σε R καταστάσεις (ώστε $R \subseteq P$)

ΟΡΙΣΜΟΣ: Ένας μηχανισμός ασφαλείας είναι:

Ασφαλής (*secure*) αν $R \subseteq Q$

Ακριβής (*precise*) αν $R = Q$

Ευρύς (*broad*) αν υπάρχουν r καταστάσεις τέτοιες ώστε

$$r \in R \text{ και } r \notin Q$$

Ιδανικά, η ένωση όλων των μηχανισμών ασφαλείας θα πρέπει να δημιουργεί έναν ακριβή μηχανισμό.

Στην πράξη οι μηχανισμοί είναι ευρείς. Επιτρέπουν το σύστημα να εισέλθει σε μη ασφαλείς καταστάσεις.

Μηχανισμοί ασφαλείας

- Η εμπιστοσύνη στους μηχανισμούς ασφαλείας προϋποθέτει ότι:

1. Κάθε μηχανισμός έχει σχεδιαστεί να υλοποιεί ένα ή περισσότερα κομμάτια (τμήματα) της πολιτικής ασφάλειας
2. Η ένωση των μηχανισμών υλοποιεί κάθε πτυχή της πολιτικής
3. Οι μηχανισμοί έχουν υλοποιηθεί σωστά
4. Οι μηχανισμοί έχουν εγκατασταθεί και διαχειρίζονται σωστά

Εξασφάλιση (assurance)

- Η εμπιστοσύνη δεν μπορεί να ποσοτικοποιηθεί

- Στο φαρμακείο αγοράζω ένα φάρμακο που το παρασκεύασε ένα γνωστό εργοστάσιο με καλή φήμη, το έλεγξε ο ΕΟΦ, και παραδίδεται σε εμένα νωρίτερα από την ημερομηνία λήξης του, μέσα σε κατάλληλη συσκευασία προφύλαξης με την ταινία ασφαλείας στη θέση της. Αυτό εν γένει θεωρείται ασφαλές φάρμακο.

Εξασφάλιση (assurance)

- Οι προδιαγραφές, ο σχεδιασμός και η υλοποίηση ενός συστήματος μπορούν να χρησιμοποιηθούν ως βάση για τον προσδιορισμό της εμπιστοσύνης στο σύστημα.
- Προδιαγραφή (*specification*) είναι μια διατύπωση της επιθυμητής λειτουργικότητας του συστήματος
- Ο σχεδιασμός (*design*) ενός συστήματος μεταφράζει τις προδιαγραφές στα συστατικά μέρη του συστήματος που θα τις υλοποιούν
- Με δοσμένο σχεδιασμό, η υλοποίηση (*implementation*) δημιουργεί ένα σύστημα που τον ικανοποιεί. Η δυσκολία βρίσκεται στην πολυπλοκότητα να αποδείξεις ότι ένα πρόγραμμα υλοποιεί με σωστό τρόπο τον σχεδιασμό και κατ'επέκταση τις προδιαγραφές

Λειτουργικά θέματα – κόστος

- Κάθε εταιρεία – οργανισμός πρέπει να εκτιμά αν το κόστος για την εφαρμογή των μέσων προστασίας ισορροπείται από το κέρδος της προστασίας που προσφέρουν.
- Μια τέτοια ανάλυση είναι συνήθως υποκειμενική και εξαρτάται από μια πληθώρα μη μετρήσιμων παραγόντων όπως είναι η νομοθεσία, το κανονιστικό πλαίσιο, η κοινωνική ή/και η εταιρική ηθική, κλπ

Λειτουργικά θέματα – κόστος

- *Cost-Benefit Analysis*: η εκτίμηση του κόστους εφαρμογής της ασφάλειας έναντι του κόστους που θα είχε η πιθανή καταστροφή και ανάνηψη των συστημάτων
- *Risk Analysis*: Ανάλυση των παραγόντων που προσδιορίζουν τους κινδύνους και οδηγούν στην απόφαση αν τα συστήματα πρέπει να προστατευτούν
  - Το ρίσκο είναι συνάρτηση του περιβάλλοντος
  - Το ρίσκο αλλάζει με το χρόνο
  - Κάποια ρίσκα φαίνονται μακρινά αλλά είναι υπαρκτά
  - *Analysis Paralysis*

Νόμοι και εθιμικό δίκαιο

- Ειδική νομοθεσία, π.χ. εξαγωγή κρυπτογραφικού λογισμικού
- Διαφορές στη νομοθεσία μεταξύ χωρών
- Διαφορές ανάμεσα στο τι είναι νόμιμο και τι ηθικό ή κοινωνικά αποδεκτό, π.χ. χρήση DNA για αυθεντικοποίηση

Ο ανθρώπινος παράγοντας (Οργανωτικά προβλήματα)

- Η ανάγκη για ασφάλεια δεν είναι προφανής σε όλους παρά μόνο αν υπάρξει πρόβλημα
- Ένας ασφαλής μηχανισμός ή διαδικασία μπορεί να είναι πιο αργός και αυτό να μεταφράζεται από κάποιους ως χαμηλή παραγωγικότητα
- Οι άνθρωποι που είναι υπεύθυνοι για την υλοποίηση των μηχανισμών ασφαλείας συνήθως δεν έχουν την εξουσία να τους επιβάλλουν. Υπευθυνότητα χωρίς εξουσία δημιουργεί τα ίδια προβλήματα που δημιουργεί και η εξουσία χωρίς υπευθυνότητα.
- Σύνηθες εταιρικό πρόβλημα είναι ότι το έμπειρο προσωπικό είναι φορτωμένο με δουλειά
- Η έλλειψη πόρων (οικονομικών, εξοπλισμού, προσωπικού,…)

Ο ανθρώπινος παράγοντας (Ανθρώπινα προβλήματα)

- Ο κίνδυνος από μέσα (insiders)
- Ελλιπής εκπαίδευση
- Κακή χρήση μηχανισμών ασφαλείας (π.χ. κακά συνθηματικά)
- Κοινωνική μηχανική (social engineering)!
- Κακές ρυθμίσεις συστημάτων (system misconfiguration)
- Εγγενείς αδυναμίες των συστημάτων

Εντοπισμένα προβλήματα

- 63% missing Microsoft patches
- 5% no antivirus
- 50% no firewall
- 81% no compliant software
- Μέσο κόστος από την απώλεια δεδομένων $202/εγγραφή από το 2006

Πηγή: SOPHOS LABS, 2009

Τιμές προϊόντων κυβερνοεγκλήματος στη μαύρη αγορά

Credit card details: $2-90

Money laundering: 10-40% of total

Card cloners: $200-1000

Spam rental: From $15

VPN rental: $20 for three months

Online Stores: $80-1500

Πηγή: Panda Security, “The-Cyber-Crime-Black-Market,” 2010
http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf

Οι 10 διασημότερες περιπτώσεις διαρροής πληροφοριών

- PFC Bradley Manning (U.S. Army): Manning is alleged to have downloaded thousands of classified documents and provided them to whistleblower organization WikiLeaks. Manning has not yet been convicted...
- Yonggang "Gary" Min (DuPont): Min had accepted position with DuPont competitor Victrex, but did not give notice for months. During this time he secretly copied thousands of confidential documents said to be worth as much as $400 million dollars. It is not clear if the documents were passed on to Victrex...
- Xiaodong Sheldon Meng (Quantum3D): Meng,while working for defense contractor Quantum3D, engaged in espionage activities in the behalf of The People's Republic of China between 2002 and 2006. Meng was the first person convicted under the Economic Espionage Act of 1996...
- Ross Klein (Starwood Hotels and Resorts Worldwide): Klein and another executive of Starwood took positions with rival Hilton and made off with some 100,000 documents that detailed a new line of "lifestyle" hotels the company was developing. They have not been charged with a crime, but have been banned from holding positions in the industry, and Hilton settled a lawsuit with Starwood out of court...
- Jose Ignacio Lopez (GM): Lopez and another executive left GM for Volkswagen, taking with them over two million pages of documents considered "top secret" by GM, including business plans, blue prints for production, and vehicle designs. Lopez has avoided prosecution and remains in Spain. Volkswagen settled with GM for $100 million dollars and committed to buying $1 billion in GM parts.

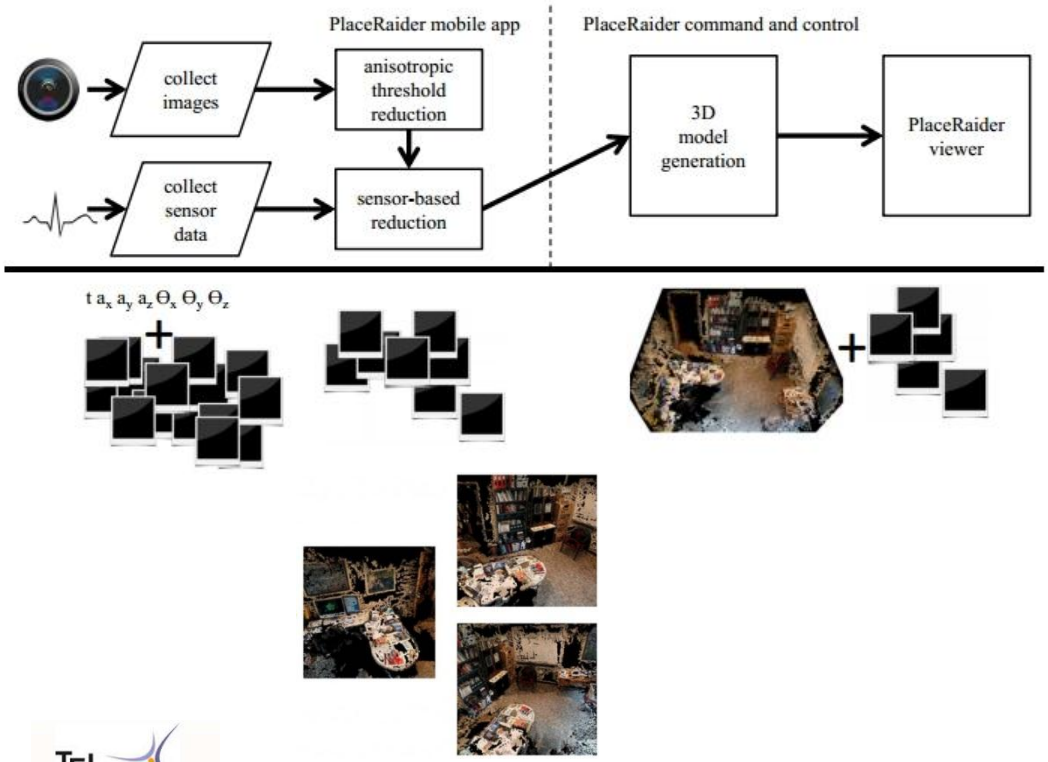
Πηγή: ThreatPost (http://threatpost.com/en_us/slideshow/Infamous%20Insiders%3A%2010%20Eye%20Popping%20Heists%20By%20Insiders?page=0)

Οι 10 διασημότερες περιπτώσεις διαρροής πληροφοριών

- Robert Hanssen (FBI): Hanssen was a career FBI agent who provided intelligence to the Soviets, including the names of operatives and double agents, in exchange for over $1 million in cash and diamonds between 1979 and 1999. At times he even headed the FBI unit responsible for tracking and arresting Soviet agents. He was sentenced to life in prison...
- Xiang Dong ("Mike") Yu (Ford Motor): Yu made copies of some 4000 confidential ford documents and provided them to Beijing Automotive Company, where he had accepted a position.The information is valued at $50 million dollars, and yu faces up to six years in prison and as much as $150,000 in fines if convicted...
- Noshir Gowadia (Northrop Grumman): Gowadia is noted for designing the propulsion systems for the B-2 bomber, and selling the information to the People's Republic of China along with information that aided the Chinese in developing a stealth cruise missile, among other acts of espionage...
- Fei Ye and Ming Zhong (Transmeta, Sun Microsoystems, NEC and Trident Microsystems): Ye and Zhong used a front company called Supervision to steal information on super integrated circuit chips from several U.S. companies, and are alleged to have made attempts to transport the information to China. they were convicted and sentenced to one year in jail...
- Dongfan "Greg" Chung (Boeing): Chung was convicted of attempting to pass along secrets related to the Space Shuttle, the C-17 military transport aircraft and Delta IV rocket to China. he had more than 300,000 sensitive documents stored on his home computer, which he claimed was research material for a book. He was sentenced to fifteen years in prison...

Sensory Malware

- PlaceRaider (Android proof of concept)
  - Robert Templemany, Zahid Rahmany, David Crandally, Apu Kapadiay, "PlaceRaider: Virtual Theft in Physical Spaces with Smartphones", 2012



!

- http://gizmodo.com/5614047/the-top-ten-most-dangerous-things-you-can-do-online

Τέλος Ενότητας