ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-Ι

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.
  - Συχνή αλλαγή συνθηματικών
  - Απαραίτητες σε μεγάλους οργανισμούς

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

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 στην Ασφάλεια – 1η Θεώρηση

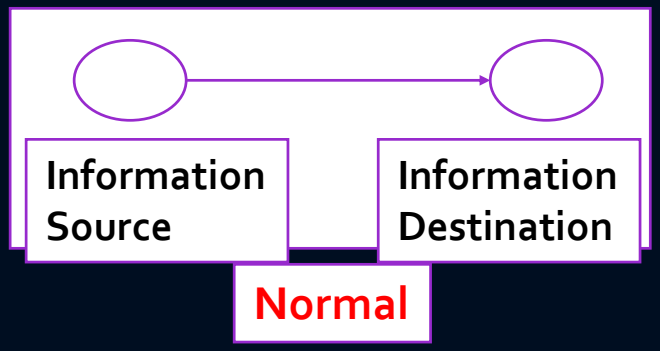
1. Παθητικές επιθέσεις: τις κάνει η Eve (eavesdrop)
   - Packet sniffing
   - Traffic analysis
   - Αλλά και: Password cracking / breaking a crypto key
   - …

2. Ενεργητικές επιθέσεις: τις κάνει ο Mallory
   - Πλαστοπροσωπία: Masquerading, Spoofing, MIM
   - Επιθέσεις επανάληψης (replay)
   - Επιθέσεις άρνησης εξυπηρέτησης (Denial Of Service – DOS)
   - Επιθέσεις Τροποποίησης (modification)
   - …

Απειλές στην Ασφάλεια – 2η Θεώρηση

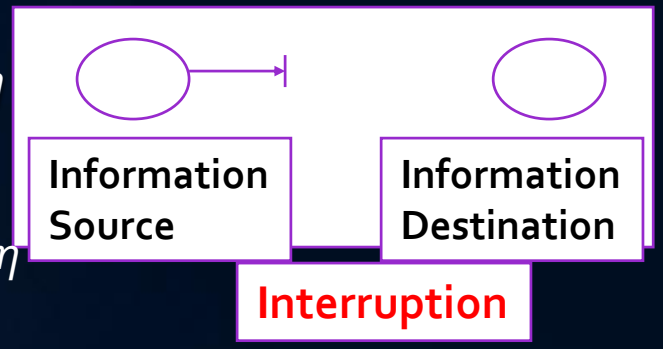
(Pfleeger, 2003)

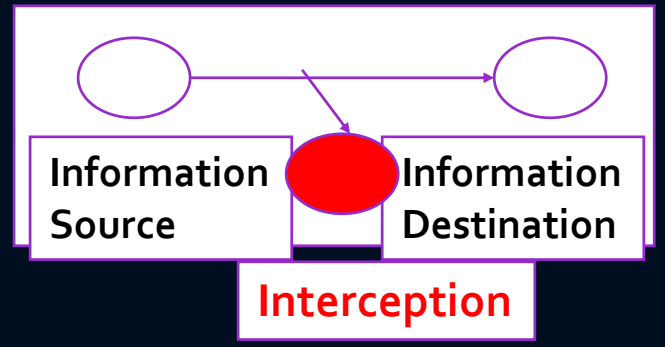
Interruption-Διακοπή *(Μια επίθεση στην διαθεσιμότητα)*
Κακόβουλη καταστροφή του τοπικού δικτύου
Διαγραφή ενός προγράμματος η δεδομένα του
Αποκοπή σύνδεσης

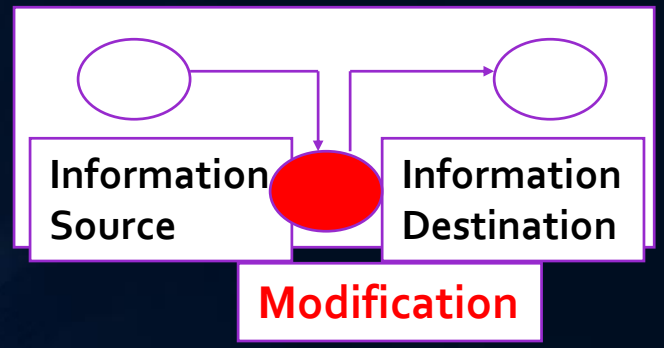


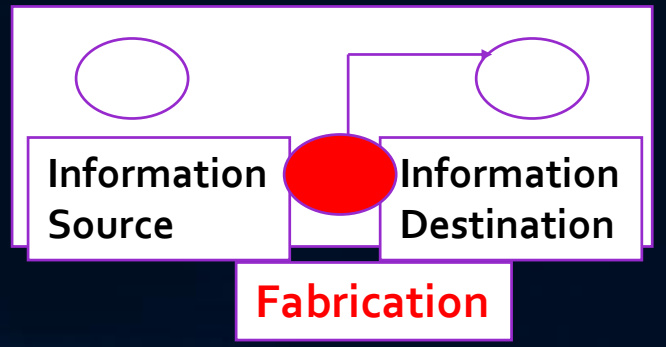
Interception-Κλοπή *(Μια επίθεση στην εμπιστευτικότητα)*
Μια μη εξουσιοδοτημένη πρόσβαση στα αρχεία
Π.χ Μη εξουσιοδοτημένη υποκλοπή δεδομένων
Ανακάλυψη μη προστατευόμενου WLAN

Modification *(Μια επίθεση στην ακεραιότητα)*
Μια μη εξουσιοδοτημένη υποκλοπή-παρακολούθηση σε μια πηγή
Αλλαγή της πληροφορίας σύνδεσης ενός δικτύου
Αλλαγή δεδομένων που μεταφέρονται σε μια δικτυακή επικοινωνία



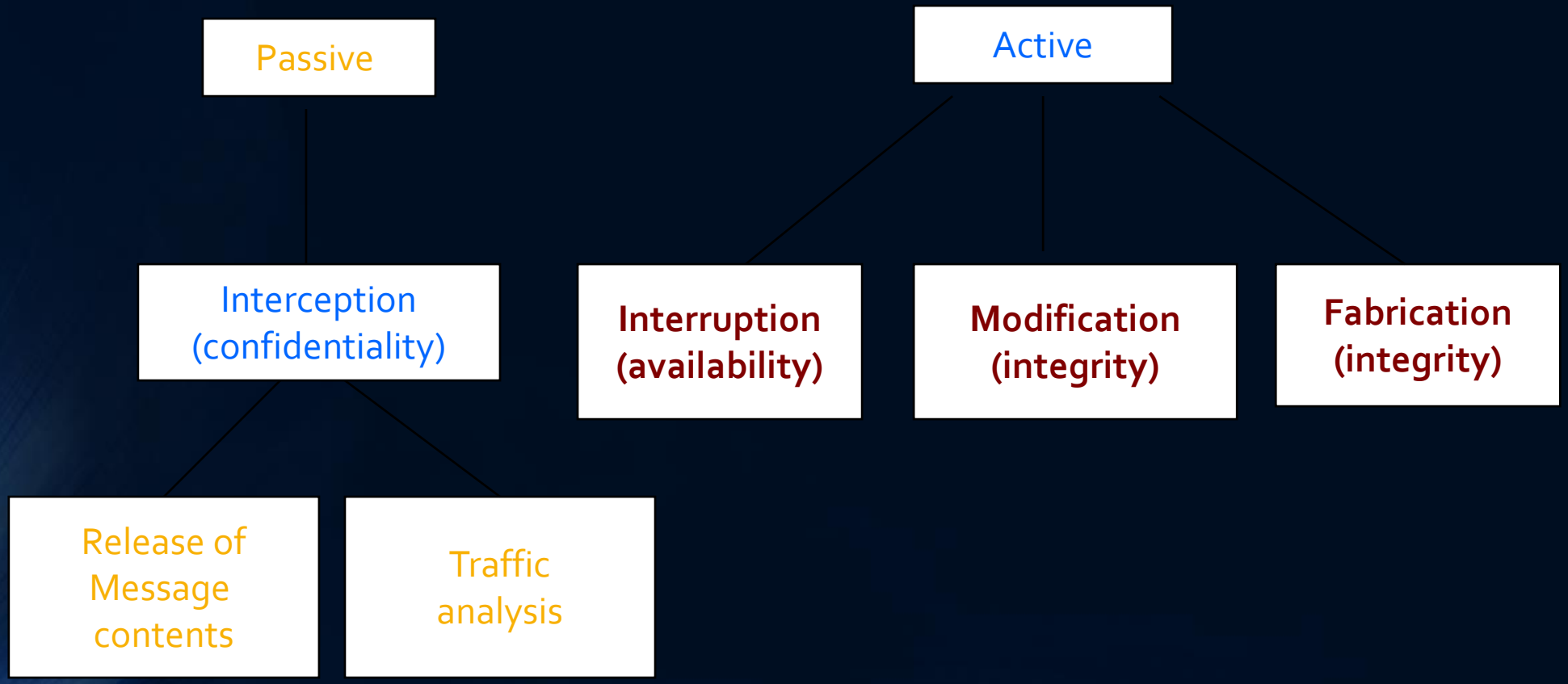




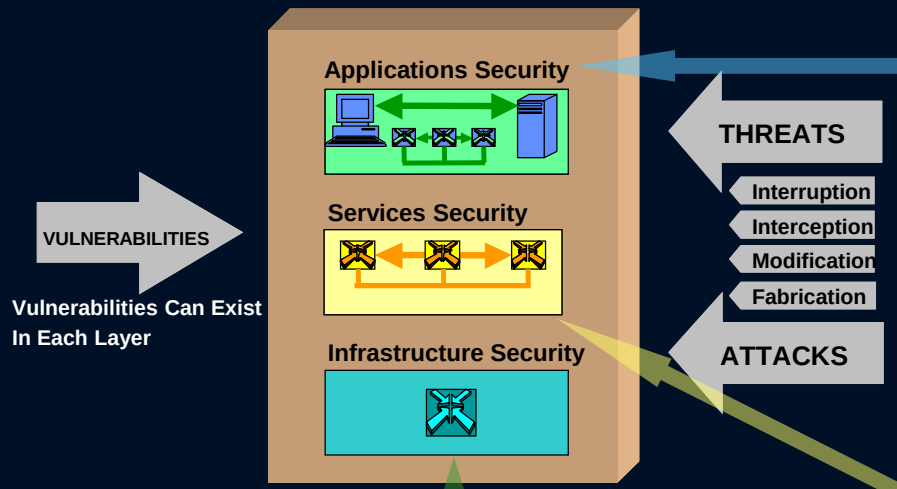


Fabrication-Κατασκευή*(Μια επίθεση στην αυθεντικοποίηση)*
Μη εξουσιοδοτημένη δημιουργία, τροποποίηση, διαγραφή αντικειμένων και δικτύων,Π.χ
Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο
Εισαγωγή ψευδών μηνυμάτων στο δίκτυο
Πρόσθεση εγγραφών σε μια Βάση Δεδομένων

A Taxonomy of Attacks (Pfleeger, 2003)



Security Layers



Applications Security Layer:

- Network-Based Applications Accessed by End-Users
- Includes:
  - Fundamental Applications (e.g., Web Browsing)
  - Basic Applications (e.g., Directory Assistance and Email)
  - High-End Applications (e.g., E-Commerce)

Infrastructure Security Layer:

- Fundamental Building Blocks of Networks, Services, and Applications.
- Individual Network Elements and the Interconnecting Communications Facilities
- Examples:
  - Individual Routers, Switches, Servers
  - Point-to-Point WAN Links
  - Ethernet Links

Services Security Layer:

- Services Provided to Customers or End-Users
- Range from Basic Transport to High-End, Value-Added Services.
- Examples:
  - Carrier Facilities (DS-1, DS-3, etc.)
  - Frame Relay, ATM, IP Connectivity
  - VoIP, QoS, IM, Location Services
  - 800-Services

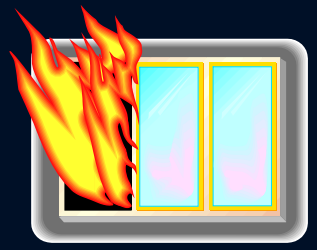
Απειλές στην Ασφάλεια – Άλλες Θεωρήσεις (1/2)

1. Εξωτερικές Απειλές: Χρήστες εκτός Επιχείρησης / Οργανισμού
   - Outsiders: Hackers / Crackers / Vandals / Hacktivists
   - Outsiders: Κοινωνικοί Μηχανικοί (Social Engineers)

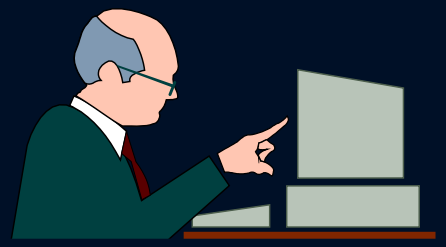
2. Εσωτερικές Απειλές: - Χρήστες εντός Επιχείρησης/Οργανισμού
   - Insiders: Παράκαμψη ελέγχου πρόσβασης «εκ των έσω»
   - π.χ. Δυσαρεστημένοι υπάλληλοι, λάθη & απροσεξίες

Απειλές στην Ασφάλεια – Άλλες Θεωρήσεις (2/2)

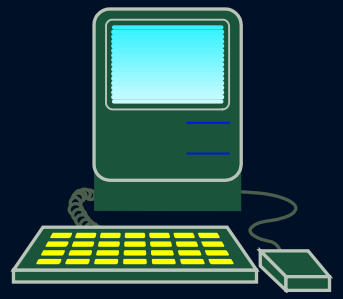
Τυχαίες ή Εσκεμμένες



Φυσικές
π.χ. φωτιά
Διακοπή ρεύματος;



Ανθρώπινες
e.g. Λάθη χρήστη,
hackers, Ιοί.



Εξοπλισμός
π.χ. CPU,
Δίκτυο, Σκληρός δίσκος,
- Σφάλμα εφαρμογής,
- Buffer overflow attacks

Ενδεικτικός Πίνακας Απειλών

	Απειλή
1.	Πλαστοπροσωπία Χρήστη από κακόβουλους Εσωτερικούς Χρήστες
2.	Πλαστοπροσωπία Χρήστη από κακόβουλους Συνεργάτες
3.	Πλαστοπροσωπία Χρήστη από κακόβουλους Εξωτερικούς Χρήστες
4.	Μη εξουσιοδοτημένη χρήση Εφαρμογής
5.	Παρακολούθηση Επικοινωνίας
6.	Παραποίηση Επικοινωνίας
7.	Αποποίηση πράξης από Χρήστη
8.	Αποτυχία Επικοινωνίας
9.	Είσοδος κακόβουλου κώδικα (virus, Trojan, spam, hoaxes κτλ)
10.	Τυχαίο λάθος δρομολόγησης επικοινωνίας
11.	Εσκεμμένη τροποποίηση δρομολόγησης επικοινωνίας
12.	Λανθασμένη χρήση συστήματος
13.	Τεχνική βλάβη υπολογιστή
14.	Βλάβη κλιματισμού
15.	Βλάβη λογισμικού συστήματος
16.	Βλάβη λογισμικού διαχείρισης δικτύου
17.	Λάθος διαχείρισης συστήματος ή δικτύου
18.	Λάθος συντήρησης υλικού (hardware)
19.	Λάθος συντήρησης λογισμικού (software)
20.	Έλλειψη προσωπικού
21.	Τεχνική βλάβη εγκατάστασης (παροχή ρεύματος, τηλεφώνου κτλ)
22.	Τεχνική βλάβη εκτυπωτών
23.	Τεχνική βλάβη δικτυακού εξοπλισμού (hub, router, switch κτλ)
24.	Τεχνική βλάβη Gateway
25.	Τεχνική βλάβη συστήματος ελέγχου πρόσβασης (firewall)
26.	Τεχνική βλάβη συστήματος εντοπισμού εισβολών (IDS)
27.	Τεχνική βλάβη υπολογιστή διαχείρισης δικτύου ή λειτουργιών
28.	Τεχνική βλάβη υπηρεσίας πρόσβασης διαδικτύου (Internet access)
29.	Τεχνική βλάβη άλλης δικτυακής υπηρεσίας (ftp, web mail κτλ)
30.	Τεχνική βλάβη υπηρεσίας e-mail
31.	Βλάβη λογισμικού εφαρμογών (application software)
32.	Λάθος χειρισμού δεδομένων

Παράδειγμα

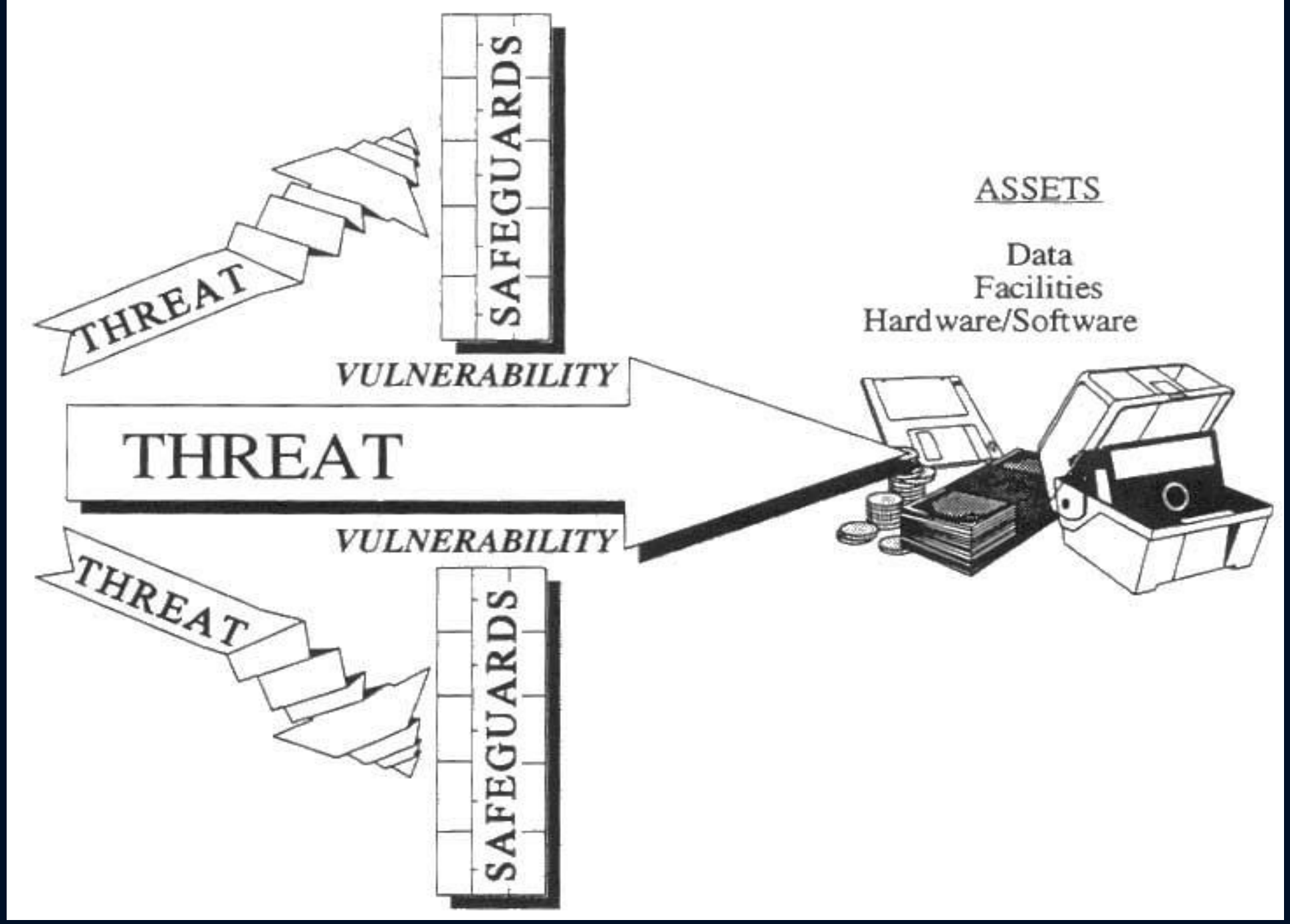
Threats (attacks) and assets

(Stallings & Brown, 2008)

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denaying access to users.	An unauthorized copy of software is made.	A working program is modified to cause it to fail or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlaying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted.	Messages are read. Traffic patterns are observed.	Messages are modified, destroyed, reordered, duplicated. False messages are injected.

Ευπάθειες (Vulnerabilities)

- Ευπάθεια ή Αδυναμία (Vulnerability)
  a) Οποιαδήποτε χαρακτηριστικά κάνουν ευάλωτο ένα αγαθό σε κάποια απειλή, δηλαδή αυξάνουν την πιθανότητα εκδήλωσης της απειλής
     - Π.χ: εάν η πρόσβαση σε ένα απόρρητο αρχείο δεν προστατεύεται, το αρχείο έχει μεγάλη αδυναμία στην απειλή της κλοπής
  b) Οτιδήποτε μεγιστοποιεί τις συνέπειες από την εκδήλωση μίας απειλής
     - Π.χ: εάν δεν υπάρχει σύστημα αυτόματης πυρόσβεσης σε ένα χώρο, η συνέπειες από μία πιθανή πυρκαγιά θα είναι πολύ μεγάλες



http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/images/figure5.jpg

Ανάλυση Κινδύνου
(Risk Analysis)

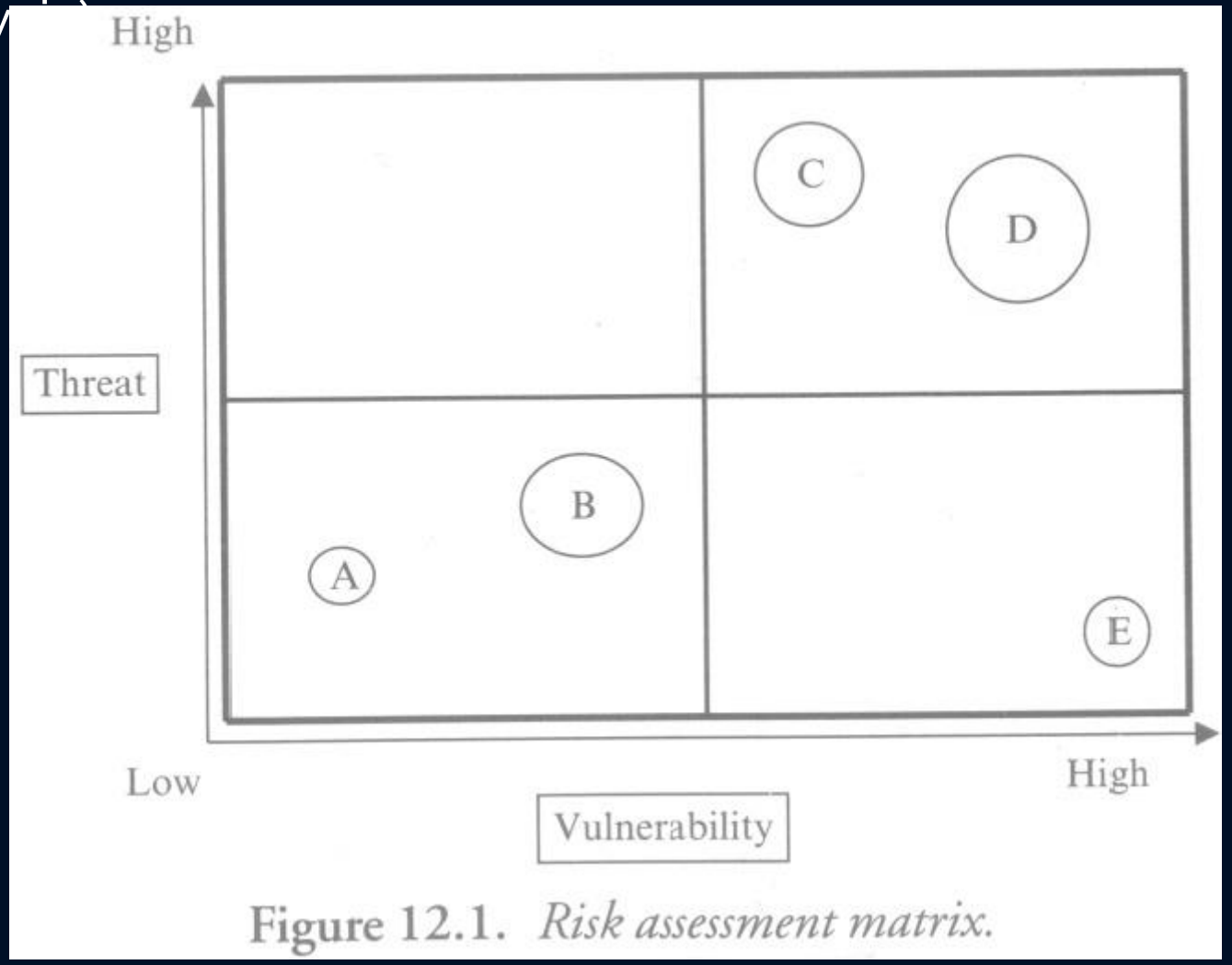
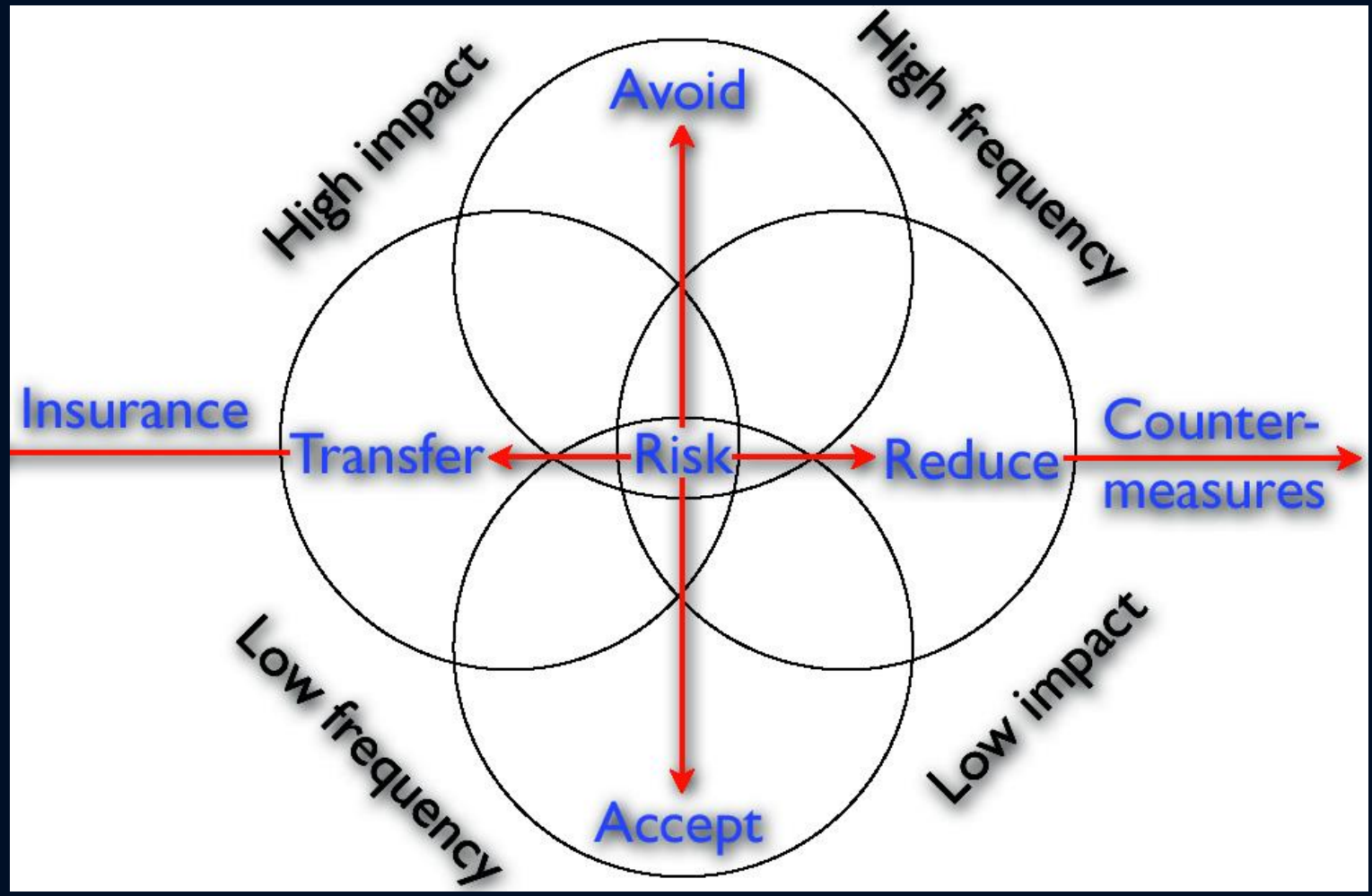


Figure 12.1. *Risk assessment matrix.*

Risk = Threat x Vulnerability x Impact (Asset value)

Διαχείριση Κινδύνου



Μια θεώρηση από τη σκοπιά των Οικονομικών της Ασφάλειας (Security Economics)

- Στόχος της ασφάλειας (Infosec goal)
  - Ο σκοπός του ιδιοκτήτη ή χρήστη ενός αγαθού: επιθυμητή ισορροπία μεταξύ του κόστους και της συνέπειας από την επίθεση σε αγαθά, π.χ.

Κόστος Μηχανισμών Ασφάλειας << Κόστος Αγαθών

Κόστος Επίθεσης >> Ενδεχόμενο Όφελος