

# ΗΡΥ-414: Ασφάλεια Συστημάτων και Υπηρεσιών

Σωτήρης Ιωαννίδης  
[sotiris@ece.tuc.gr](mailto:sotiris@ece.tuc.gr)

# Ταυτότητα

- “Systems person”
- 25+ χρόνια έρευνα σε συστήματα και ασφάλεια
- Θέματα:
  - Ασφάλεια συστημάτων, ασφάλεια σε υλικό, ασφάλεια σε κινητά/αντικείμενα, ασφάλεια στον παγκόσμιο ιστό, ανάλυση δεδομένων σε πραγματικό χρόνο, επιταχυντές (GPUs, FPGAs), κοινωνικά δίκτυα, κλπ.
- Άλλα Θέματα:
  - Κυκλική οικονομία, μεταεπιφάνειες, κυβερνοασφάλεια
- Follow me on Twitter! @sotirisioannidi

# Πληροφορίες

- Βιβλίο: «Ασφάλεια Υπολογιστών: Αρχές και Πρακτική», 3<sup>η</sup> έκδοση, William Stallings και Lawrie Brown
- Γνώσεις:
  - Προγραμματισμός
  - Λειτουργικά
  - Δίκτυα
  - Βάσεις
- Βαθμολόγηση:
  - 10 σειρές ασκήσεων
  - 'Όχι πρόοδος, όχι τελική εξέταση
  - Φροντιστήρια + εργαστήρια αν χρειαστεί, αλλά χρήση των ωρών για τυχών διαλέξεις
- Ήρες γραφείου με συνεννόηση
- Σχεδιάζω να δίνω το μάθημα κάθε χρόνο, δεν είναι ανάγκη να το πάρετε όλοι τώρα!

# Ασκήσεις (1/2)

1. Implement 3-4 simple algorithms from scratch using
2. Implement AES and HMACs with OpenSSL using C
3. Simple RSA / Diffie Hellman / privKey storage from scratch using C
4. Access control lib
5. Implement a simple ransomware
6. Simple libpcap reporting tool
7. IPTables
8. Buffer overflow
9. Simple Linux driver implementation
10. Backdoors through drivers

# Ασκήσεις (2/2)

- Υποθέτω ότι μπορείτε να διαβάσετε manuals
- Υποθέτω ότι μπορείτε να προγραμματίστε σε C
- Υποθέτω ότι δεν αντιγράφετε
  - Τυχαίες προφορικές εξετάσεις αν χρειαστεί
- Αυτόματη βαθμολόγηση ασκήσεων
  - Συγκεκριμένη είσοδος πρέπει να δίνει συγκεκριμένη έξοδο

# Ασφάλεια δικτύων και συστημάτων

- Διαφορετική νοοτροπία από άλλους τομείς
  - «Δουλεύει;» -> «Μπορεί να σπάσει;»
  - Τι σημαίνει «σπάσει»;
- Ακουμπά κάθε πλευρά της σχεδίασης και υλοποίησης ενός συστήματος
  - Αδύναμος κρίκος
- Σκέψου διαφορετικά!
- Να είσαι δημιουργικός!

# Σημασία της ασφάλειας

- Τα πάντα συνδέονται
- Τα πάντα έχουν ευαίσθητες πληροφορίες
- Τα πάντα έχουν πόρους
- Τα πάντα έχουν χρήστες
- Τα πάντα έχουν χρήματα

# Θέματα

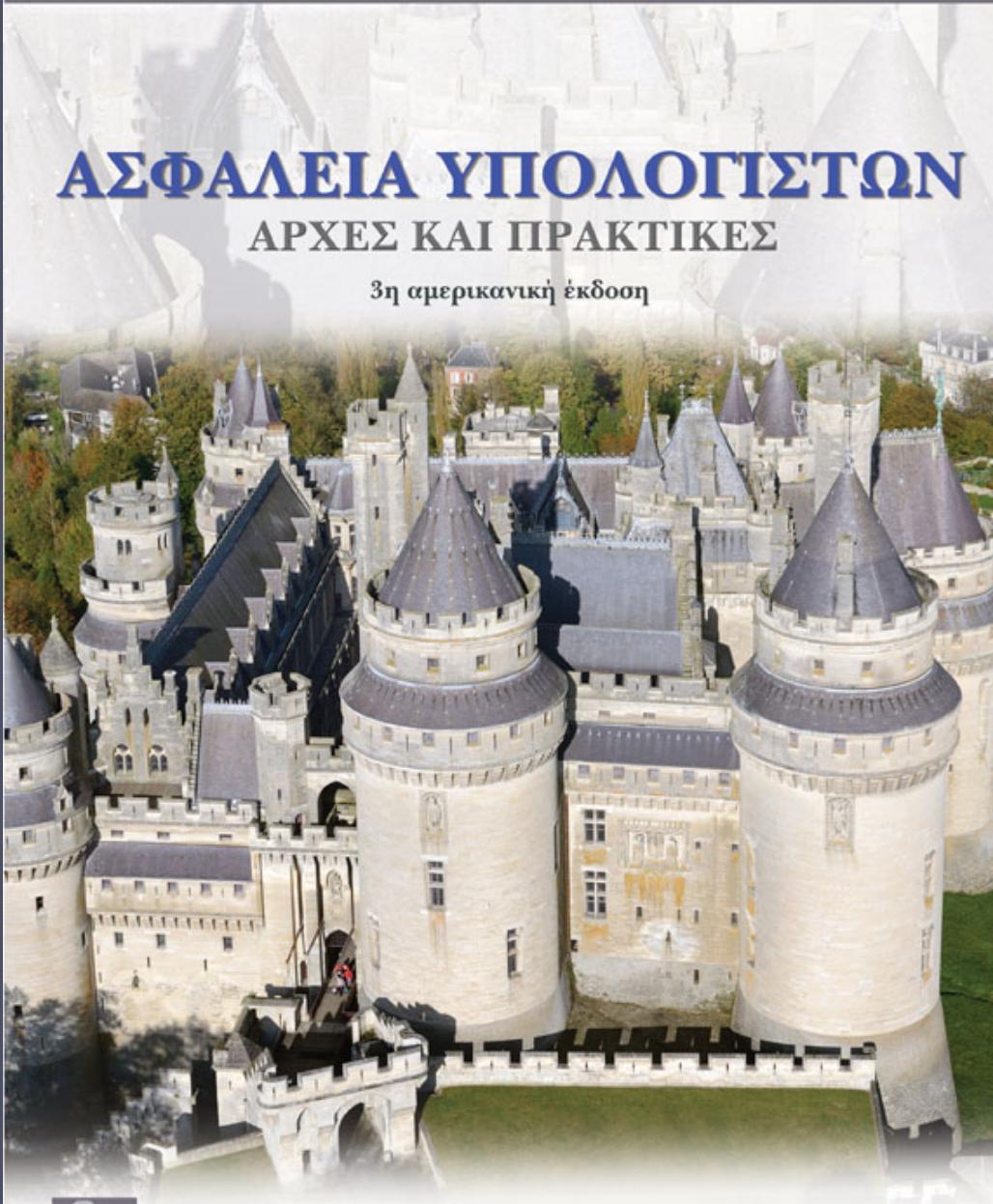
- Επιβεβαίωση, εξουσιοδότηση, έλεγχος πρόσβασης
- Προγράμματα προστασίας
- Ασφάλεια λογισμικού
- Άρνηση υπηρεσιών
- Ιοί και σκουλήκια
- Κρυπτογραφία
- Ανίχνευση εισβολών
- Ασφάλεια στον ιστό
- Ασφάλεια σε ασύρματα δίκτυα
- Ασφάλεια συστημάτων
- Πρωτόκολλα ασφάλειας

Ε Κ Δ Ο Σ Ε Ι Σ Κ Λ Ε Ι Δ Α Ρ Ι Θ Μ Ο Σ

# ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ

## ΑΡΧΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ

3η αμερικανική έκδοση



William Stallings • Lawrie Brown



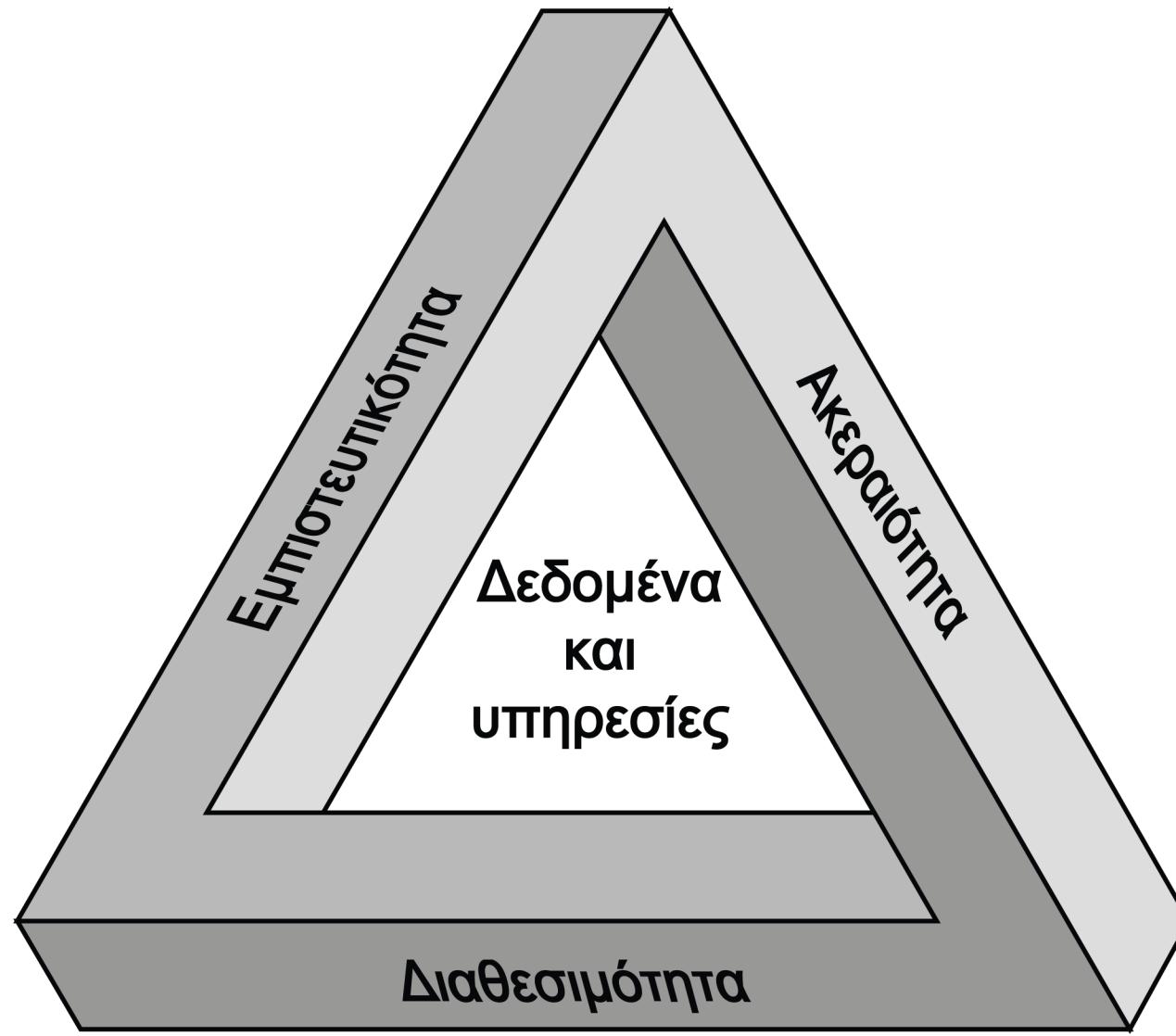
# Κεφάλαιο 1

## Επισκόπηση

Η ασφάλεια υπολογιστών ορίζεται στο *Εγχειρίδιο ασφάλειας υπολογιστών* (Computer Security Handbook) του NIST ως εξής:

«Η προστασία που παρέχεται σε ένα αυτοματοποιημένο πληροφοριακό σύστημα ώστε να εκπληρώνει τους ζητούμενους στόχους της διαφύλαξης της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των πόρων του (στους οποίους συγκαταλέγονται το υλικό (hardware), το λογισμικό (software), το υλικολογισμικό (firmware), οι πληροφορίες και τα δεδομένα, και οι τηλεπικοινωνίες)».

# Η τριάδα CIA



# Βασικές έννοιες της ασφάλειας

## Εμπιστευτικότητα

- Η διατήρηση των εξουσιοδοτημένων περιορισμών που έχουν επιβληθεί στην προσπέλαση και γνωστοποίηση πληροφοριών, συμπεριλαμβανομένων και τρόπων για την προστασία του προσωπικού απορρήτου και των πληροφοριών αποκλειστικής εκμετάλλευσης (proprietary information)

## Ακεραιότητα

- Η προστασία από την αθέμιτη τροποποίηση ή καταστροφή πληροφοριών, η οποία περιλαμβάνει και τη διασφάλιση της μη αποποίησης (nonrepudiation) των πληροφοριών και της αυθεντικότητάς τους

## Διαθεσιμότητα

- Η διασφάλιση της έγκαιρης και αξιόπιστης προσπέλασης και χρήσης των πληροφοριών.



# Επίπεδα αντίκτυπου

## Χαμηλό

Η απώλεια αναμένεται να έχει περιορισμένο αντίκτυπο στις λειτουργίες και τους πόρους του οργανισμού ή σε μεμονωμένους χρήστες

## Μεσαίο

Η απώλεια αναμένεται να έχει σοβαρό αντίκτυπο στις λειτουργίες και τους πόρους του οργανισμού ή σε μεμονωμένους χρήστες

## Υψηλό

Η απώλεια αναμένεται να έχει οδυνηρό ή καταστροφικό αντίκτυπο στις λειτουργίες και τους πόρους του οργανισμού ή σε μεμονωμένους χρήστες

# Οι προκλήσεις της ασφάλειας υπολογιστών

- Η ασφάλεια δεν τόσο απλή όσο θα φαινόταν σε κάποιον αρχάριο
- Πρέπει να λαμβάνονται υπόψη πιθανές επιθέσεις που έχουν ως στόχο τα παραπάνω χαρακτηριστικά της ασφάλειας
- Οι διαδικασίες που χρησιμοποιούνται για την παροχή συγκεκριμένων υπηρεσιών συχνά στερούνται λογικής
- Πρέπει να προσδιοριστεί η φυσική και λογική θέση
- Ενδέχεται να απαιτηθούν πρόσθετοι αλγόριθμοι ή πρωτόκολλα
- Ο επιτιθέμενος αρκεί να εντοπίσει μία και μόνη αδυναμία στο σύστημα, ενώ ο σχεδιαστής πρέπει να εντοπίσει και να εξαλείψει όλες τις αδυναμίες
- Οι χρήστες και οι διαχειριστές των συστημάτων δεν δείχνουν να εκτιμούν τα οφέλη που προκύπτουν από την ασφάλεια παρά μόνο μετά από κάποια παραβίαση
- Η ασφάλεια απαιτεί τακτική και αδιάκοπη, παρακολούθηση
- Αντιμετωπίζεται πολύ συχνά ως κάτι που μπορεί να παραπεμφθεί στο μέλλον –με άλλα λόγια να συμπεριληφθεί σε ένα σύστημα μετά την ολοκλήρωση του σχεδιασμού του
- Πολλοί θεωρούν ότι αποτελεί τροχοπέδη στην αποδοτική και φιλική προς τον χρήστη λειτουργία

# Πίνακας 1.1

**Αντίπαλος** (adversary) ή **πράκτορας απειλής** (threat agent)

Μια οντότητα που πραγματοποιεί επίθεση σε ένα σύστημα ή αποτελεί απειλή γι' αυτό.

**Επίθεση** (attack)

Η προσβολή της ασφάλειας του συστήματος που προκύπτει από μια ευφυή απειλή· με άλλα λόγια, μια ευφυής ενέργεια που αποτελεί προμελετημένη απόπειρα (ειδικά με την έννοια της μεθόδου ή τεχνικής) με σκοπό την παράκαμψη των υπηρεσιών ασφαλείας και την παραβίαση της πολιτικής ασφαλείας ενός συστήματος.

**Αντίμετρα** (countermeasures)

Ενέργειες, συσκευές, διαδικασίες, ή τεχνικές που μετριάζουν τις απειλές, περιορίζουν τις ευπάθειες, ή καταστέλλουν επιθέσεις εξαλείφοντας ή αποτρέποντάς τες, ελαχιστοποιώντας τη ζημιά που μπορούν να προκαλέσουν αυτές, ή ανιχνεύοντας και αναφέροντάς τες έτσι ώστε να ληφθούν μέτρα αντιμετώπισης.

**Κίνδυνος** (risk)

Η προοπτική απώλειας η οποία εκφράζεται ως η πιθανότητα εκμετάλλευσης μιας συγκεκριμένης ευπάθειας από μια συγκεκριμένη απειλή με στόχο ένα συγκεκριμένο επιβλαβές αποτέλεσμα.

**Πολιτική ασφαλείας** (security policy)

Ένα σύνολο κανόνων και πρακτικών που καθορίζουν ή ρυθμίζουν τον τρόπο με τον οποίο ένα σύστημα ή ένας οργανισμός παρέχει υπηρεσίες ασφαλείας για την προστασία ευαίσθητων και κρίσιμων πόρων του συστήματος.

**Πόρος συστήματος** (system resource ή asset)

Δεδομένα που περιέχονται σε ένα πληροφοριακό σύστημα· ή μια υπηρεσία που παρέχεται από ένα σύστημα· ή μια δυνατότητα του συστήματος, όπως η επεξεργαστική ισχύς ή το εύρος ζώνης της επικοινωνίας· ή ένα στοιχείο του εξοπλισμού του συστήματος (π.χ. ένα συστατικό στοιχείο του –υλικό, υλικολογισμικό, λογισμικό, ή τεκμηρίωση)· ή μια κτιριακή εγκατάσταση που στεγάζει τον εξοπλισμό και τις λειτουργίες του συστήματος.

**Απειλή** (threat)

Το ενδεχόμενο παραβίασης της ασφάλειας, το οποίο καθίσταται δυνατό όταν προκύπτει περίσταση, δυνατότητα, ενέργεια, ή συμβάν που θα μπορούσε να προκαλέσει ρίγμα στην ασφάλεια με πιθανές αρνητικές συνέπειες. Με άλλα λόγια, η απειλή είναι ο πιθανός κίνδυνος να εκμεταλλευθεί κάποιος μια ευπάθεια του συστήματος.

**Ευπάθεια** (vulnerability)

Μια ατέλεια ή αδυναμία στον σχεδιασμό, την υλοποίηση, ή τη λειτουργία και διαχείριση ενός συστήματος, την οποία θα μπορούσε να εκμεταλλευθεί κάποιος για να παραβιάσει την πολιτική ασφαλείας του συστήματος.

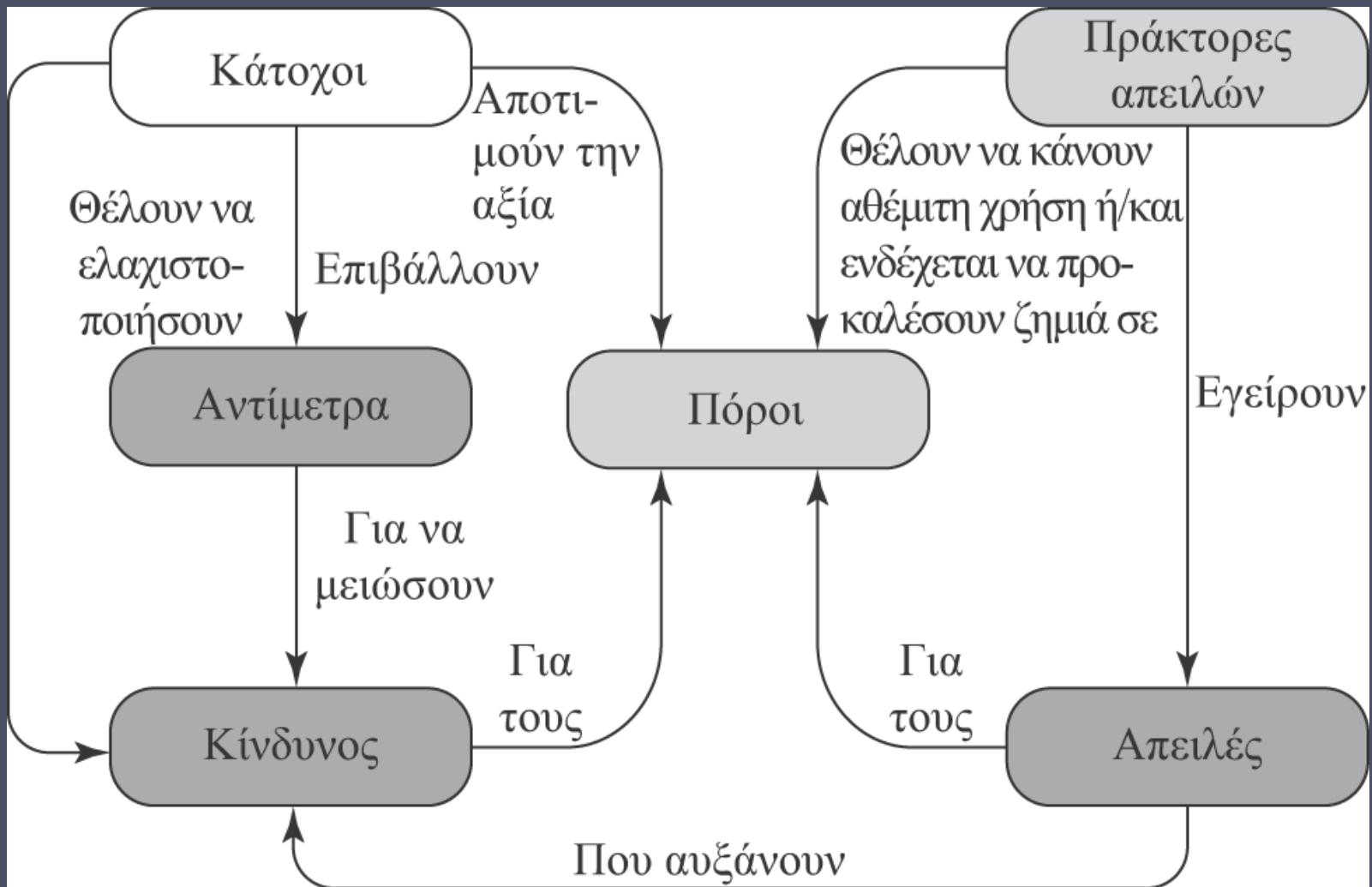
Ορολογία της  
ασφάλειας  
υπολογιστών

RFC 4949,

*Internet Security Glossary,*

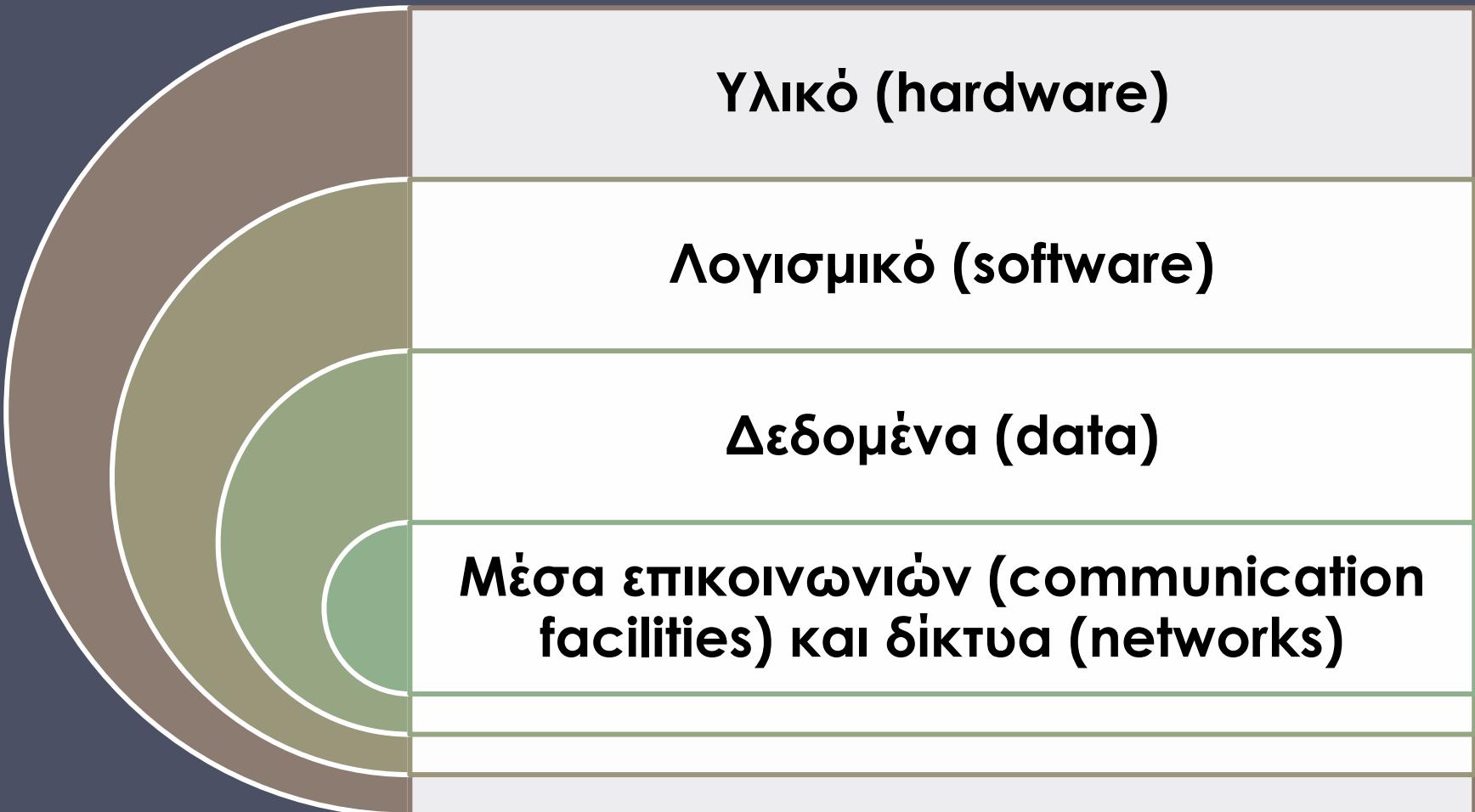
Μάιος 2000





Εικόνα 1.1 Οι έννοιες της ασφάλειας και οι μεταξύ τους σχέσεις

# Πόροι ενός υπολογιστικού συστήματος



# Ευπάθειες, απειλές και επιθέσεις

## • Κατηγορίες ευπαθειών

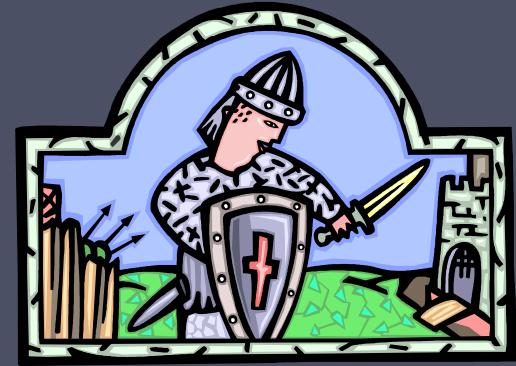
- Άλλοιωση (απώλεια της ακεραιότητας)
- Διαρροίες (απώλεια της εμπιστευτικότητας)
- Μη διαθεσιμότητα ή πολύ αργή απόκριση (απώλεια της διαθεσιμότητας)

## • Απειλές

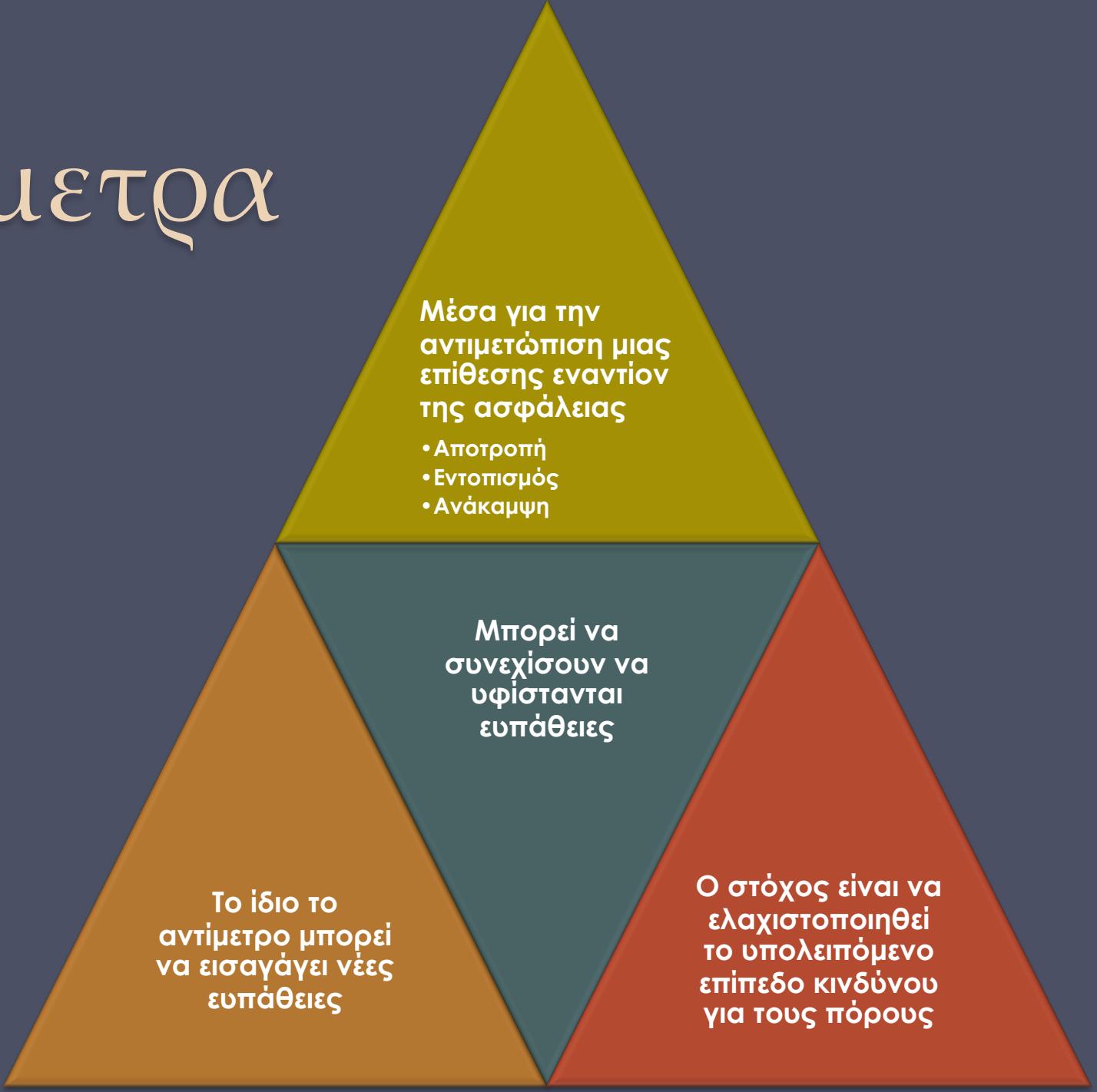
- Έχουν τη δυνατότητα να εκμεταλλεύονται ευπάθειες
- Αντιπροσωπεύουν μια πιθανή πρόκληση ζημιάς που σχετίζεται με την ασφάλεια ενός πόρου

## • Επιθέσεις (απειλές που υλοποιούνται)

- Παθητικές – προσπαθούν να μάθουν ή να χρησιμοποιήσουν πληροφορίες του συστήματος, χωρίς όμως να επηρεάζουν τους πόρους του
- Ενεργητικές – προσπαθούν να τροποποιήσουν τους πόρους του συστήματος ή να επηρεάσουν τη λειτουργία τους
- Εκ των ίσω – ξεκινούν από μια οντότητα που βρίσκεται εντός της περιμέτρου ασφαλείας
- Εξωτερικές – εξαπολύονται από κάποιο σημείο εκτός της περιμέτρου



# Αντίμετρα

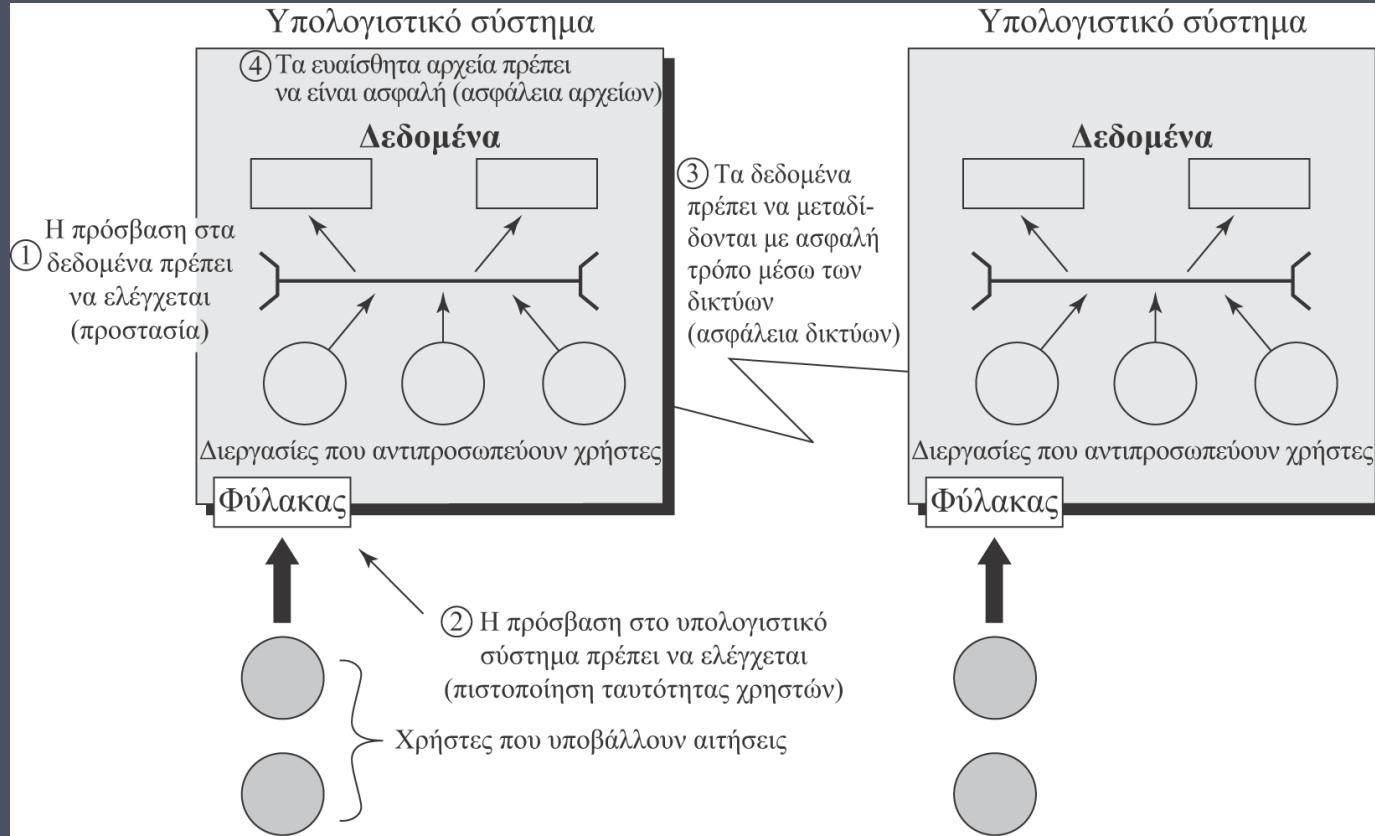


# Πίνακας 1.2

Συνέπεια απειλής	Ενέργεια απειλής (επίθεση)
<b>Μη εξουσιοδοτημένη γνωστοποίηση</b> (unauthorized disclosure) Μια περίσταση ή ένα συμβάν κατά το οποίο μια οντότητα αποκτά πρόσβαση σε δεδομένα για τα οποία δεν έχει εξουσιοδότηση.	<b>Αποκάλυψη</b> (exposure): Διατίθενται με άμεσο τρόπο ευαίσθητα δεδομένα σε μια μη εξουσιοδοτημένη οντότητα. <b>Υποκλοπή</b> (interception): Μια μη εξουσιοδοτημένη οντότητα αποκτά άμεση πρόσβαση σε ευαίσθητα δεδομένα που διακινούνται μεταξύ εξουσιοδοτημένων αποστολέων και παραληπτών. <b>Συμπερασμός</b> (inference): Μια ενέργεια απειλής μέσω της οποίας μια μη εξουσιοδοτημένη οντότητα αποκτά έμμεση πρόσβαση σε ευαίσθητα δεδομένα (αλλά όχι απαραίτητα τα δεδομένα που περιέχονται στην επικοινωνία) με τη βοήθεια συλλογισμών που βασίζονται σε χαρακτηριστικά ή παραπροϊόντα της επικοινωνίας. <b>Εισβολή</b> (intrusion): Μια μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση σε ευαίσθητα δεδομένα παρακάμπτοντας τα προστατευτικά μέτρα ασφαλείας ενός συστήματος.
<b>Εξαπάτηση</b> (deception) Μια περίσταση ή ένα συμβάν κατά το οποίο μια εξουσιοδοτημένη οντότητα ενδέχεται να λάβει ψευδή δεδομένα τα οποία εκλαμβάνει ως αληθή.	<b>Μεταμφίεση</b> (masquerade): Μια μη εξουσιοδοτημένη οντότητα υποδύεται μια εξουσιοδοτημένη οντότητα προκειμένου να αποκτήσει πρόσβαση σε ένα σύστημα ή να προβεί σε μια κακόβουλη ενέργεια. <b>Παραποίηση</b> (falsification): Μια εξουσιοδοτημένη οντότητα εξαπατάται με ψευδή δεδομένα. <b>Αποποίηση</b> (repudiation): Μια οντότητα αρνείται ψευδώς να αναλάβει την ευθύνη για μια ενέργεια προκειμένου να εξαπατήσει μια άλλη οντότητα.
<b>Διακοπή</b> (disruption) Μια περίσταση ή ένα συμβάν που διακόπτει ή αποτρέπει την ορθή εκτέλεση υπηρεσιών και λειτουργιών ενός συστήματος.	<b>Εξουδετέρωση</b> (incapacitation): Διακόπτει ή αποτρέπει τη λειτουργία ενός συστήματος απενεργοποιώντας κάποιο συστατικό στοιχείο του. <b>Αλλοίωση</b> (corruption): Αλλάζει τη λειτουργία ενός συστήματος με ανεπιθύμητο τρόπο, τροποποιώντας δυσμενώς λειτουργίες ή δεδομένα του. <b>Παρακώλυση</b> (obstruction): Μια ενέργεια απειλής η οποία διακόπτει την εκτέλεση υπηρεσιών του συστήματος παρακωλύοντας τη λειτουργία του.
<b>Ιδιοποίηση</b> (usurpation) Μια περίσταση ή ένα συμβάν που επιτρέπει τον έλεγχο υπηρεσιών ή λειτουργιών του συστήματος από κάποια μη εξουσιοδοτημένη οντότητα.	<b>Σφετερισμός</b> (misappropriation): Μια οντότητα αναλαμβάνει χωρίς εξουσιοδότηση τον έλεγχο, σε φυσικό ή λογικό επίπεδο, ενός πόρου του συστήματος. <b>Αθέμιτη χρήση</b> (misuse): Εξαναγκάζει ένα συστατικό στοιχείο του συστήματος να εκτελέσει μια λειτουργία ή υπηρεσία επιζήμια για την ασφάλεια του συστήματος.

Συνέπειες  
των απειλών και  
οι τύποι  
των ενεργειών  
απειλών που  
προκαλούν κάθε  
συνέπεια

Πηγή:  
RFC 4949



Εικόνα 1.2 Το εύρος της ασφάλειας υπολογιστών. Στην εικόνα παρουσιάζονται άλλα ζητήματα ασφαλείας που δεν αφορούν τη φυσική ασφάλεια, στα οποία συμπεριλαμβάνονται ο έλεγχος πρόσβασης σε υπολογιστικά συστήματα, η περιφρούρηση δεδομένων που μεταδίδονται μέσω συστημάτων επικοινωνιών, και η περιφρούρηση αποθηκευμένων δεδομένων.



# Πίνακας 1.3

## Υπολογιστικοί και δικτυακοί πόροι, με παραδείγματα απειλών

	<b>Διαθεσιμότητα</b>	<b>Εμπιστευτικότητα</b>	<b>Ακεραιότητα</b>
<b>Υλικό</b>	Λαμβάνει χώρα κλοπή ή απενεργοποίηση εξοπλισμού, με αποτέλεσμα την άρνηση εξυπηρέτησης.	Λαμβάνει χώρα κλοπή κάποιου μη κρυπτογραφημένου δίσκου CD-ROM ή DVD.	
<b>Λογισμικό</b>	Διαγράφονται προγράμματα, με αποτέλεσμα την άρνηση πρόσβασης στους χρήστες	Δημιουργείται ένα μη εξουσιοδοτημένο αντίγραφο του λογισμικού.	Τροποποιείται ένα λειτουργικό πρόγραμμα, με σκοπό είτε να προκληθεί αστοχία κατά την εκτέλεσή του είτε να εξαναγκαστεί να επιτελέσει κάποια μη προβλεπόμενη εργασία.
<b>Δεδομένα</b>	Διαγράφονται αρχεία, με αποτέλεσμα την άρνηση πρόσβασης στους χρήστες.	Πραγματοποιείται μη εξουσιοδοτημένη ανάγνωση δεδομένων. Η ανάλυση των στατιστικών στοιχείων αποκαλύπτει ότι υπάρχουν υποκείμενα δεδομένα.	Τροποποιούνται υπάρχοντα αρχεία ή κατασκευάζονται ψευδή, νέα αρχεία.
<b>Γραμμές και δίκτυα επικοινωνιών</b>	Διαγράφονται ή καταστρέφονται μηνύματα. Οι γραμμές ή τα δίκτυα επικοινωνιών παύουν να είναι στη διάθεση των χρηστών.	Γίνεται ανάγνωση μηνυμάτων. Παρατηρείται το μοτίβο της κυκλοφορίας τους.	Τροποποιούνται, καθυστερούν, αναδιατάσσονται ή αντιγράφονται μηνύματα. Κατασκευάζονται ψευδή μηνύματα.



# Παθητικές και ενεργητικές επιθέσεις

## Παθητική επίθεση

- Προσπαθεί να μάθει ή να χρησιμοποιήσει πληροφορίες του συστήματος, χωρίς όμως να επηρεάζει τους πόρους του
- Υποκλοπή (eavesdropping), ή παρακολούθηση (monitoring), μιας μετάδοσης
- Σκοπός του επιτιθέμενου είναι να αποκτήσει πληροφορίες καθώς εκείνες μεταδίδονται
- Δύο τύποι :
  - Απελευθέρωση του περιεχομένου ενός μηνύματος (release of message contents)
  - Ανάλυση κυκλοφορίας (traffic analysis)

## Ενεργητική επίθεση

- Προσπαθεί να τροποποιήσει τους πόρους του συστήματος ή να επηρεάσει τη λειτουργία τους
- Περιλαμβάνουν κάποια τροποποίηση του ρεύματος δεδομένων (data stream), ή τη δημιουργία ενός ψεύτικου ρεύματος
- Τέσσερις κατηγορίες:
  - Αναπαραγωγή (replay)
  - Μεταμφίεση (masquerade)
  - Τροποποίηση μηνυμάτων (modification of messages)
  - Άρνηση εξυπηρέτησης (denial of service)

**Έλεγχος πρόσβασης** (access control): Η πρόσβαση στα πληροφοριακά συστήματα περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες, σε διεργασίες που ενεργούν εκ μέρους εξουσιοδοτημένων χρηστών, ή σε συσκευές (συμπεριλαμβανομένων άλλων πληροφοριακών συστημάτων), καθώς και στους τύπους συναλλαγών και λειτουργιών που οι εξουσιοδοτημένοι χρήστες έχουν το δικαίωμα να εκτελούν.

**Ενημέρωση και εκπαίδευση** (awareness and training): (i) Εξασφαλίζεται ότι οι διαχειριστές και οι χρήστες των πληροφοριακών συστημάτων του οργανισμού είναι ενήμεροι για τους πιθανούς κινδύνους της ασφάλειας που σχετίζονται με τις δραστηριότητές τους, καθώς και για τους ισχύοντες νόμους, κανονισμούς και πολιτικές που αφορούν την ασφάλεια των συστημάτων αυτών· και (ii) εξασφαλίζεται ότι τα μέλη του προσωπικού είναι επαρκώς εκπαιδευμένα για να φέρουν σε πέρας τα καθήκοντα που τους έχουν ανατεθεί και αφορούν την ασφάλεια των πληροφοριών.

**Διαχειριστική παρακολούθηση και απόδοση ευθυνών** (audit and accountability): (i) Δημιουργούνται, προστατεύονται και τηρούνται εγγραφές διαχειριστικής παρακολούθησης των πληροφοριακών συστημάτων στον βαθμό που είναι απαραίτητος για να είναι εφικτή η παρακολούθηση (monitoring), ανάλυση και αναφορά παράνομων, μη εξουσιοδοτημένων ή ανάρμοστων δραστηριοτήτων των πληροφοριακών συστημάτων· και (ii) εξασφαλίζεται ότι οι ενέργειες κάθε χρήστη ενός πληροφοριακού συστήματος μπορούν να αποδοθούν αποκλειστικά σε αυτόν ώστε να μπορεί να λογοδοτήσει για τις πράξεις του.

**Πιστοποίηση, διαπίστευση και αξιολογήσεις ασφαλείας** (certification, accreditation, and security assessments): (i) Οι μηχανισμοί ελέγχου της ασφάλειας στα πληροφοριακά συστήματα του οργανισμού αξιολογούνται περιοδικά προκειμένου να προσδιοριστεί η αποτελεσματικότητα της εφαρμογής τους· (ii) αναπτύσσονται και υλοποιούνται σχέδια δράσης που αποσκοπούν στη διόρθωση των ανεπαρκειών και τη μείωση ή εξάλειψη των ευπαθειών στα πληροφοριακά συστήματα του οργανισμού· (iii) εξουσιοδοτείται η λειτουργία των πληροφοριακών συστημάτων του οργανισμού και των σχετικών συνδέσεων· και (iv) παρακολουθούνται οι μηχανισμοί ελέγχου της ασφάλειας των πληροφοριακών συστημάτων σε μόνιμη βάση προκειμένου να διασφαλιστεί η συνεχιζόμενη αποτελεσματικότητά τους.

**Διαχείριση διευθετήσεων** (configuration management): (i) Δημιουργούνται και τηρούνται διευθετήσεις αναφοράς και κατάλογοι των πληροφοριακών συστημάτων του οργανισμού (συμπεριλαμβανομένου του υλικού, του λογισμικού, του υλικολογισμικού και της τεκμηρίωσης) καθ' όλη τη διάρκεια του κύκλου ζωής της ανάπτυξης του αντίστοιχου συστήματος· και (ii) καθιερώνονται και επιβάλλονται ρυθμίσεις ασφαλείας για τα προϊόντα της τεχνολογίας πληροφοριών (information technology) που χρησιμοποιούνται στα πληροφοριακά συστήματα του οργανισμού.

# Πίνακας 1.4

## Απαιτήσεις ασφαλείας

(FIPS PUB 200)

(σελ. 1 από 3)

(Ο πίνακας βρίσκεται στις σελ. 52-53 του βιβλίου.)

**Εκπόνηση σχεδίων έκτακτης ανάγκης** (contingency planning): Δημιουργούνται, διατηρούνται και υλοποιούνται σχέδια σχετικά με τα πληροφοριακά συστήματα του οργανισμού, που αφορούν την αντιμετώπιση έκτακτων περιστατικών, τις λειτουργίες λήψης αντιγράφων ασφαλείας και την ανάκαμψή τους μετά από ενδεχόμενη καταστροφή, με απότερο σκοπό την εξασφάλιση της διαθεσιμότητας κρίσιμων πληροφοριακών πόρων και τη συνέχιση των λειτουργιών σε καταστάσεις έκτακτης ανάγκης.

**Ταυτοποίηση και πιστοποίηση ταυτότητας** (identification and authentication): Ταυτοποιούνται οι χρήστες των πληροφοριακών συστημάτων, οι διεργασίες που ενεργούν εκ μέρους εξουσιοδοτημένων χρηστών, ή οι συσκευές, και πιστοποιείται (ή επαληθεύεται) η ταυτότητα των χρηστών, διεργασιών, ή συσκευών, ως προαπαιτούμενο προκειμένου να επιτρέπεται η πρόσβαση στα πληροφοριακά συστήματα του οργανισμού.

**Αντιμετώπιση περιστατικών** (incident response): (i) Αναπτύσσεται η λειτουργική ικανότητα αντιμετώπισης περιστατικών με τα πληροφοριακά συστήματα του οργανισμού, η οποία περιλαμβάνει επαρκή μέτρα προετοιμασίας, ανίχνευσης, ανάλυσης, ανάσχεσης, ανάκαμψης, και απόκρισης στους χρήστες· και (ii) ενεργοποιείται η παρακολούθηση, τεκμηρίωση και αναφορά περιστατικών στους αρμόδιους αξιωματούχους του οργανισμού ή/και στις αρχές.

**Συντήρηση** (maintenance): (i) Πραγματοποιείται περιοδική και έγκαιρη συντήρηση των πληροφοριακών συστημάτων του οργανισμού· και (ii) προβλέπονται αποτελεσματικοί τρόποι ελέγχου για τα εργαλεία, τις τεχνικές, τους μηχανισμούς και το προσωπικό που εμπλέκεται στη διεξαγωγή της συντήρησης των πληροφοριακών συστημάτων.

**Προστασία μέσων καταγραφής/αναπαραγωγής** (media protection): (i) Παρέχεται προστασία των έντυπων και ψηφιακών μέσων καταγραφής/αναπαραγωγής που διαθέτουν τα πληροφοριακά συστήματα· (ii) περιορίζεται μόνο σε εξουσιοδοτημένους χρήστες η πρόσβαση σε πληροφορίες οι οποίες περιέχονται στα μέσα καταγραφής/αναπαραγωγής που διαθέτουν τα πληροφοριακά συστήματα· και (iii) «απολυμαίνονται» ή καταστρέφονται τα μέσα καταγραφής/αναπαραγωγής των πληροφοριακών συστημάτων πριν από την απόρριψή τους ή τη διάθεσή τους για επαναχρησιμοποίηση.

**Φυσική και περιβαλλοντική προστασία** (physical and environmental protection): (i) Περιορίζεται η πρόσβαση στα πληροφοριακά συστήματα, τον εξοπλισμό και τα αντίστοιχα περιβάλλοντα λειτουργίας μόνο σε εξουσιοδοτημένα άτομα· (ii) προβλέπεται φύλαξη των κτιριακών εγκαταστάσεων και της υποδομής υποστήριξης των πληροφοριακών συστημάτων· (iii) διατίθενται βιοθητικά προγράμματα υποστήριξης για τα πληροφοριακά συστήματα· (iv) παρέχεται προστασία των πληροφοριακών συστημάτων από περιβαλλοντικούς κινδύνους· και (v) προβλέπονται κατάλληλοι μηχανισμοί ελέγχου του περιβάλλοντος των εγκαταστάσεων που στεγάζουν τα πληροφοριακά συστήματα.

**Σχεδιασμός** (planning): Αφορά την ανάπτυξη, τεκμηρίωση, περιοδική ενημέρωση και υλοποίηση σχεδίων ασφαλείας, τα οποία περιγράφουν τους υπάρχοντες μηχανισμούς ελέγχου της ασφάλειας ή εκείνους που πρόκειται να ενταχθούν στα πληροφοριακά συστήματα του οργανισμού, καθώς και τους κανόνες συμπεριφοράς των ατόμων που έχουν πρόσβαση στα συστήματα αυτά.

**Ασφάλεια προσωπικού** (personnel security): (i) Εξασφαλίζεται ότι τα άτομα που κατέχουν θέσεις ευθύνης στους οργανισμούς (συμπεριλαμβανομένων των ανεξάρτητων παρόχων υπηρεσιών) είναι αξιόπιστα και πληρούν τα καθιερωμένα κριτήρια ασφαλείας για τις θέσεις αυτές· (ii) εξασφαλίζεται ότι οι πληροφορίες και τα πληροφοριακά συστήματα του οργανισμού είναι προστατευμένα τόσο κατά τη διάρκεια μεταβολών των προσωπικού, όπως απολύσεις και μεταθέσεις, όσο και μετά από αυτές· και (iii) επιβάλλονται κυρώσεις σε μέλη του προσωπικού που δεν συμμορφώνονται με τις πολιτικές και τις διαδικασίες ασφαλείας του οργανισμού.

# Πίνακας 1.4

## Απαιτήσεις ασφαλείας

(FIPS PUB 200)

(σελ. 2 από 3)

(Ο πίνακας βρίσκεται στις σελ. 52-53 του βιβλίου.)

**Εκτίμηση κινδύνου** (risk assessment): Πραγματοποιείται περιοδική εκτίμηση του κινδύνου για τις λειτουργίες (συμπεριλαμβανομένων του γενικού στόχου, των σκοπών, της εικόνας, ή της φήμης), τους πόρους και τα άτομα του οργανισμού, όπως αυτός απορρέει από τη χρήση των πληροφοριακών συστημάτων και τη σχετική επεξεργασία, αποθήκευση, ή μετάδοση των πληροφοριών του οργανισμού.

**Απόκτηση συστημάτων και υπηρεσιών** (systems and services acquisition): (i) Δεσμεύονται επαρκείς πόροι για την ικανοποιητική προστασία των πληροφοριακών συστημάτων του οργανισμού· (ii) χρησιμοποιούνται διαδικασίες οι οποίες λαμβάνουν υπόψη την ασφάλεια των πληροφοριών σε ολόκληρο τον κύκλο ζωής της ανάπτυξης συστημάτων· (iii) επιβάλλονται περιορισμοί στη χρήση και την εγκατάσταση λογισμικού· και (iv) εξασφαλίζεται ότι οι ανεξάρτητοι πάροχοι χρησιμοποιούν επαρκή μέτρα ασφαλείας για την προστασία των πληροφοριών, των εφαρμογών και των υπηρεσιών που τους εκχωρούν οι εταιρείες.

**Προστασία συστημάτων και επικοινωνιών** (system and communications protection): (i) Παρακολουθούνται, ελέγχονται και προστατεύονται οι επικοινωνίες του οργανισμού (δηλαδή οι πληροφορίες που μεταδίδονται ή λαμβάνονται από τα πληροφοριακά συστήματα του οργανισμού) στα εξωτερικά όρια και σε βασικά εσωτερικά όρια των πληροφοριακών συστημάτων· και (ii) γίνεται χρήση αρχιτεκτονικών σχεδιασμών, τεχνικών ανάπτυξης λογισμικού, και αρχών τεχνολογίας συστημάτων που προάγουν την αποτελεσματικότητα της ασφάλειας των πληροφοριών εντός των πληροφοριακών συστημάτων του οργανισμού.

**Ακεραιότητα συστημάτων και πληροφοριών** (system and information integrity): (i) Προσδιορίζονται, γνωστοποιούνται και διορθώνονται αδυναμίες των πληροφοριών και των πληροφοριακών συστημάτων· (ii) παρέχεται προστασία από κακόβουλο κώδικα σε κατάλληλες θέσεις μέσα στα πληροφοριακά συστήματα του οργανισμού· και (iii) παρακολουθούνται οι ειδοποιήσεις και οι αναφορές ασφαλείας των πληροφοριακών συστημάτων του οργανισμού ώστε να λαμβάνονται τα κατάλληλα μέτρα.

# Πίνακας 1.4

## Απαιτήσεις ασφαλείας

(FIPS PUB 200)

(σελ. 3 από 3)

(Ο πίνακας βρίσκεται στις σελ. 52-53 του βιβλίου.)

# Θεμελιώδεις αρχές σχεδιασμού της ασφάλειας

Οικονομία του  
μηχανισμού

Ασφαλείς από  
αποτυχίες  
προεπιλογές

Πλήρης  
μεσολάβηση

Ανοικτός  
σχεδιασμός

Διαχωρισμός των  
προνομίων

Ελάχιστα  
προνόμια

Ελάχιστος κοινός  
μηχανισμός

Ψυχολογικά  
αποδεκτό

Απομόνωση

Ενθυλάκωση

Τμηματικότητα

Διαστρωμάτωση

Ελάχιστη  
έκπληξη

# Επιφάνειες επίθεσης

Αποτελούνται από τις προσιτές και εκμεταλλεύσιμες ευπάθειες ενός συστήματος

## Παραδείγματα:

Ανοικτές θύρες σε διακομιστές Ιστού ή διακομιστές άλλου τύπου οι οποίοι διαθέτουν σύνδεση με τον έξω κόσμο, καθώς και κώδικας που «ακούει» σε αυτές τις θύρες

Υπηρεσίες διαθέσιμες στο εσωτερικό ενός τείχους προστασίας (firewall)

Κώδικας που επεξεργάζεται εισερχόμενα δεδομένα, μηνύματα ηλεκτρονικού ταχυδρομείου, XML (eXtensible Markup Language, Επεκτάσιμη Γλώσσα Σήμανσης), έγγραφα, καθώς και προσαρμοσμένες μορφές ανταλλαγής δεδομένων εξειδικευμένες για συγκεκριμένους κλάδους

Διασυνδέσεις, SQL (Structured Query Language, Δομημένη Γλώσσα Ερωτημάτων), και φόρμες Ιστού

Ένας εργαζόμενος με πρόσβαση σε ευαίσθητες πληροφορίες, ο οποίος είναι ευάλωτος σε επιθέσεις κοινωνικής μηχανικής (social engineering)

# Κατηγορίες επιφανειών επίθεσης

## Επιφάνεια επίθεσης δικτύου

Ευπάθειες εταιρικών δικτύων,  
δικτύων ευρείας περιοχής,  
ή του Διαδικτύου

Στη συγκεκριμένη κατηγορία  
περιλαμβάνονται ευπάθειες  
των πρωτοκόλλων δικτύου, όπως  
εκείνες που χρησιμοποιούνται  
για μια επίθεση άρνησης  
εξυπηρέτησης, για τη διακοπή  
συνδέσμων επικοινωνίας, καθώς  
και για διάφορες μορφές  
επιθέσεων από εισβολείς

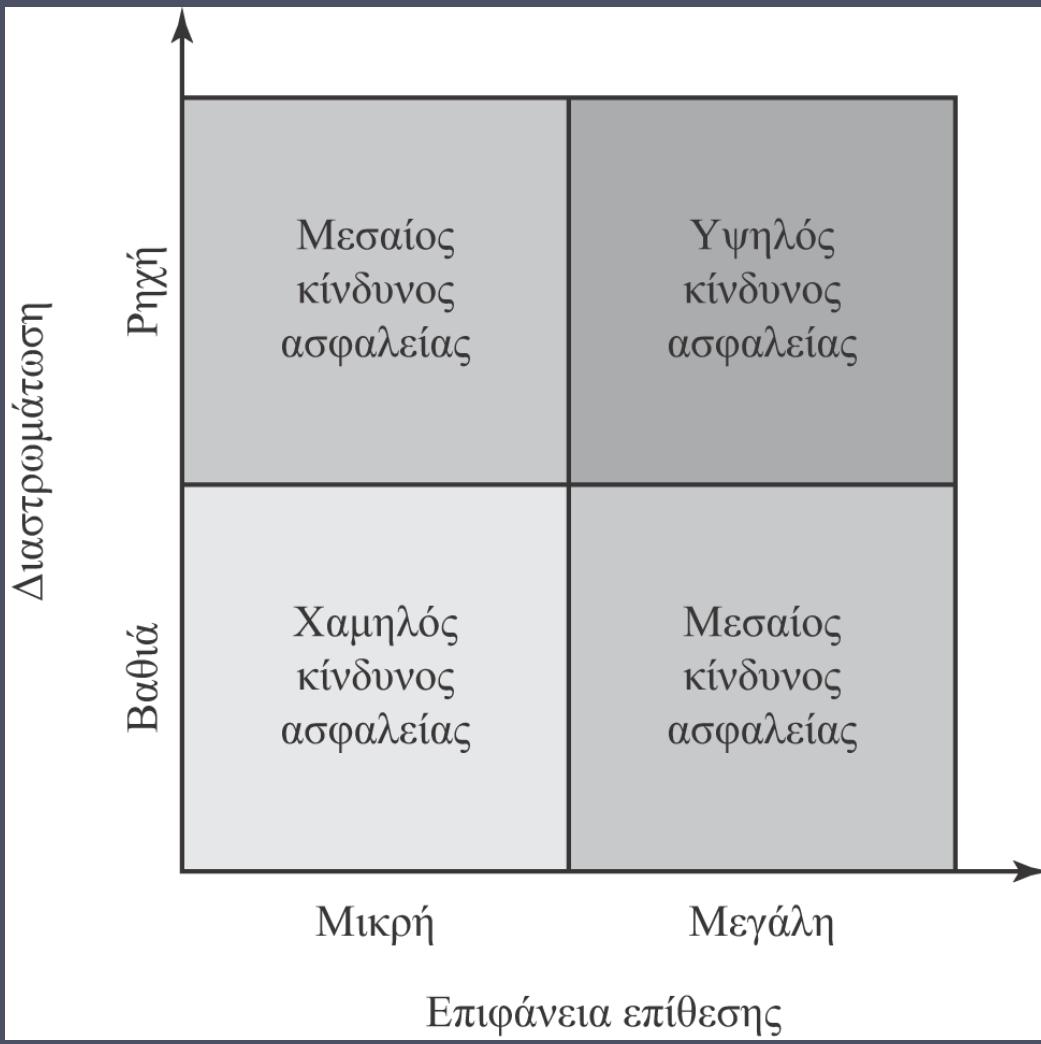
## Επιφάνεια επίθεσης λογισμικού

Ευπάθειες του κώδικα  
εφαρμογών, βιοηθητικών  
προγραμμάτων,  
ή λειτουργικών συστημάτων

Ιδιαίτερης προσοχής στη  
συγκεκριμένη κατηγορία χρήζει  
το λογισμικό των διακομιστών  
Ιστού

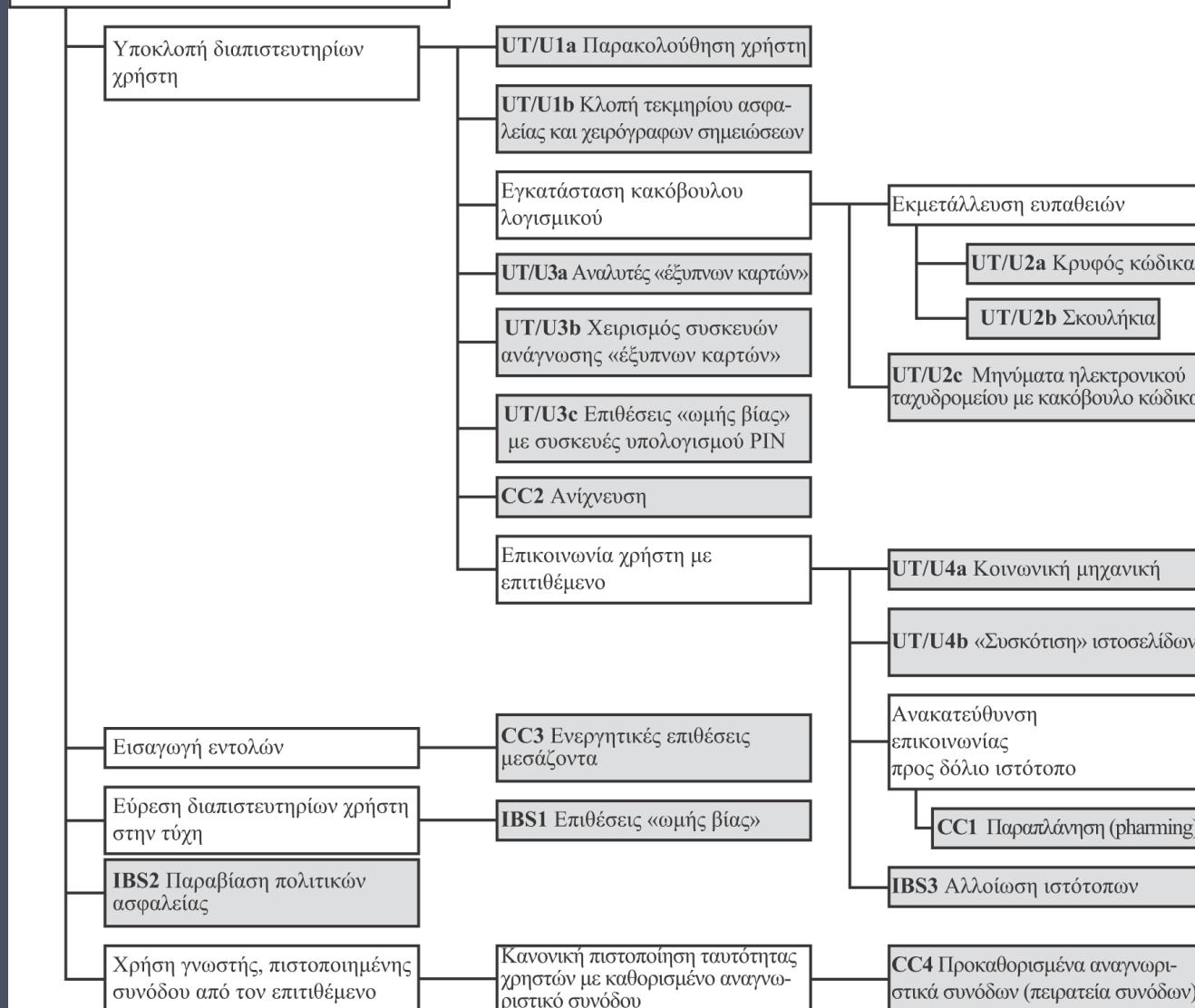
## Επιφάνεια επίθεσης ανθρώπων

Ευπάθειες που  
δημιουργούνται  
από το προσωπικό ή από  
παρείσακτους, όπως  
η κοινωνική μηχανική,  
τα ανθρώπινα σφάλματα  
και οι έμπιστοι χρήστες  
εκ των έσω



Εικόνα 1.3 Άμυνα σε βάθος και επιφάνεια επίθεσης

**Παραβίαση τραπεζικού λογαριασμού**



**Εικόνα 1.4 Ένα δένδρο επίθεσης για πιστοποίηση ταυτότητας τραπεζικών συναλλαγών μέσω του Διαδικτύου**

# Στρατηγική της ασφάλειας υπολογιστών

## Πολιτική ασφαλείας

- Τυπική διατύπωση κανόνων και πρακτικών που καθορίζουν ή ρυθμίζουν τον τρόπο με τον οποίο ένα σύστημα ή ένας οργανισμός παρέχει υπηρεσίες ασφαλείας για την προστασία ευαίσθητων και κρίσιμων πόρων του συστήματος

## Υλοποίηση της ασφάλειας

- Περιλαμβάνει τέσσερις συμπληρωματικές κατευθύνσεις δράσης:
- Αποτροπή
- Ανίχνευση
- Απόκριση
- Ανάκαρψη

## Διαβεβαίωση

- Ο βαθμός εμπιστοσύνης που μπορεί να έχει κάποιος ότι τα μέτρα ασφαλείας, τόσα τεχνικά όσα και λειτουργικά, λειτουργούν κατά αναμενόμενο τρόπο για την προστασία του συστήματος και των επεξεργαζόμενων πληροφοριών

## Αξιολόγηση

- Διαδικασία της εξέτασης ενός υπολογιστικού προϊόντος ή συστήματος με βάση ορισμένα κριτήρια

# Σύνοψη

- Έννοιες της ασφάλειας υπολογιστών
  - Ορισμός
  - Προκλήσεις
  - Μοντέλο
- Απειλές, επιθέσεις και πόροι
  - Απειλές και επιθέσεις
  - Απειλές και πόροι
- Λειτουργικές απαιτήσεις της ασφάλειας
- Θεμελιώδεις αρχές σχεδιασμού της ασφάλειας
- Επιφάνειες επίθεσης και δένδρα επίθεσης
  - Επιφάνειες επίθεσης
  - Δένδρα επίθεσης
- Στρατηγική της ασφάλειας υπολογιστών
  - Πολιτική ασφαλείας
  - Υλοποίηση της ασφάλειας
  - Διαβεβαίωση και αξιολόγηση

