Εισαγωγή στην ασφάλεια

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

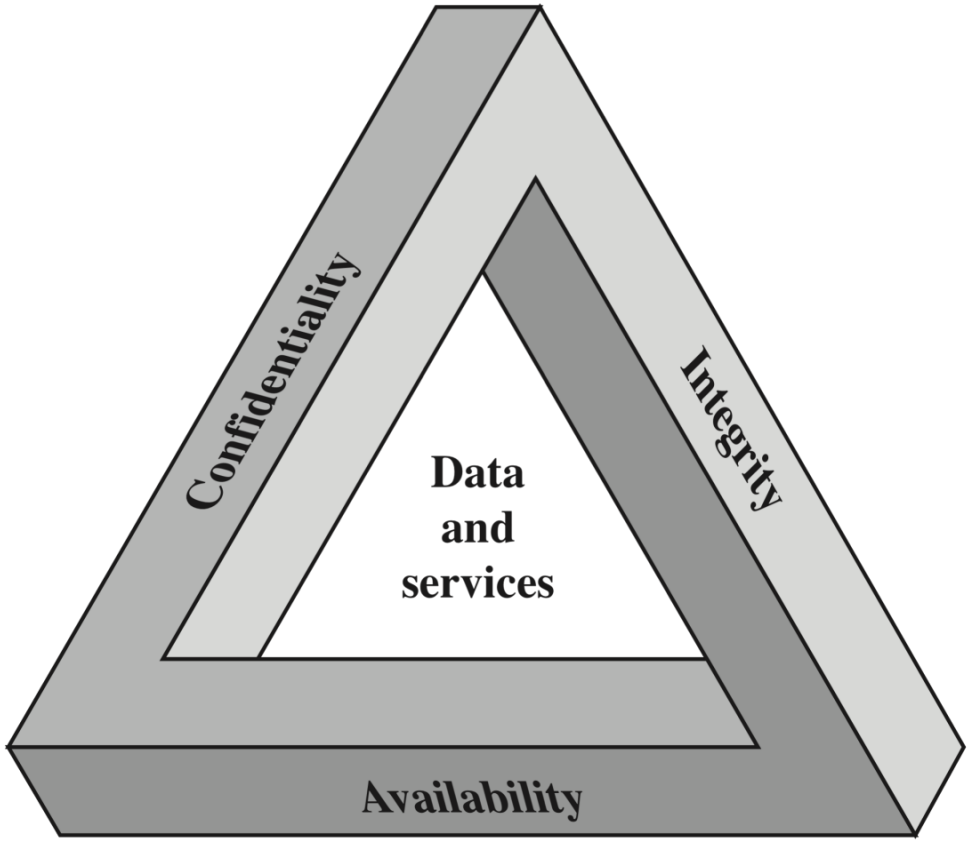
Περιεχόμενα

- Βασικοί ορισμοί
- Κατηγορίες επιθέσεων
- Μέτρα ασφάλειας
- Τρέχουσα κατάσταση

Ορισμός ασφάλειας

- Από το βιβλίο του Stallings:
- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the confidentiality, integrity, and availability of information system resources, including:
  - hardware, software, and firmware,
  - information/data,
  - telecommunication infrastructure

Ορισμός ασφάλειας: CIA



Ορισμός ασφάλειας

- Η προστασία των «αντικειμένων» ενός υπολογιστικού συστήματος
- Η προστασία από μη εξουσιοδοτημένες ενέργειες στο υπολογιστικό σύστημα
- Η διασφάλιση της:
  - Εμπιστευτικότητας των πληροφοριών,
  - Ακεραιότητας των πληροφοριών, και
  - Διαθεσιμότητας των πληροφοριών & υπολογιστικών πόρων

Κύριοι στόχοι/υπηρεσίες

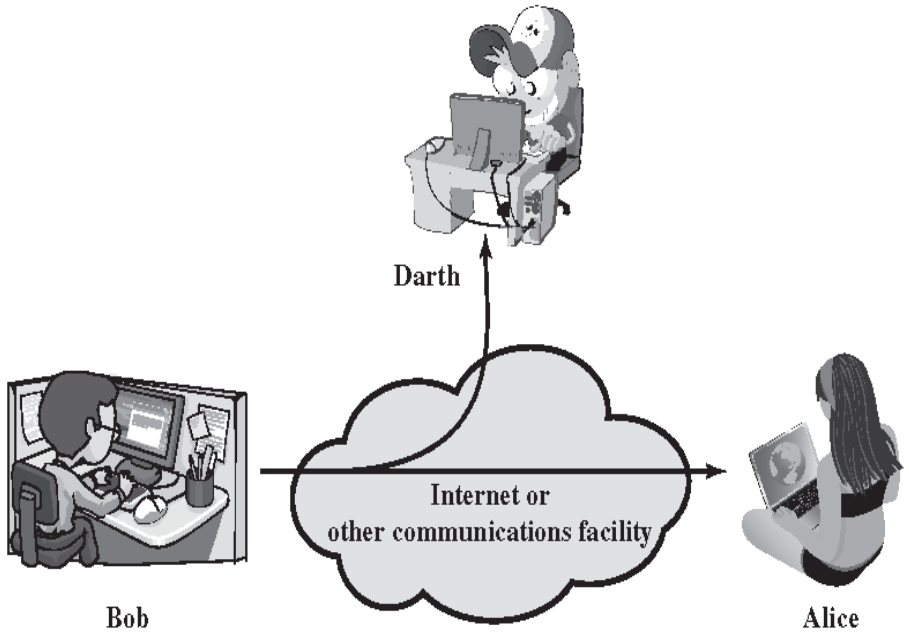
- Εμπιστευτικότητα
  Η προστασία από μη-εξουσιοδοτημένη αποκάλυψη πληροφορίας
- Ακεραιότητα
  Η προστασία από μη-εξουσιοδοτημένη τροποποίηση πληροφορίας
- Διαθεσιμότητα
  Η διατήρηση της ιδιότητας πρόσβασης σε δεδομένα ή/και πληροφοριακά συστήματα σε οποιαδήποτε χρονική στιγμή και με οποιοδήποτε τρόπο

Κύριοι στόχοι/υπηρεσίες

- Αυθεντικοποίηση
  Επαλήθευση της ταυτότητας ενός χρήστη, μηχανής ή άλλης οντότητας σε πληροφοριακά/επικοινωνιακά συστήματα
- Έλεγχος πρόσβασης
  Διατήρηση του ελέγχου των δεδομένων στα οποία μπορεί να αποκτήσει πρόσβαση μία οντότητα
- Μη-αποποίηση
  Προστασία από αποποίηση παραλαβής ή αποστολής δεδομένων

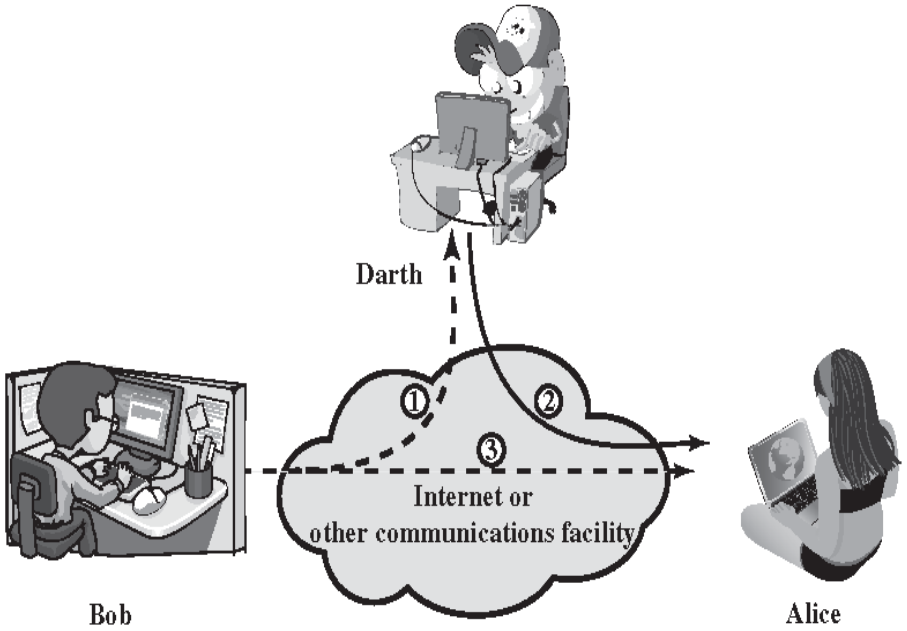
Επιθέσεις: βασικές κατηγορίες

- Παθητικές επιθέσεις
  - Λήψη & πρόσβαση στην πληροφορία
  - Χωρίς άλλες (εμφανείς) συνέπειες
  - Δύσκολες στην ανίχνευση

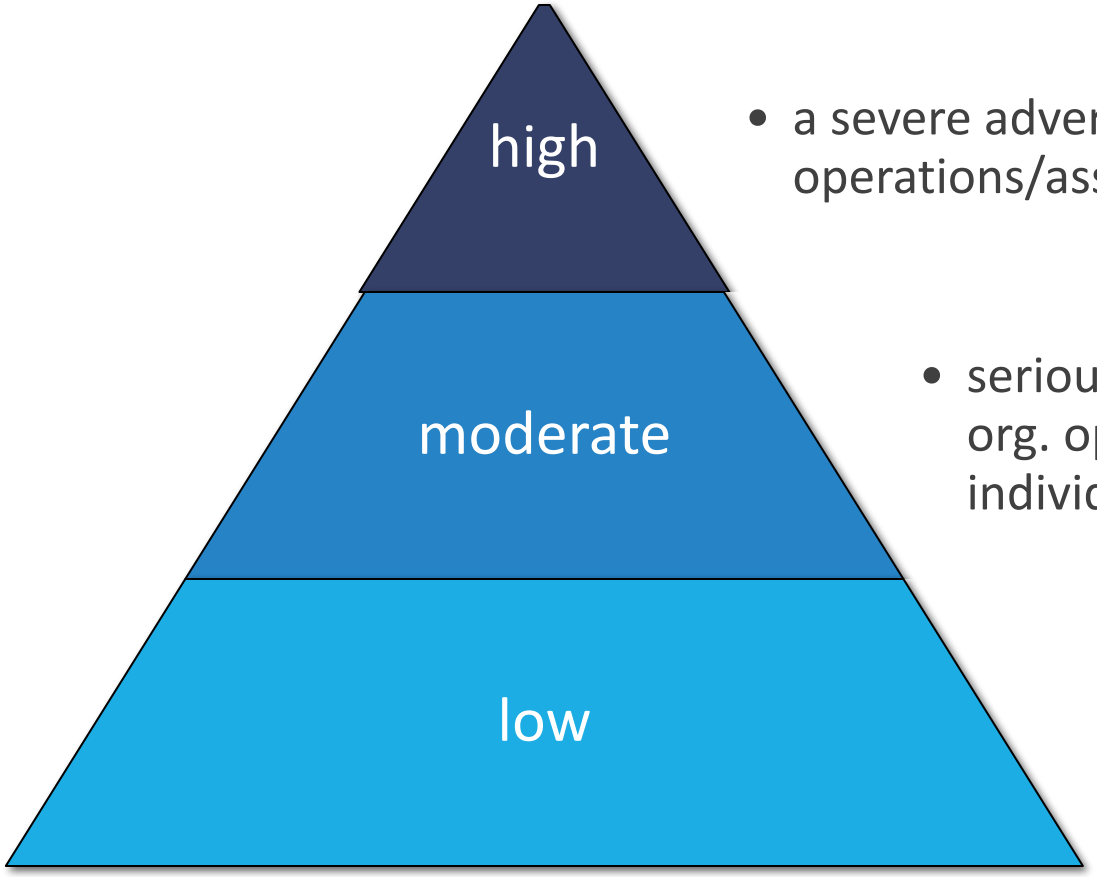


Επιθέσεις: βασικές κατηγορίες

- Ενεργητικές επιθέσεις
  - Αλλοίωση πληροφορίας, μείωση απόδοσης ΠΣ
  - Τρόπος πραγματο-ποίησης εξαρτάται από το δίκτυο
  - Δυσκολότερο να επιτευχθεί / μεγαλύτερες ζημιές



Επιθέσεις: επίπεδα επιπτώσεων



- a severe adverse effect on org. operations/assets or individuals
- serious adverse effect on org. operations/assets or individuals
- limited adverse effect on org. operations/assets or individuals

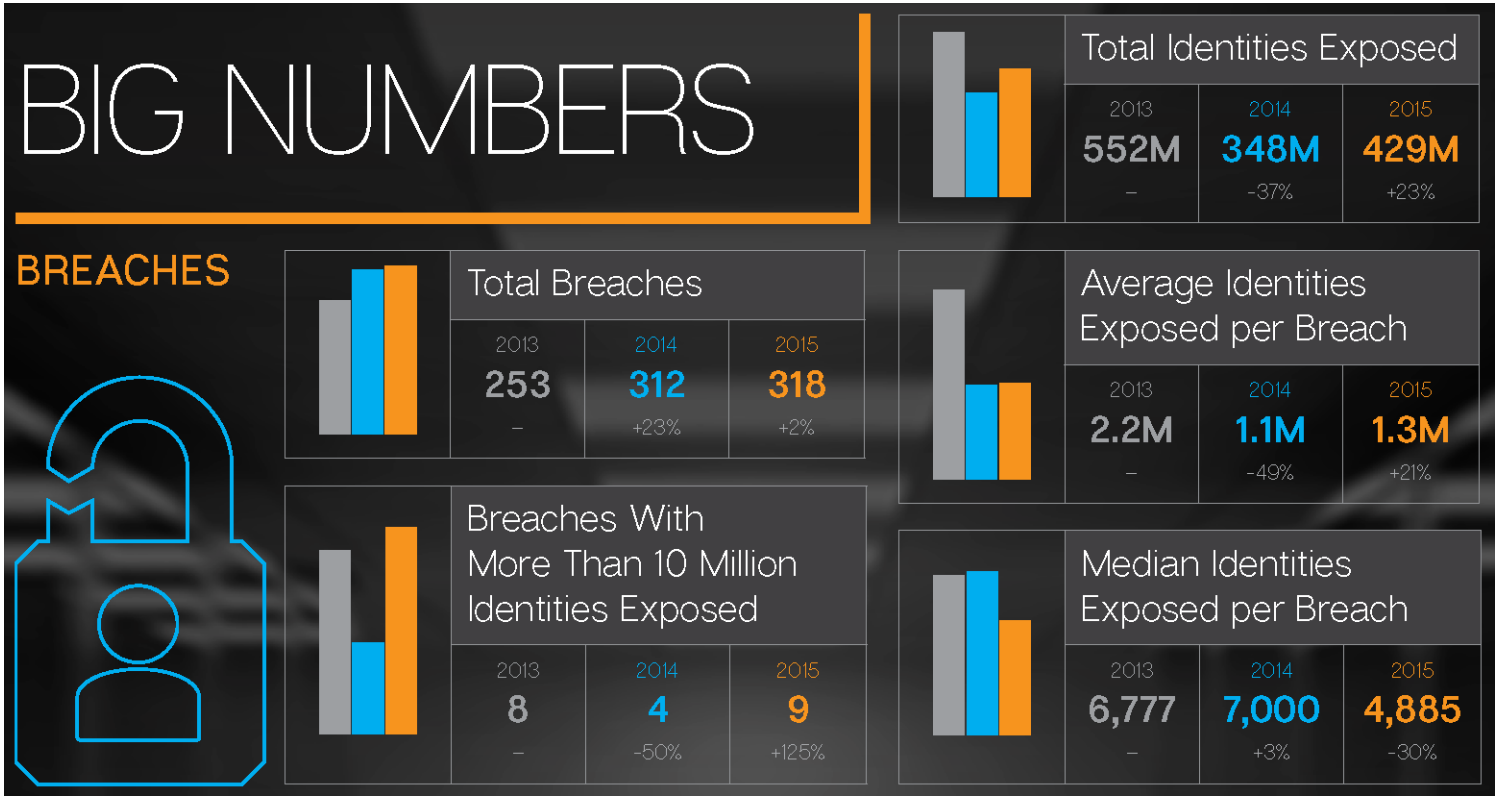
Παραδείγματα απειλών

- Παρακολούθηση επικοινωνιών
  - Αποκάλυψη ευαίσθητων πληροφοριών (κλοπή συνθηματικών)
  - Ανάλυση επικοινωνίας και εξαγωγή στατιστικών συμπερασμάτων
- Αλλοίωση/καταστροφή πληροφοριών
  - Κατά την αποθήκευσή ή μετάδοσή τους
- Μείωση απόδοσης ΠΣ
  - Παρεμπόδιση της επικοινωνίας μεταξύ δύο οντοτήτων
  - Παρεμπόδιση της ομαλής λειτουργίας δικτύου (DoS)

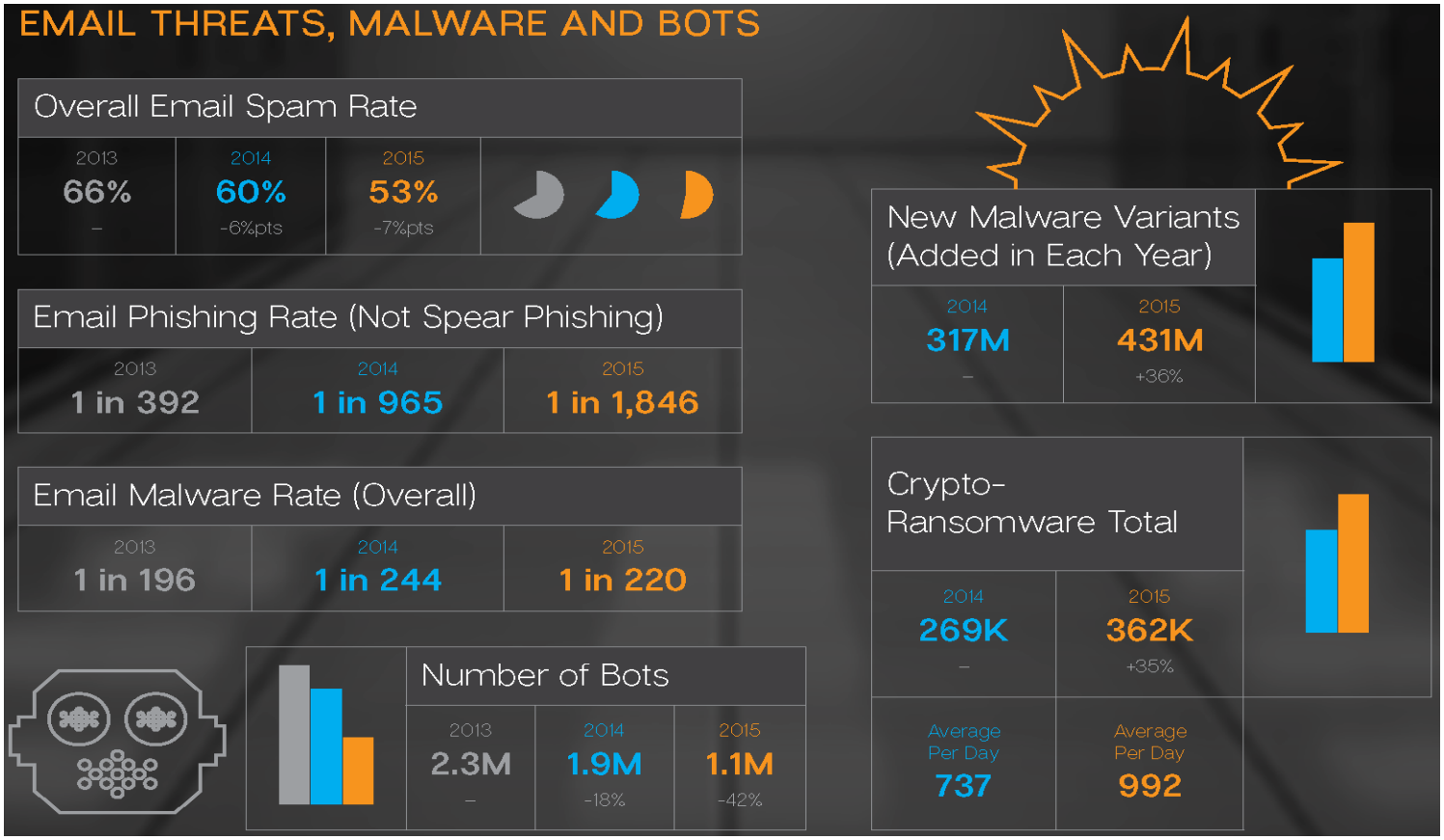
Παραδείγματα απειλών

- Η ετεροπροσωπία (χρήση διαφορετικής ταυτότητας)
  - Διαφορετικό e-mail address, IP address, κ.λπ.
- Επανεκπομπή μηνυμάτων
  - Καταγραφή έγκυρων μηνυμάτων άλλων χρηστών
  - Προσποίηση σε ΠΣ ότι ο εισβολέας είναι εξουσιοδοτημένος χρήστης
- Χρήση κακόβουλου λογισμικού
  - Προϋποθέσεις για επιθέσεις άρνησης υπηρεσίας
  - Προϋποθέσεις για καλυμμένες επιθέσεις

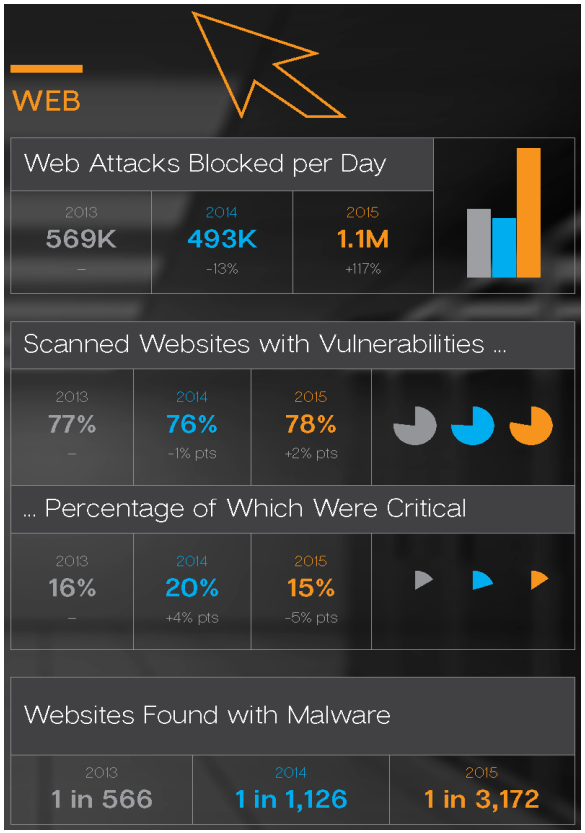
Απειλές: τρέχουσα κατάσταση

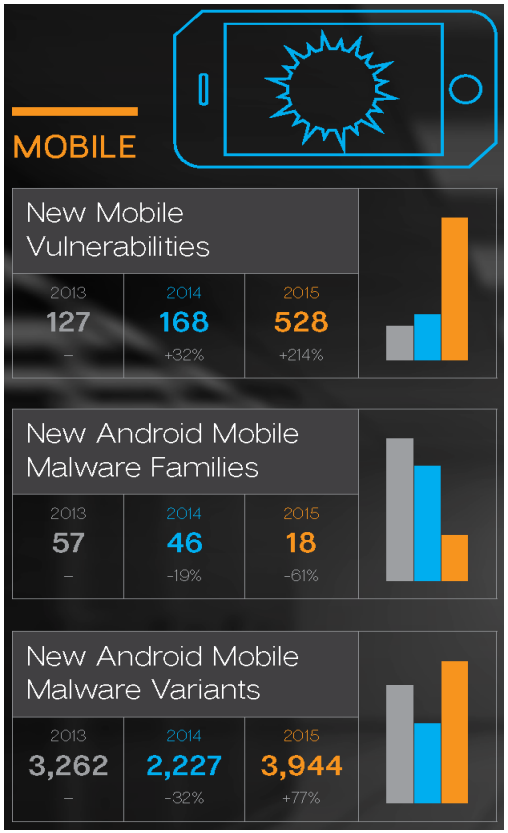


Απειλές: τρέχουσα κατάσταση

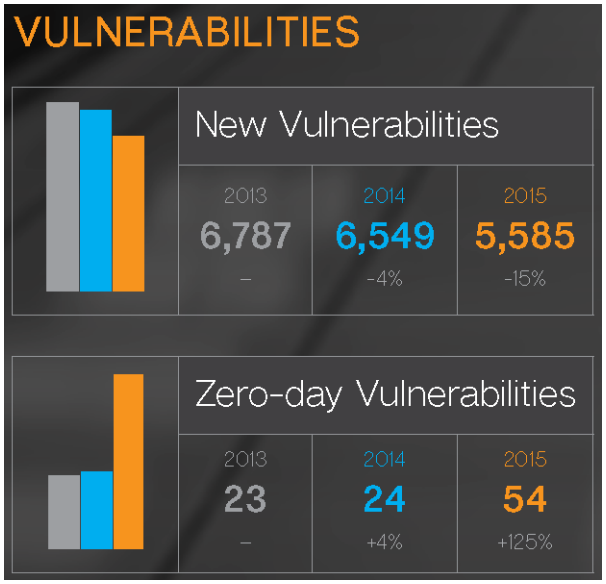


Απειλές: τρέχουσα κατάσταση

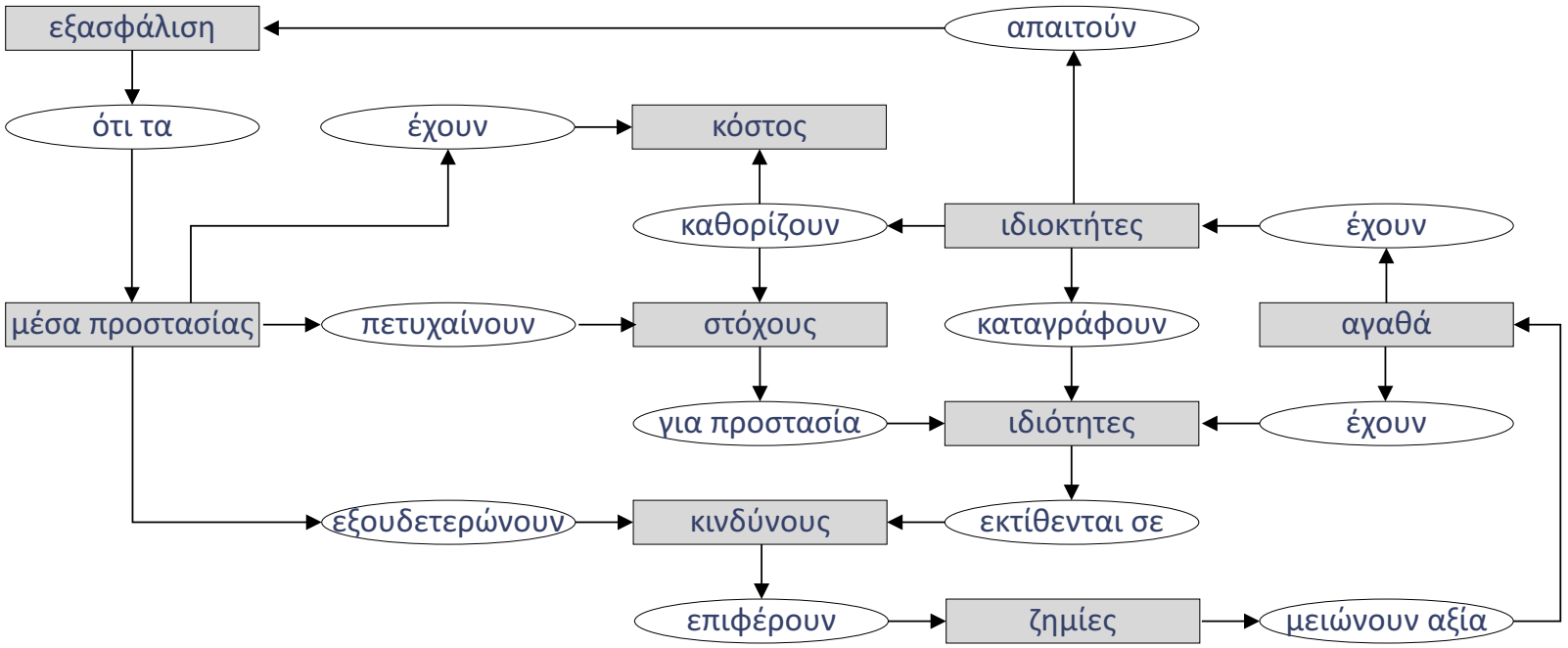




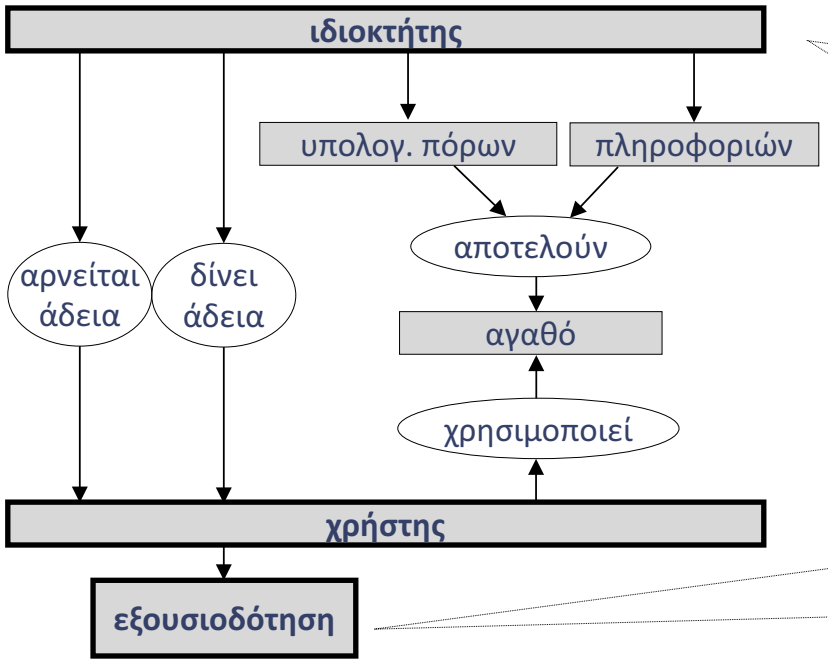
Απειλές: τρέχουσα κατάσταση



Έννοιες ασφάλειας πληροφοριών



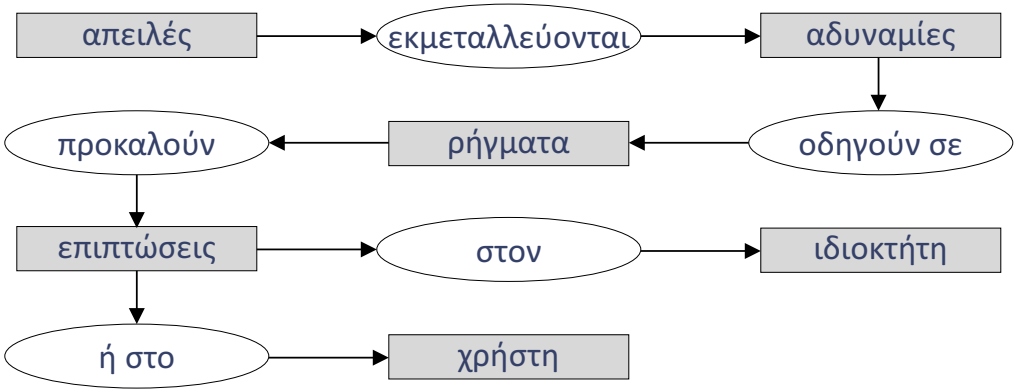
Έννοιες ασφάλειας πληροφοριών



Ιδιοκτήτης είναι η οντότητα που κατέχει ένα Αγαθού και έχει το δικαίωμα να καθορίσει πώς αυτό μπορεί να χρησιμοποιηθεί, να μεταβληθεί, κ.λπ.

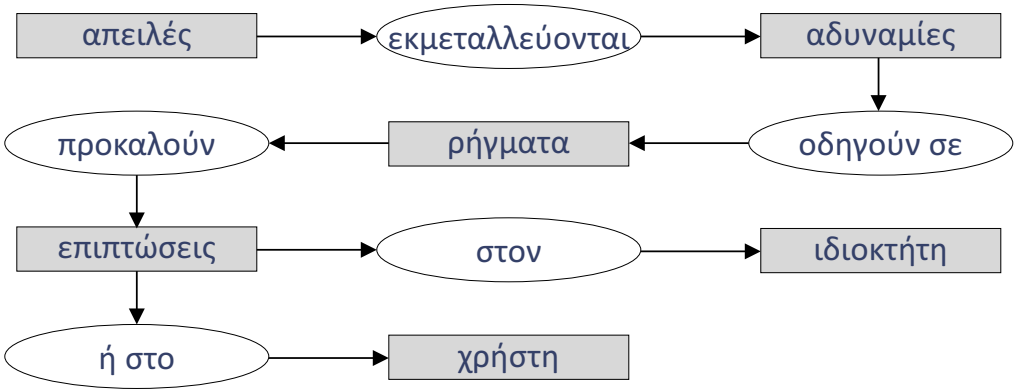
Εξουσιοδότηση είναι μια άδεια που παρέχεται από τον Ιδιοκτήτη για ένα συγκεκριμένο σκοπό

Έννοιες ασφάλειας πληροφοριών



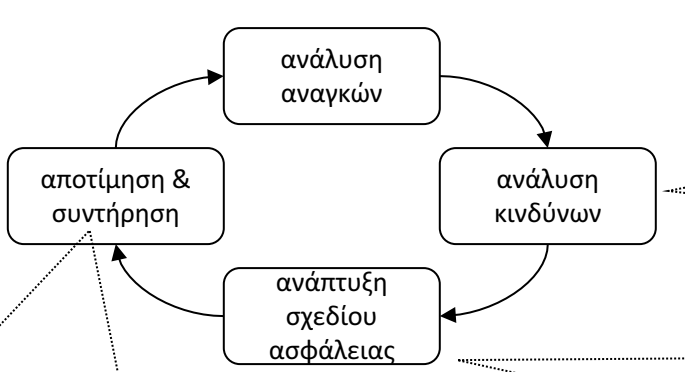
- Τα **Μέτρα Προστασίας** σχεδιάζονται ώστε να εμποδίζουν την εμφάνιση Ρηγμάτων Ασφάλειας ή να μειώνουν τις επιπτώσεις τους
- Κατηγορίες Μέτρων Προστασίας αναλόγως της χρονική στιγμή δράσης τους: Μέτρα πρόληψης, Μέτρα ανίχνευσης, Μέτρα αντίδρασης
- Το σύνολο σχεδίων πραγματοποίησης των Αντικειμενικών Σκοπών ενός ΠΣ ονομάζεται **Στρατηγική**

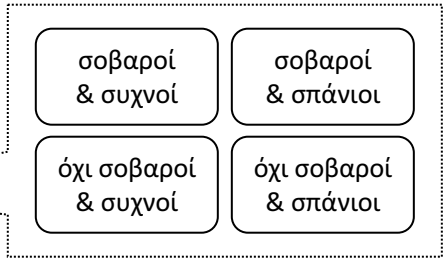
Έννοιες ασφάλειας πληροφοριών

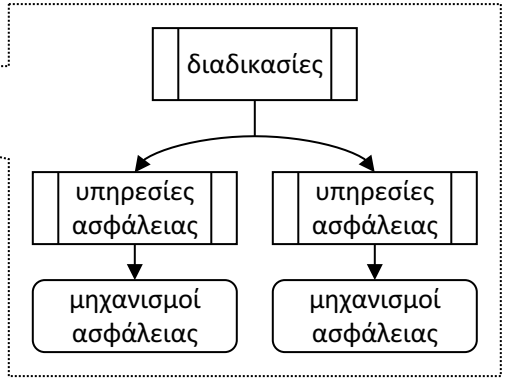


- **Επίπτωση** είναι η απώλεια Αξίας, η αύξηση Κόστους ή άλλη απώλεια, που θα μπορούσε να προκύψει ως συνέπεια ενός Ρήγματος Ασφάλειας
- **Επισφάλεια** είναι η πιθανότητα να συμβεί ένα Ρήγμα Ασφάλειας
- **Επικινδυνότητα** είναι το γινόμενο της Επίπτωσης και της Επισφάλειας

Κύκλος ζωής σχεδίων ασφάλειας

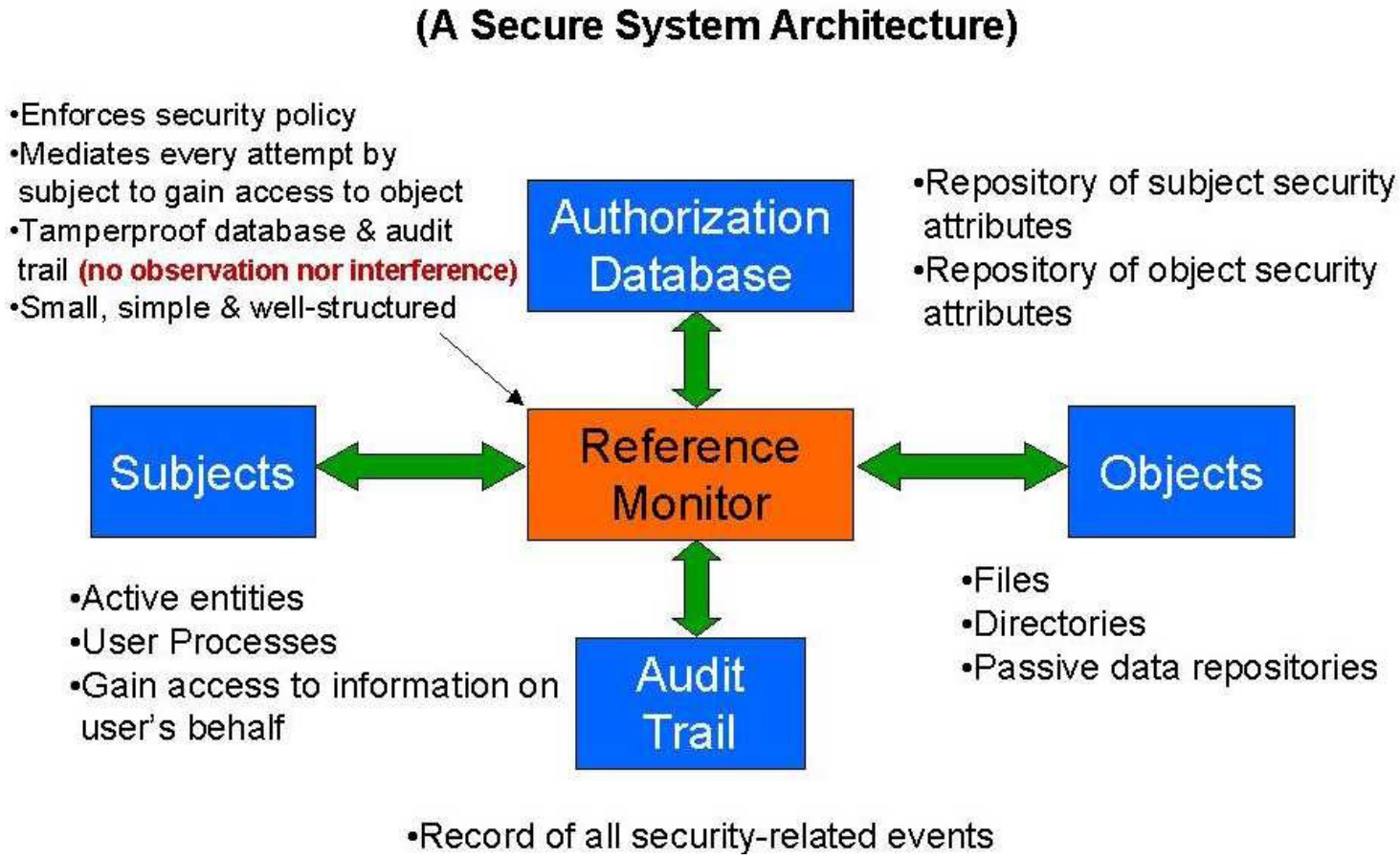




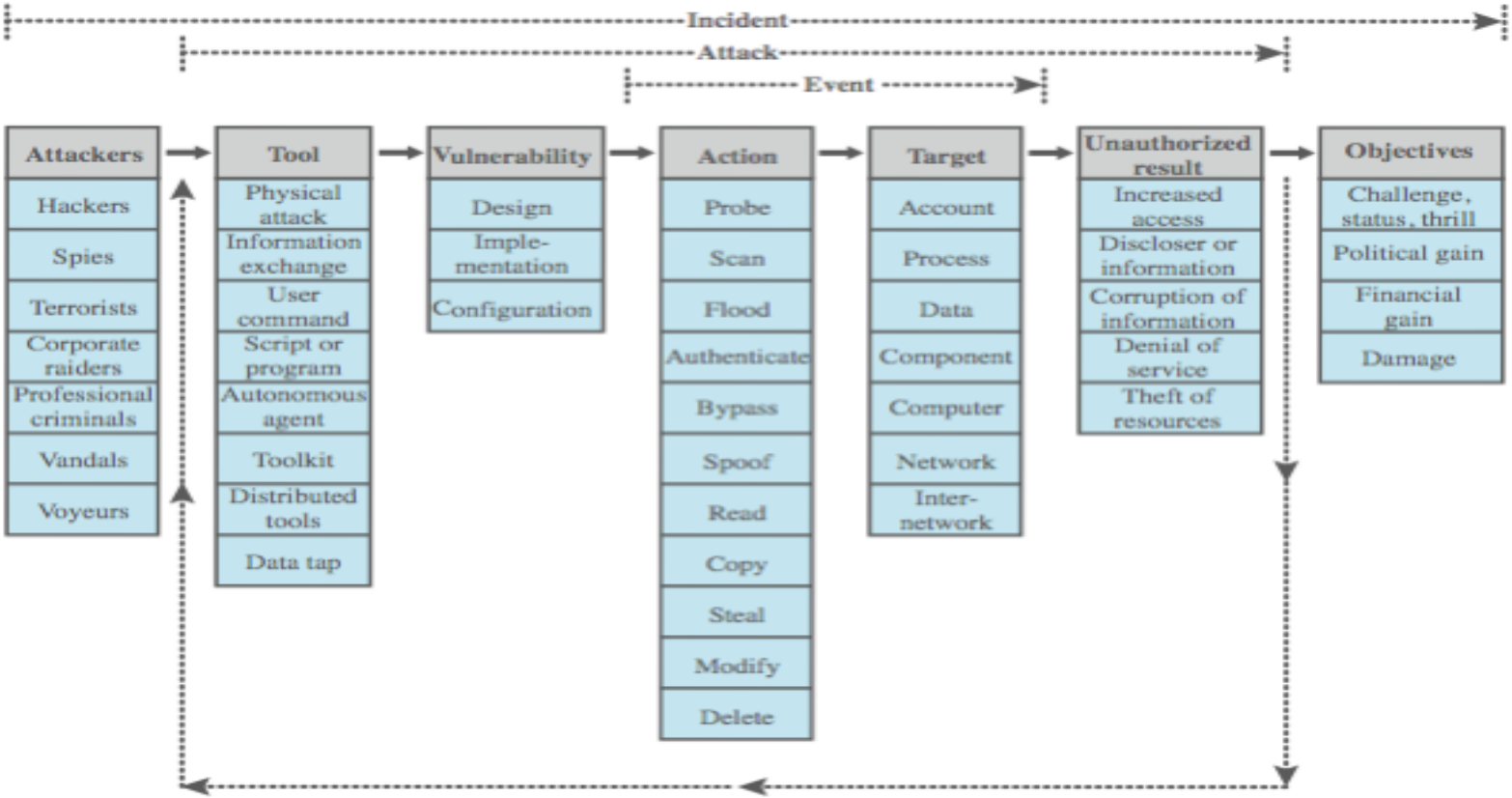


- πρότυπες μεθοδολογίες αποτίμησης πλαισίου ασφάλειας (NIST)
- έρευνα αδυναμιών τεχνικών ασφάλειας και αλγορίθμων κρυπτογραφίας
- ανάλυση συμπεριφοράς συστήματος σε τεχνητές επιθέσεις (αρχεία καταγραφής)

Πλαίσιο αναφοράς



Security Taxonomy



Μέτρα Ασφάλειας ΠΣ

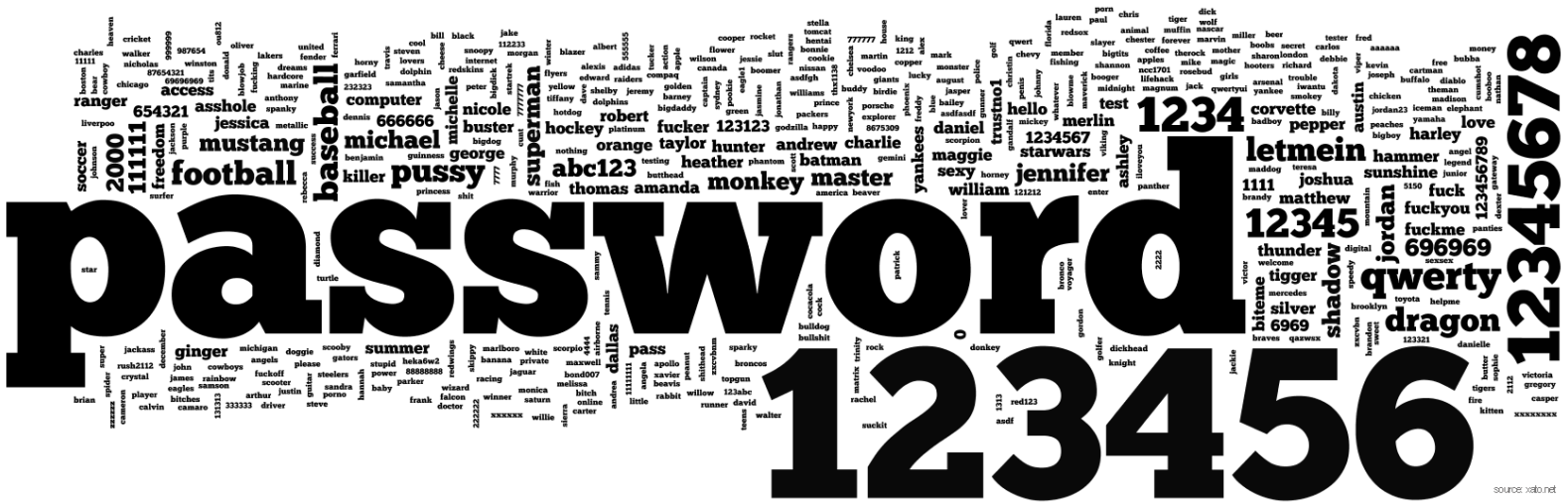
Type		Mechanism
hardware		♦ smart cards and other tamper-proof devices ♦ cryptographic (e.g. SSL) accelerators ♦ screening routers/firewalls and biometric devices
software	operating system level	♦ password authentication, expiration, and filtering ♦ kerberos-based distributed authentication ♦ access control lists and security identifiers
	database management system level	♦ password standards enforcement ♦ break-in detection and evasion ♦ centralized security administration ♦ comprehensive report generation
	application level	♦ anti-virus software, firewalls, and backup utilities ♦ maintenance of audit-logs and audit-log analysers

Συχνά λάθη: κοινοί κωδικοί

- Συχνότητες PINs
- http://mashable.com/2012/09/24/pin-number-top-20

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%

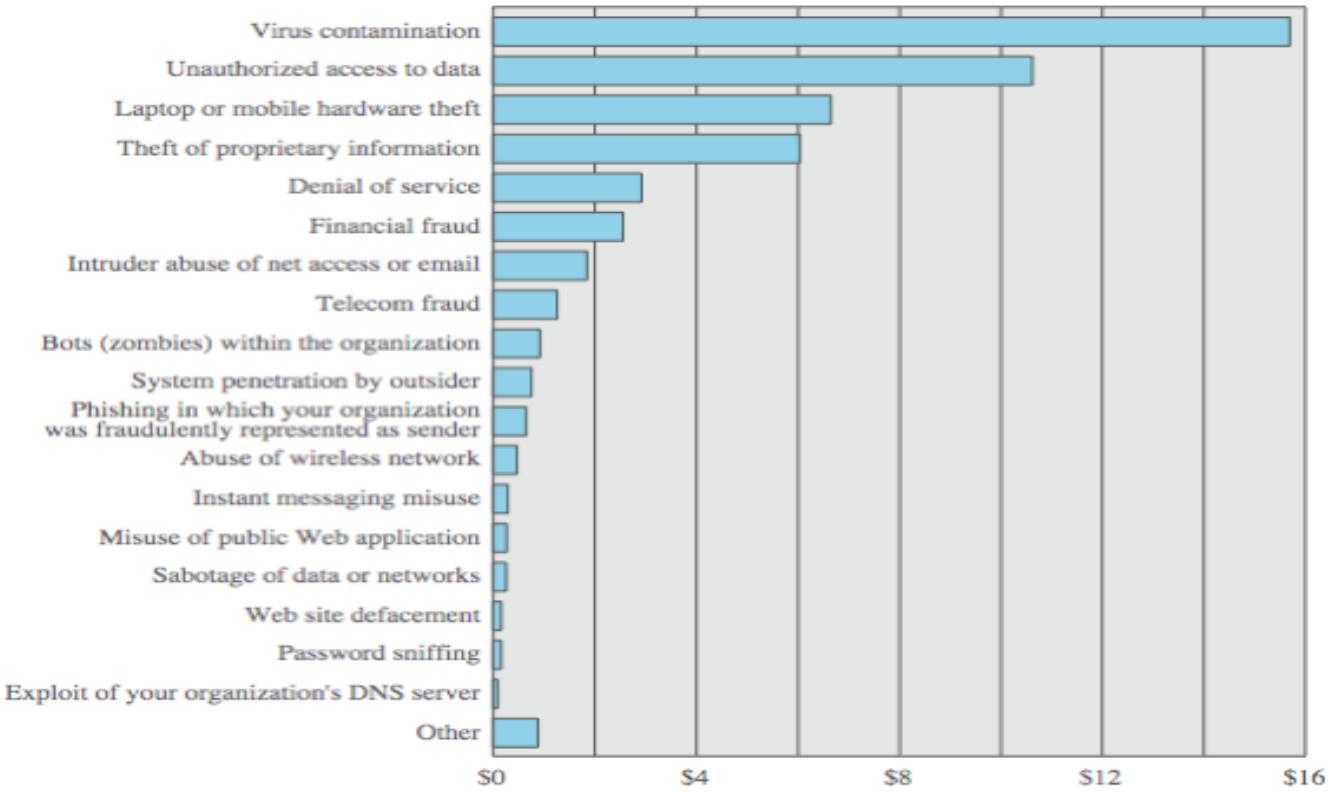
Συχνά λάθη: κοινοί κωδικοί



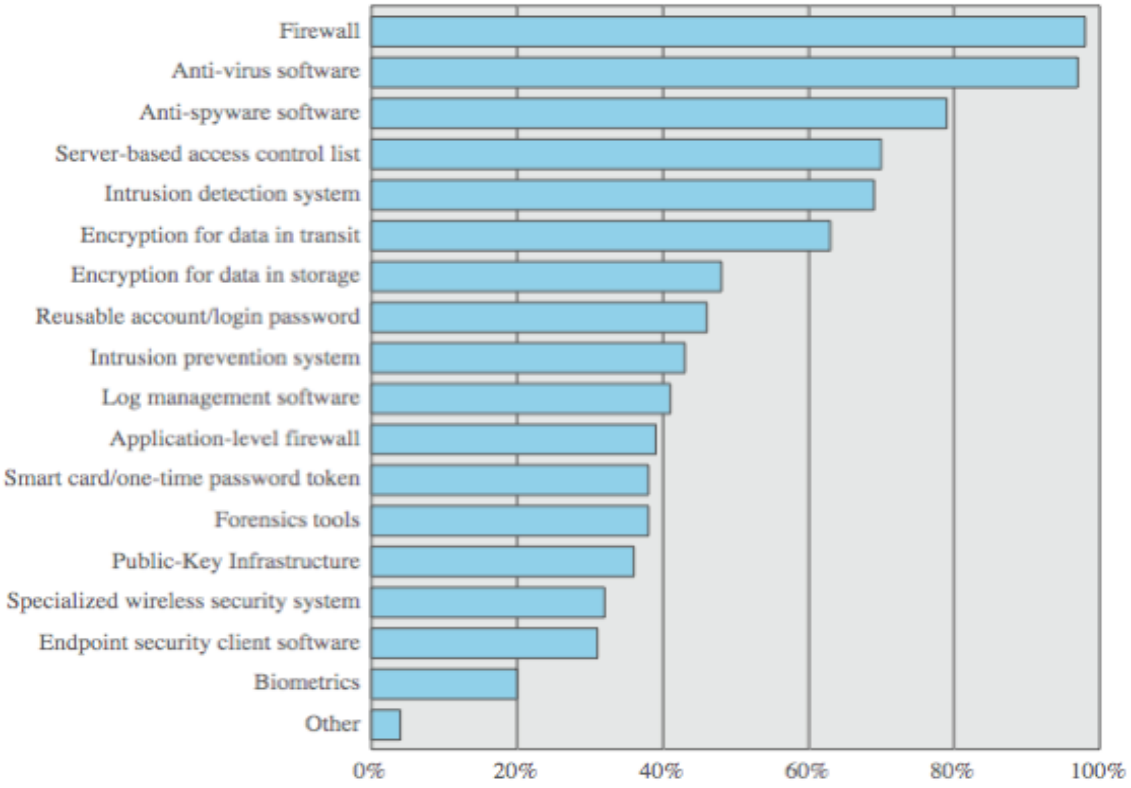
Συχνά λάθη: κοινοί κωδικοί

- Περίπτωση του LinkedIn
- 6.46 εκ. κλεμμένοι κωδικοί
- http://mashable.com/2012/06/08/linkedin-stolen-passwords-list

Computer security losses (m$)



Security technologies use (%orgs)

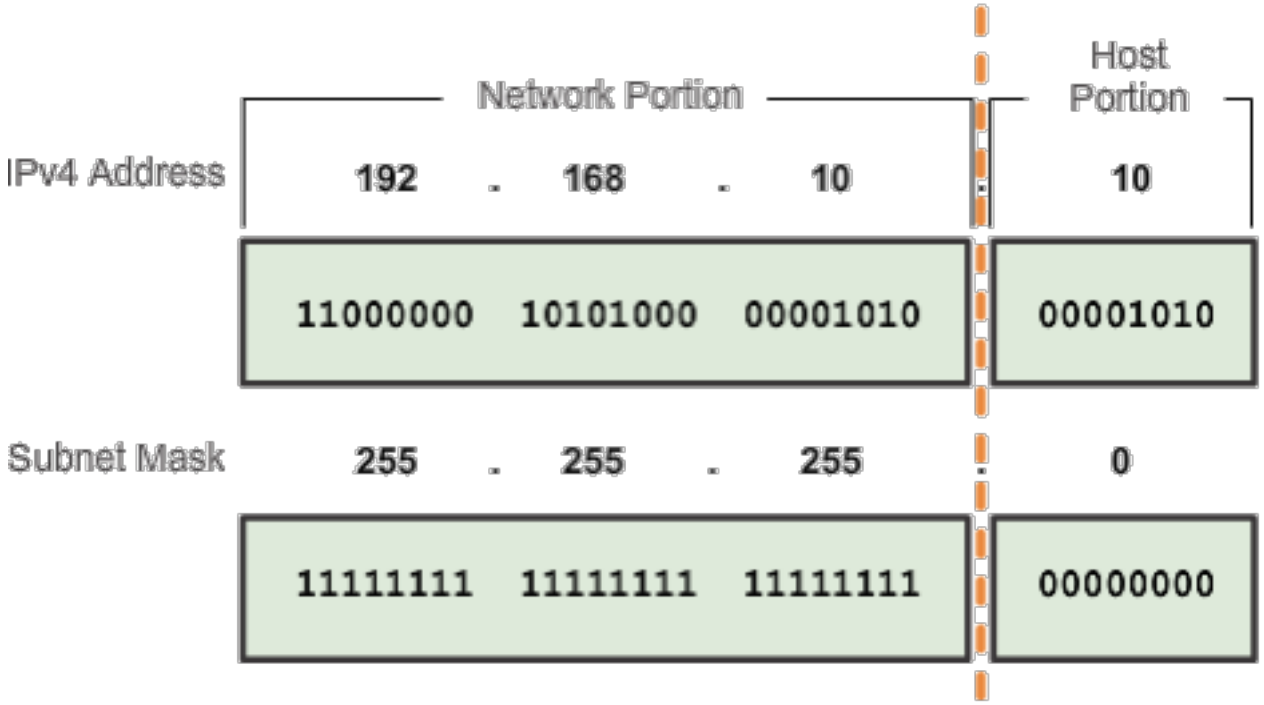


Μέτρα ασφάλειας δικτύων

OSI Layer	Protection	Protocol
data link	host-to-host	♦ point-to-point tunnelling protocol (PPTP) ♦ serial line Internet protocol (SLIP)
transport/ network	process-to-process	♦ secure sockets layer (SSL) ♦ transport layer security (TLS) ♦ secure shell (SSH) ♦ Internet protocol security (IPSEC) ♦ network layer security protocol (NLSP)
application	data specific	♦ secure hypertext transfer protocol (S-HTTP) ♦ secure file transfer protocol (S-FTP) ♦ pretty good privacy (PGP) ♦ privacy enhanced mail (PEM) ♦ secure multipurpose Internet mail extensions (S/MIME) ♦ secure electronic transactions (SET)

Περί δικτύων: διευθύνσεις

- Το τμήμα της διεύθυνσης που αφορά το δίκτυο είναι ίδιο για όλες τις συσκευές που βρίσκονται στο ίδιο δίκτυο



Περί δικτύων: διευθύνσεις

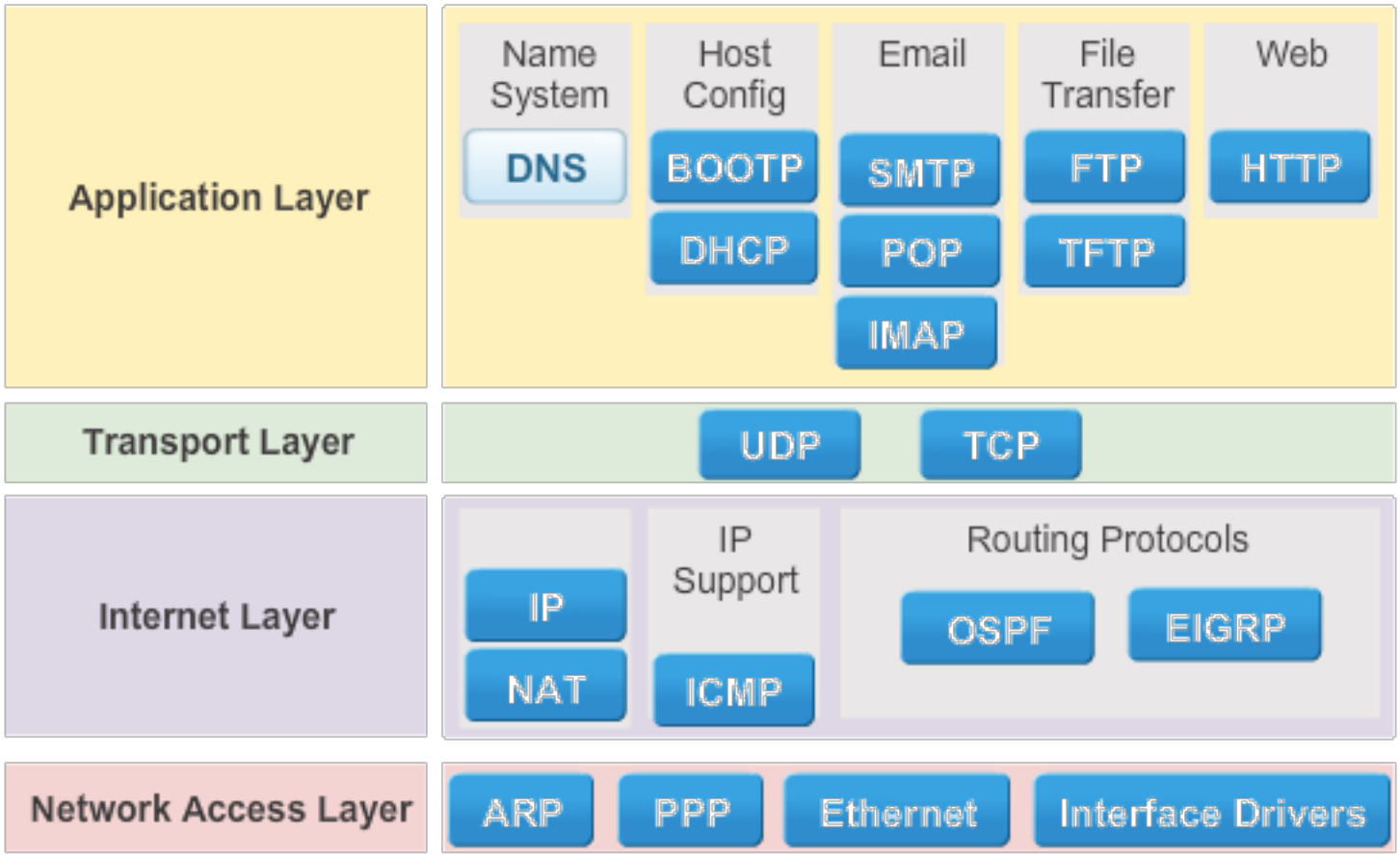
	Dotted Decimal	Significant bits shown in binary
Network Address	10.1.1.0/24	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: 2^8 – 2 = 254 hosts		

Network Address	10.1.1.0/25	10.1.1.00000000
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: 2^7 – 2 = 126 hosts		

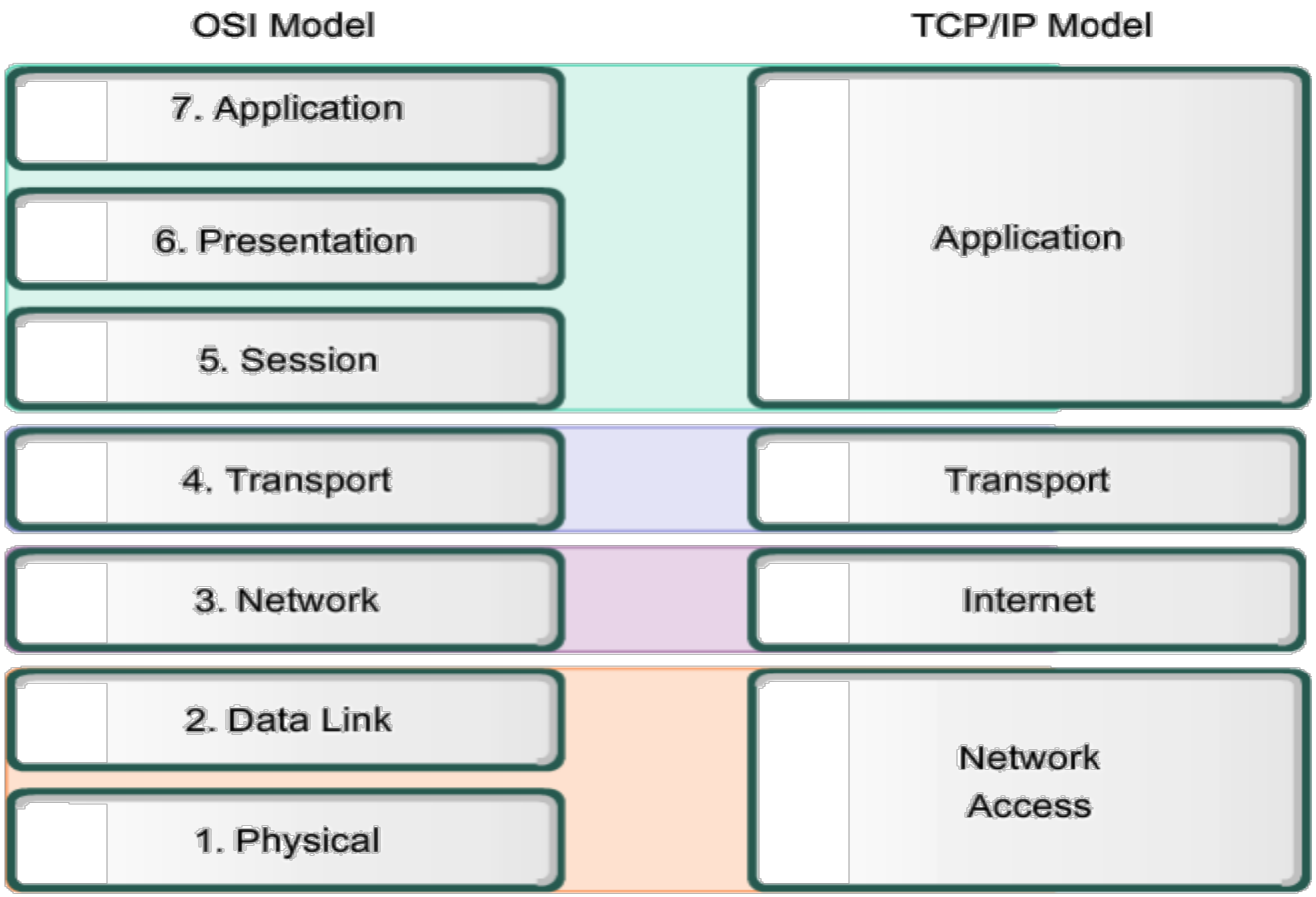
Περί δικτύων: κλάσεις

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)

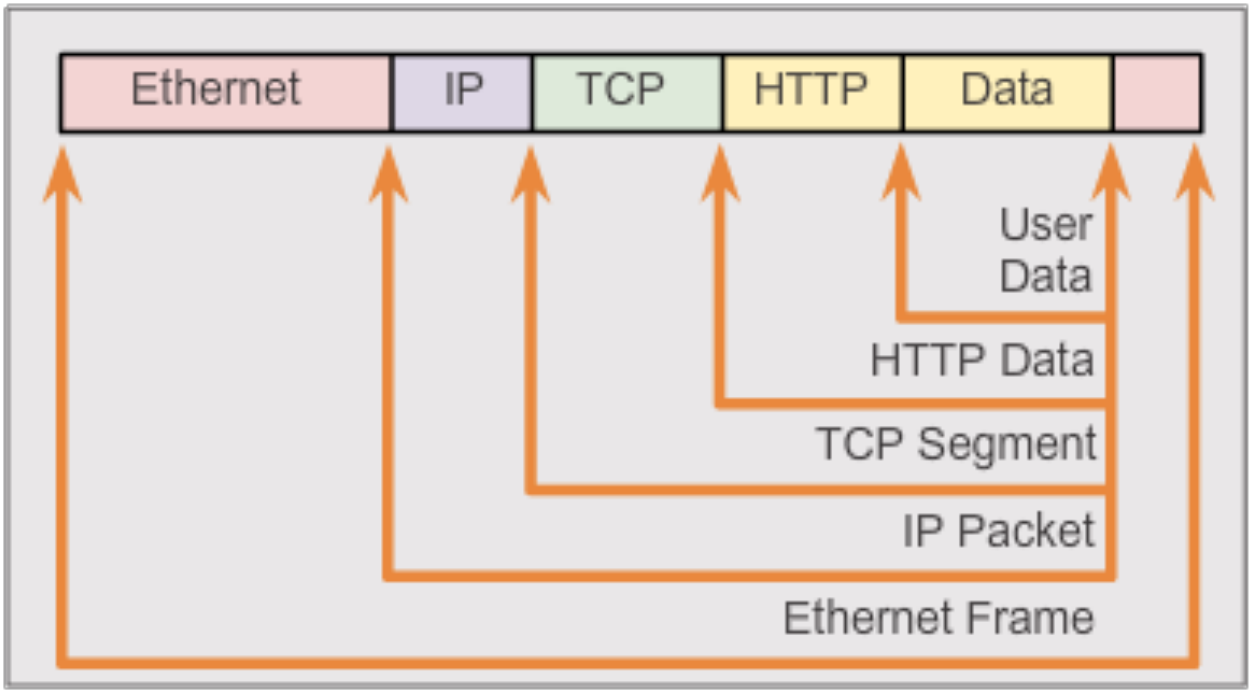
Περί δικτύων: σουίτα TCP/IP



Περί δικτύων: μοντέλα

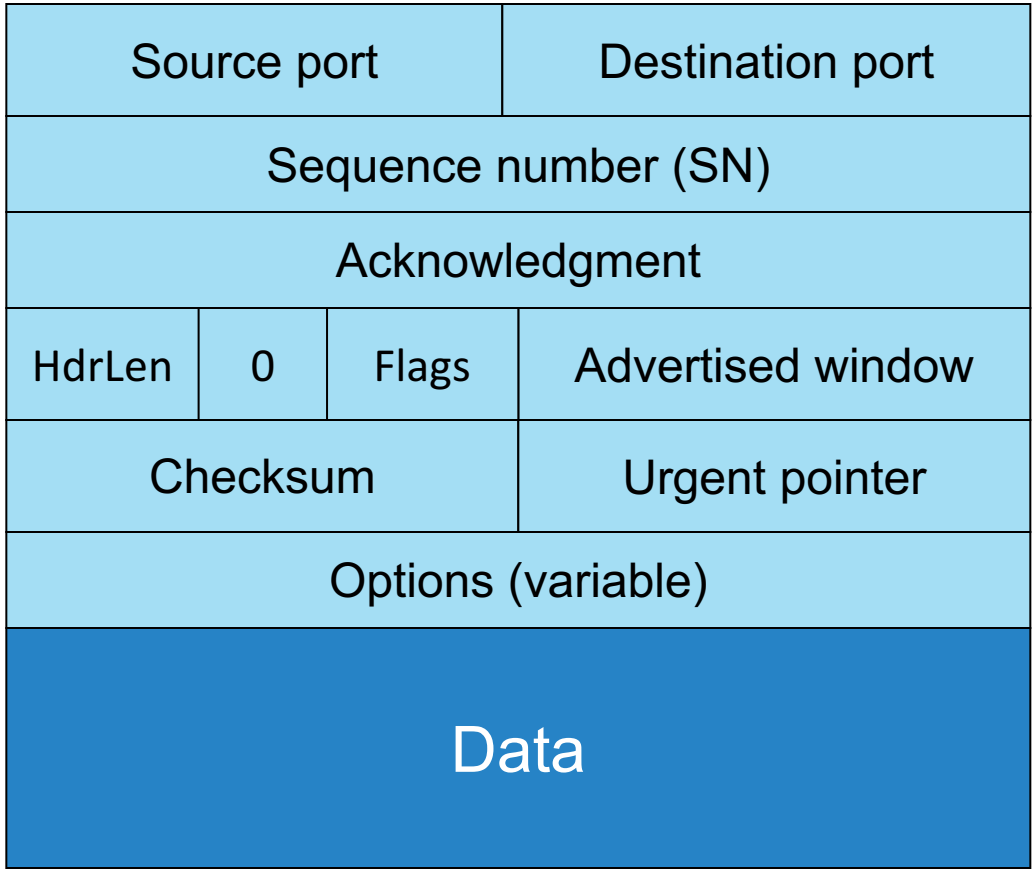


Περί δικτύων: ενθυλάκωση



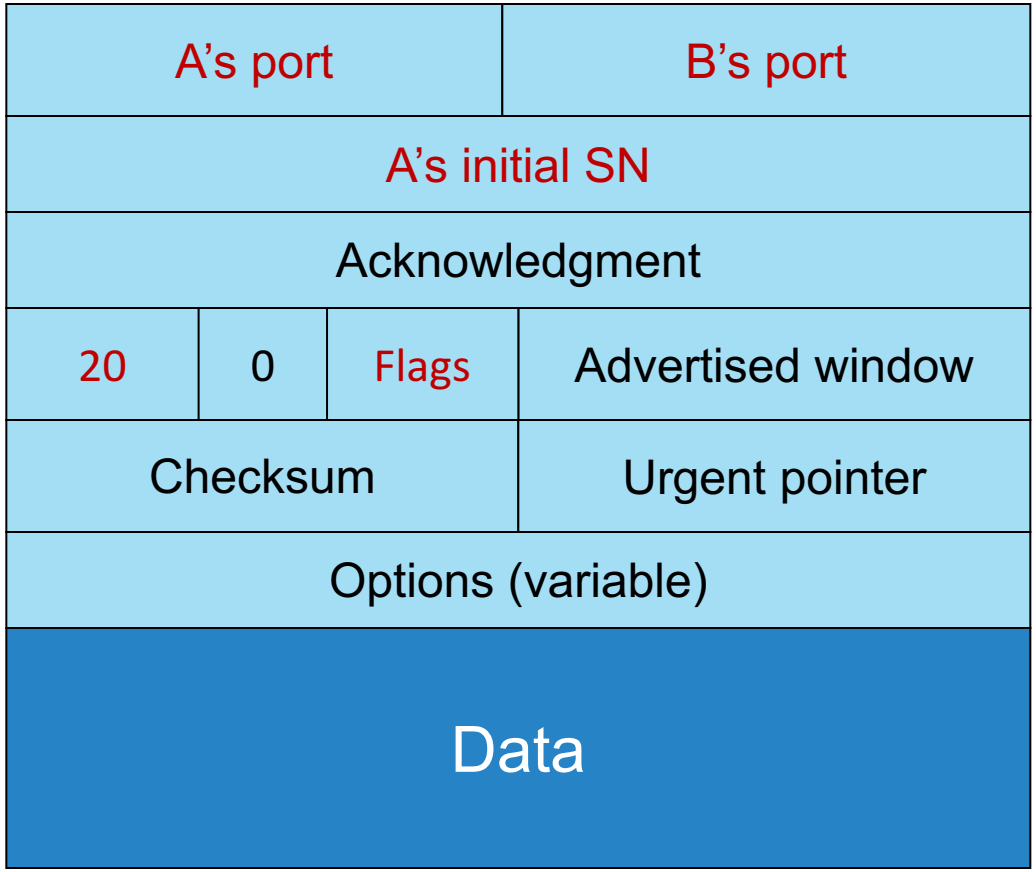
Περί δικτύων: TCP επικεφαλίδα

- TCP Flags
  - SYN
  - FIN
  - RST
  - PSH
  - URG
  - ACK



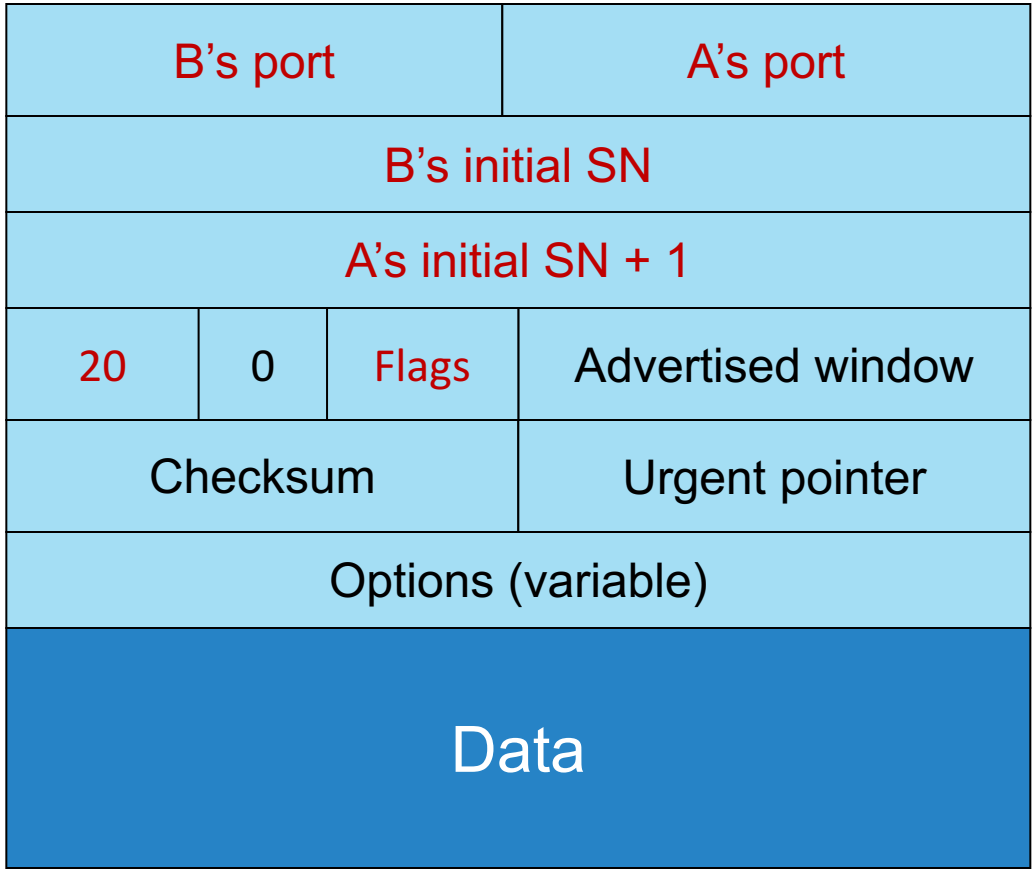
Περί δικτύων: TCP χειραψία

- TCP Flags
  - SYN
  - FIN
  - RST
  - PSH
  - URG
  - ACK
- Βήμα 1: A → B
  - Ο Α ενημερώνει τον Β ότι θέλει να δημιουργήσει μια νέα σύνδεση



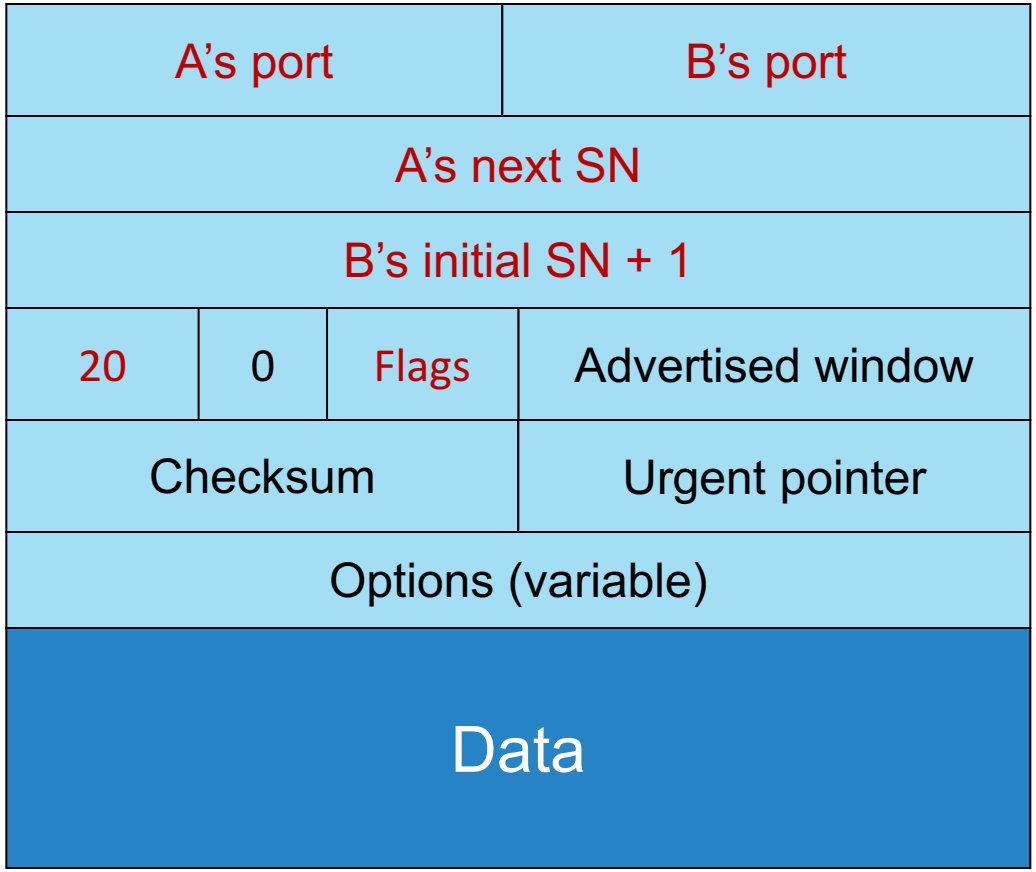
Περί δικτύων: TCP χειραψία

- TCP Flags
  - SYN
  - FIN
  - RST
  - PSH
  - URG
  - ACK
- Βήμα 1: A ← B
  - Ο Β ενημερώνει τον Α ότι δέχεται και περιμένει το τελικό πακέτο



Περί δικτύων: TCP χειραψία

- TCP Flags
  - SYN
  - FIN
  - RST
  - PSH
  - URG
  - ACK
- Βήμα 1: A → B
  - Ο Α ενημερώνει τον Β ότι μπορεί πλέον να στείλει δεδομένα



OSI security architecture

- ITU-T X.800 Security Architecture for OSI
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Υπηρεσίες ασφάλειας

- **RFC 2929 defines it as:** a processing or communication service provided by a system to give a specific kind of protection to system resources
- **X.800 defines it as:** a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
  - X.800 defines it in 5 major categories

Υπηρεσίες ασφάλειας (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access control** - prevention of the unauthorized use of a resource
- **Data confidentiality** –protection of data from unauthorized disclosure
- **Data integrity** - assurance that data received is as sent by an authorized entity
- **Non-repudiation** - protection against denial by one of the parties in a communication

Υπηρεσίες ασφάλειας (X.800)

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

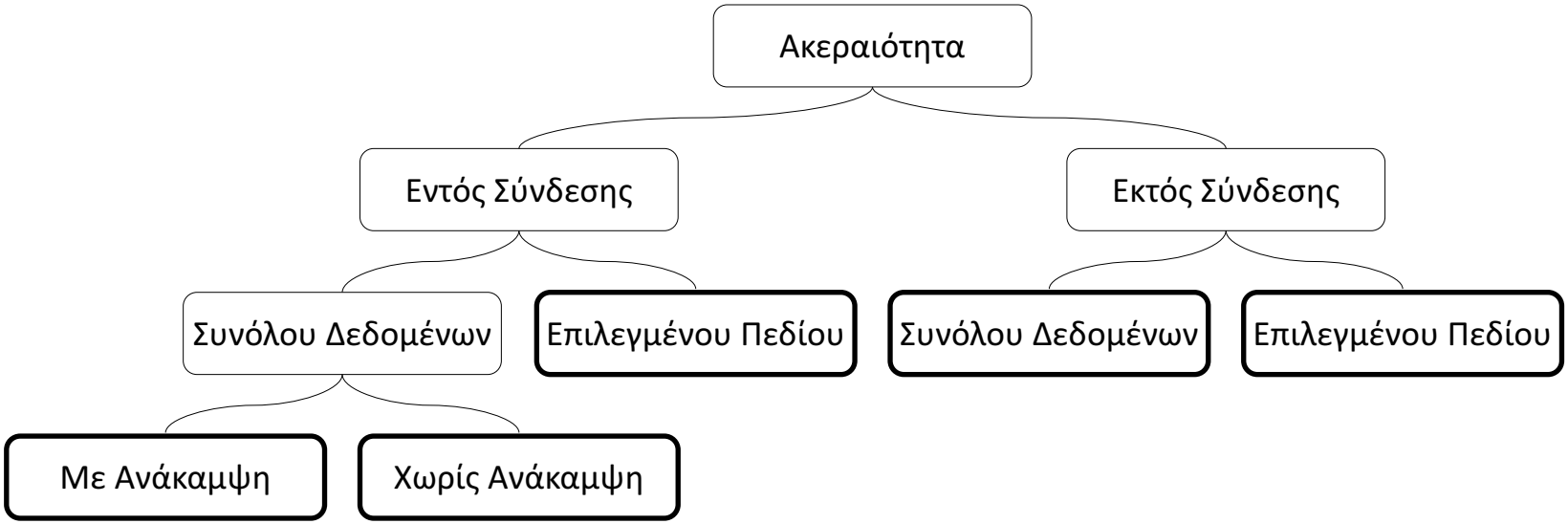
Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Υπηρεσίες: κλάσεις

- Οι υπηρεσίες αυτές κατηγοριοποιούνται στις εξής:
  - Υπηρεσίες προστασίας ακεραιότητας
  - Υπηρεσίες προστασίας εμπιστευτικότητας
  - Υπηρεσίες αυθεντικοποίησης
  - Υπηρεσίες ελέγχου πρόσβασης
  - Υπηρεσίες υποστήριξης μη αμφισβήτησης

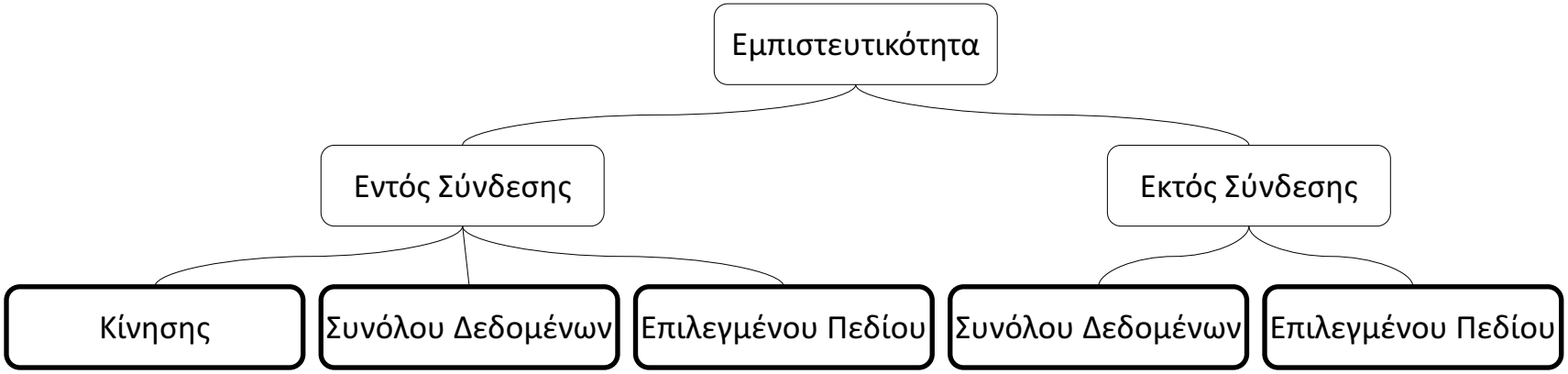
Υπηρεσίες: ακεραιότητα



- Ακεραιότητα δεδομένων μιας μονάδας και ανάκαμψη σύνδεσης
- Ανίχνευση αλλοίωσης δεδομένων
- Ακεραιότητα ενός ΕΠ των δεδομένων

- Ακεραιότητα μιας μόνο μονάδας δεδομένων
- Ακεραιότητα ενός ΕΠ μιας μόνο μονάδας δεδομένων

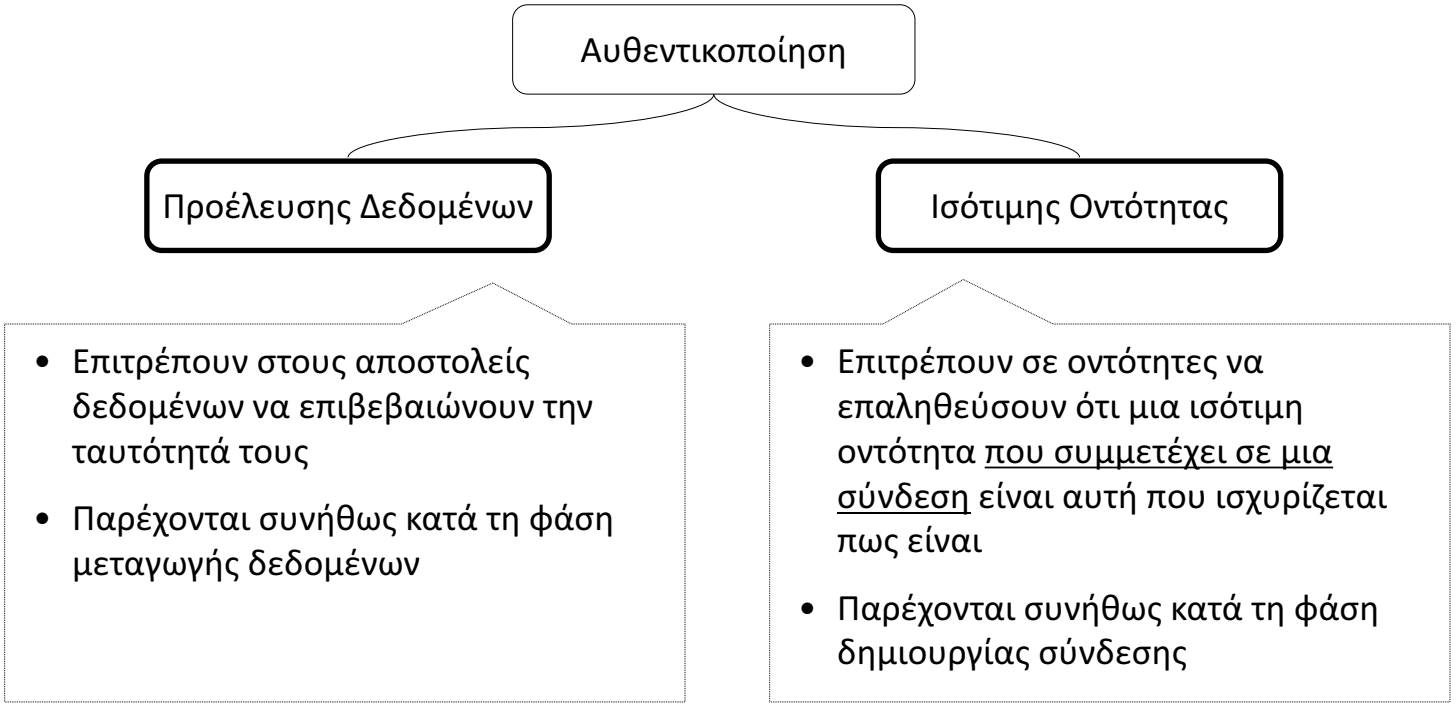
Υπηρεσίες: εμπιστευτικότητα



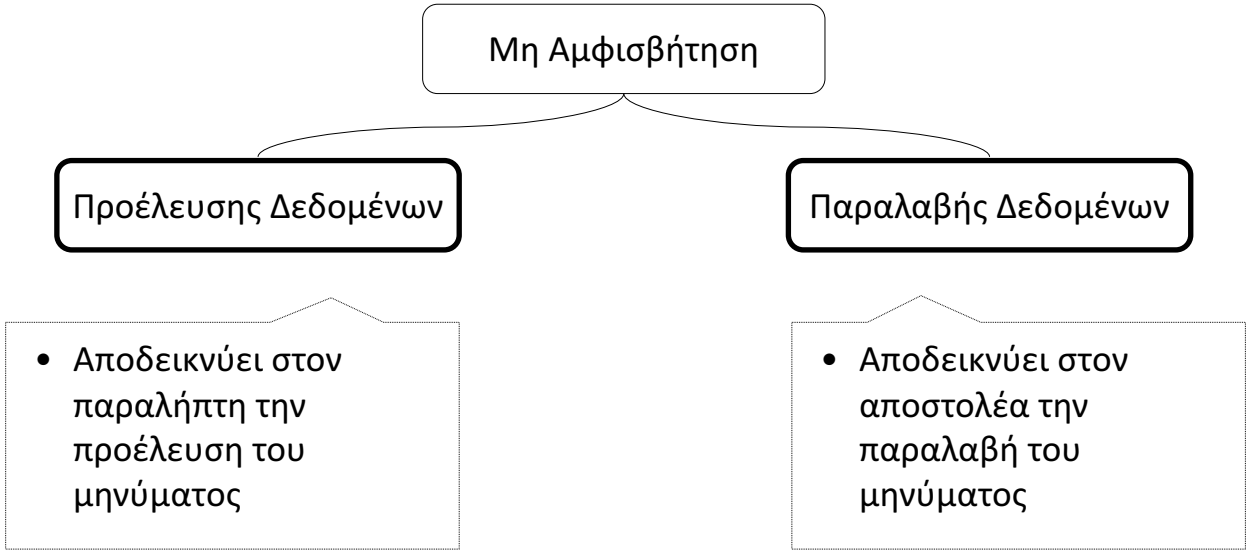
- Εμπιστευτικότητα δεδομένων μιας μονάδας και ανάκαμψη σύνδεσης
- Ανίχνευση αποκάλυψης δεδομένων
- Εμπιστευτικότητα ενός ΕΠ των δεδομένων

- Εμπιστευτικότητα μιας μόνο μονάδας δεδομένων
- Εμπιστευτικότητα ενός ΕΠ μιας μόνο μονάδας δεδομένων

Υπηρεσίες: αυθεντικοποίηση



Υπηρεσίες: μη αμφισβήτηση



Μηχανισμοί ασφάλειας (X.800)

- specific security mechanisms:
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Μηχανισμοί ασφάλειας (X.800)

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

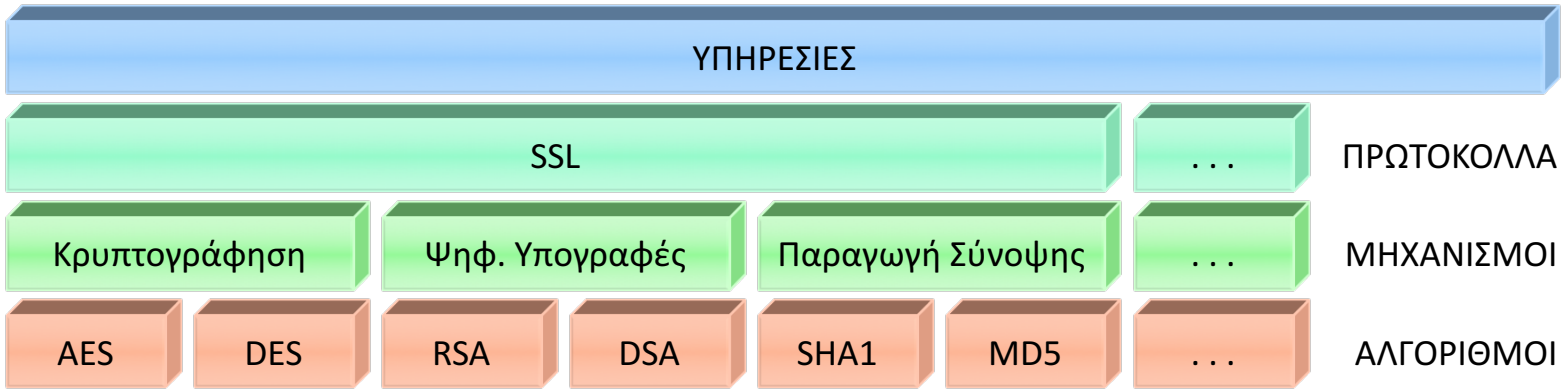
Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

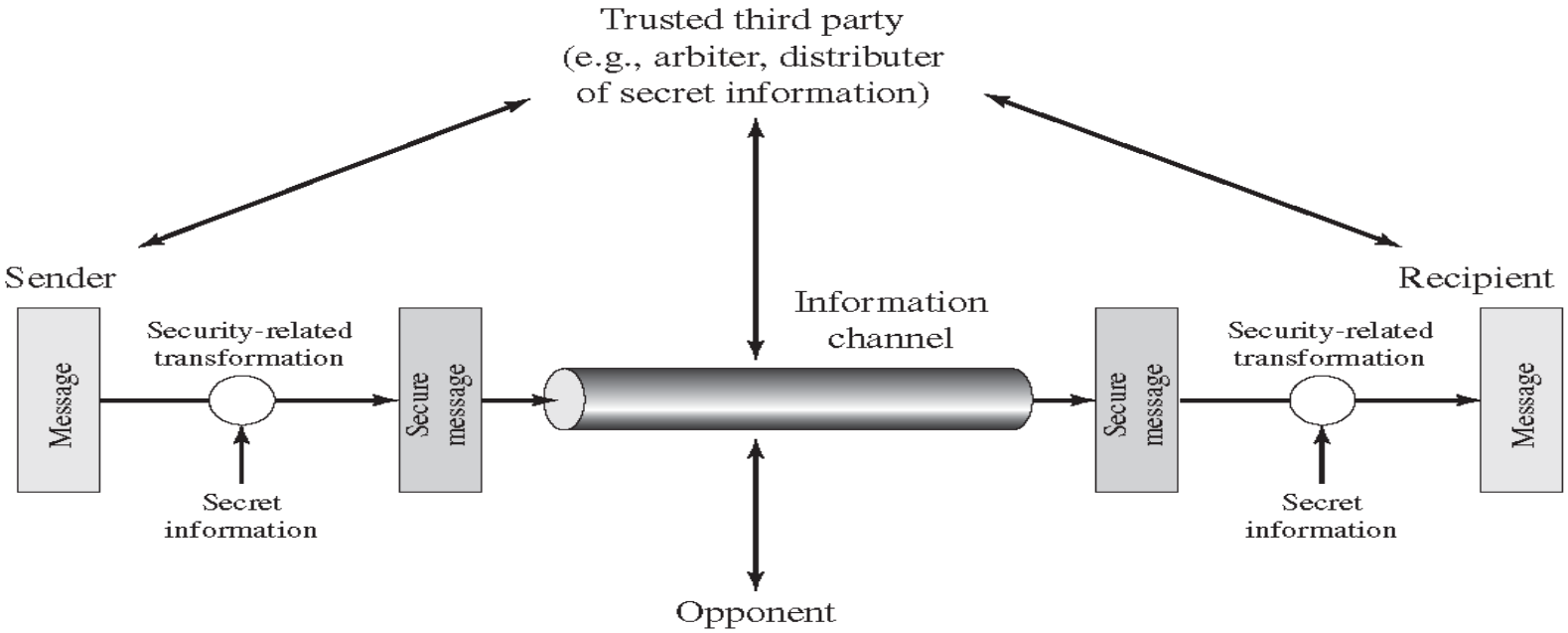
Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Υπηρεσίες και μηχανισμοί



- Οι υπηρεσίες ασφάλειας διασφαλίζουν την προστασία ΠΣ
- Ιεραρχία εννοιών:
  - Τα πρωτόκολλα ασφάλειας βασίζονται σε μηχανισμούς
  - Οι μηχανισμοί υλοποιούνται με χρήση των αλγορίθμων

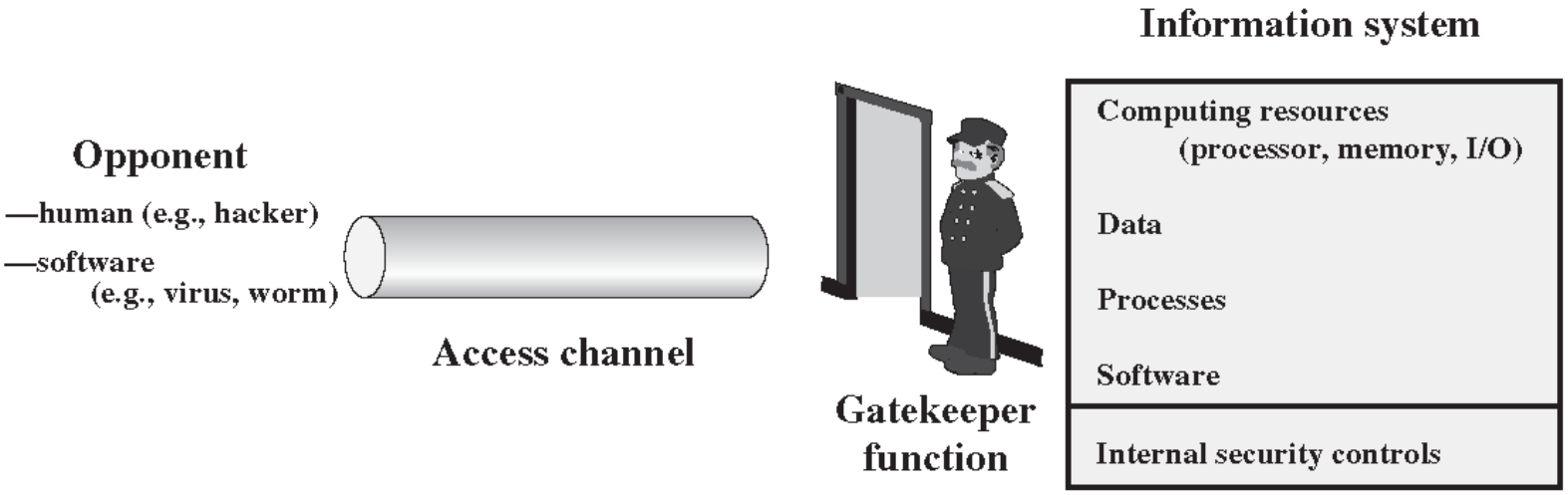
Network security model



Network security model

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Network access security model



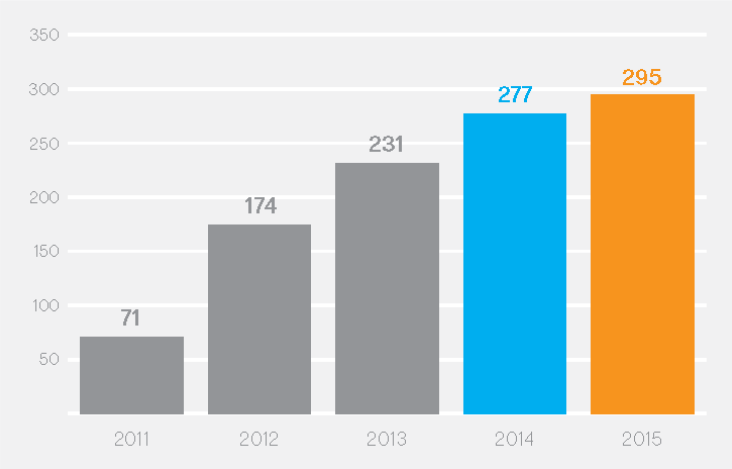
Network access security model

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

Στατιστικά ασφάλειας

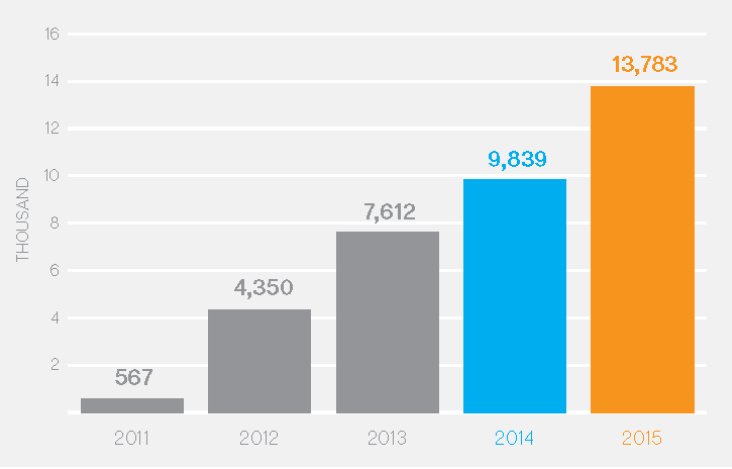
Cumulative Android Mobile Malware Families

- *The number of Android malware families added in 2015 grew by 6 percent, compared with the 20 percent growth in 2014.*



Cumulative Android Mobile Malware Variants

- *The volume of Android variants increased by 40 percent in 2015, compared with 29 percent growth in the previous year.*



Στατιστικά ασφάλειας

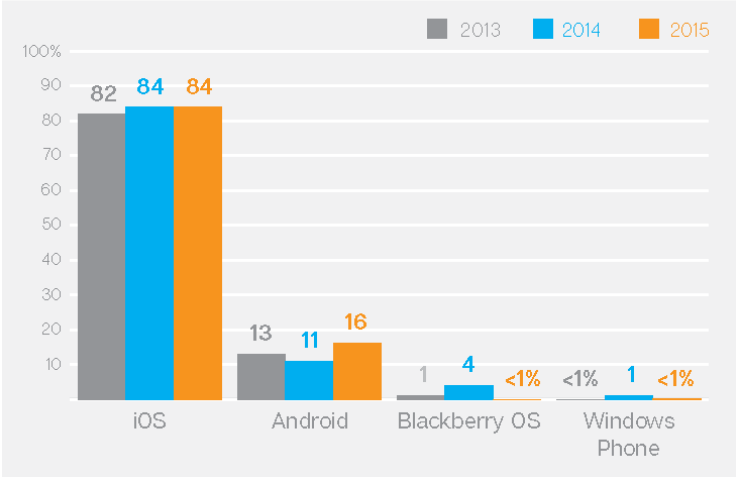
Top Ten Android Malware

- *Thirty-seven percent of Android malware blocked by Symantec in 2015 related to variants of Android.Lotoor, which is generic detection for hacking tools that can exploit vulnerabilities in Android in order to gain root privilege access on compromised Android devices.*

Rank	Malware	Percentage
1	Android.Lotoor	36.8%
2	Android.RevMob	10.0%
3	Android.Malapp	6.1%
4	Android.Fakebank.B	5.4%
5	Android.Generisk	5.2%
6	Android.AdMob	3.3%
7	Android.Iconosis	3.1%
8	Android.Opfake	2.7%
9	Android.Premiumtext	2.0%
10	Android.Basebridge	1.7%

Mobile Vulnerabilities by Operating System

- *Vulnerabilities on the iOS platform have accounted for the greatest number of mobile vulnerabilities in recent years, with research often fueled by the interest to jail-break devices or gain unauthorized access to install malware.*



Στατιστικά ασφάλειας

Scanned Websites with Vulnerabilities

- *A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.*

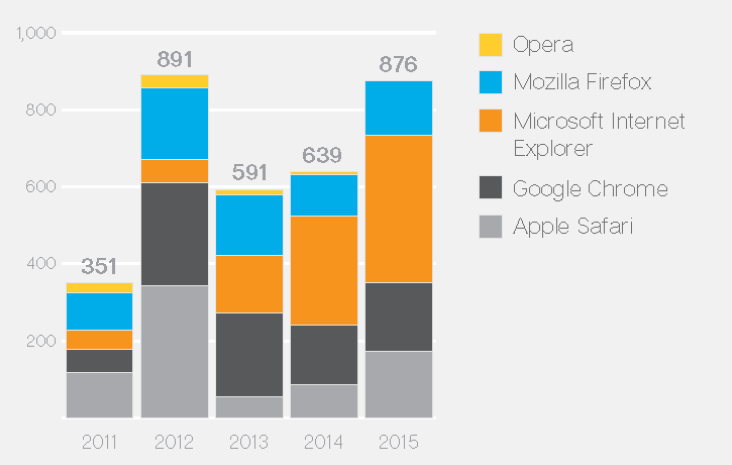
2013	2014	2015
		
77%	76%	78%
	-1% pts	+2% pts

Percentage of Vulnerabilities Which Were Critical

2013	2014	2015
		
16%	20%	15%
	+4% pts	-5% pts

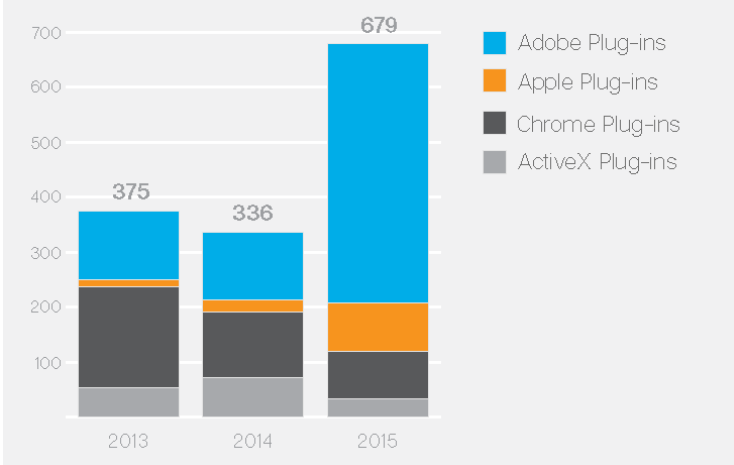
Στατιστικά ασφάλειας

Browser Vulnerabilities



Annual Plugin Vulnerabilities

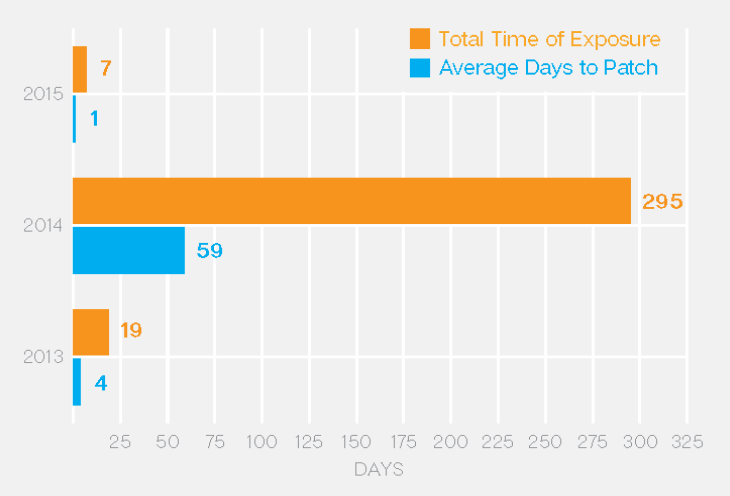
- *The number of vulnerabilities in Adobe plugins has grown in 2015, an indication that attackers are seeking to exploit plugins that are not only cross-platform, but also ubiquitous. Most Adobe vulnerabilities are related to Adobe Flash Player (also known as Shockwave Flash).*



Στατιστικά ασφάλειας

Top 5 Zero-Day Vulnerabilities, Patch and Signature Duration

- *While there were more zero-day vulnerabilities disclosed in 2015, some were proof-of-concept, but vendors were generally quicker to provide fixes in 2015 than in 2014..*

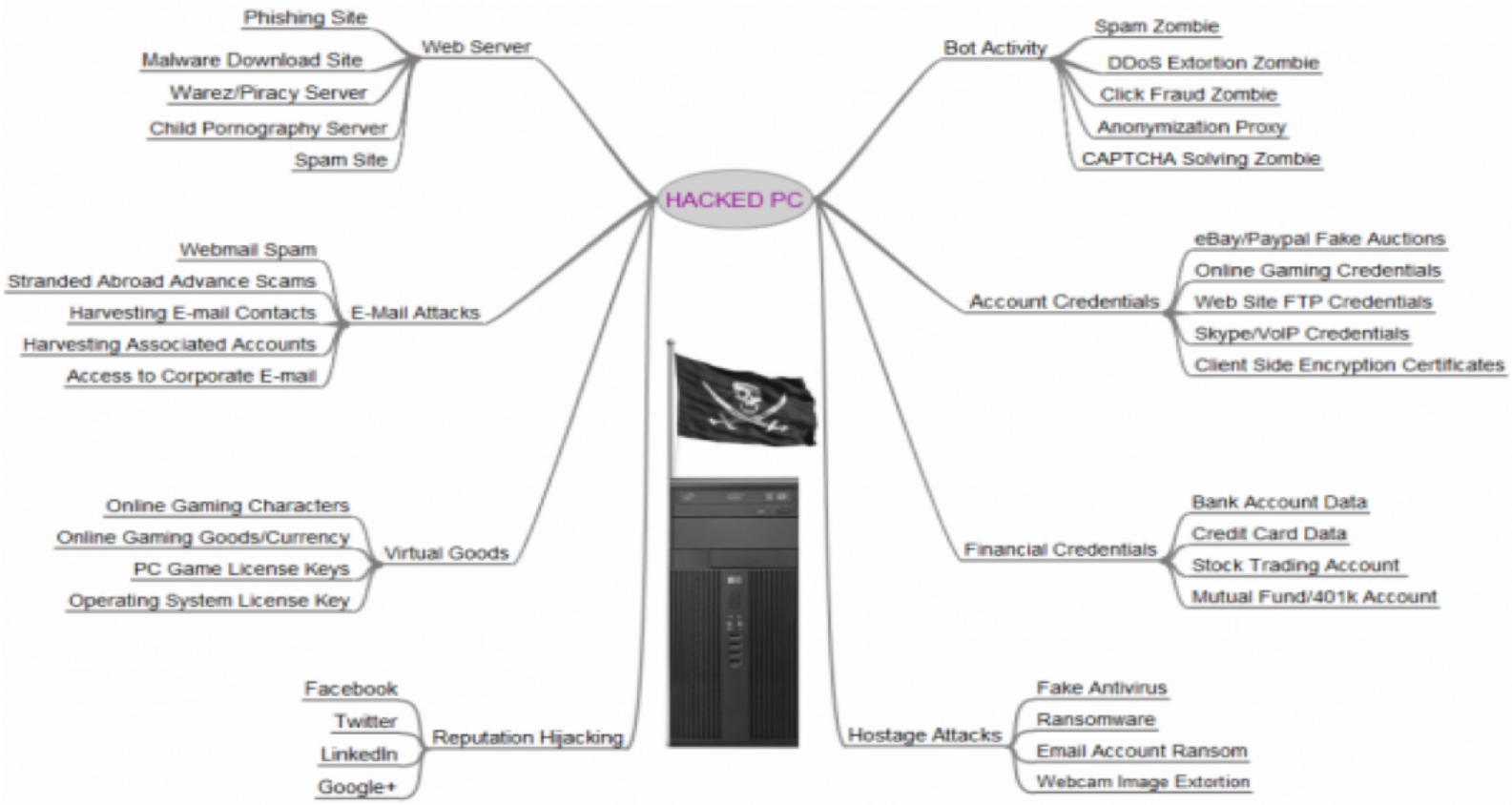


Top 5 Most Frequently Exploited Zero-Day Vulnerabilities

- *With the exception of CVE-2015-0235, the most frequently targeted zero-day exploits were related to vulnerabilities in Adobe's Flash Player.*
- *This data is based on exploitation after the vulnerability has become public.*

	2015 Exploit	2015	2014 Exploit	2014
1	Adobe Flash Player CVE-2015-0313	81%	Microsoft ActiveX Control CVE-2013-7331	81%
2	Adobe Flash Player CVE-2015-5119	14%	Microsoft Internet Explorer CVE-2014-0322	10%
3	Adobe Flash Player CVE-2015-5122	5%	Adobe Flash Player CVE-2014-0515	7%
4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%	Adobe Flash Player CVE-2014-0497	2%
5	Adobe Flash Player CVE-2015-3113	<1%	Microsoft Windows CVE-2014-4114 OLE	<1%

Χρησιμότητα ενός hacked PC

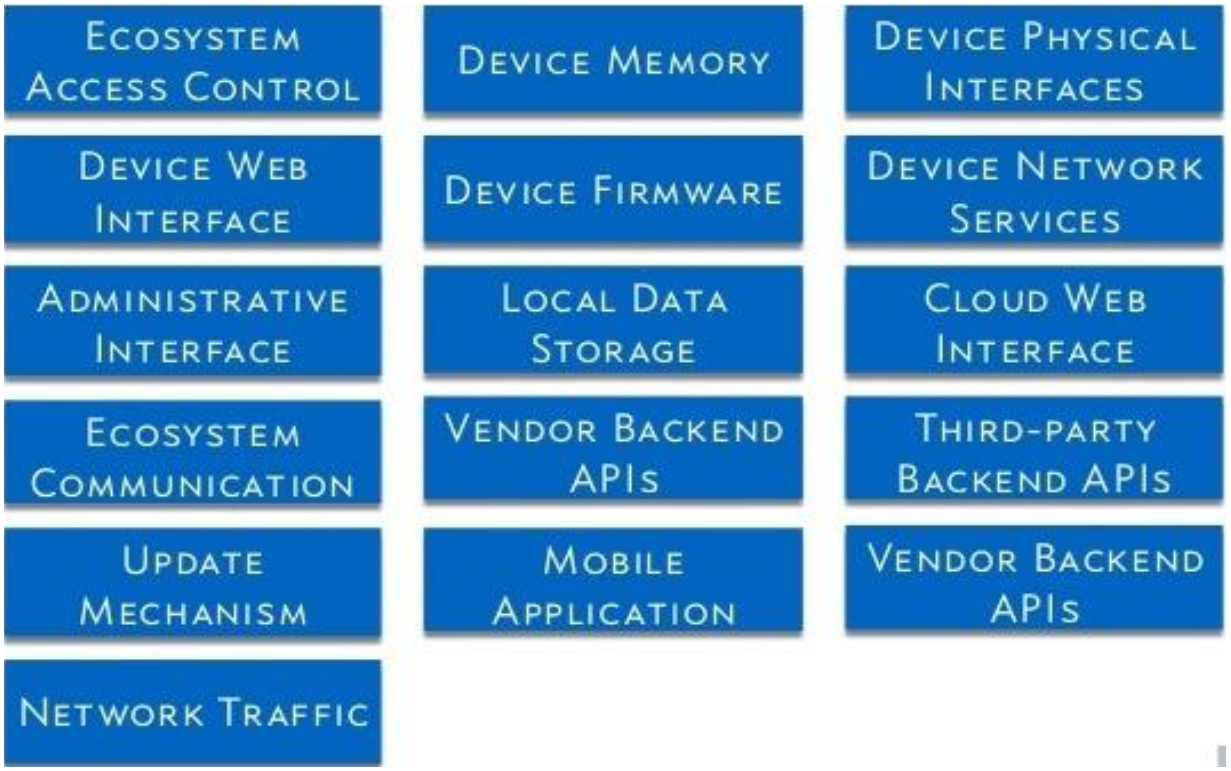


Γιατί (δεν;) μας αρέσει το IoT

- Top IoT security targets

Γιατί (δεν;) μας αρέσει το IoT

- IoT attack surface areas



Πολλές προσεγγίσεις

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017
- W. Stallings and L. Brown
  Computer Security: Principles & Practice
  3rd Ed., Prentice Hall, 2015
- M. Bishop
  Computer Security: Art and Science
  Addison Wesley, 2003