ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-Ι

Syllabus

A. Λίγα λόγια για το μάθημα
B. Κίνητρα για την Ασφάλεια
C. Η έννοια της Ασφάλειας Συστημάτων και Δικτύων
D. Το γνωστικό αντικείμενο της Ασφάλειας

Ιστορία της Ασφάλειας (1/3)

- 1940s: Πρώτοι Η/Υ (Colossus, EDVAC, ENIAC)
- 1960's Πολυχρηστικά συστήματα (multi-user). Ανάγκη προστασίας:
  1. Του συστήματος από τους χρήστες
  2. Των χρηστών (μεταξύ τους) (Graham, 1968)
- 1970's: Η εποχή των Mainframes:
  - RAND Report (Ware, 1970)
  - Anderson Report (Anderson, 1972)
  - Μοντέλο Bell-Lapadula (Bell and LaPadula, 1973)
  - Multics project (Organick, 1972)
  - Data Encryption Standard (DES) (USDoC, 1977)
  - Public Key Cryptography (Diffie-Hellmann, 1976)

Security Controls for Computer Systems--NIST

Threat monitoring functions in state applications

μοντέλο για έλεγχο της πρόσβασης σε στρατιωτικές εφαρμογές

time-sharing λειτουργικό σύστημα (high availability)

Εισαγωγή της Κρυπτογραφίας

Ιστορία της Ασφάλειας (2/3)

MS-DOS

United States Government Department of Defense (DoD) standard (basic requirements for assessing the effectiveness of computer security controls)

- 1980's: Η εποχή των PC's
  - Single-user systems… (more or less security?)
  - Orange Book (DoD 1985)
  - MLS, Information Flow,… (Clark & Wilson 1987, Brewer & Nash, 1989)
  - Internet Worm (1988) (Shoch and Hupp 1980, Cohen, 1985)

Ακεραιότητα Δεδομένων,κ.α

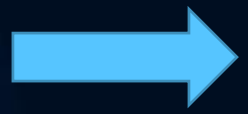
- 1990's: Η Εποχή του Internet
  - Internet security ≡ Communications Security (?)
  - Buffer Overflow (Phrack, 1996)
  - Digital Rights Management (DRM)

Mail Worms, DOS attacks (Grover, 1992)

Β. Μα, γιατί μιλάμε για την ασφάλεια;

- Κακόβουλο λογισμικό (botnets, trojans, rootkits),….
- Παράνομη εισβολή σε συστήματα, (Hacking, cracking…),
- Μη εξουσιοδοτημένη πρόσβαση σε πληροφορία (read, write)
- Επιθέσεις Άρνησης Εξυπηρέτησης (DOS, DDOS).
- Επιθέσεις Πλαστοπροσωπίας (Spoofing / Masquerading), Κλοπή Ταυτότητας (Identity Theft)
- Υποκλοπές Επικοινωνιών, Πρόσβαση σε προσωπικά δεδομένα
- Μη ζητηθείσα επικοινωνία (spam), «Ηλ. Ψάρεμα» (Phishing)
- Ηλεκτρονικό έγκλημα (cyber-crime), παιδική πορνογραφία,…
- Παραβίαση δικαιωμάτων πνευματικής ιδιοκτησίας…

Μα, γιατί μιλάμε για την ασφάλεια;

- Για να 
- Για την προστασία πολίτιμης πληροφορίας, ενώ εξακολουθεί να επιτρέπει την πρόσβαση σε όσους την χρειάζονται
- Για τα ευαίσθητα δεδομένα, κρίσιμες εμπορικές πληροφορίες, ιατρικά αρχεία, κ.λπ.
- Για την πιστοποίηση και τον έλεγχο της πρόσβασης σε πόρους π.χ AFS
- Εγγύηση διαθεσιμότητας των πόρων (99,999% αξιοπιστία)

Ποιος είναι ευάλωτος

- Τα χρηματοπιστωτικά ιδρύματα και οι τράπεζες
- Οι πάροχοι υπηρεσιών Διαδικτύου
- Οι φαρμακευτικές εταιρείες
- Κυβέρνηση και οργανισμοί άμυνας
- Εργολάβοι σε διάφορες κυβερνητικές υπηρεσίες
- πολυεθνικές επιχειρήσεις
- Οποιονδήποτε στο δίκτυο

Spoofing / Masquerading

- Επιθέσεις Πλαστοπροσωπίας (Spoofing / Masquerading). Χρήση «πλαστής» ταυτότητας με σκοπό τη μη ανίχνευση του επιτιθέμενου, ή/και την παράκαμψη των τεχνικών ελέγχου πρόσβασης του συστήματος.

Spoofing / Masquerading

Phishing -Κοινωνική μηχανική (social engineering)

From: Owen Geven ([redacted])
To: Christopher Burgess ([redacted])
Subject: Work Online From Home!

My name is Owen Geven, a designer and also the Manager of Owen Geven Fabric and Consultant and I live and work here in United Kingdom, Would you like to work online from home and get paid without affecting your present job? Actually I need a representative who can be working for the company as online book-keeper. We make lots of supplies to some of our clients in the EUROPE/USA/CANADA, for which I do come to USA/CANADA to receive payment and have it cashed after I supply them raw materials. It's always too expensive and stressful for me to come down and receive such payment twice in a month so I therefore decided to contact you. I am willing to pay you 10% for every payment receives by you from our clients who make payment through you. Please note you don't have to be a book keeper to apply for the job. Kindly get back to me as soon as possible if you are interested in this job offer with you're:

1. FULL NAMES..... 2. ADDRESS (not P.O.box).....
..... 3. STATE..... 4. ZIPCODE.....
5. COUNTRY..... 6. PHONE NUMBER(S).....7. GENDER.....
8. AGE..... 9. OCCUPATION.....

PLEASE SEND YOUR REPLY ASAP TO: ([redacted])

Social engineering

Facebook clickjacking

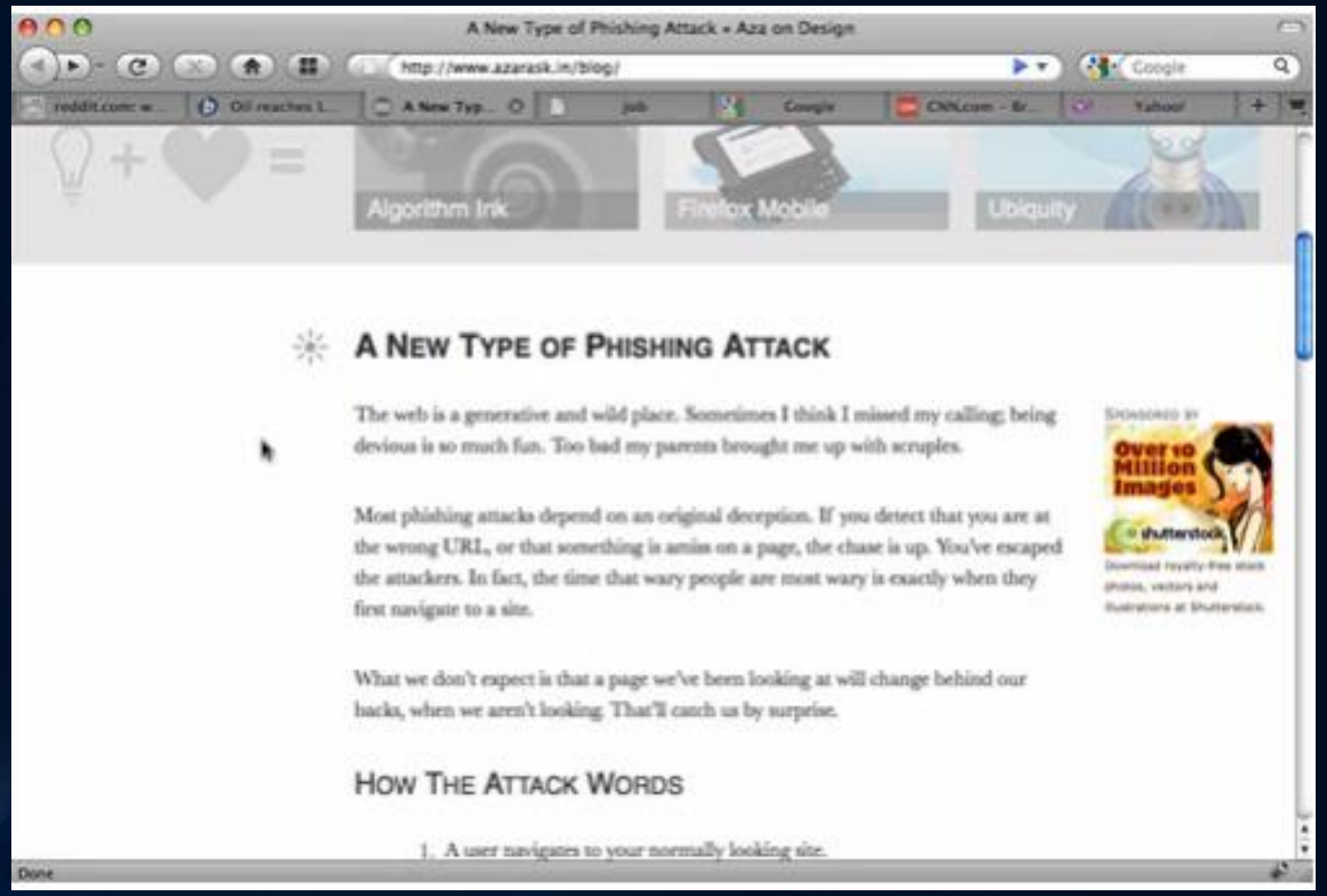
Panda Labs, Quarterly Report, April-June 2010

όταν οι hackers χρησιμοποιούν ψεύτικα κουμπιά και εικονίδια για να ξεγελάσουν τους χρήστες να κάνουν τις ανεπιθύμητες ενέργειες στο Facebook. Για παράδειγμα, οι απατεώνες μπορεί να φορτώσει ένα αόρατο κουμπί στο Facebook και να το τοποθετήσει σε ένα διαφορετικό κουμπί. Στη συνέχεια, όταν κάνετε κλικ στο ορατό κουμπί, να γίνει μια ενέργεια που δεν επιθυμούσατε.

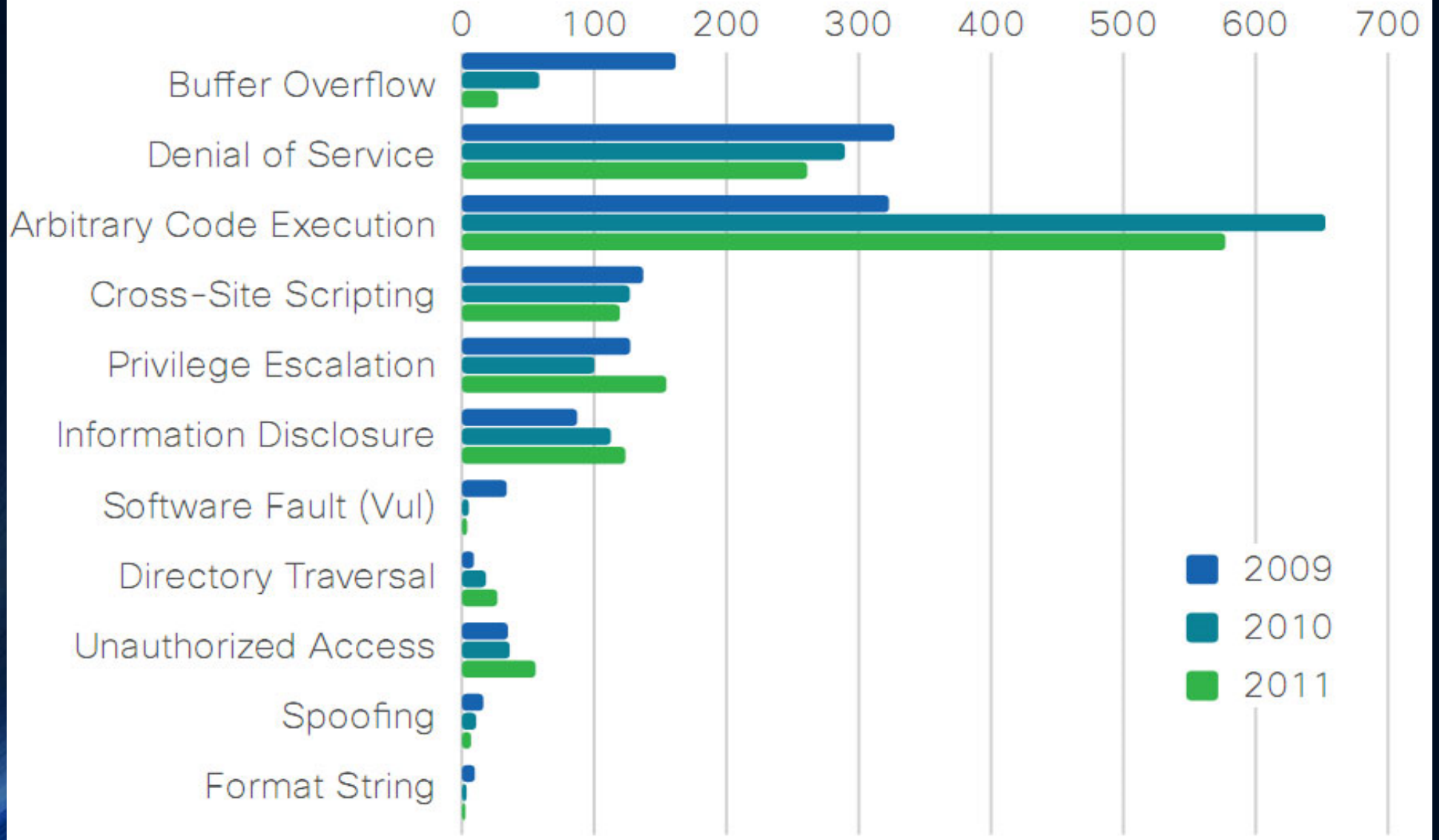
Tabnabbing

- Μια phishing επίθεση, η οποία πείθει τους χρήστες να υποβάλουν τα στοιχεία σύνδεσής τους κωδικούς πρόσβασης και σε δημοφιλείς δικτυακούς τόπους
- Υπάρχει πλαστογραφία ιστοσελίδων ώστενα πεισθεί ο χρήστης για την γνησιότητα ότι η τοποθεσία είναι γνήσια.
- Η επίθεση εκμεταλλεύεται την εμπιστοσύνη των χρηστών και η απροσεξία στη λεπτομέρεια σε σχέση με τα tabs
- και στο γεγονός ότι οι σύγχρονες ιστοσελίδεςκαθυστερούν να φορτώσουν τα tabs.
- Tabnabbing λειτουργεί αντίστροφα από περισσότερες επιθέσεις phishing στο ότι δεν ζητούν από τους χρήστες να κάνουν κλικ , αλλά αντ 'αυτού φορτώνει μια ψεύτικη σελίδα σε μία από τις ανοιχτές καρτέλες στον browser σας.

Tabnapping


A New Type of Phishing Attack « Aza on Design
http://www.azarask.in/blog/
Google
Algorithm Ink
Firefox Mobile
Ubiquity
A New Type of Phishing Attack
The web is a generative and wild place. Sometimes I think I missed my calling; being devious is so much fun. Too bad my parents brought me up with scruples.
Most phishing attacks depend on an original deception. If you detect that you are at the wrong URL, or that something is amiss on a page, the chase is up. You've escaped the attackers. In fact, the time that wary people are most wary is exactly when they first navigate to a site.
What we don't expect is that a page we've been looking at will change behind our backs, when we aren't looking. That'll catch us by surprise.
How The Attack Words
1. A user navigates to your normally looking site.
Over 10 Million Images
shutterstock
Done

Vulnerability and Threat Categories



Quarterly Report, Panda Labs, July-September 2011

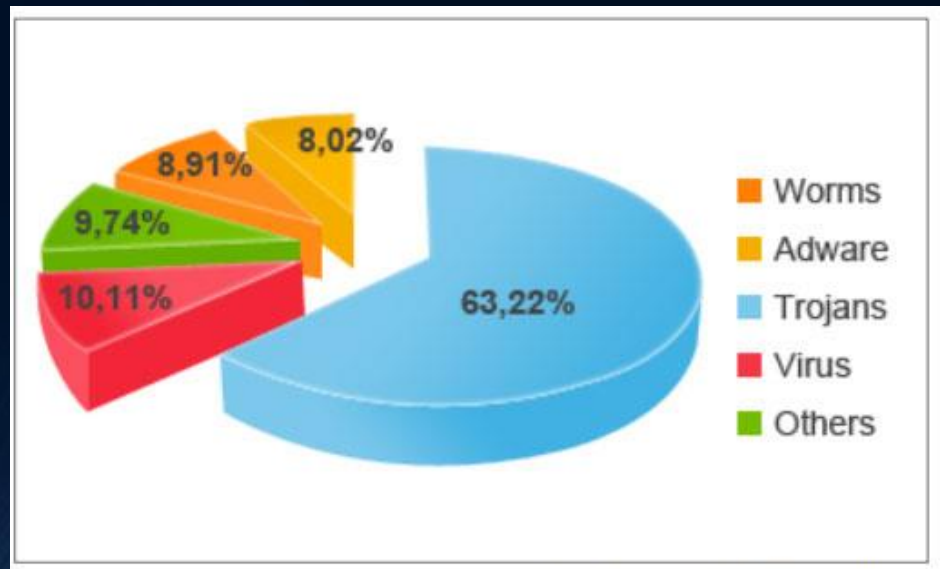


FIG.07. *INFECTIONS PER TYPE OF MALWARE.*

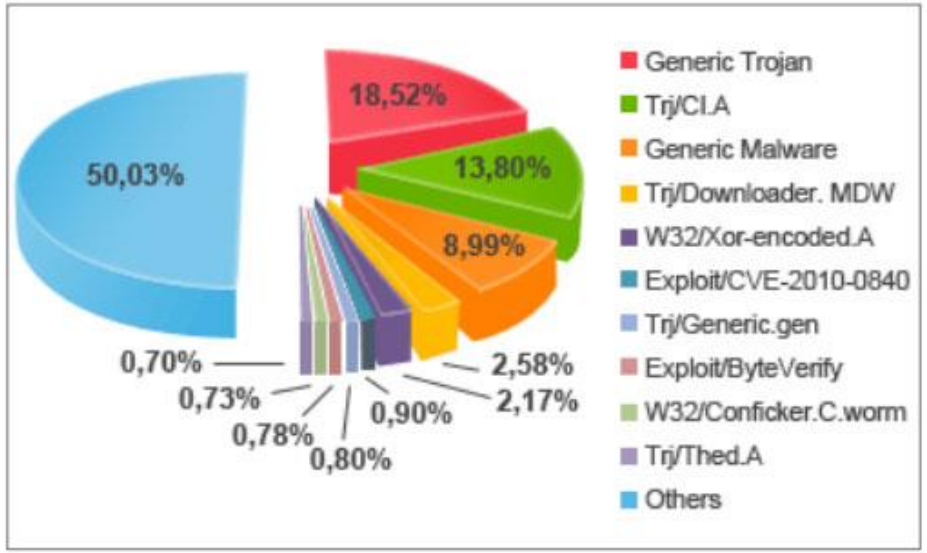
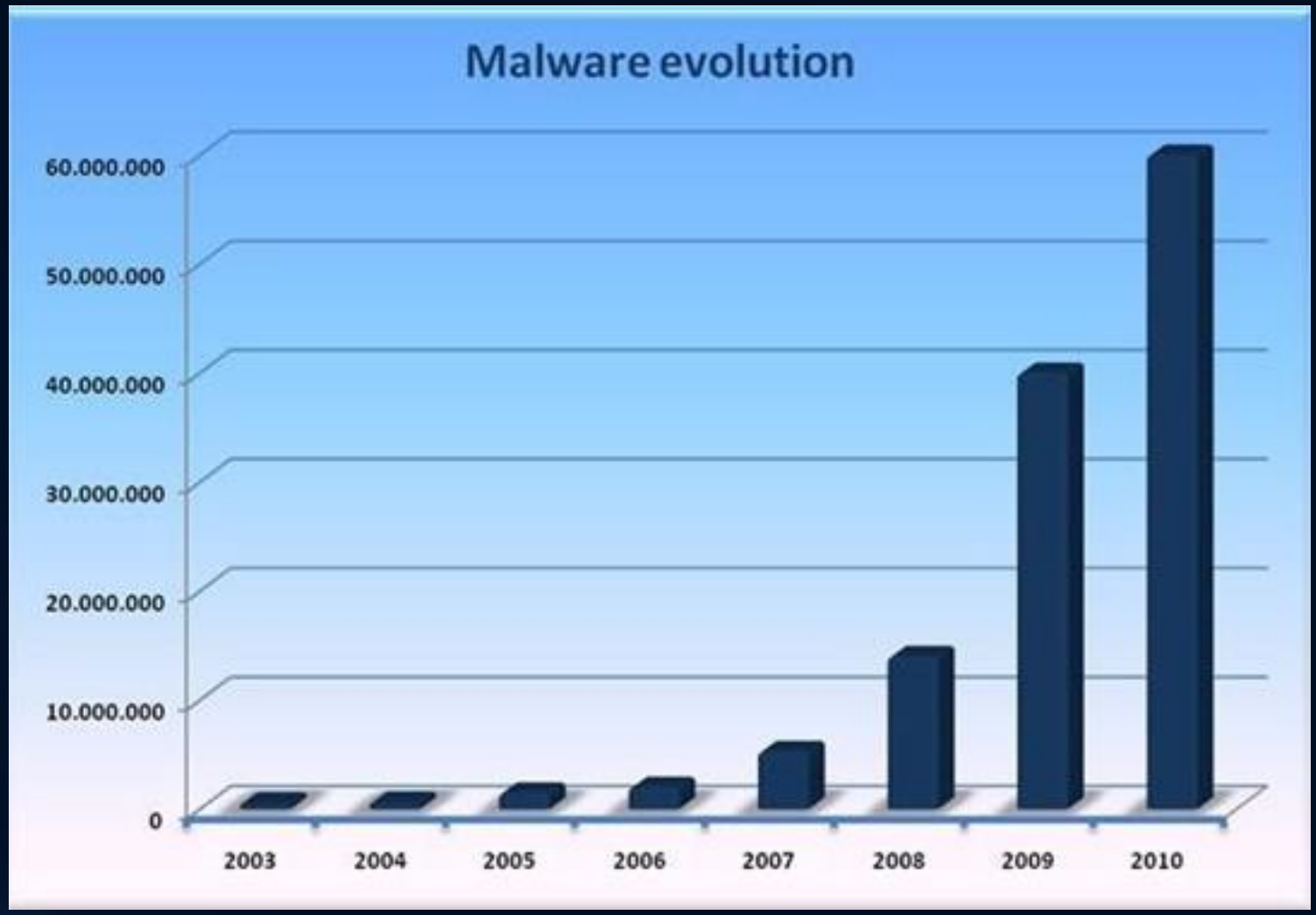


FIG.08. *MALWARE FAMILIES.*


Malware evolution
60.000.000
50.000.000
40.000.000
30.000.000
20.000.000
10.000.000
0
2003
2004
2005
2006
2007
2008
2009
2010

Cisco 2011 Annual Sec. Report

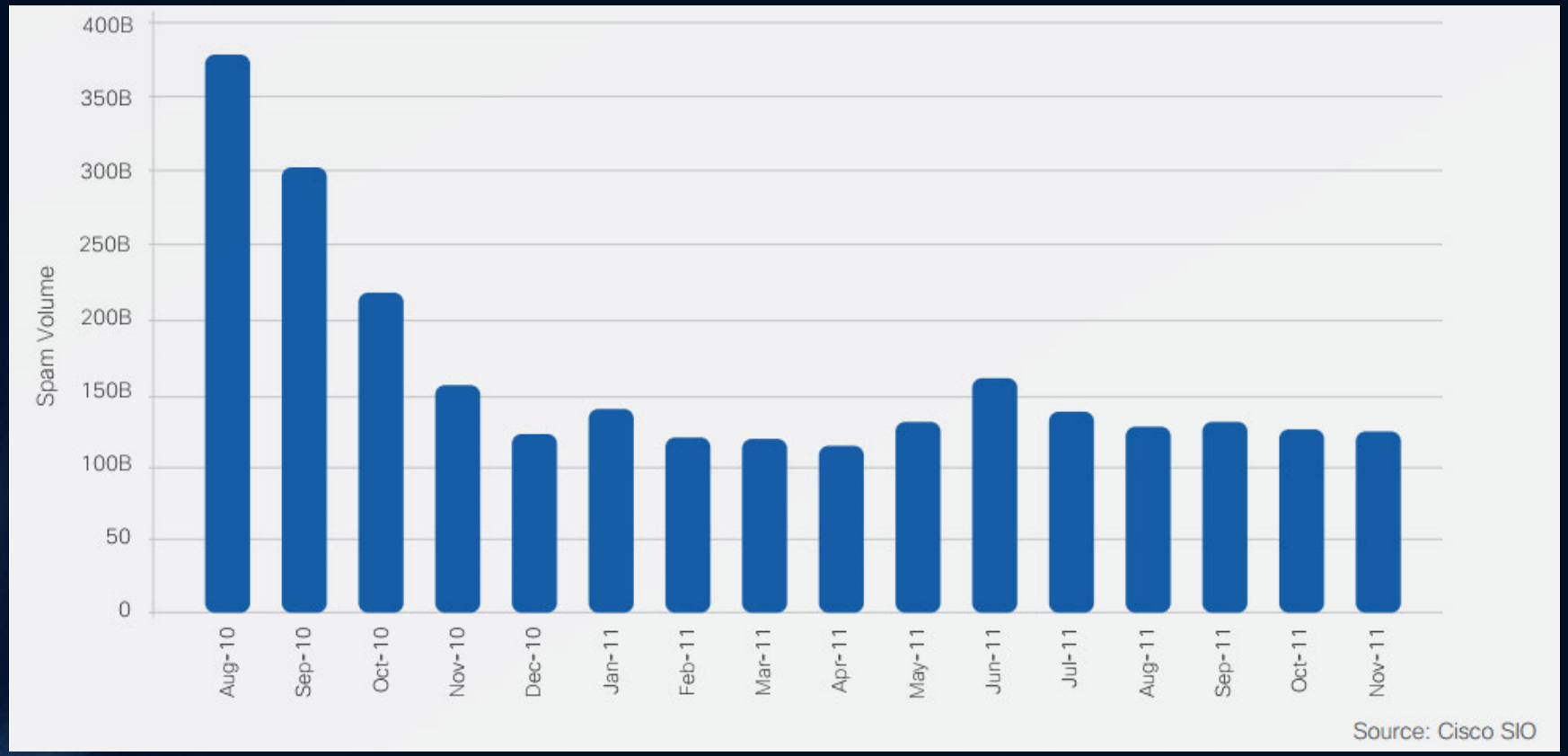
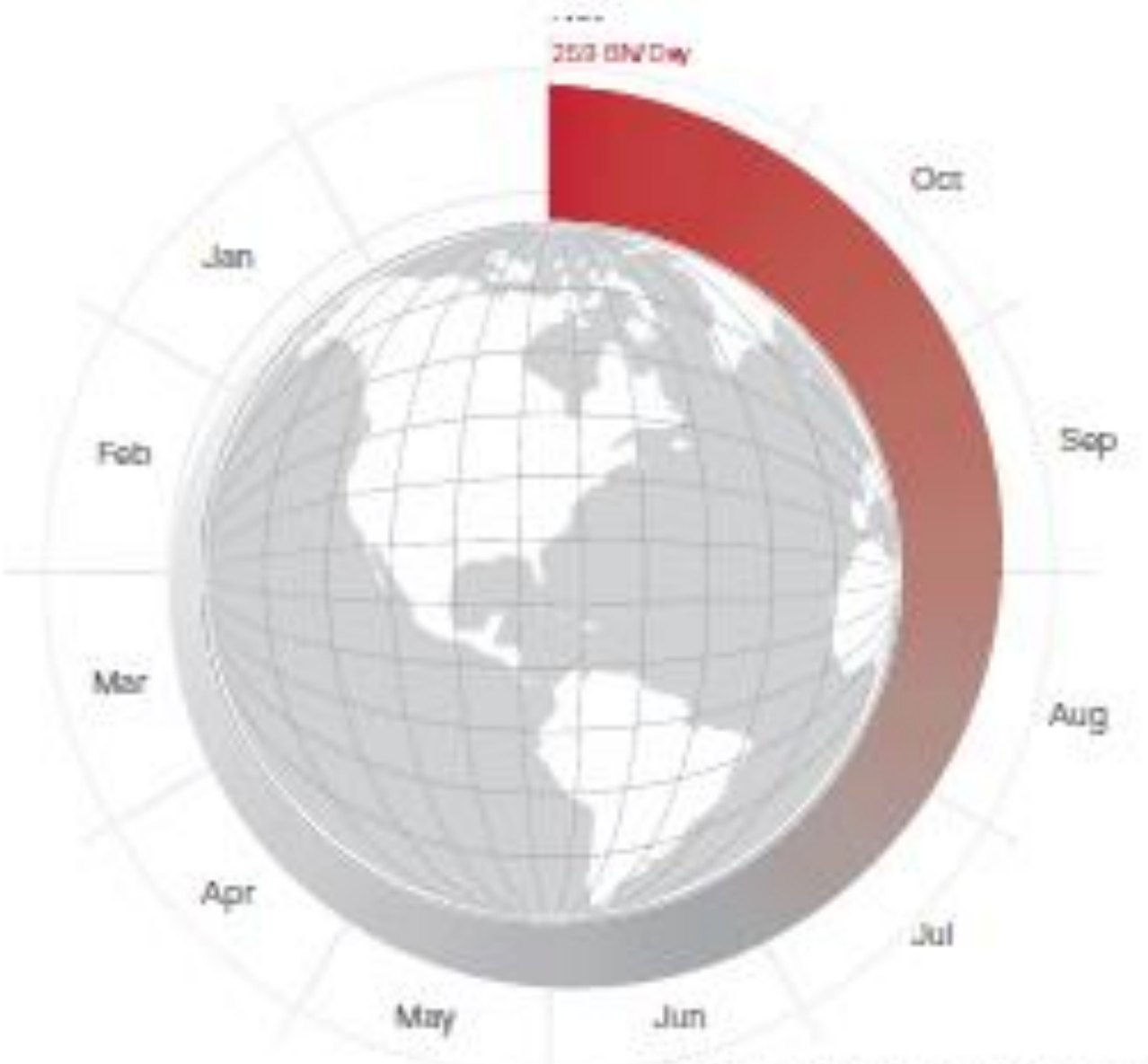


Figure 16. Worldwide Spam Volume Increase in 2014

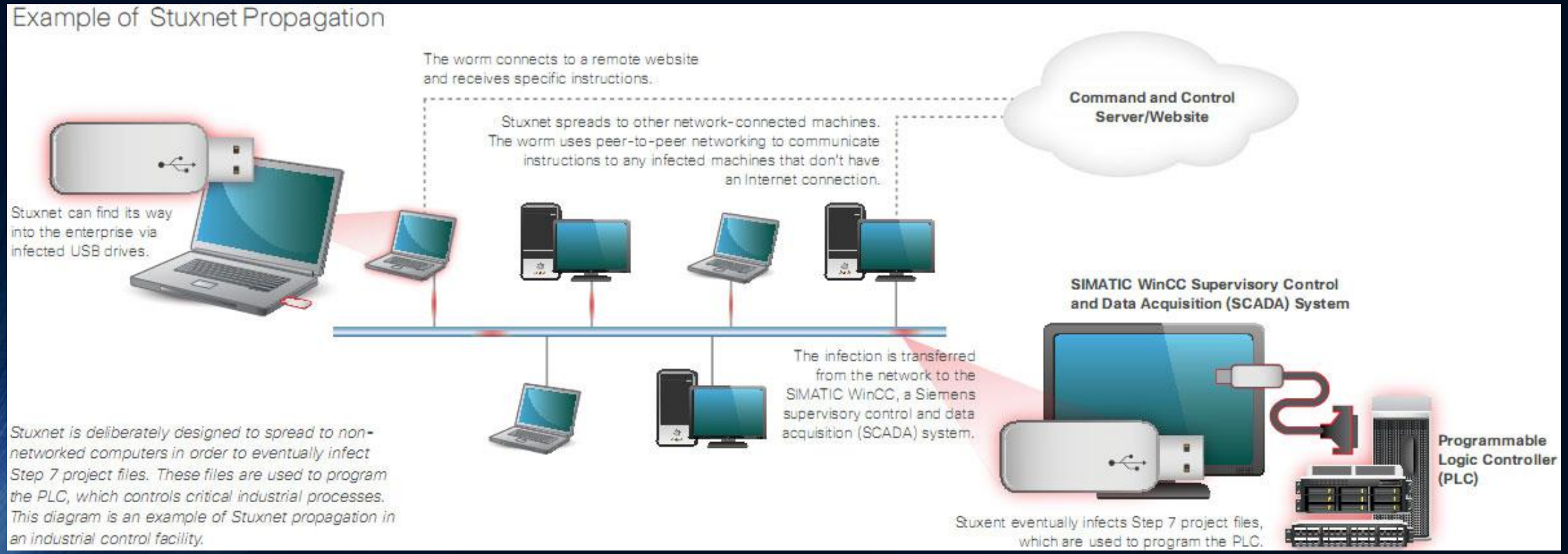


Source: Cisco Security Research

Cisco 2015 Annual Sec. Report

Cyber-Physical Security (CPS)

Case: Stuxnet Worm



C. Ασφάλεια – Ορισμοί

- Security: (Oxford Dictionary)
  - Freedom from danger or anxiety
- Ασφάλεια: (Μπαμπινιώτης)
  - Η κατάσταση στην οποία … αισθάνεται κανείς ότι δεν απειλείται.
  - Η αποτροπή κινδύνου ή απειλής…
- Ασφάλεια (Security) & Ασφάλεια (Safety)
  - Security: Προστασία έναντι εχθρού
  - Safety: Προστασία έναντι σφαλμάτων, λαθών, ατυχημάτων, παραλείψεων

Η "ασφάλεια" στα ελληνικά: Ένα σημαίνον για δύο σημαινόμενα

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.

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 έλαβε ένα μήνυμα ή ότι πραγματικά έστειλε αυτός ένα μήνυμα και όχι κάποιος άλλος.

Ακεραιότητα (Integrity):

- Συνέπεια της ακεραιότητας είναι κάθε αλλαγή (π.χ. του περιεχομένου των δεδομένων) να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας, ενώ παράλληλα μη εξουσιοδοτημένη αλλαγή να μην είναι δυνατή.
- Ακριβής (precise)
- Ορθός (accurate)
- Τροποποίηση μόνο με αποδεκτούς τρόπους (modified only in acceptable ways)
- Τροποποίηση μόνο από εξουσιοδοτημένους ανθρώπους (modified only by authorised people)
- Τροποποίηση μόνο από εξουσιοδοτημένες διεργασίες (modified only by authorised processes)
- Συνέπεια (consistent)

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. Οι ενέργειες κατά της διαθεσιμότητας εντάσσουν

Οι προσδοκίες του χαρακτηριστικού της Διαθεσιμότητας περιλαμβάνουν:

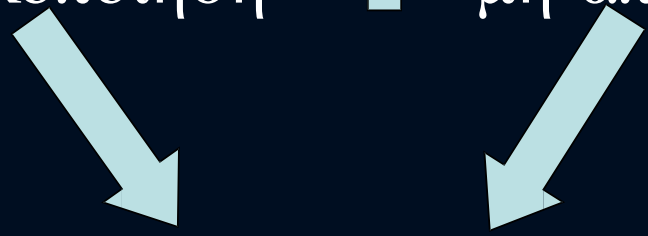
- παρουσία του αντικειμένου και της υπηρεσίας με χρησιμοποιήσιμο τρόπο.
- Ικανότητα χειρισμού των απαιτούμενων πόρων
- Συγκεκριμένος χρόνος αναμονής
- Κατάλληλος χρόνος διάθεσης των πόρων

Σκοπός της Διαθεσιμότητας είναι:

- Δίκαιη κατανομή των πόρων
- Έγκαιρη ανταπόκριση στη διάθεση των δεδομένων
- Ελεγχόμενη συμφωνία, δηλαδή χειρισμός δοσοληψιών, αποκλειστική πρόσβαση, χειρισμός του φαινομένου deadlock.
- Χρησιμότητα, οι πόροι και τα δεδομένα μπορούν να χρησιμοποιηθούν όπως σχεδιάστηκαν.

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

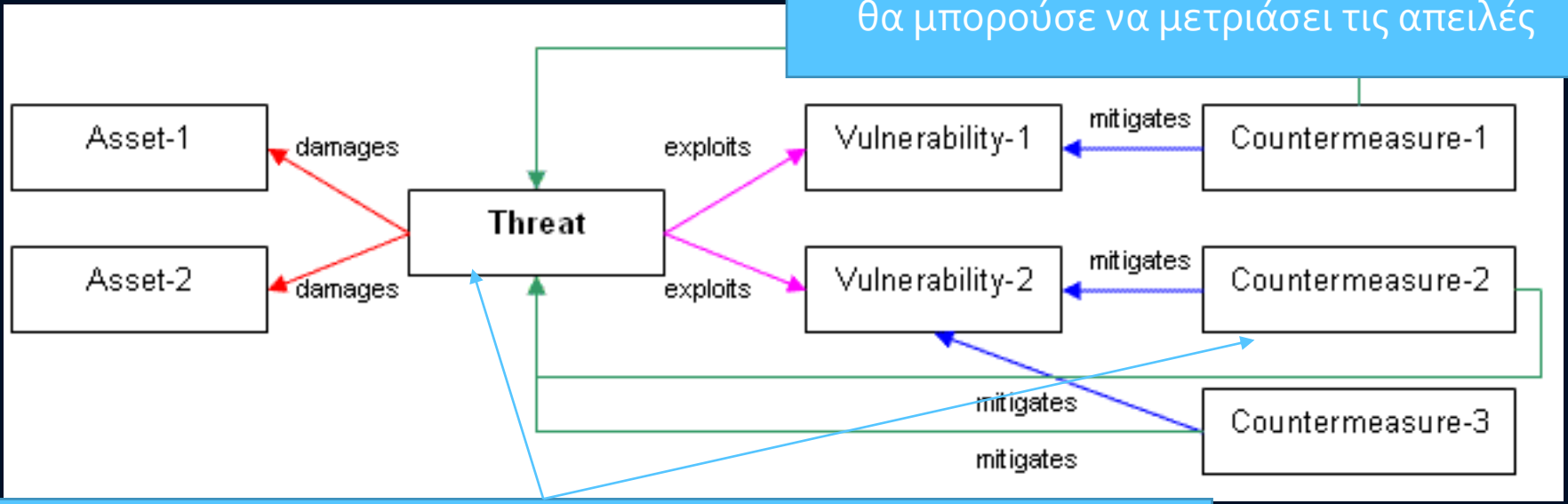
Ευπάθειες

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

Τι σημαίνει

Θεώρηση από τη σκ

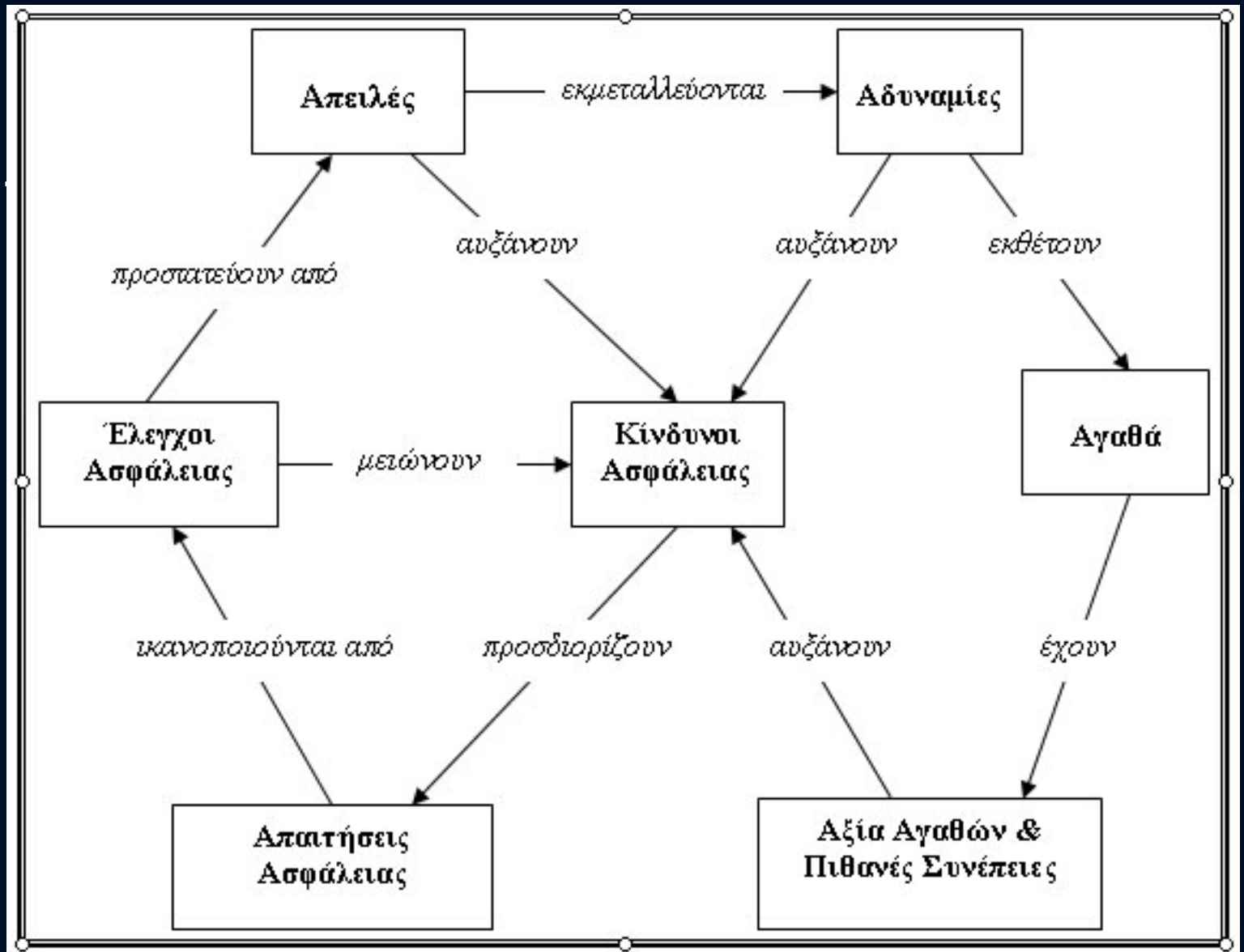
- Μια απειλή μπορεί να εκμεταλλευτεί αρκετά τρωτά σημεία, το σύνολο των πιθανών αντισταθμιστικών μέτρων που θα μπορούσαν να μετριάσουν απειλή ορίζεται πλήρως από το σύνολο των τρωτών σημείων που χρησιμοποιούνται σε ένα σενάριο απειλής ως εξής:
- Η απειλή μπορεί να μετριαστεί από τρία αντισταθμιστικά μέτρα
- Με λίγα λόγια:
- Απειλές εκμεταλλεύονται τρωτά σημεία και προκαλούν βλάβη στα Asset
- Τα αντισταθμιστικά μέτρα μετριάζουν τις αδυναμίες και ως εκ τούτου θα μπορούσε να μετριάσει τις απειλές



Η απειλή προκαλεί βλάβες στο Asset-1 και Asset-2
Η απειλή εκμεταλλεύεται δύο ευπάθειες
Η ευπάθεια-1 μετριάζεται από αντισταθμιστικό μέτρο-1.
Η ευπάθεια-2 μετριάζεται από αντισταθμιστικό μέτρο-2 και 3.

http://www.ptatechnologies.com/PTA3.htm

Τι σ

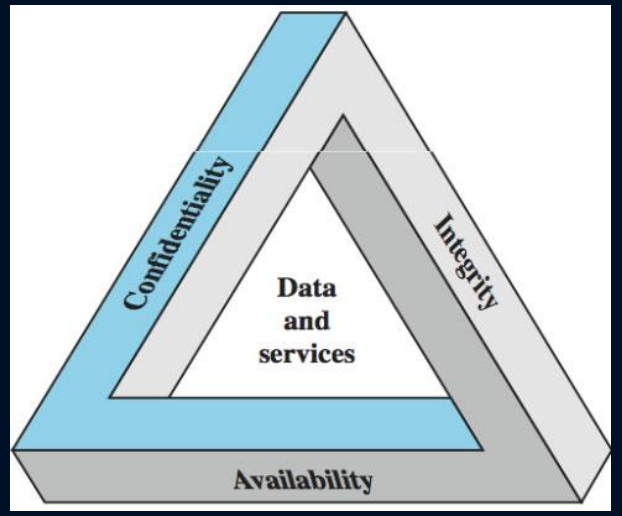


Σχήμα 3. Σύνδεση όρων ανάλυσης και διαχείρισης κινδύνου

Δρ. Π. Κοτζανικολάου, «Τεχνολογία και Πολιτικές Ασφάλειας», Πανεπιστήμιο Πειραιώς, 2009

Computer Security (NIST, 1995) - The CIA Triad

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources includes hardware, software, firmware, information/data, and telecommunications



The CIA Security Requirements Triad

CIA Security Triad (FIPS PUB 199)

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

- **Ακεραιότητα (Integrity):** Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή/και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

- **Διαθεσιμότητα (Availability):** Η διαθεσιμότητα των δεδομένων και των υπολογιστικών πόρων είναι η εξασφάλιση ότι οι υπολογιστές, τα δίκτυα και τα δεδομένα θα είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους. Μία τυπική απειλή που αντιμετωπίζουν τα σύγχρονα πληροφοριακά συστήματα είναι η επίθεση άρνησης υπηρεσιών (DOS attack), που έχει ως σκοπό να τεθούν εκτός λειτουργίας οι στοχευμένοι πόροι, είτε προσωρινά είτε μόνιμα. Η άρνηση υπηρεσιών δεν προκαλείται αναγκαία από εχθρική επίθεση.

- **Εμπιστευτικότητα (Confidentiality):** Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα. Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή.

CIA

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

Αγαθά, Αξία Αγαθών (Σχετ: Συνέπεια) & Κατηγοριοποίηση Αγαθών (FIPS PUB 199)

- 3 Levels of Impact (from a security breach)
  1. Low
  2. Moderate
  3. High

A. Security Categorization applied to Information Types

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},
where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

SC public information = {(**confidentiality**, NA), (**integrity**, MODERATE), (**availability**, MODERATE)}

SC investigative information = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

Αγαθά, Αξία Αγαθών (Σχετ: Συνέπεια) & Κατηγοριοποίηση Αγαθών (FIPS PUB 199)

- 3 Levels of Impact (from a security breach)
  1. Low
  2. Moderate
  3. High

B. Security Categorization applied to Information Systems

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

SC sensor data = {(**confidentiality**, NA), (**integrity**, HIGH), (**availability**, HIGH)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)},

Απειλές στην Ασφάλεια

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack
An assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

(RFC 2828, 2000) – Internet Security Glossary