Segurança em Redes de Computadores
Computer Network Security
(SRC)

(MIETI 4º Ano/S2 - 6707N5)

Henrique Santos (hsantos@dsi.uminho.pt)

Dpt. Sistemas de Informação

Ext. 510302

Sumary

- InfoSec Fundamentals
  - Simple Model for InfoSec (ISO 27k)
  - Attacks, Threats and Vulnerabilities in computer networks
  - InfoSec Policies
- Applied cryptography
- Access Control
- Security in TCP/IP based networks
- InfoSec Technologies
  - Biometrics
  - IPSec
  - SSL/TLS
  - Firewalls
  - Intrusion Detection Systems
  - VPN
  - …
- Introduction to forensic analysis

Teaching Objectives

- Develop essential knowledge on various information security technologies as well as the technical skills required for its correct implementation, which together are critical to enabling a conscious and effective involvement in designing and implementing an Information Security Management process; and
- Alert to issues related to the topic of Information Security in the current context of "Cyberspace"

Learning Outcomes

- Recognize the importance of a culture of security with respect to the use of computer systems and networks
- Identify the technical aspects of computer systems and networks that expose them more to security risks
- Recognize the main threats and the typical way the attacks are carried out
- Analyze vulnerabilities in networked systems
- Plan security strategies for networked computers
- Implement continuous management and control processes, defined in the context of a security policy for networked computers
- Use security analysis and auditing tools for computer and networks

Assessment Strategy

- Homework (50%~60%)
- Final “cyber exercise” or essay (20%~40%)
- Participation in group discussion and other UC initiatives (10%)

- Late delivery concerning homework and other evaluation material is accepted with a penalty of 5%/hour!
- Attendance control in theoretical lessons is applied, but there are no absence limit. In the TPs **is mandatory** the presence of the 2/3 classes
- The UC monitoring will be done by Moodle platform

Bibliography

- Pfleeger, Charles P., Pfleeger, Shari L., “Security in Computing”, Fourth Edition, Prentice Hall PTR, 2007.
- C. Douligeris and D. N. Serpanos, “Network Security: Current Status and Future Directions” Wiley-IEEE Press, 2007. http://www.ebook3000.com/Network-Security--Current-Status-and-Future-Directions_22046.html
- Stallings, W., “Cryptography and Network Security: Principles and Practice”,5th., Prentice Hall Press, 2010.
- Bishop, M., “Introduction to Computer Security”. Prentice Hall PTR, 2004.
- Kaufman, C., Perlman, R., and Speciner, M., “Network Security: Private Communication in a Public World”. Second ed., Prentice Hall PTR, 2002.
- Bosworth, S., and Kabay, M. E., “Computer Security Handbook” 4th ed.: John Wiley & Sons, Inc., 2002.
- Anderson, R. J. ,“Security Engineering: A Guide to Building Dependable Distributed Systems”, 2nd Ed., Wiley Publishing, 2008. (http://www.cl.cam.ac.uk/~rja14/book.html)
- Santos, H. D., “A norma das normas em Segurança da Informação”, Publicação da Associação Portuguesa para a Qualidade, XXXV, 1 (Primavera, 2006), 11-19.
- Zúquete, A., “Segurança em Redes Informáticas”, 3ª ed., FCA – Editora Informática, 2010.

- CERT Coordination Center, http://www.cert.org/
- NIST Computer Security Division 893 and CSRC Home Page, http://csrc.nist.gov/
- Resources for Security Risk Analysis, Security Policies, ISO 17799 (or BS7799) and Security Audit, http://www.securityauditor.net/
- The Computer Security Institute, http://www.gocsi.com/
- ...

Initial Reflection

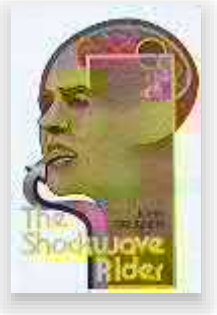
"*The world is never going to be perfect, either on- or offline; so let's not set impossibly high standards for online.*"

— Esther Dyson

Contextualization

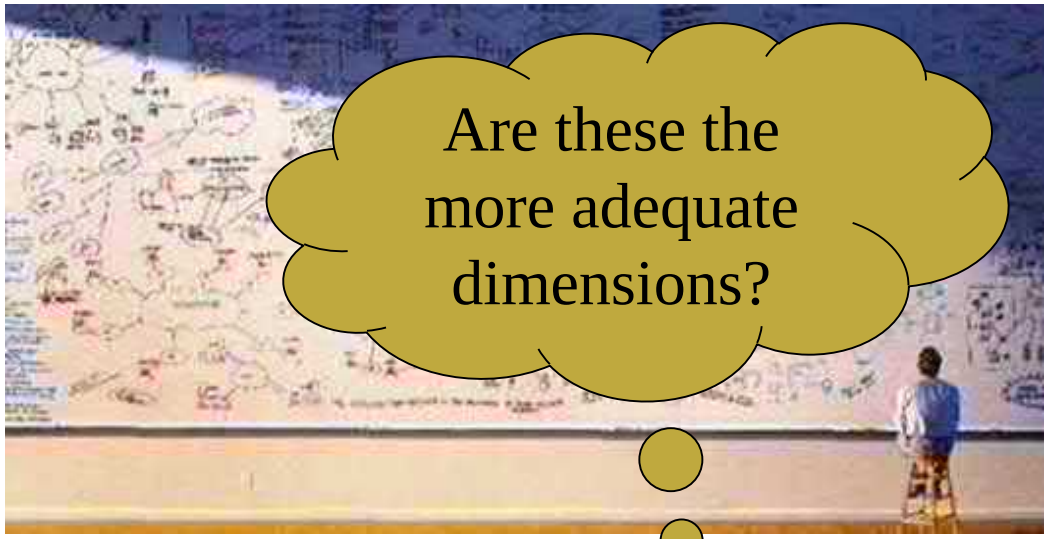
- Evolution of information technology (≈50 years)
  - Few computer centers isolated
  - Time-sharing
  - Data networks (Distributed Systems)
  - Personal computers
  - Ubiquitous computing, mobility and the technology convergence

- The first “worm”
  - In 1975, the scientific fiction classic from John Brunner, *The Shockwave Rider*, provided the first computer program that replicates itself and propagates itself



Contextualization

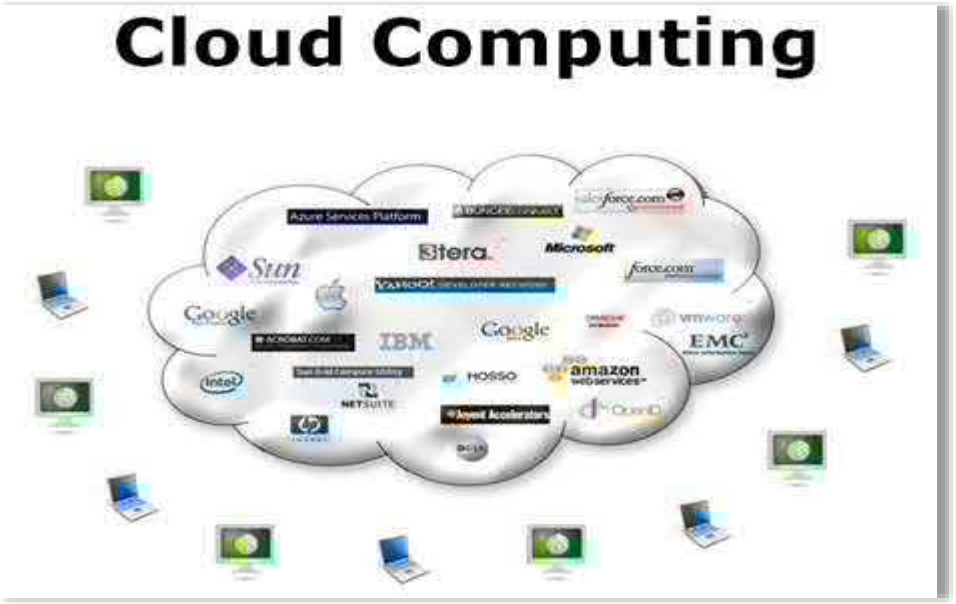
- **Complexity:**
  - Non rigorous engineering process
  - Legacy systems
  - Component integration (COTS)
  - Diversity and flexibility
  - Short life cycle
  - …



- **Risks**:
  - Availability
  - Confidentiality
  - Integrity

Technological complexity

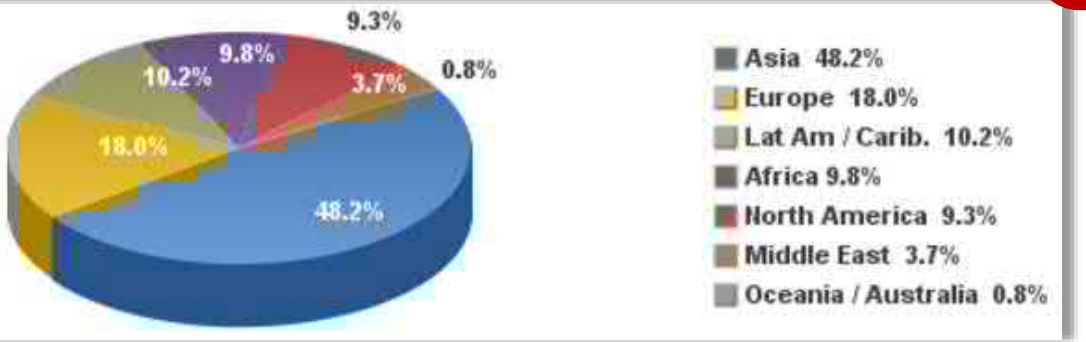
Disruptive technologies



Complexity in social networks

- Internet statistics

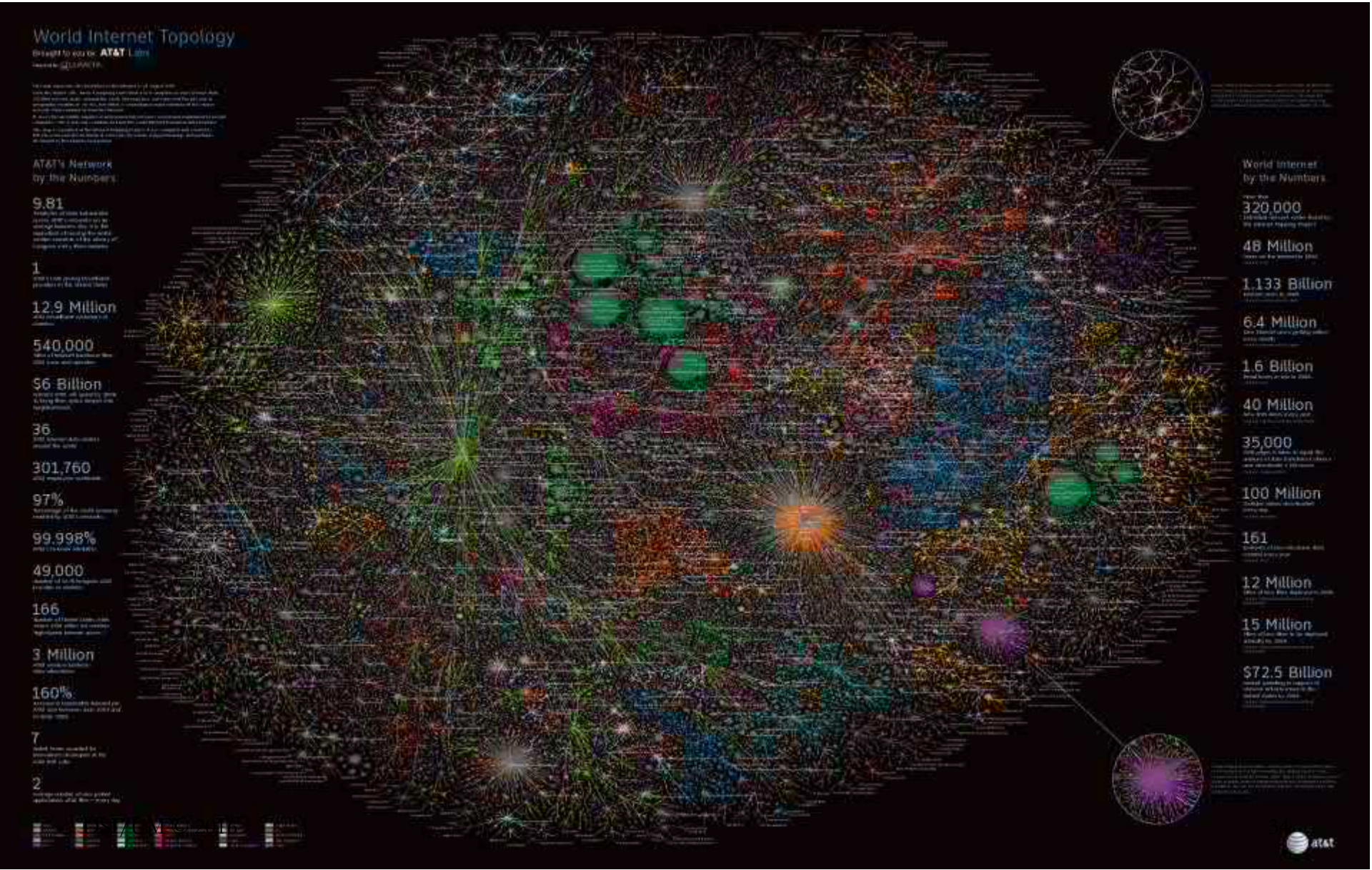
WORLD INTERNET USAGE AND POPULATION STATISTICS NOVEMBER 30, 2015 - Update						
World Regions	Population (2015 Est.)	Population % of World	Internet Users 30 Nov 2015	Penetration (% Population)	Growth 2000-2015	Users % of Table
Africa	1,158,355,663	16.0 %	330,965,359	28.6 %	7,231.3%	9.8 %
Asia	4,032,466,882	55.5 %	1,622,084,293	40.2 %	1,319.1%	48.2 %
Europe	821,555,904	11.3 %	604,147,280	73.5 %	474.9%	18.0 %
Middle East	236,137,235	3.3 %	123,172,132	52.2 %	3,649.8%	3.7 %
North America	357,178,284	4.9 %	313,867,363	87.9 %	190.4%	9.3 %
Latin America / Caribbean	617,049,712	8.5 %	344,824,199	55.9 %	1,808.4%	10.2 %
Oceania / Australia	37,158,563	0.5 %	27,200,530	73.2 %	256.9%	0.8 %
WORLD TOTAL	7,259,902,243	100.0 %	3,366,261,156	46.4 %	832.5%	100.0 %



http://www.internetworldstats.com/stats.htm

Ciber *backbone* – AT&T (2007)

http://javiergs.com/?p=983

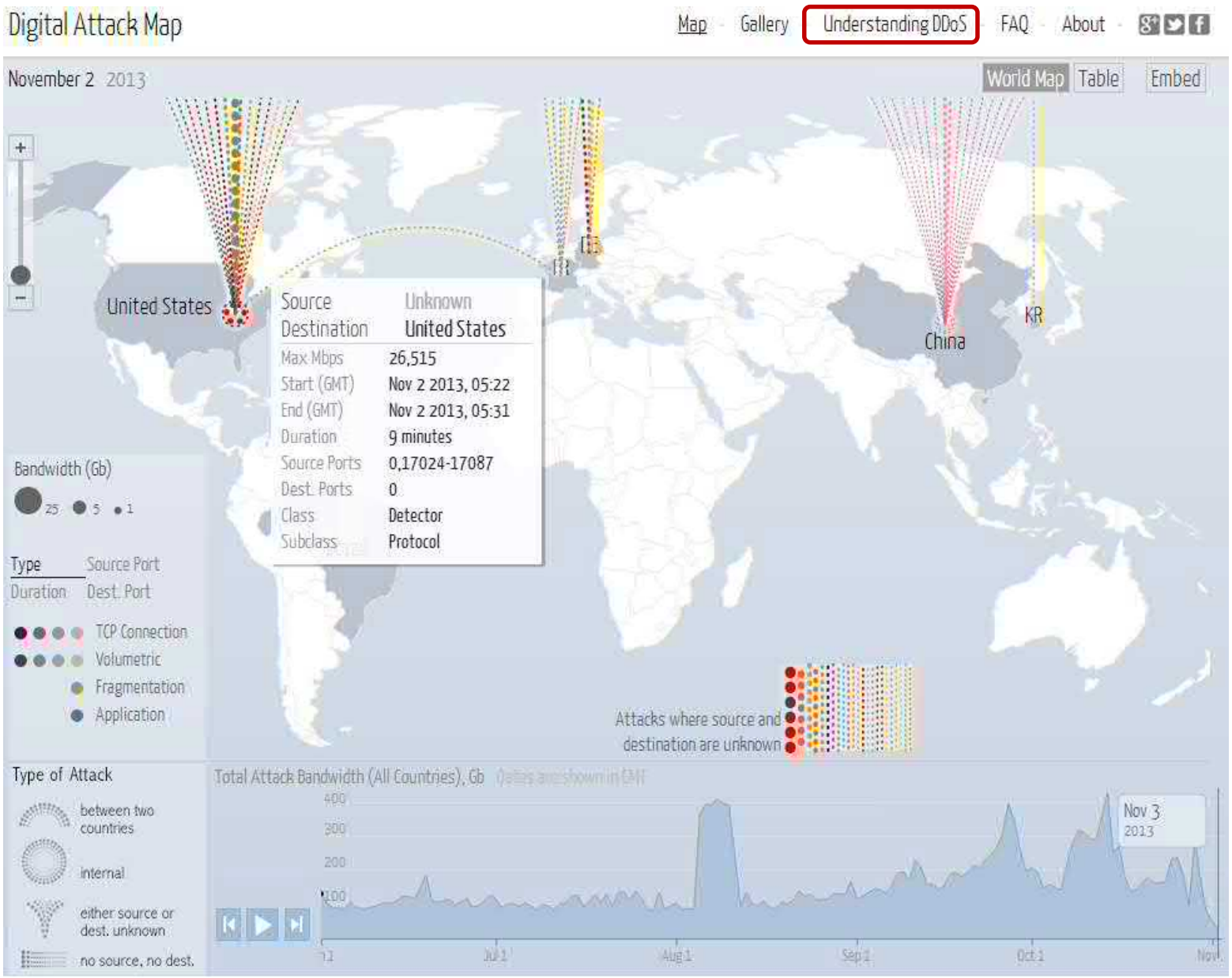


Security incidents evolution

Overall Age Gender 2013 Statistics

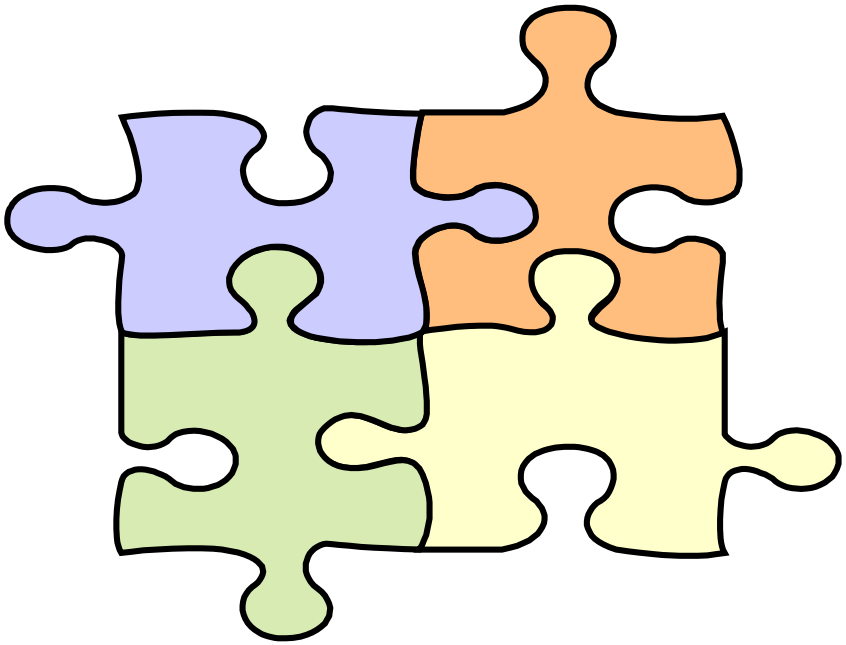
Age Range	Male Count	Male Loss	Female Count	Female Loss	Total Complaints	Total Combined Losses
Under 20	5,194	$103,298,649	3,602	$2,364,515	8,796	$105,663,164
20 – 29	24,549	$42,144,452	23,483	$23,619,502	48,032	$65,763,954
30 – 39	28,391	$71,022,425	26,389	$41,784,048	54,780	$112,806,473
40 – 49	26,668	$89,559,205	29,170	$70,355,407	55,838	$159,914,612
50 – 59	29,220	$93,705,383	26,239	$83,858,340	55,459	$177,563,723
Over 60	23,074	$87,244,816	16,834	$72,884,870	39,908	$160,129,686
Totals	137,096	$486,974,929	125,717	$294,866,681	262,813	$781,841,611

Fonte: FBI, 2013 Internet Crime Report


Digital Attack Map
Map
Gallery
Understanding DDoS
FAQ
About
November 2 2013
World Map
Table
Embed
United States
China
KR
Source Unknown
Destination United States
Max Mbps 26,515
Start (GMT) Nov 2 2013, 05:22
End (GMT) Nov 2 2013, 05:31
Duration 9 minutes
Source Ports 0,17024-17087
Dest. Ports 0
Class Detector
Subclass Protocol
Bandwidth (Gb)
25
5
1
Type
Source Port
Duration
Dest. Port
TCP Connection
Volumetric
Fragmentation
Application
Attacks where source and destination are unknown
Type of Attack
between two countries
internal
either source or dest. unknown
no source, no dest.
Total Attack Bandwidth (All Countries), Gb
400
300
200
100
Nov 3
2013
Jul 1
Aug 1
Sep 1
Oct 1
Nov

Cyber Attack Alerts

What security/safety measures (controls) are available, which should be used and when and how to implement them?



InfoSec fundamental concepts

- **Security** is a “measure” of **dependability** (quality of a system that allows us to trust, in a justified way, in its service) against **faults** affecting integrity, confidentiality and availability (!?)
- Security is not safety…
  but security contributes to safety

InfoSec fundamental concepts

- Terms and definitions (ISO/IEC 27000)
  - Resource
    - Any good or asset that **has value** to the organization
  - Information Security Event
    - Occurrence in a system, service or network, of an **identifiable state** which shows:
      - A possible **violation of security policy**;
      - A **failure of a defense**; or
      - A previously unknown situation with security relevance
  - Security Incident
    - Occurrence of one or more unexpected or unwanted security events, which have a **significant probability of compromising the operation of the organization** and threaten the information security.

(Bosworth, 2002)

InfoSec fundamental concepts

- Terms and definitions (ISO/IEC 27000)
  - Controls
    - '*means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. Control is also used as a synonym for safeguard or countermeasure*'
  - Risk
    - *'Effect of uncertainty on objectives*'
      …'*An effect is a deviation from the expected — positive or negative'*
      … 'Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood'
      …

(ISO 27000, 2012)

InfoSec fundamental concepts

- **Security objectives** – preservation of certain information properties (or attributes) :
  - C **Confidentiality**
    - Restricted access to legitimate users
  - I **Integrity**
    - Content is not modified unexpectedly
  - A **Availability**
    - Accessible when needed
  - Authenticity
    - Unambiguous identification of the **responsible**
  - Utility
    - It serves the **purpose** for which it was created
  - Possession
    - Sole control by the **holder**

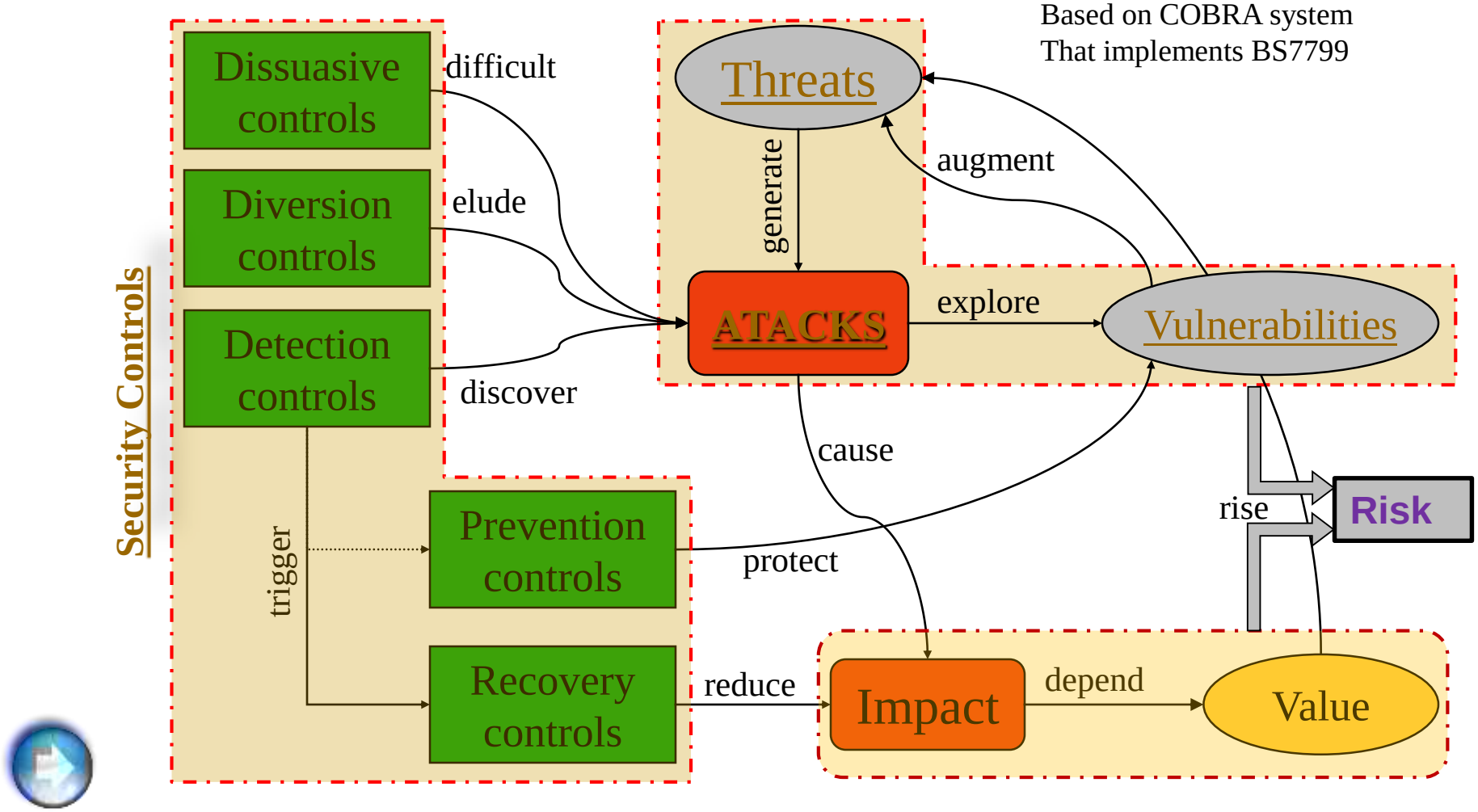
Integrity

Availability?!

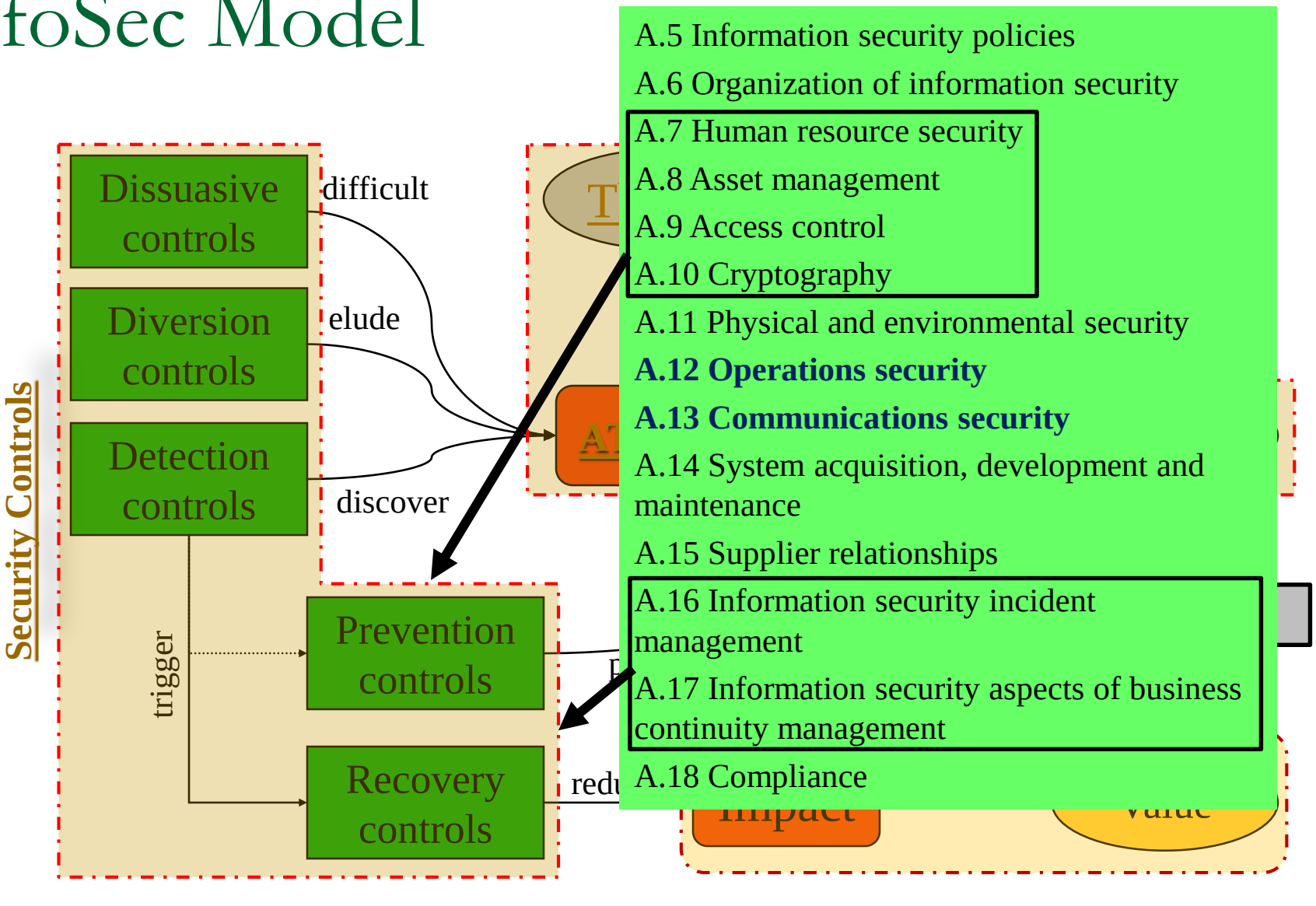
Availability

Confidentiality?!

InfoSec Model



InfoSec Model



Threat Landscape

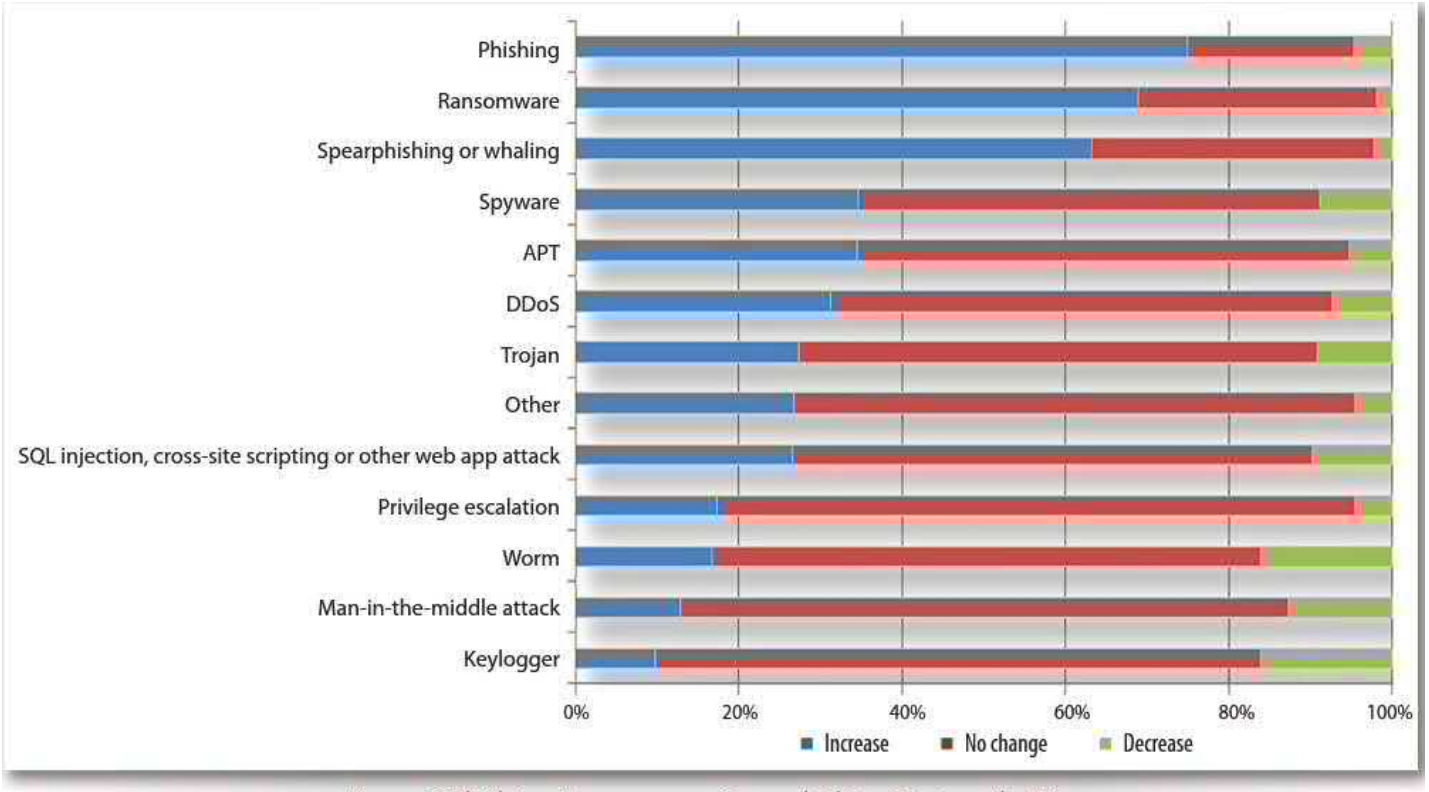


Figure 5. Phishing, Ransomware, Spearphishing Most on the Rise

Key Findings

How Attackers Get into User Endpoints

75% of identified, impactful threats initially entered via email attachment

46% of attacks were executed by users clicking web links in email

41% also experienced attacks involving web drive-by or downloads

How Attackers Bypass Endpoint Defenses

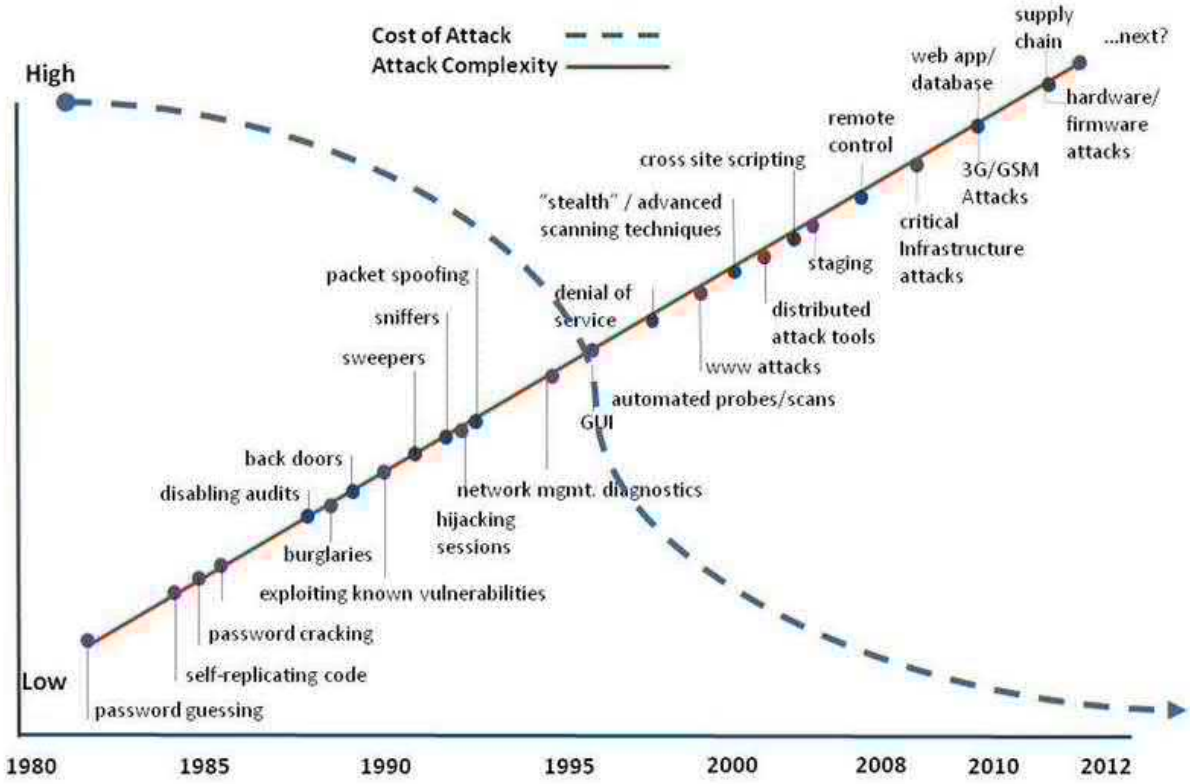
48% through user error

38% through social engineering

37% through zero-day/unknown

Exploits at the Endpoint: SANS 2016 Threat Landscape Survey

Threat Landscape

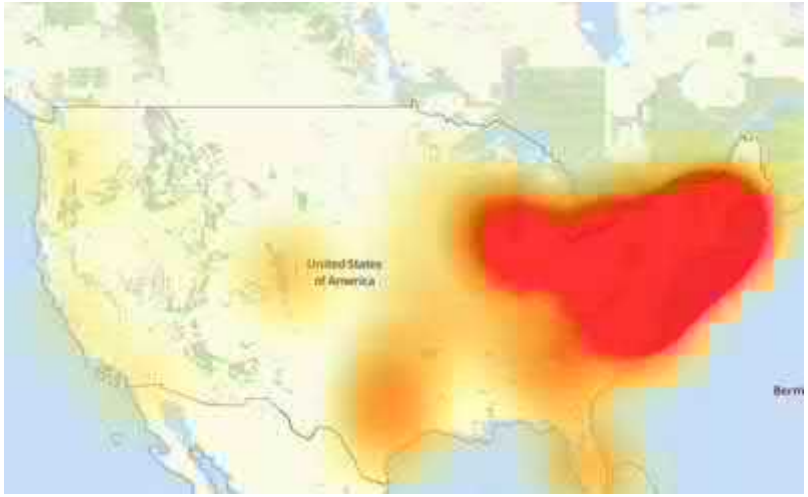


Fonte: *infosecurityinc.net/...-/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-Increasing-Complexity4.jpg*

Threat Landscape

Denial-of-service attacks are shutting down major websites across the internet

- Starting at **11:10 UTC on October 21th-Friday 2016** we began monitoring and mitigating a DDoS attack against our Dyn Managed DNS infrastructure. Some customers may experience increased DNS query latency and delayed zone propagation during this time. Updates will be posted as information becomes available.
- …
- **The Department of Homeland Security is reportedly investigating the incidents**.
- Several other websites were shut down as an apparent result of the attack. Among those appeared to be Reddit, Airbnb, Tumblr, Amazon, and The New York Times, although the final list of those affected seems to be much longer.
- …
- Update October 21st, 9:49AM ET: In another update, Dyn says the issues have been resolved.
- Update October 21st, 1:02PM ET: Dyn now writes it is once again under attack.
- Update October 21st, 4:28PM ET: Dyn reportedly hit by a third DDoS attack.

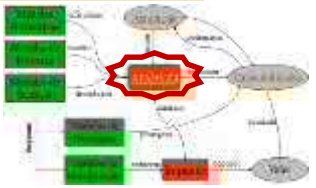


SOURCE: Dyn

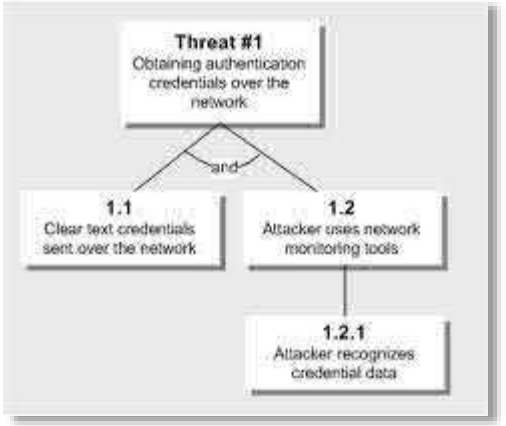
Threats

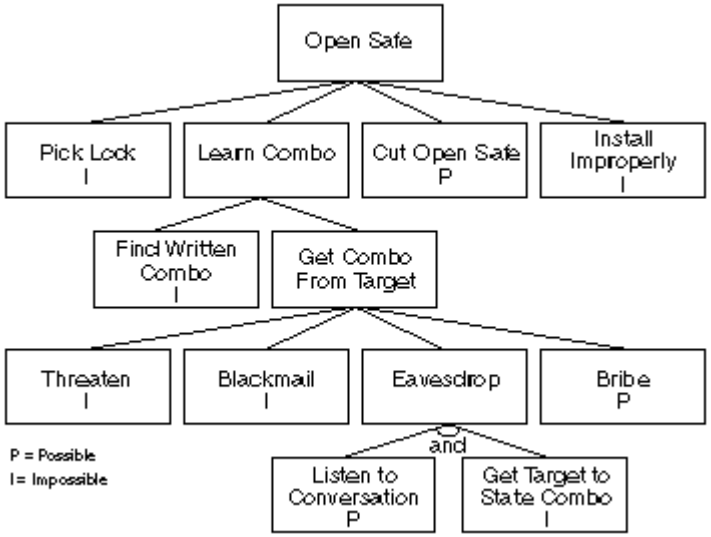
- What threats impend on (critical) resources?
  - Availability (and Utility) – **Interruption**
    - Destruction, damage, or contamination
    - Refusal or delay in access
    - Dislocation or obscuration
  - Integrity (and Authenticity) – **Modification / Fabrication**
    - Insert or production of false data
    - Replacement, removal, separation or reorganization
    - Representation or encoding
    - Repudiation
  - Confidentiality (and Possession) – **Interception**
    - Illicit copy, observation, monitoring, or inference
    - Unwanted transfer of control or custody
    - Disclosure (in particular by legitimate users, by negligence or fraud)

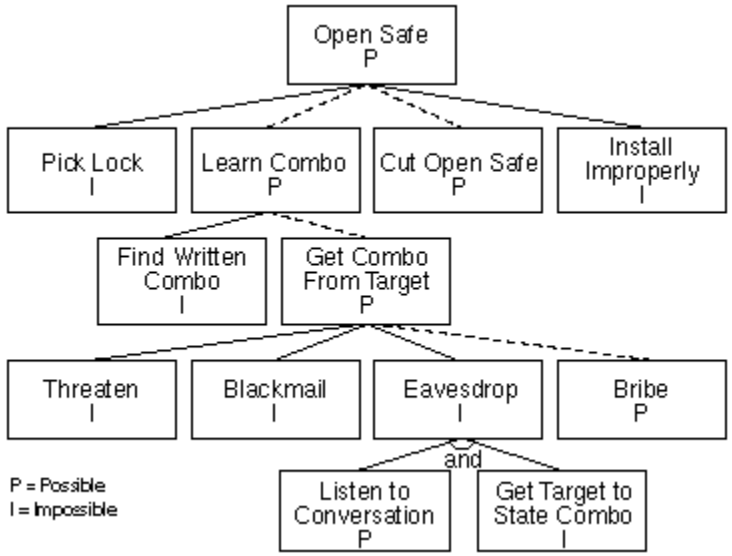
Attacks

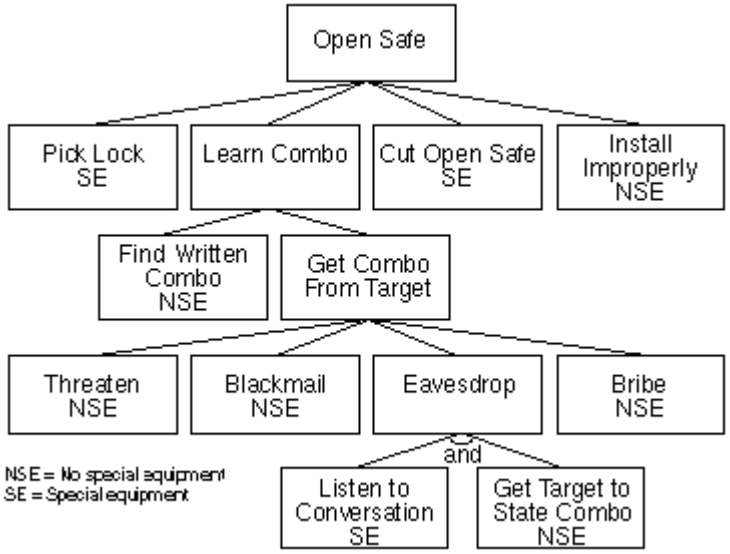


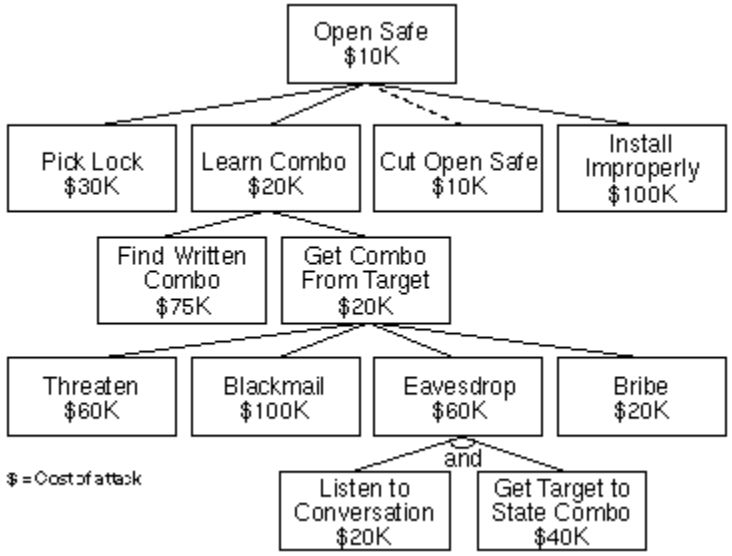
- An attack (or attacker) appears when there is:
  - ***Method***: knowledge, skills and tools to exploit vulnerabilities
  - ***Opportunity***: time and conditions to access
  - ***Motive***: a reason to carry out the attack
- A well known analysis model: Tree Modeling
  Moore, AP (2001)
  Tool: AttackTree++





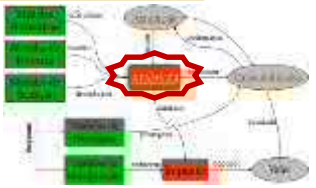






https://www.schneier.com/paper-attacktrees-ddj-ft.html

Well known attacks



- Denial of Service (DoS/DDoS)
- Spam
- Mail Bombing
- Pharming
- Social Engineering
- Hoaxes and Phishing
- Malicious code (virus; Trojans; worms; ram…)
- Back Doors
- Password Crack
- Man-in-the-Middle (or Hijacking)
- Spoofing
- Sniffers

External (very difficult to avoid)

External (targeted to users)

Internal or external (affect machines)

Internal (require access to LAN)

Well known attacks

- Harder to recognize attacks:
  - Human error
  - Failures in the and the analysis and design of Information Systems
  - Violation of safe places by "trustable people"
  - Intrusions
  - Natural disasters
- Some important efforts to "normalize" the description of attacks:
  - http://capec.mitre.org/data/index.html

Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Home > CAPEC List | Search by ID: Go

About CAPEC
Documents
Glossary
FAQs
CAPEC List
Search
Review
Downloads
Documentation
Release Notes
Archive
Submit Content
Community
Use & Citations
Related Activities
Discussion List
Contact Us
Compatibility
Program
Requirements
Participants
Make a Declaration
News & Events
Calendar
Free Newsletter
Search the Site

CAPEC List Version 2.6

Total Attack Patterns: 463

Search CAPEC | Review CAPEC List | Downloads | Schema Documentation | Release Notes | Archive

The Common Attack Pattern Enumeration and Classification (CAPEC™) effort provides a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy. The entire list of CAPEC entries developed to date is accessible below for review or download.

Search CAPEC

Easily find a specific attack pattern by performing a search of the CAPEC List by keywords(s) or by CAPEC-ID Number. To search by multiple keywords, separate each by a space.

Google™ Custom Search Search ×

BACK TO TOP

Review CAPEC List

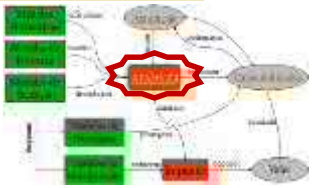
A number of review methods have been produced to help navigate the list including: by hierarchical representation, by relationships to external factors, and by relationships to specific attributes. Each of these methods provides a unique view into the CAPEC List to help you find a specific attack pattern or to show the relationships amongst different patterns.

By Hierarchical Representation (Graph)

A "graph" is a hierarchical representation of attack patterns based on a specific vantage point. The hierarchy often starts with a category, followed by a standard/meta attack pattern, and ends with a detailed attack pattern.

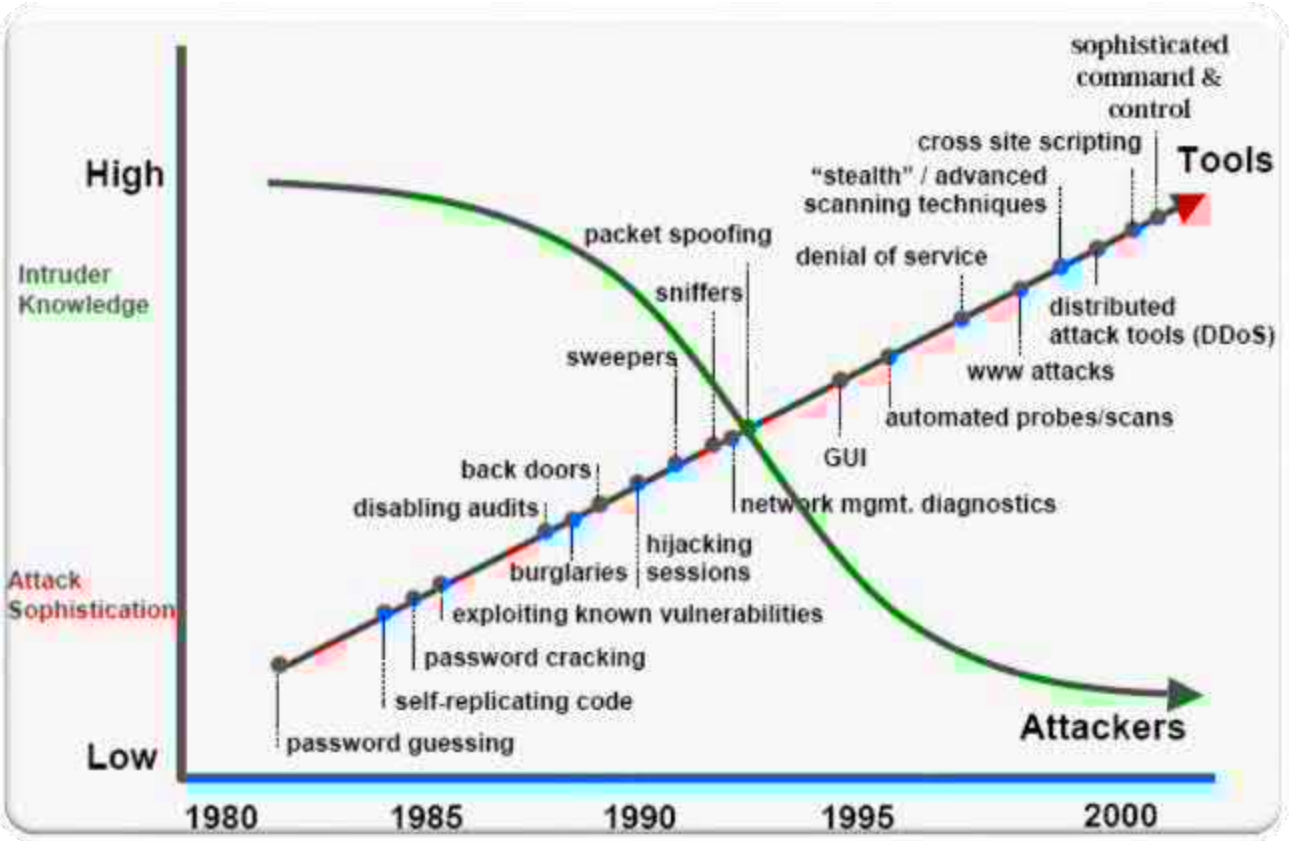
Title	Review	Download
Mechanisms of Attack	View	XML.zip
Domains of Attack	View	XML.zip

Attackers



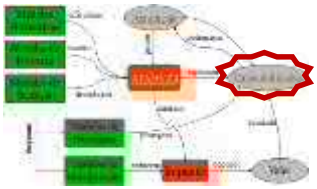
- Concerning Information Systems, who are the attackers?
  - Amateur: driven by curiosity and the prospect of social role
  - *Crackers* and *Hackers*: often students, with high technical expertise; typically they want to take over computers, for mere pleasure or for any economic advantage; often organized in Internet communities
  - Criminals: there is some evidence that organized crime and international groups have been increasing its involvement in computer crime (the profit opportunities are increasing)
  - Terrorists: increasingly evident and at various levels
    - Targeting ISs as critical infra-structures
    - Using SIs as a mean of propaganda
    - Using SIs as a mean of attack

Attacks and attackers



Fonte: H.F. Lipson, CERT Coordination Center, CMU/DEI-2002-SR-009

Vulnerabilities



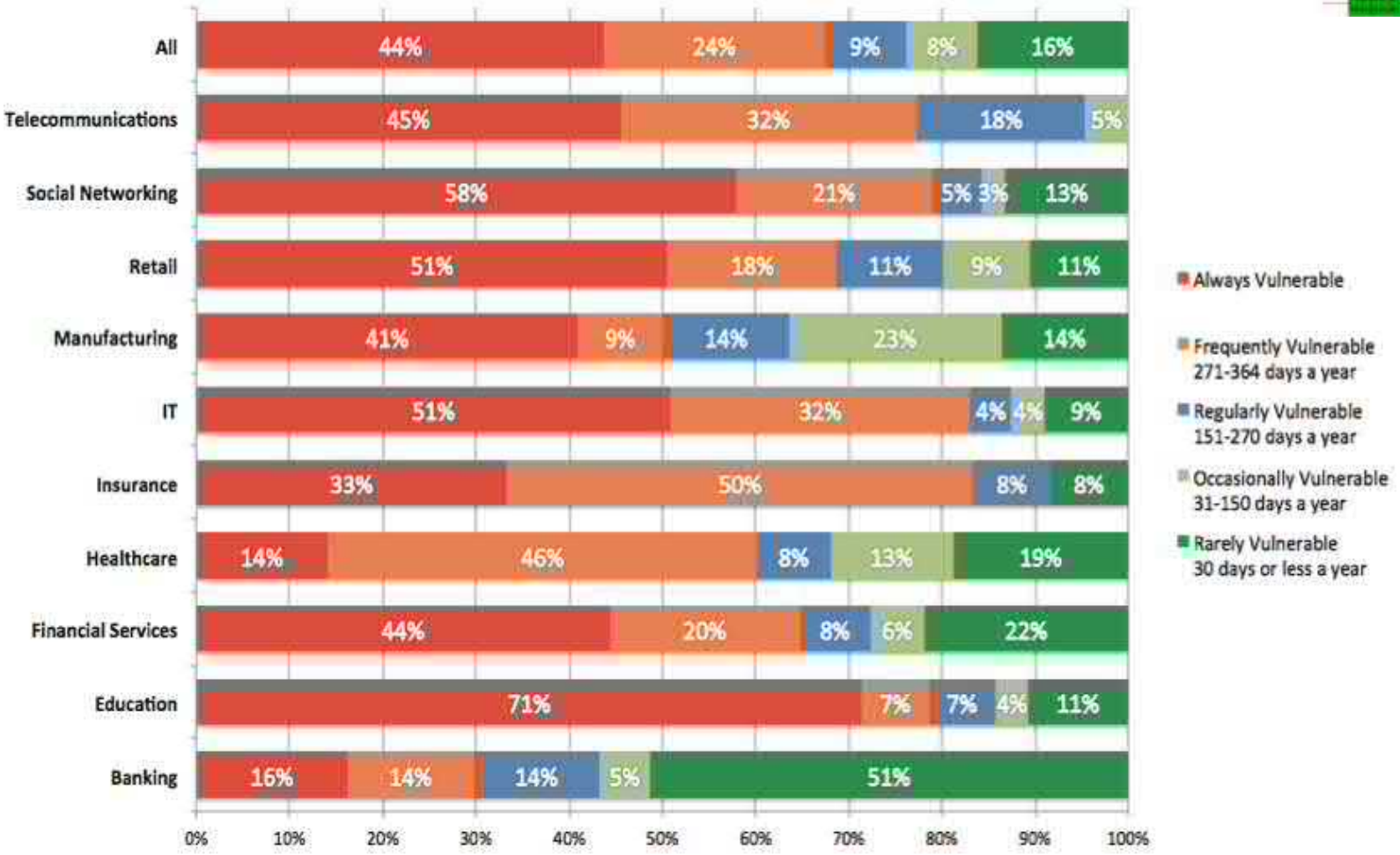
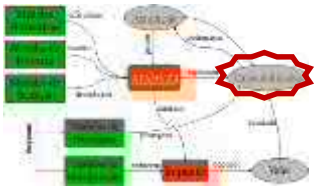


Figure 2. Window of Exposure by Industry (2010)

Source: http://jeremiahgrossman.blogspot.pt/2011/03/11th-whitehat-website-security.html

Vulnerabilities



- Vulnerabilities origin
  - An IS is generally made of hardware (execute simple instructions and transactions), software (create operations as logical sequences of instructions and transactions) and data (information)
  - Computer Systems
    - Complexity, degree of autonomy, miniaturization and dematerialization, ubiquity, interconnect, are factors that contribute to increased vulnerability
    - Vulnerabilities detection/management support
      - Tools like NESSUS, SAINT, Grabber,…
      - Resources like CVS, NIST, SANS

CVE LIST | COMPATIBILITY | NEWS — JULY 30, 2014 | SEARCH

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

CVE-IDs have a new format –**Click here to see the new format**

TOTAL CVEs: 63391

HOME > CVE LIST

About CVE
Terminology
Documents
FAQs

CVE List
CVE-ID Syntax Change
About CVE Identifiers
Search CVE
Search NVD
Updates & RSS Feeds
Request a CVE-ID

CVE In Use
CVE-Compatible Products
NVD for CVE Fix Information
CVE Numbering Authorities

News & Events
Calendar
Free Newsletter

Community
CVE Editorial Board
Sponsor
Contact Us

Search the Site
Site Map

CVE List Main Page

CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

IMPORTANT: CVE-ID Syntax Change took effect on January 1, 2014.

National Vulnerability Database

Full database functionality for the CVE List is provided through MITRE's partnership with the U.S. National Vulnerability Database (NVD).

- CVE Search on NVD
- CVE Fix Information
- CVE SCAP Mappings

CVE List Master Copy

The master copy of the CVE List is maintained for the community by MITRE on this public CVE Web site.

- Search Master Copy of CVE
- Download CVE List
- View CVE List

You may download the CVE List, copy it, redistribute it, reference it, and analyze it, provided you **do not modify** CVE itself as per our Terms of Use. CVE and NVD are both sponsored by the office of Cybersecurity and Communications at the U.S. Department of Homeland Security.

CVE List
CVE-ID Syntax Change
CVE Usage of CVRF
About CVE Identifiers
Editorial Policies
Data Sources/Product Coverage
Reference Key/Maps
Search Tips
Updates & RSS Feeds
Request a CVE Identifier

ITEMS OF INTEREST
Terminology
NVD

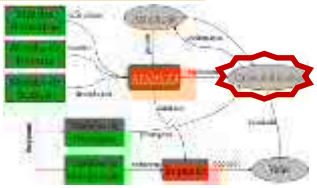
Page Last Updated: January 22, 2014

MITRE

Site Map
Privacy policy
Terms of use
Contact us

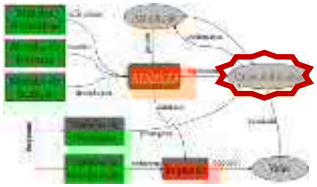
Member of Making Security Measurable™

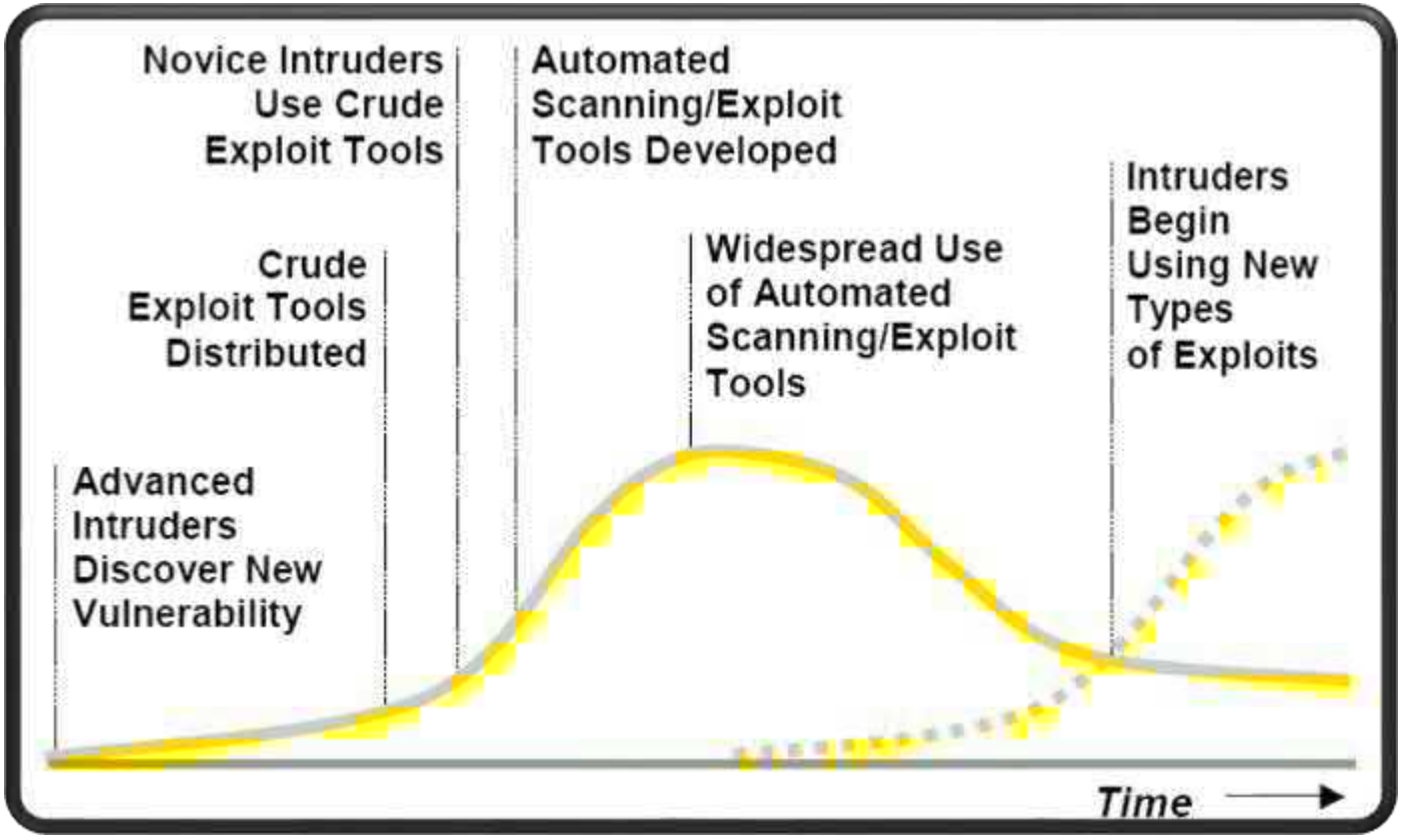
Vulnerabilities



- Vulnerabilities origin (cont)
  - Inadequate user behaviors
- Vulnerabilities recognition can derive from reflection on what can go wrong
  - Interruptible
  - Modifiable
  - “Manufacturable”
  - “Interceptable”
  - Incomplete (incomplete or misunderstood specifications)
  - …

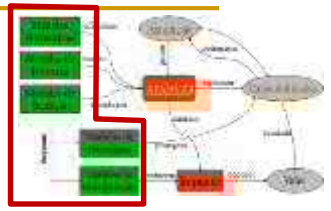
Cycle of vulnerabilities exploitation





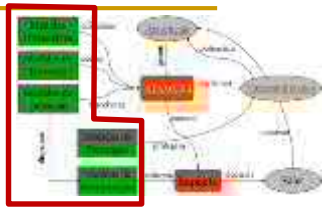
Fonte: H.F. Lipson, CERT Coordination Center, CMU/DEI-2002-SR-009

Security Controls



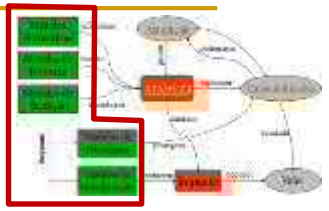
- Security properties driven classification
  - CIA oriented
    - User and organization policies
    - Access Control
      - Users; Networks; Applications; Physical
    - Antivirus and antimalware
    - Intrusion Detection Systems (IDS)
  - CI oriented
    - Cryptography, Digital Signatures; Digital Certificates
  - IA oriented
    - Backups
  - A oriented
    - Disaster Recovery
    - Redundancy (data and services)
  - I oriented
    - Integrity verifiers

Security Controls



- **Policies**, **procedures**, **guides**, good practices, **hardware and software devices** or even organizational initiatives aiming to manage risk …
- Organizational oriented
  - **Resources** are main targets; objectives: **what to assure**
- Security "mechanisms"
  - Technologies or actions to implement security policies
  - Standards define mainly security mechanisms:
    - http://www.27000.org/index.htm
    - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-12.pdf
    - http://www.itu.int/rec/T-REC-X.800-199103-I/en

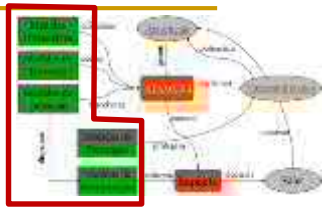
Security Controls



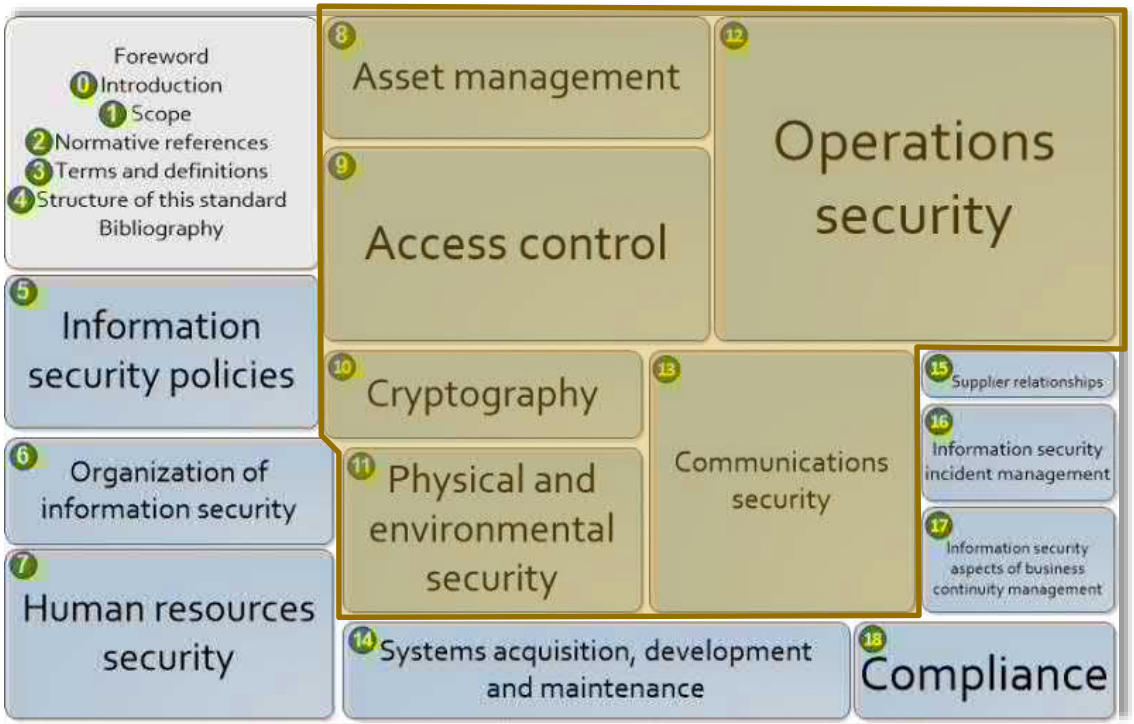
- Policies or procedures in use:
  - Password management politics – 74%
  - Inappropriate use politics – 71%
  - Education and awareness politics – 67%
  - Internet access monitoring – 65%
  - Corporate security politics – 62%
  - Risk Management practices – ≈ 55%
  - ...
  - Employing ex-hackers – 14%

Source: 2005 E-Crime Watch Survey – CSO magazine

Security Controls

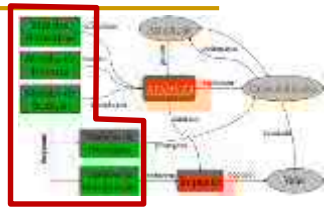


- ISO/IEC **27002:2013** (Code of Practice for InfoSec Management)
  - 14 classes (clauses) – sections 5 to 18
  - 35 control objectives
  - 114 security controls
  - About one half are technological
  - About one half are organizational or managerial

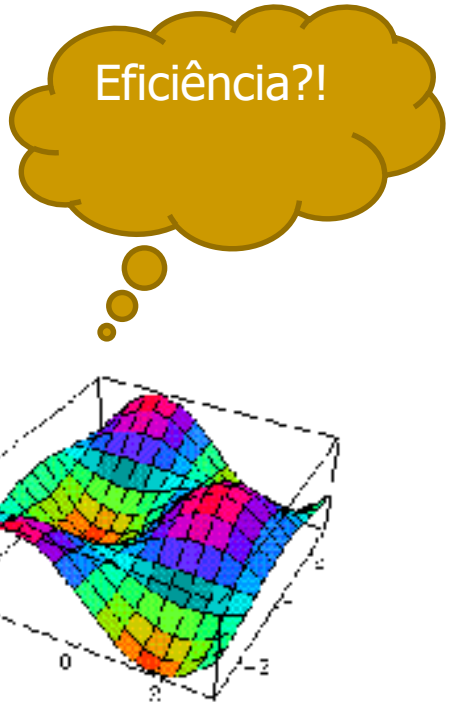


http://www.iso27001security.com/html/27002.html

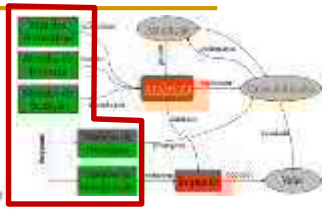
Security Controls



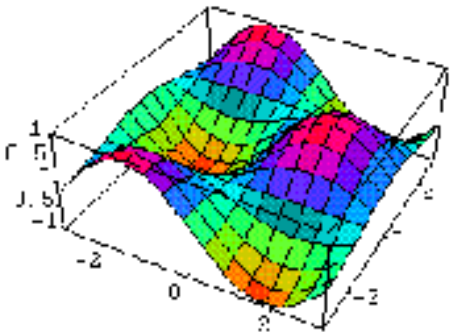
- Most used security technologies :
  - Antivirus – 97%
  - Antispam – 95%
  - *Firewalls* – 94%
  - Virtual Private Network (VPN) – 85%
  - Antispyware/adware – 80%
  - Cipher (data in transit) – 71% (↑)
  - Intrusion Detection (IDS) – 69%
  - Vulnerability scanners and patch – 65%
  - Web/URL filtering – 61%
  - Application level Firewalls – 53% (↑)
  - ...
  - PKI – 36%
  - Smartcards and other OTP devices – 36%
  - Integrated NAC solutions – 34% (↑)
  - Virtualization specific tools – 29%
  - Wireless tools – 27% (↓)
  - Biometrics – 23%



Source: CSI Computer Crime & Security Survey, 2008

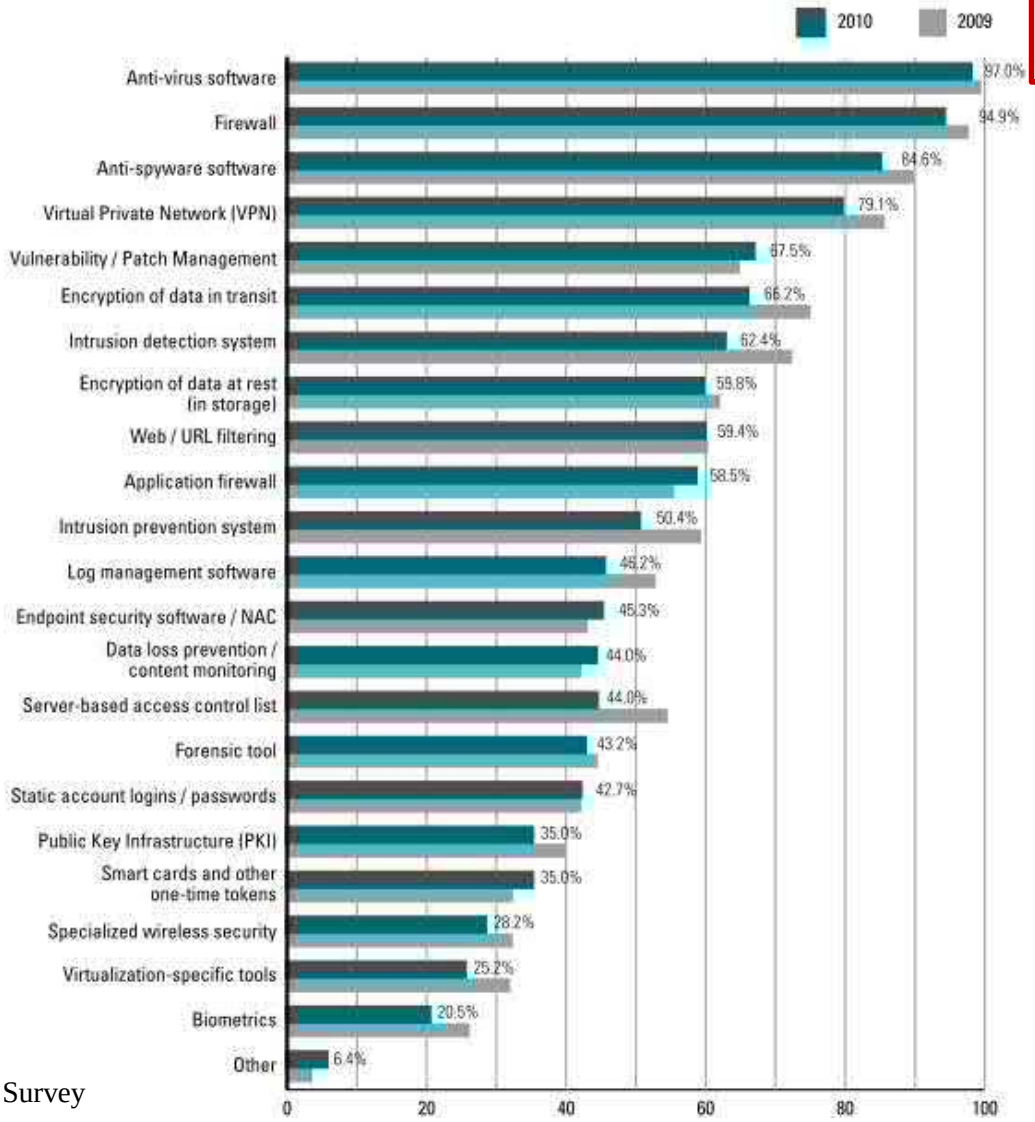


Efficiency?!



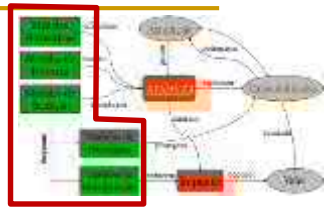
Types of Security Technology Used

By Percent of Respondents



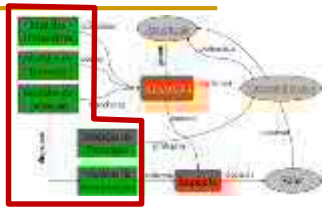
2010/2011 CSI Computer Crime and Security Survey

Controls' efficiency



- A *metagoal*
  - Awareness of the need to use - the establishment of a "safety culture"
  - Guarantee of service
  - Overlap effect of different controls
  - Periodic review
- **Principle of efficiency**: to ensure that controls produce results, they must be appropriate and used properly
- **Principle of adequate protection**: resources must be protected to a degree consistent with its **value**

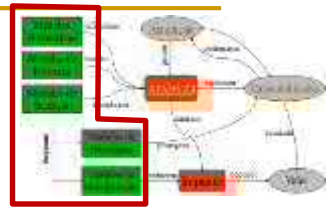
Controls' efficiency



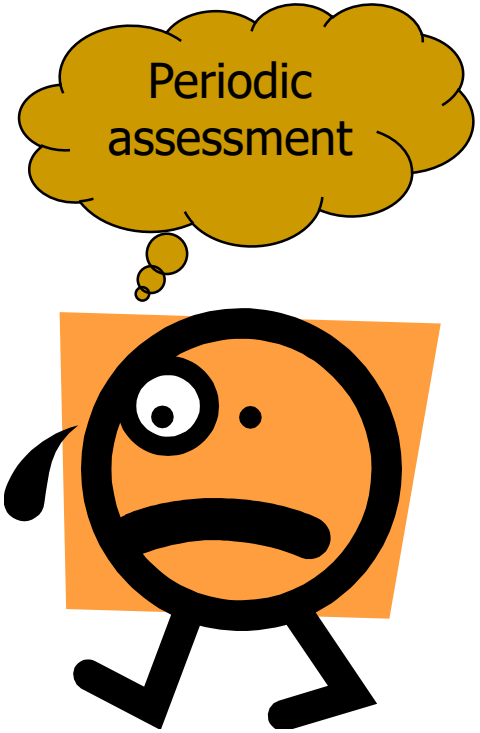
- Techniques used to evaluate efficiency
  - Internal auditing (82%)
  - Penetration test (66%)
  - Automatic tools (66%)
  - External auditing (62%)
  - Monitoring software:
    - e-mails (61%)
    - Web activity (58%)

What exactly is being measured?

Controls' effectiveness

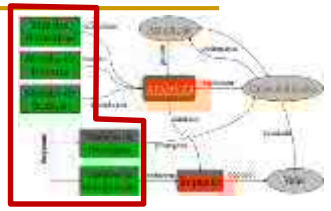


- More effective technologies:
  - *Firewalls* – 68%
  - Anti-Vírus – 66%
  - Cipher – 58%
  - Two-phase authentication – 56%
  - Intrusion Detection (IDS) – 50%
  - Physical Security – 49%
  - Network traffic monitoring – 46%
  - Spyware/Adware – 43%
  - ...
  - Manual patches – 26%



Source: 2005 E-Crime Watch Survey – CSO magazine

About metrics



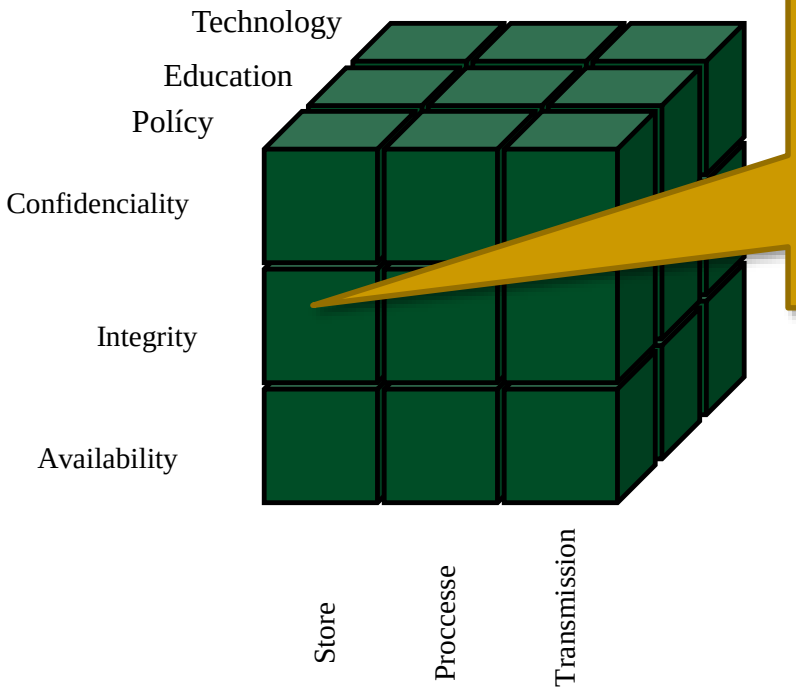
- NIST SP800-55 (*Security Metrics Guide for Information Technology Systems*) defines three metric types:
  - Implementation metrics
  - Efficacy/Efficiency metrics
  - Impact metrics

…

- A lot of (very hard) work to do ☹

InfoSec Model

CNSS Model (*McCumber Cube*) - *Committee on National Security Systems*, a NSA group (NSTISSI-4011)



Involves the need for technology to protect the integrity of the stored data:

Exemples: HIDS, integrity checker software

InfoSec Model

- The previous approaches are centered on effects, but there are other possible perspectives (e.g., centered on environmental factors):

> "*The absence of threats that can affect our expectations about information systems equivalently protected in equivalent environments.*"

(Canal, 2005)

About Models

"All Models Are Wrong But Some Are Useful"

Author: George Box