Introduction

INGI2347: COMPUTER SYSTEM SECURITY (Spring 2014)

Marco Canini

UCL Université catholique de Louvain

Lecture slides adapted from UCL INGI2347 by Gildas Avoine and Upenn CSE331 by Steve Zdancewic

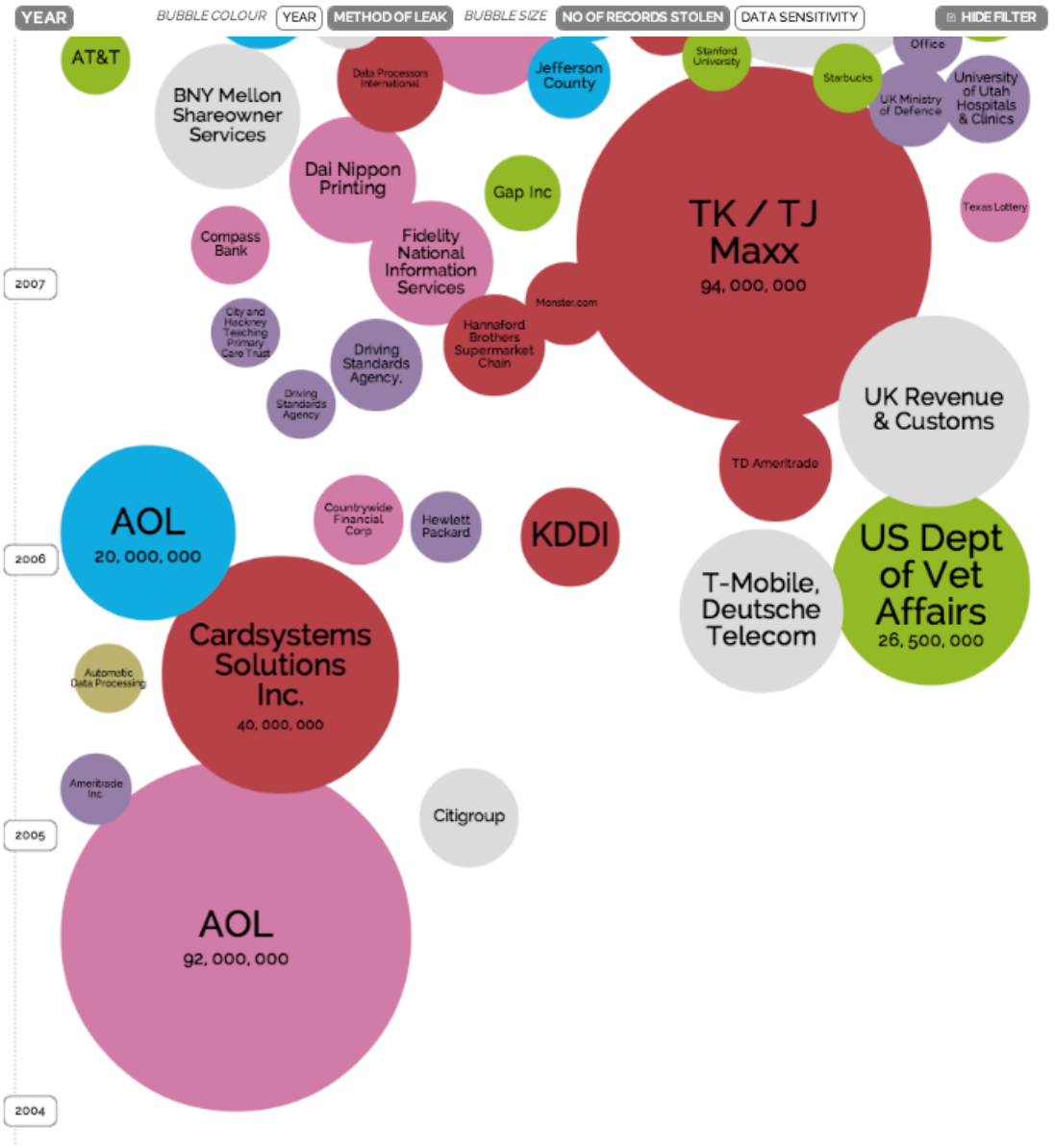
Welcome!

- My name: Marco Canini
- New faculty member at INGI
  - Supplying Gildas Avoine for this course
- Research interests:
  - Software-Defined, Reliable Networked Systems
  - Cloud Computing
  - See also: http://perso.uclouvain.be/marco.canini/

Let's start

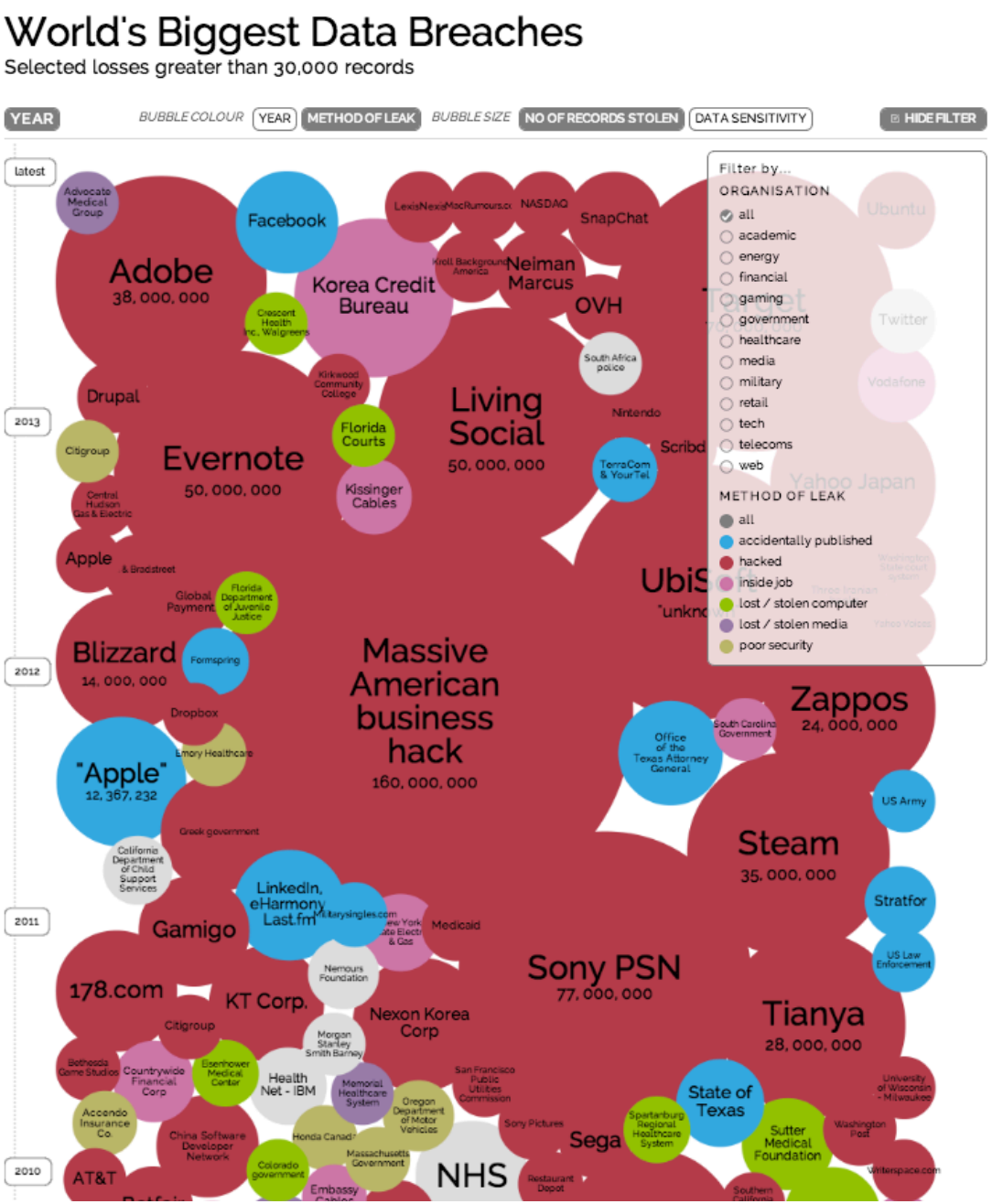
Every day news about new attacks and vulnerabilities

- Check out www.cert.org for plenty of examples



Exponential growth of security incidents over the past 25+ years

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Exponential growth of security incidents over the past 25+ years

Networked systems are more and more complex

Difficult to protect them from ever more sophisticated attacks

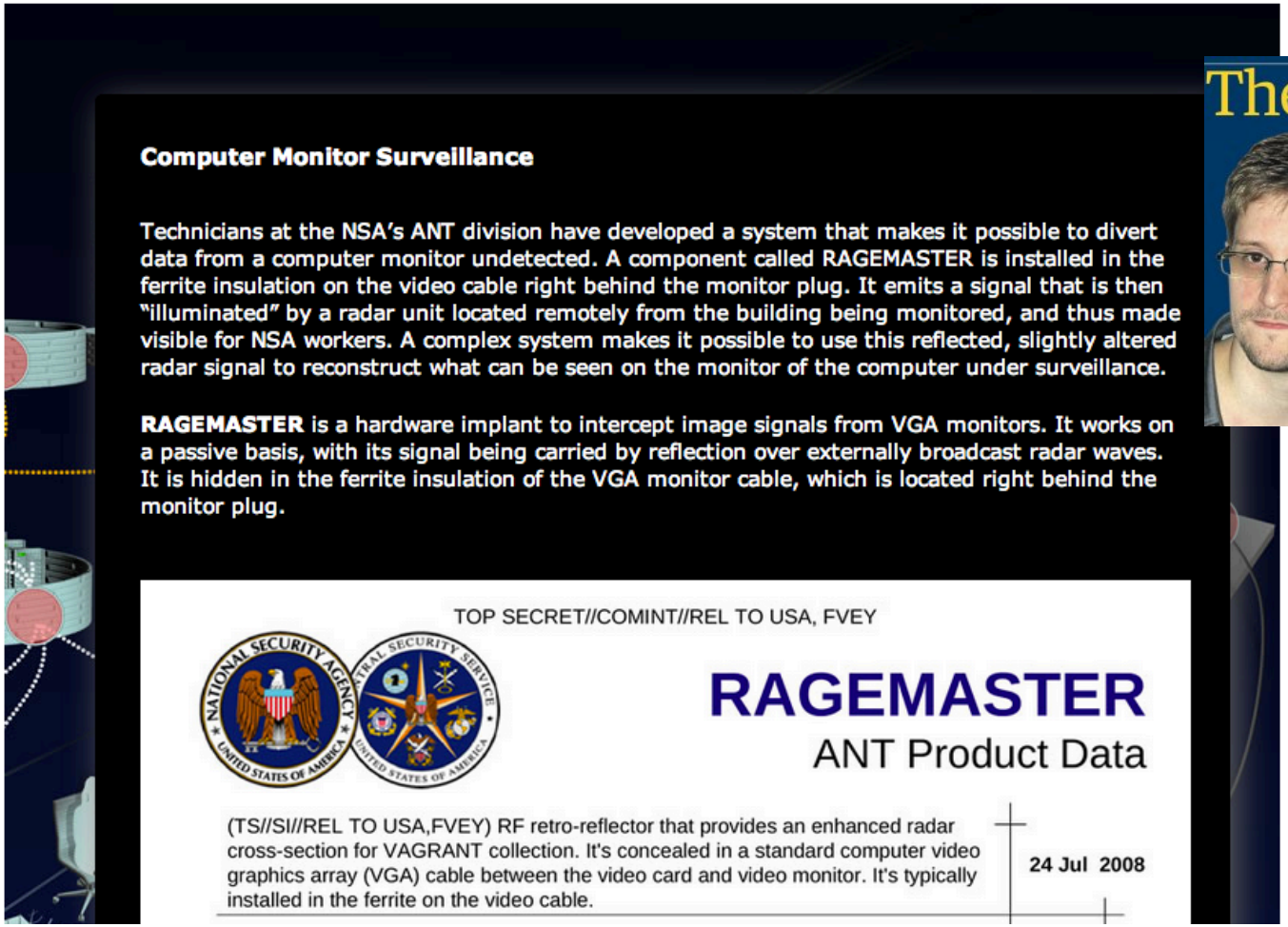
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Stuxnet

Stuxnet: Anatomy of a Computer Virus (watch at https://vimeo.com/25118844)
Direction and Motion Graphics: Patrick Clair http://patrickclair.com
Written by: Scott Mitchell
Production Company: Zapruder's Other Films.

Recently heard about NSA?

Interactive Graphic: The NSA's Spy Catalog



Checkout
"Jacob Applebaum:
To protect And Infect, Part 2"
http://youtu.be/vILAlhwUgIU

http://www.spiegel.de/international/world/a-941262.html

What is INGI2347 about?

- Wide view of security
  - Mosaic of security problems and solutions
- Objective
  - Provide basic concepts and principles for a wide spectrum of security problems
  - A base for future security specialists
  - General knowledge for non-specialists
- More descriptive than analytical
  - Technical approach

Course Contents

- Spam and Malware
- Forged E-Mail
- Network vulnerabilities
- Firewalls
- Proxies | IDS
- Cryptography | Certificates
- Passwords | Time-memory trade-off
- WEP | WPA
- IPSec | SSL/TLS
- Kerberos | PGP
- Cloud computing security
- Guest lecture: security viewed by the Compute Crime Unit

Plan for today

Lecture 1

- Introduction 
- Course logistics 

- What is security?
- CSI Survey
- Risk Analysis

Course Staff

- Marco Canini
  - Réaumur A-049, x7-4832

- Xavier Carpent (TA)
  - Réaumur A-140, x7-9102

Schedule and Rooms

- Mondays 14:00 to 16:00, BARB 11
- Tuesdays 8:30 to 10:30, BARB 20
- Check regularly the online calendar!

Language

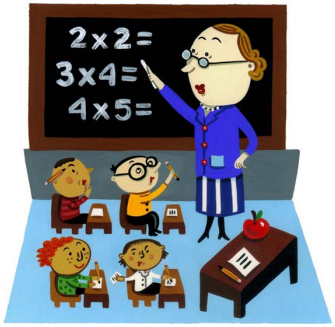
- This course – including all supports (lectures, exercises, exam) – is in English
  - French if necessary
    - If you plan to give your answers in French, contact the course staff by end of Feb

Prerequisites

- A priori Master 1st or 2nd Year
- Would like to learn basic security principles
- Background knowledge in computer networks
  - (e.g., INGI2141 or ELEC2920)
  - SMTP, Telnet, IP, TCP, UDP, ARP, MAC, OSI layered model
  - Reference: "Computer Networks" by Andrew Tanenbaum
- Basic programming skills
  - (FSAB1401 or equiv.)
  - Familiarity with Java or C/C++, Python, bash scripting…

Teaching Activities

- Lectures
  - No lecture notes but reference book



http://peerprograms.ubc.ca/2011/01/12/what-i-learned-in-class-today/

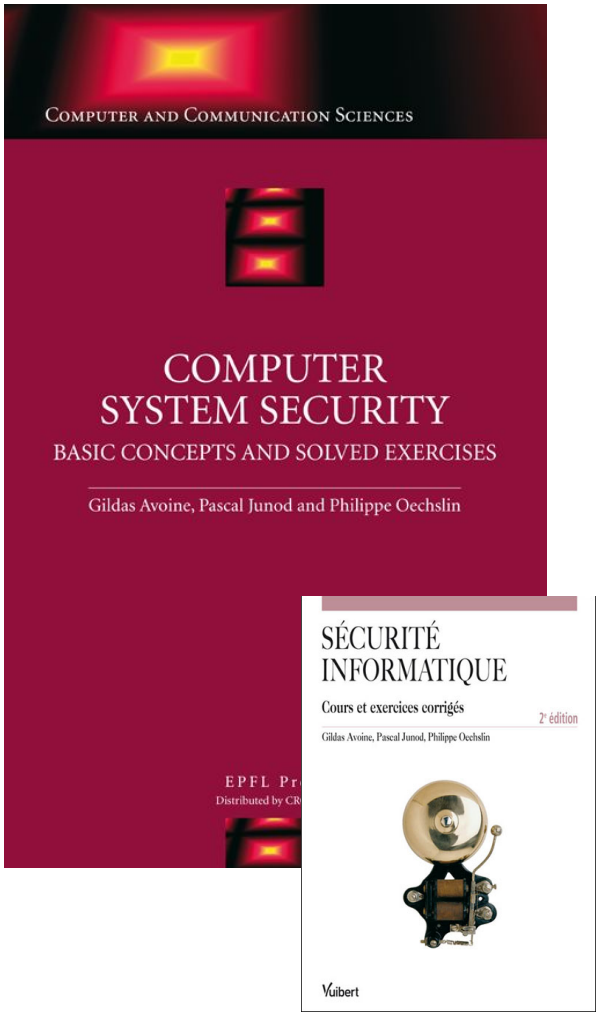
- Exercises (classroom or computer room)
- Challenges (taken into account for grading)

Lectures

- Be on time!

- If you come, this means you studied the previous lecture

Textbook



- "Computer System Security, Basic Concepts and Solved Exercises", Avoine, Junod, and Oechslin, 270 pages, EPFL Press & CRC Press, English, 978-1420046209, 2007
- Book is not mandatory
- Available in the library or at the bookstore Agora
- 2nd version 2010 in French available
- INGI2347 covers chapters 1 to 7

In-class Exercises

- Exercise and solution sheets provided (printed)
- Do not distribute (copyrighted)

Challenges

- Practical exercises to be done «at home»
  - Challenge on TMTO evaluated in INTEL room
- Challenges announced during the lectures or the exercises, solved during the exercises
- 1 to 4 weeks to solve each challenge
- **3 challenges** over this term; **all mandatory**
- Each challenge gives **2 pts**
- **No collaboration on individual homework**
  - (remember when posting messages on Piazza)

Challenges (2013/14)

Number	Points	Announced	Deadline	Content
Challenge 1	2	4 Feb	24 Feb (23:59)	Web Security
Challenge 2	2	18 Mar	3 Apr (23:59)	Password Cracking
Challenge 3	2	18 Mar	23 Apr (23:59)	Time-memory Trade-off

June Examination

- Challenges (6 pts)
  - The 3 challenges are considered

- Written examination (14 pts)
  - 3 hours, **closed book**

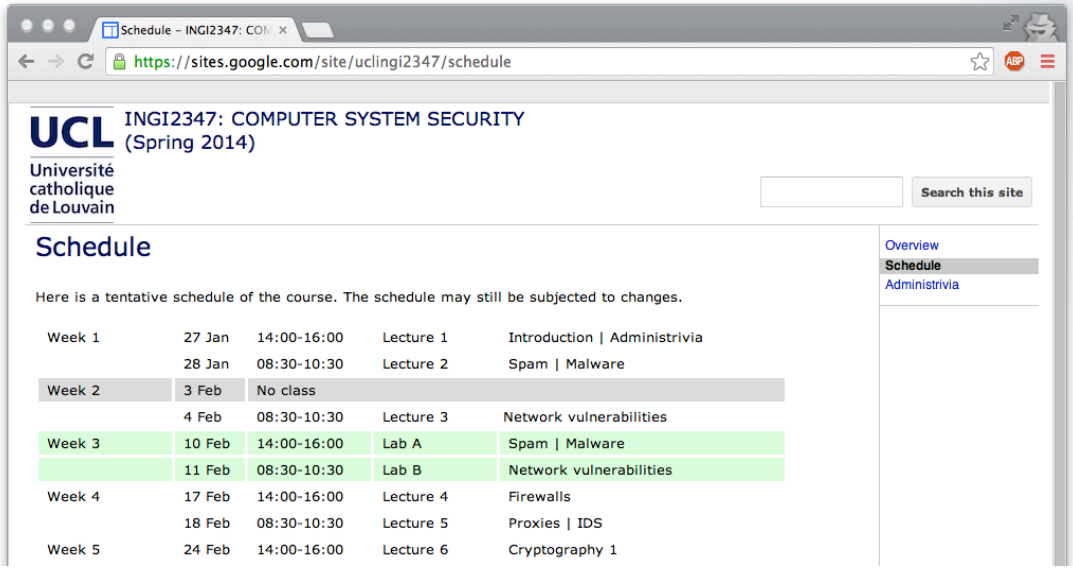
September Examination

- Challenges (6pts)
  - The 3 challenges are considered
- Oral examination (14 pts)
  - **Closed book**
  - Preparation (40'), presentation (20')
- If the challenges decrease the grade, then the oral examination only is considered
  - Grade = max(grade oral examination,
    grade oral examination * 14/20 + grade challenges)

Course website

https://sites.google.com/site/uclingi2347/

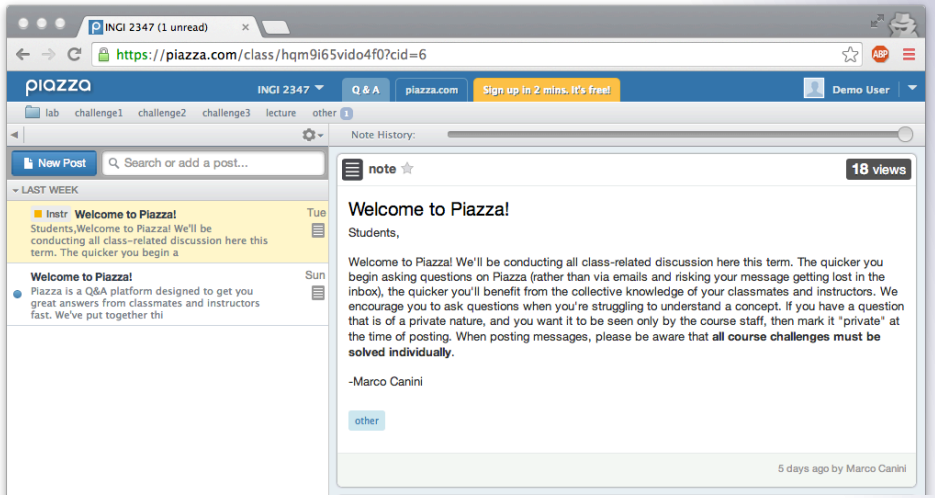
- Course schedule
- Slides will be available on the web site
  - Linked to from the course schedule page



Course discussion group

- We will be using piazza for discussions related to this course
  - The TA and I will read the posts and respond to questions
  - Recall: no collaboration on challenges
    - Consider posting as private message to course staff only
- Piazza will also be used for
  - **Announce Challenges**
  - Corrections/clarifications
- Got the invite?
  - If not, enroll officially
- Please sign up at https://piazza.com/uclouvain.be/spring2014/ingi2347

TODO



Ethics

- This is a course on computer and network system security. Although the course is primarily concerned with techniques that are designed to ensure security of such systems, a proper understanding of those systems requires that you be versed in their vulnerabilities and failings as well. Nevertheless, unless you have explicit written authorization from the owner and operators of a computer network or system, you should never attempt to penetrate that system or adversely affect that system's operation. Such actions are a violation of the law and UCL's policy.
- You are required to read and understand UCL's rules available at http://www.uclouvain.be/22811.html
- If you would not be able to read or understand these rules, you must contact the teaching assistant or the lecturer

Supplementary reading (not mandatory)

- *Security Engineering* by Ross Anderson
  - Freely available online: http://www.cl.cam.ac.uk/~rja14/book.html
- *Building Secure Software: How to Avoid Security Problems the Right Way* by John Viega and Gary McGraw
- *The Protection of Information in Computer Systems* by Saltzer and Schroeder, 1975

What do we mean by security?

What do we mean by security?

- Information security is larger than computer security
  - Defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction [Wikipedia]
- What does it mean for a computer system to be secure?

What do we mean by security?

- What does it mean for a computer system to be secure?
  - The system only does what it is expected to
  - Should prevent unathorized use
  - What is “unathorized”?
  - What about spam?

When is a computer system secure?

- When it does exactly what it should?
  - Not more
  - Not less
- But how do we know what a system is supposed to do?
  - Somebody tells us?
    - But do we trust them?
  - We write the specification ourselves?
    - How do we verify that the software meets the specification?
  - We write the code ourselves?
    - But what fraction of the software you use have you written?
    - Can you trust the hardware it runs on?

When is a computer system secure?

- 2nd try: A program is secure when it doesn't do something it shouldn't
- Easier to specify a list of "bad" things:
  - Delete or corrupt important files
  - Crash my system
  - Send my password or credit card details over the Internet
- But... what if most of the time the program doesn't do bad things, but occasionally it does? Is it secure?
- Difficult to verify that a system does what it is expected to, impossible to verify that it does not what it is not expected to

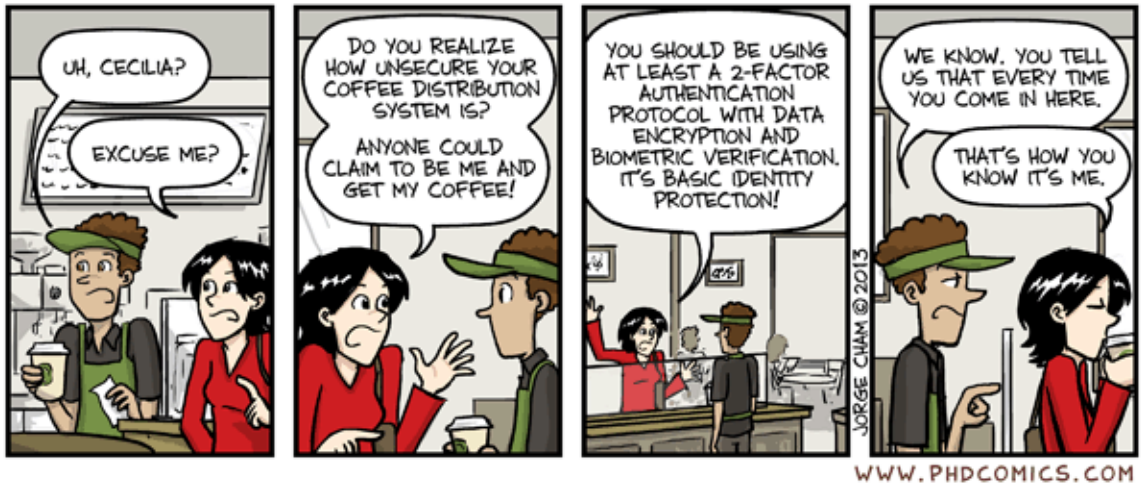
"Security is mostly a superstition […]"

– Helen Keller (1880-1968), American writer and activist

- Security is all about trade-offs
  - Performance
  - Cost
  - Usability
  - Functionality
- The right question is: how do you know when something is secure enough?
  - Still a hard question
  - Requires understanding of the trade-offs involved

How to think about trade-offs?

- What are you trying to protect? How valuable is it?
  - Nuclear missile launch station vs. … coffee machine



- In what way is it valuable?
  - May be important only to one person (e.g. private e-mail or passwords)
  - May be important because accurate and reliable (e.g. bank's accounting logs)
  - May be important because of a service it provides (e.g. Google's web servers)

Classic CIA triad

- **Confidentiality**
  - Unathorized disclosure of information
    - E.g. a credit card transaction system attempts to enforce confidentiality by encrypting credit card details over the Internet and in the transaction processing network
- **Integrity**
  - Unathorized information modification
    - E.g. traditional Unix file permissions can be an important factor in single system measures for protecting data integrity
- **Availability**
  - Unathorized denial of use
    - High availability systems aim to remain available at all times, preventing disruptions due to power outages, upgrades, hardware failures, Denial of Service (DoS) attacks, …

Example security techniques

- Verifying the identity of a prospective user by demanding a password
  - Authentication
- Shielding the computer to prevent interception and subsequent interpretation of electromagnetic radiation
  - Covert channels
- Enciphering information sent communication channels
  - Cryptography
- Locking the room containing the computer
  - Physical aspects of security
- Controlling who is allowed to make changes to a computer system
  - Social aspects of security

Security goals

- Prevent common vulnerabilities from occurring (e.g. buffer overflows)
  - Recover from attacks
- Traceability, accountability and auditing of security-relevant actions
  - Monitoring
- Detect attacks
  - Privacy, confidentiality, anonymity – Protect secrets
- Authenticity
  - Needed for access control, authorization, etc.
- Integrity
  - Prevent unwanted modification or tampering
- Availability and reliability
  - Reduce risk of DoS

CSI Survey

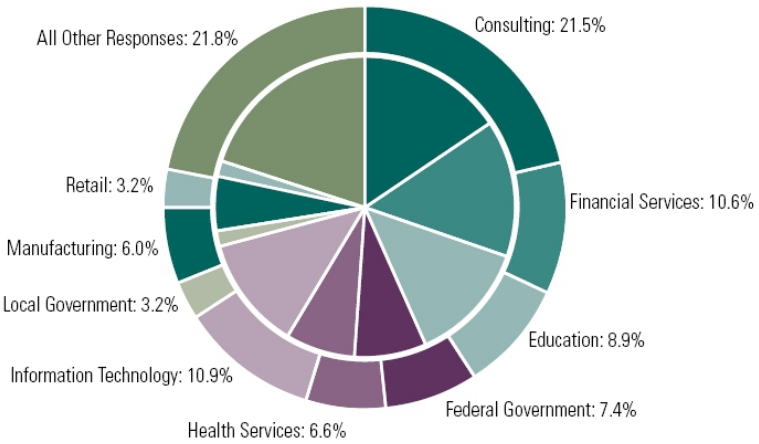
"For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations"

- Checkout http://www.gocsi.com/

Statistics: Respondents' Profile

Respondents by Industry Sector

2010 figures on outside, 2009 figures on inside

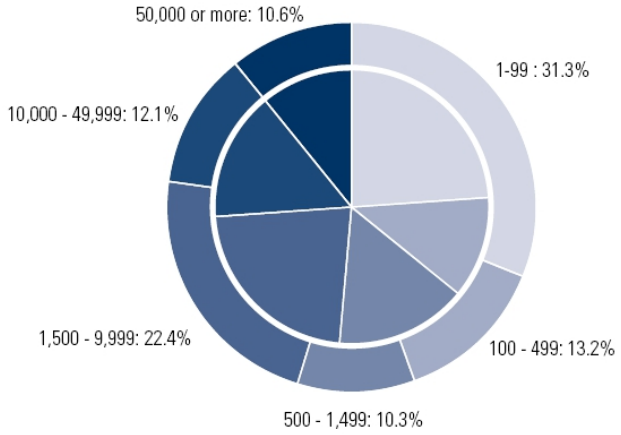


2010 CSI Computer Crime and Security Survey

2010: 349 Respondents

Respondents by Number of Employees

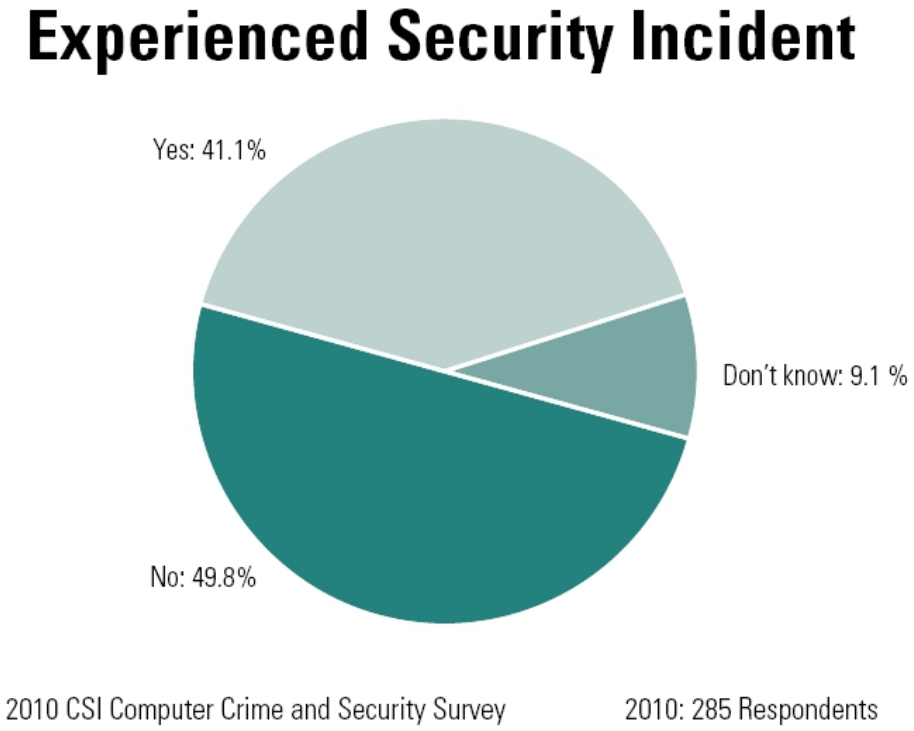
2010 figures on outside, 2009 figures on inside



2010 CSI Computer Crime and Security Survey

2010: 348 Respondents

Statistics: Security Incidents



Statistics: Types of Attacks

Types of Attacks Experienced
By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e., pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	13%
System penetration by outsider	option altered in 2009				14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%	5%

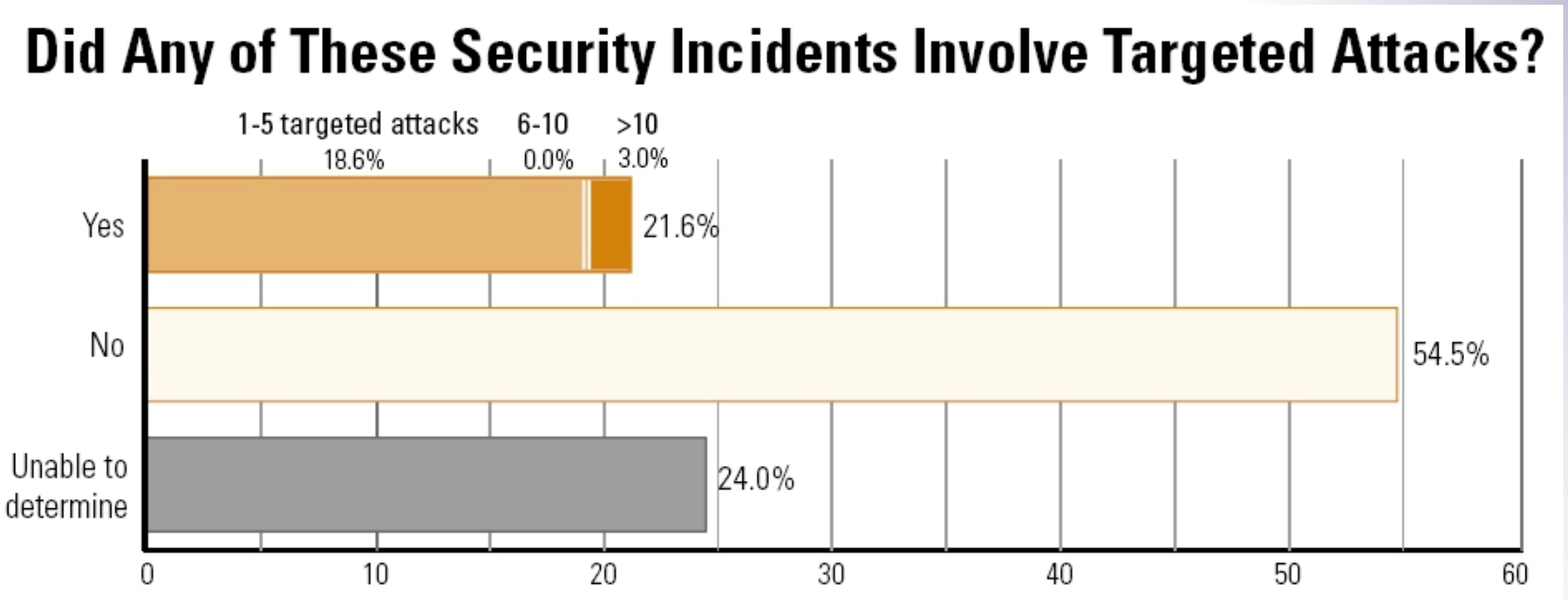
2010 CSI Computer Crime and Security Survey — 2010: 149 Respondents

Statistics: Insiders

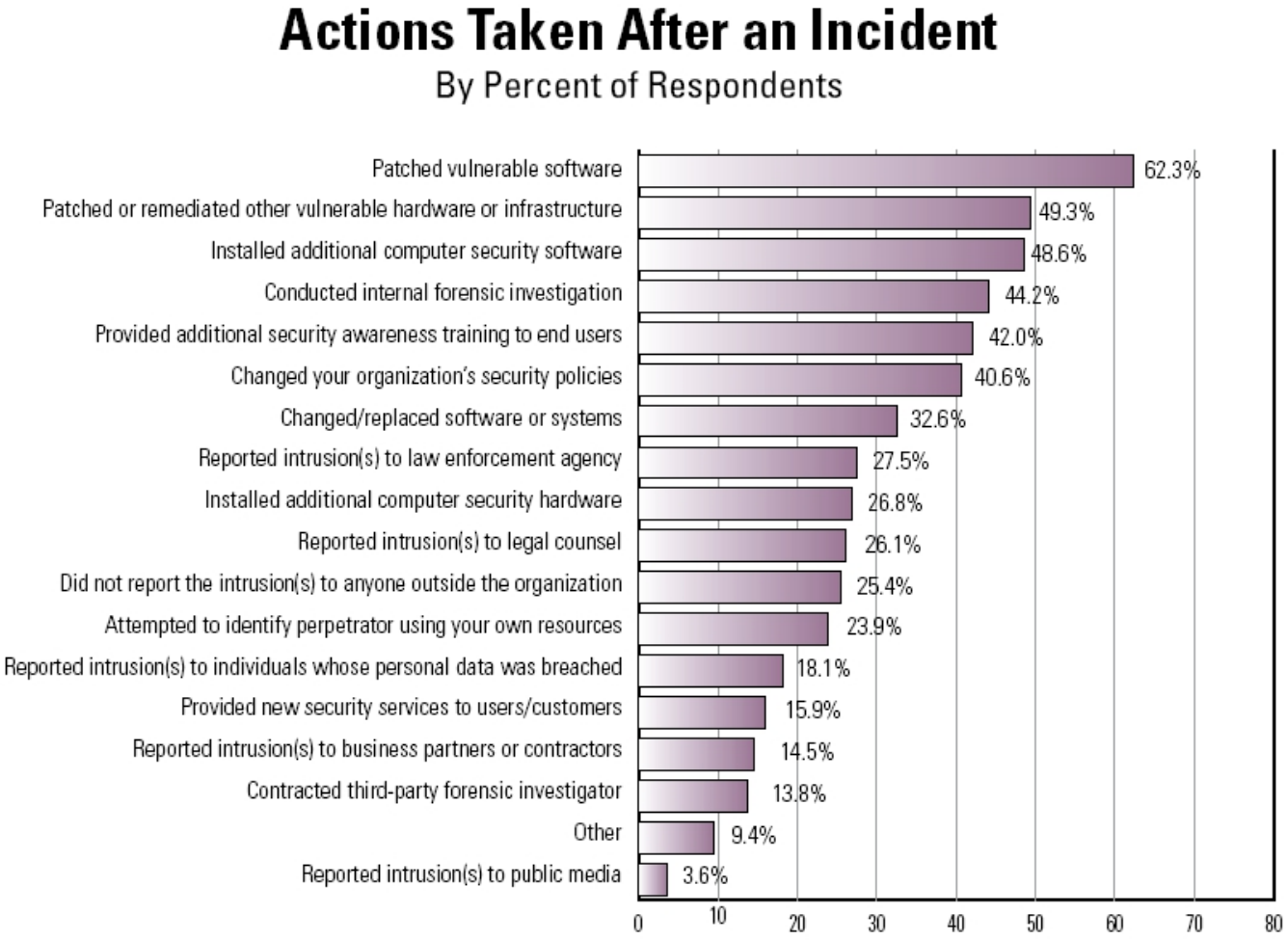
What percentage of monetary losses were attributable to actions or errors by individuals within the organization?

	None	Up to 20%	21 to 40%	41 to 60%	61 to 80%	81 to 100%
Malicious insider actions	59.1%	28.0%	5.3%	0.8%	3.8%	3.0%
Non-malicious insider actions	39.5%	26.6%	6.5%	8.9%	4.0%	14.5%

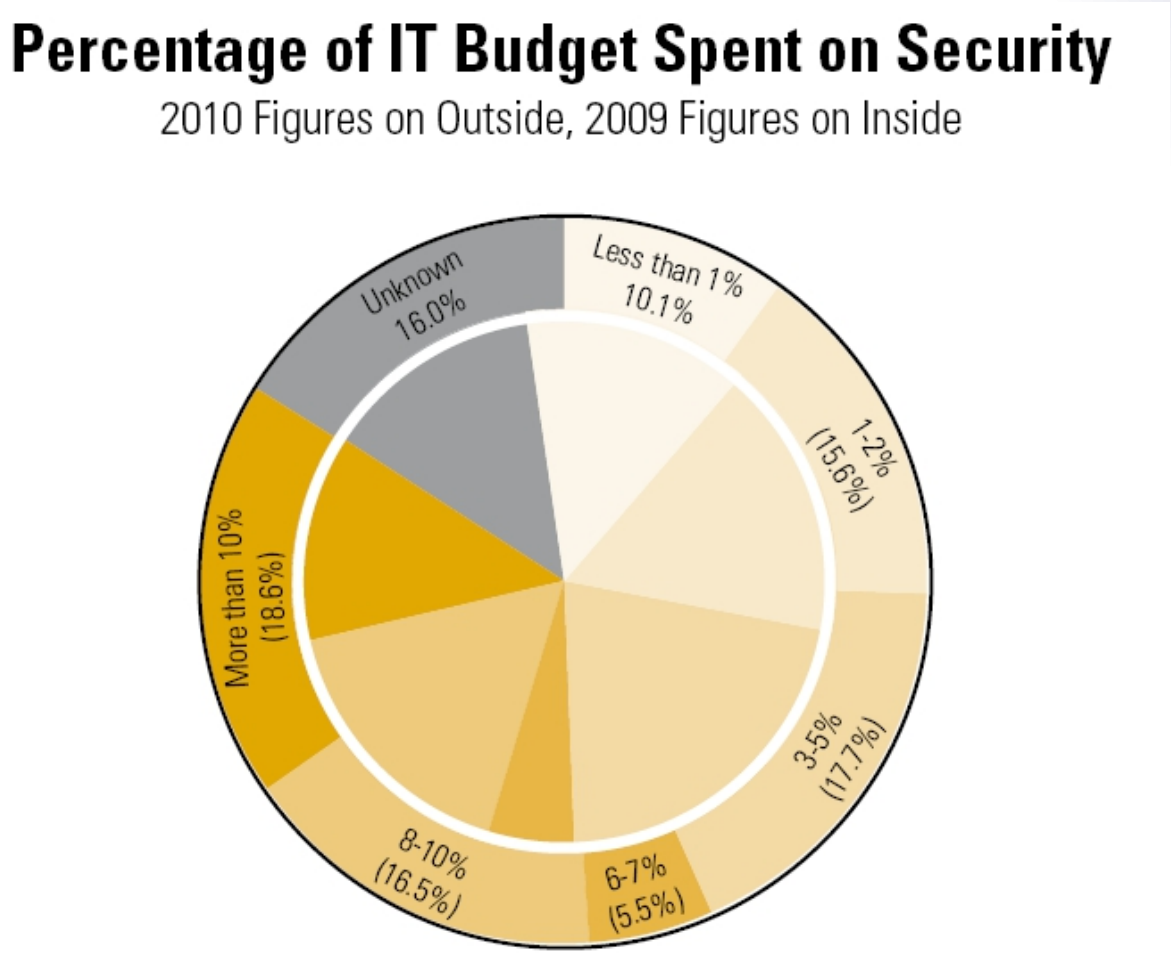
Statistics: Targeted Attacks



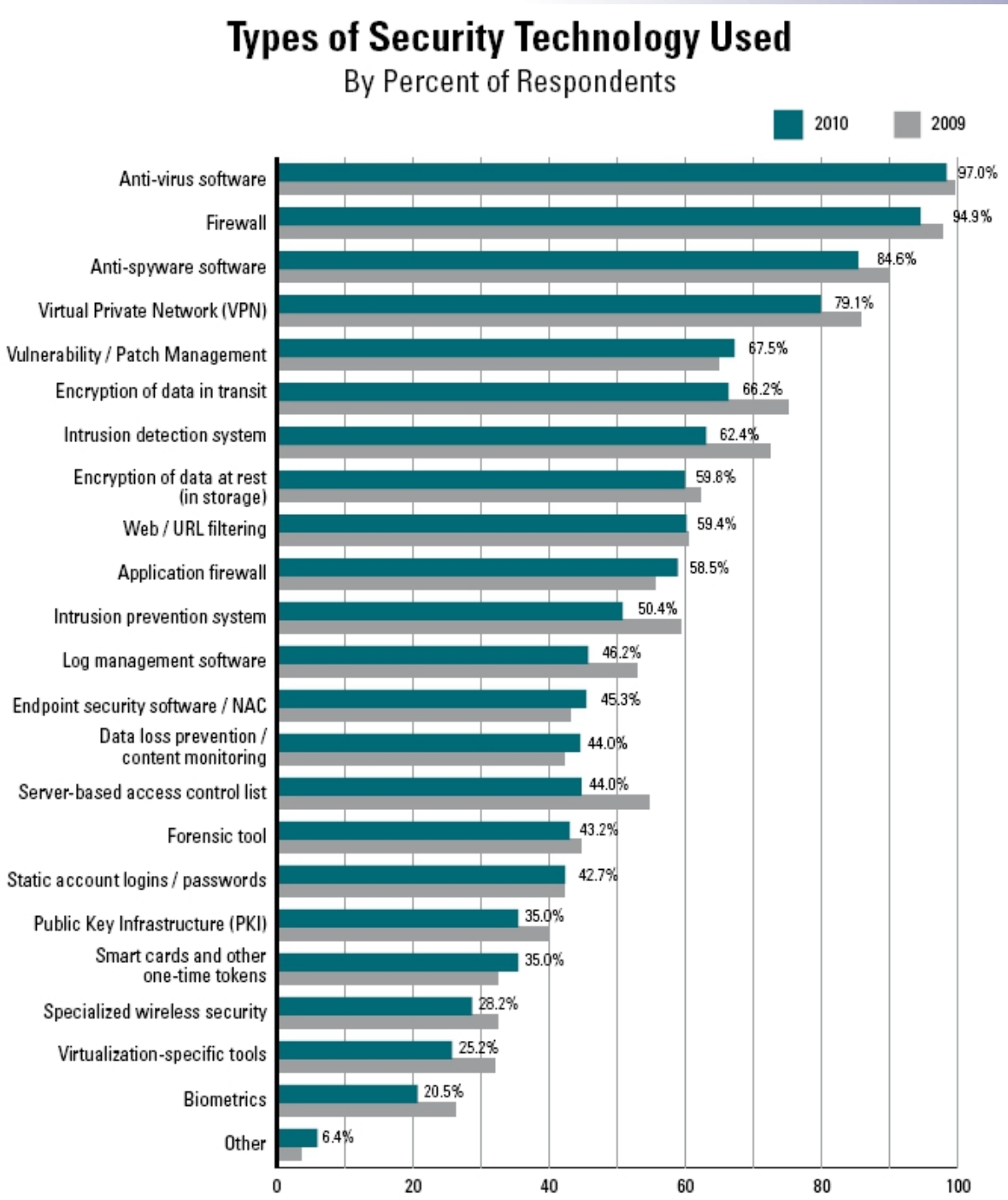
Statistics: After an Incident



Statistics: IT Budget



Statistics: Types of Security Techno-logy Used



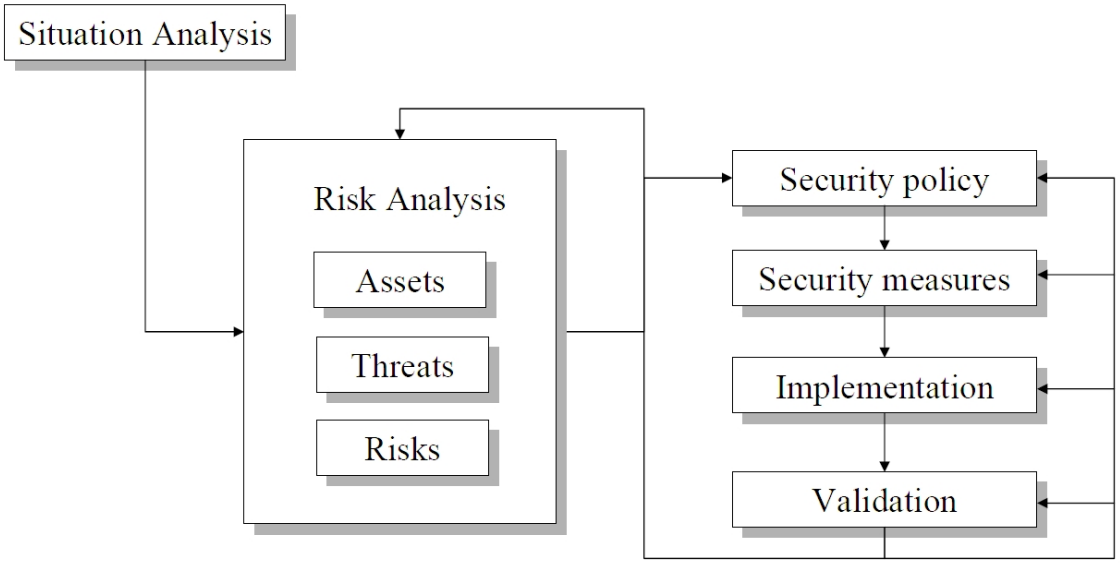
Risk Analysis

Security Incident: A Real Issue

- Issues are real and have significant consequences
- Direct financial losses
- Indirect losses
  - Image of the company
  - Spying activities

- Manage security in a general and systematic manner

A Systematic Approach



Identify:

- What needs to be protected?
- From whom?
- For how long?
- How much is the protection worth?
- Refine specifications:
- More detailed the better
  - e.g. "Use crypto where appropriate." vs. "Credit card numbers should be encrypted when sent over the network."
- How urgent are the risks?

Risk Analysis

- Importance of assets (V)
- Potential threats (M)
- Evaluate probability of threat (P)

$$\text{Risk} = \sum P(M_i)\, V_i$$

- We must reach a reasonable residual risk
  - If interested, checkout Ch. 8 of the textbook to find more details, which are not covered in this course

Qualitative vs. Quantitative

- Quantitative evaluation
  - Example:
    - Prob. to get a virus=10%
    - Cost to restore system=$1000
    - Risk is $100
- Qualitative evaluation

	Importance of impact		
Prob. of occur.	Low	Medium	High
High	Low	Medium	High
Medium	Low	Medium	Medium
Low	Low	Low	Low

Any questions?

Tips

https://BetterCrypto.org

- This project aims at creating a simple, copy & paste-able HOWTO for secure crypto settings of the most common services (webservers, mail, ssh, etc.)

https://www.howsmyssl.com/

- A website that tells you how secure your TLS client is

Follow good software engineering principles, but take into account malicious behavior

- Thirteen principles to ensure enterprise system security
- http://searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security
- Use community resources (CERT, BugTraq, etc.)

Stay tuned

+

Next time you will learn about

Spam | Malware