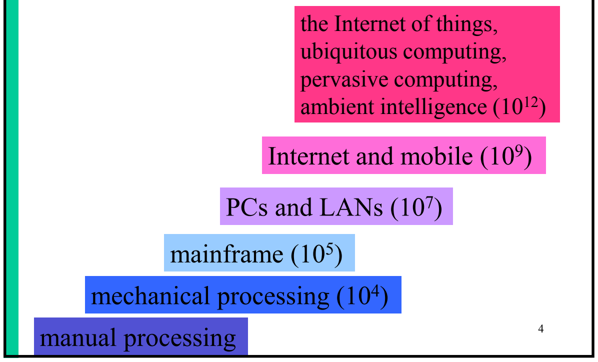
Challenges in Information Security

Prof. Bart Preneel
COSIC – KU Leuven – Belgium
Firstname.Lastname(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel
December 2014

Learning goals

- What are the goals for information security and privacy?
- What are the threats and causes that create these problems?
- Why is securing information systems hard?
  - – technical aspects
  - – non-technical aspects: legal, economical, psychological

Information processing



the Internet of things, ubiquitous computing, pervasive computing, ambient intelligence (10^{12})

Internet and mobile (10^{9})

PCs and LANs (10^{7})

mainframe (10^{5})

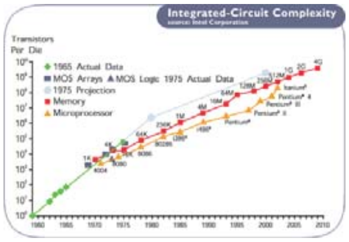
mechanical processing (10^{4})

manual processing

Exponential growth

Ray Kurzweil, KurzweilAI.net

- Human brain: 10^{14} …10^{15} ops and 10^{13} bits memory
- 2025: 1 computer can perform 10^{16} ops (2^{53})
- 2013: 10^{13} RAM bits (1 Terabyte) cost 1000$



Outline

- COMSEC versus COMPUSEC
- IT Security threats
- Privacy risks
- e-Business
- Taking a step backwards
- Non-technical dimension
- Conclusions

Military security terminology

INFOSEC

- COMSEC: securing (electronic) communications
- COMPUSEC: computer security

Information Collection

- Signal Intelligence (SIGINT)
  - COMINT: communications intelligence
    - traffic analysis
  - ELINT: electronic intelligence
    - TEMPEST: electromagnetic emanations
- …
- Human Intelligence (HUMINT)
- Imagery Intelligence (IMINT)
- Measurement and Signature Intelligence (MASINT)
- Technical Intelligence (TECHINT)
- Open Source Intelligence (OSINT)

COMSEC

- pre-1915: manual encryption or simple devices

- 1917: one time pad
- 1915: rotor machines: (electro-)mechanical

- 1960's: electronic encryption
- 1975: integrated hardware
- 1990: software

COMSEC in practice

- wired
  - SSL/TLS
  - VPN: IPsec
  - VOIP
- wireless
  - GSM, 3G
  - WLAN: WPA2 (RSN)
  - PAN: Bluetooth, Zigbee

COMSEC

	Confidentiality	Data authentication	Entity authentication
1 G (analog)	🟥	🟥	🟥
2 G (GSM)	🟧 weak	🟥	🟧 unilateral
3G	🟧	🟧	🟧
WLAN	🟧	🟧	🟧
TLS	🟩	🟩	🟩 unilateral
IPsec	🟩	🟩 optional ☹	🟩
Skype	🟩 not open	🟩 not open	🟧 not open/meet in the middle attack

Not end to end

COMSEC: network security

- fundamental protocols of the Internet do not have adequate security
- this is well understood, but there is no preventive patching
  - panic response to ever improving attacks
- changing widely used protocols is hard

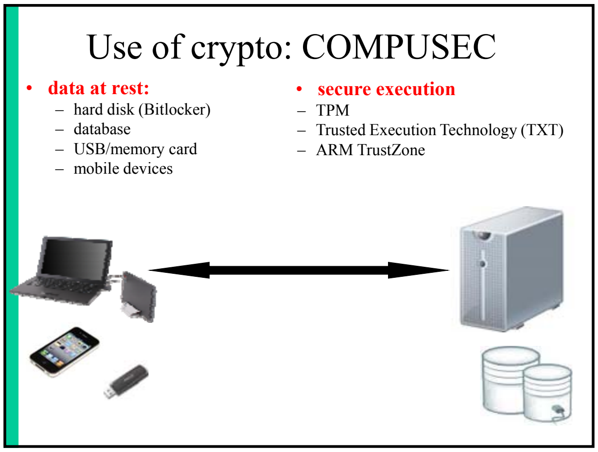
- DNS attack [Kaminsky, Black Hat '08]
- BGP attack [Kapela-Pilosov, Defcon'08]

- More examples:
  - **IPV6 attacks**
  - **SNMPv3 Bug [Wes Hardakar]**
  - **Insecure SSL-VPN [Mike Zusman]**
  - **Insecure Cookies [Mike Perry]**

COMSEC: DNSSec

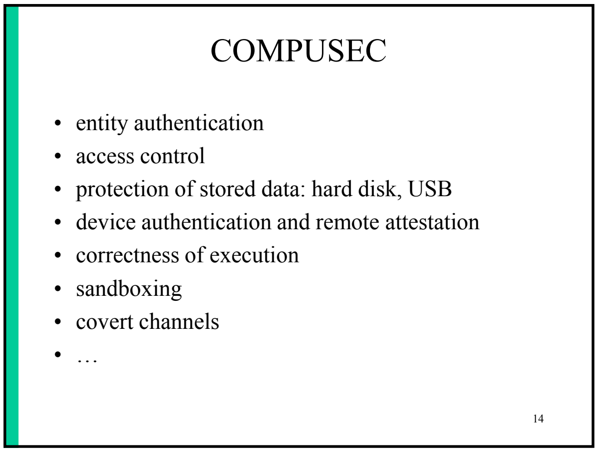
- long and winding road (started in 1997)
- several attacks (e.g. cache poisoning [Kaminsky08])
- several TLDs signed 2005-2009
- live in July 2010 for root
- Versign signed .com early 2011

- http://www.root-dnssec.org/
- http://ispcolumn.isoc.org/2006-08/dnssec.html



Use of crypto: COMPUSEC

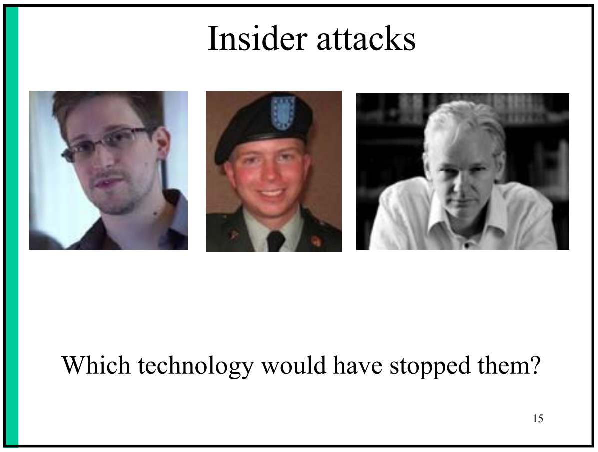
- **data at rest:**
  - hard disk (Bitlocker)
  - database
  - USB/memory card
  - mobile devices
- **secure execution**
  - TPM
  - Trusted Execution Technology (TXT)
  - ARM TrustZone



COMPUSEC

- entity authentication
- access control
- protection of stored data: hard disk, USB
- device authentication and remote attestation
- correctness of execution
- sandboxing
- covert channels
- …

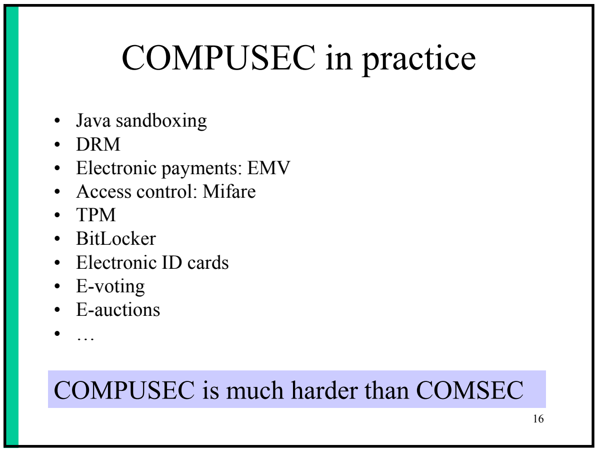
14



Insider attacks

Which technology would have stopped them?

15

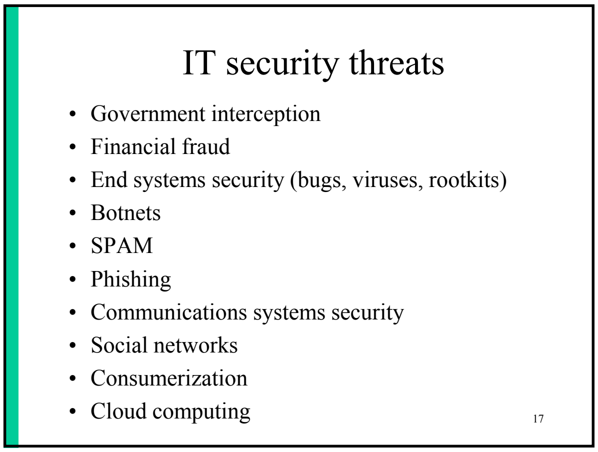


COMPUSEC in practice

- Java sandboxing
- DRM
- Electronic payments: EMV
- Access control: Mifare
- TPM
- BitLocker
- Electronic ID cards
- E-voting
- E-auctions
- …

COMPUSEC is much harder than COMSEC

16



IT security threats

- Government interception
- Financial fraud
- End systems security (bugs, viruses, rootkits)
- Botnets
- SPAM
- Phishing
- Communications systems security
- Social networks
- Consumerization
- Cloud computing

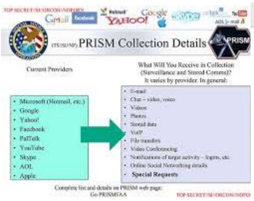
17

data retention
privacy
national security
undermining competition
legal interception
forensics
DDOS
Digital Rights Management
fraud
phishing
content filtering
spyware
SPAM
botnets
illegal software
Malware: viruses, worms, Trojans, rootkits

18

Interception by governments

1. PRISM (server) 2. Upstream (fiber)



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

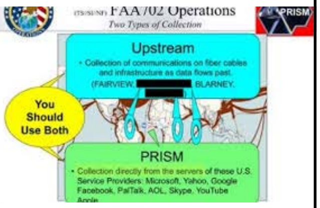
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page: Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, [redacted] BLARNEY, [redacted]

You Should Use Both

PRISM

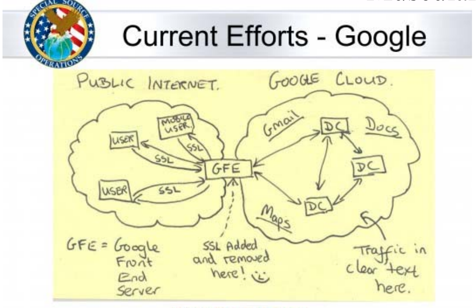
- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple

3. Traffic data (DNR)

- traffic data is not plaintext itself, but it is very informative
  - it may contain URLs of websites
  - it allows to map networks
- **6 June 2013: NSA collecting phone records of millions of Verizon customers daily**
- Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama
- **EU: data retention directive (2006/24/EC)**

Muscular

TOP SECRET//SI//NOFORN



Current Efforts - Google

PUBLIC INTERNET.
GOOGLE CLOUD.
USER
MOBILE USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

TOP SECRET//SI//NOFORN

Jan 9 2013: In the preceding 30 days, field collectors had processed and sent back 181,280,466 new records — including "metadata," which would indicate who sent or received e-mails and when, as well as content such as text, audio and video (from Yahoo! and Google)

Snowden revelations (ctd)

Most spectacular: **active defense**

- networks
  - Quantum insertion: answer before the legitimate website
  - inject malware in devices
- devices
  - malware based on backdoors and 0-days (FoxAcid)
  - supply chain subversion

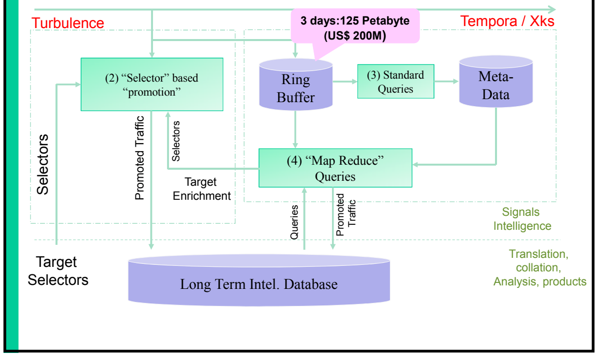
Translation in human terms: **complete control** of networks and systems, including bridging the air gaps

No longer deniable

Oversight weak

TEMPORA architecture (GCHQ)

(1) Gain "access" to raw content: intercept (cable, satellite), hack, buy, ask.



Turbulence

3 days:125 Petabyte (US$ 200M)

Tempora / Xks

(2) "Selector" based "promotion"

Ring Buffer

(3) Standard Queries

Meta-Data

Selectors

Promoted Traffic

Selectors

Target Enrichment

(4) "Map Reduce" Queries

Queries

Promoted Traffic

Signals Intelligence

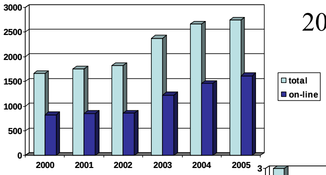
Target Selectors

Long Term Intel. Database

Translation, collation, Analysis, products

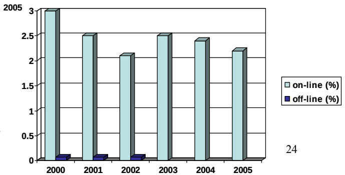
Credit Card Fraud (USA)

Fraud (Million US$)



2009: 2.0-8.6B$

Fraud rates



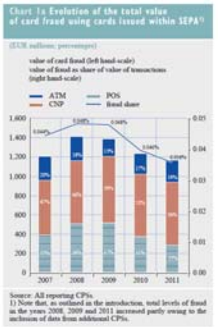
Source: Celent Communications, via Lafferty Publications

24

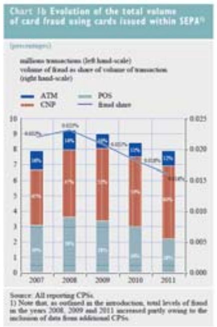
Financial fraud SEPA

https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf

2011: 1.16 billion EUR, 0.04% of transactions
Share of Card Not Present increased to more than 50%



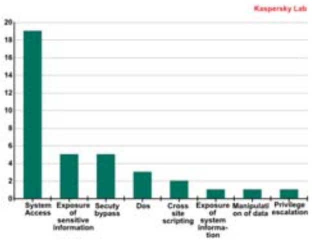
Source: All reporting CPSs.
1) Note that, as outlined in the introduction, total levels of fraud in the years 2008, 2009 and 2011 increased partly owing to the inclusion of data from additional CPSs.



Source: All reporting CPSs.
1) Note that, as outlined in the introduction, total levels of fraud in the years 2008, 2009 and 2011 increased partly owing to the inclusion of data from additional CPSs.

Malware

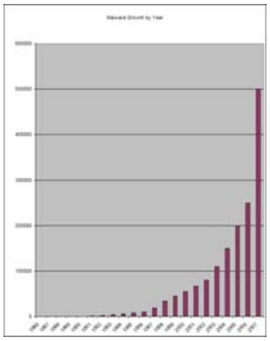
- Virus: spread via executables (software, Word documents, …)
- Worm: spread via network
- Trojan horse: secret malicious functionality
- Rootkit: control computer
- Ransomeware: encrypt



Transmission: email, Internet, intranet, web pages, GSM, 3G, Bluetooth, WiFi, USB drives, CDs, memory cards,…

Virus

- Proof of concept: 1970s
- First threat: mid 1980s
- Explosion: mid 1990s
- 6.3 Million in 2011



Source: F-Secure

Malware trends

Some anti-virus companies have stopped counting in 2009

- Kaspersky
  http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013
  - detected and neutralized almost 1 billion malicious objects
  - millions of malicious URLs
  - mobile malware reached 100K
- Sophos
  http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf
  - growth: Facebook, cloud, Android, OS X
  - polymorphism and targeting

APT – Advanced Persistent Threats

- Targeted theft or damage, but less visible

- Google Aurora Q3/Q4 2009
- Stuxnet – July 2010
- Duqu – September 2011
- Flame – May 2012
- Red October – October 2012
- Regin – November 2014

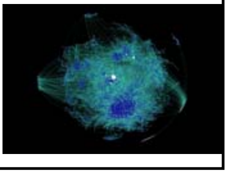
Stuxnet

- used four 0-day vulnerabilities, 2 specific for Siemens PLCs
- PLC rootkit
- 2 stolen private keys to sign its files
- 7 forms of replication (rather than 2)
- bridged air gap via USB
- meant to destroy: from espionage to sabotage (high speed spinning of centrifugres
- deception: recorded normal operation and played them back
- could disable the kill switch of the device (to prevent operator intervention)
- affected 20% of nuclear centrifuges in Iran

Is this the tip of the iceberg?

Botnets

- Attacker controls 10.000-100.000 computers



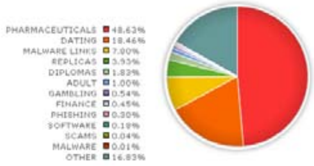
Application: rent for SPAM, hacking, DDOS (distributed denial of service)

SPAM in 2012

- SPAM makes up 65% of the Internet email traffic
  - 7% in 2001; 90-95% around 2005; 82% in 2010
  - 90-200 billion SPAM messages/day
  - 5% carries malware
- 40% of all social media accounts are created by spammers
- billions of dollars spent on spam defense
- cost to large company a few million $/year
- cost to society
  - vector for malware
  - spoiling e-mail as communication tool: time and attention
  - ISP/mobile fees
  - storage and bandwidth

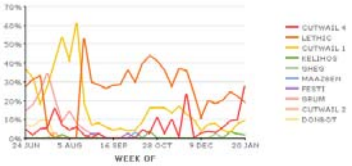
Bill Gates (2004): Spam Will Be 'Solved' In 2 Years

SPAM 2013 statistics



SPAM content
[Source: M86 security lab]

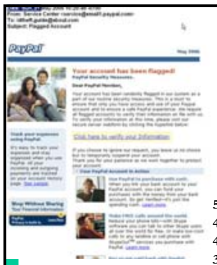
Latest trend:
on-line casinos



SPAM by botnet
[Source: M86 security lab]

SPAM and economics

- list of 10^8-10^9 “good” names
- cost per message: ~ 10^{-4} -10^{-5} €; total cost 10^4-10^5 €
- hit ratio: 10^{-3} to 10^{-4}: 30,000-300,000 responses
  - SPAM only works because users respond
- cost per click is 0.30 € compared to 0.07 € for commercial advertising – this explains reduction
- botnet: machines for sale for a few dozen EURO
  - can be used for SPAM and for DDOS attacks
  - most SPAM messages come from a dozen botnets
- see e.g., http://www.marshal.com/trace/spam_statistics.asp



From: Service Center <service@email1.paypal.com>
Subject: Flagged Account

Your account has been flagged!
PayPal Security Measures.

Dear PayPal Member,

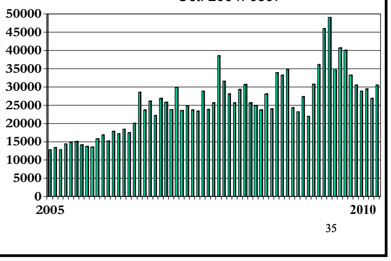
[illegible]

Click here to verify your Information

[illegible]

Phishing reports received
Jan ’05-March’10
(source www.antiphishing.org)

Oct. 2004: 6597

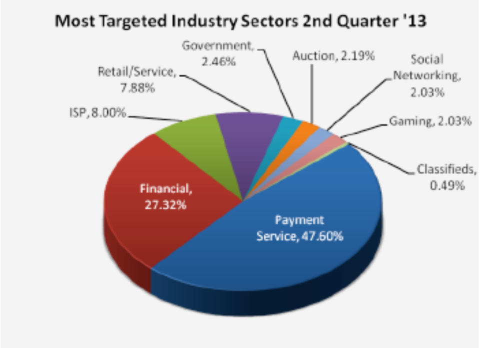


Phishing

- 0.1%-1% of email is phishing related
- more than 31,000 new phishing sites per month
  - peak of 41,000 in 2009; “only” 25,000 in 2006
- consumers react very naively (human factor)
- even experts can’t distinguish some phishing messages from real ones
- direct losses from Phishing costed banks and credit card issuers $2.8 Billion per year (e.g., theft, call center activity)
- targeted attack: spear phishing

Phishing targets by industry

http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf



Spying: war driving and Bluetooth

Bluesniper rifle (2004):

10m becomes 1km

Spying: surveillance software and key loggers

eBLASTER
Knowing EVERYTHING They Do Online
Is as Easy as Checking Your Email.

99.95$ at eblaster.com

67.88$ at keyLlama.com

- can memorize 8 MByte key presses

100.00$ WiFi Pineapple

- 4 Mbyte key PS/2 key logger
- hard to detect

74.88$ at keyLlama.com

Social networks

- vector for malware
  - Facebook rogue application toolkit
- social engineering
- leaking company secrets
- personal privacy risk

- establish your organization's presence before anyone else does

NETLOG f Linked in twitter

Consumerization

- Personal smart phones, tablets,… enter the workplace, not provisioned by company
- March 2011 survey by Vanson Bourne of 300 CIOs of companies with more than 3000 employees
  - 67% concerned about protecting their corporate data since WikiLeaks
  - 78% don't know what devices are connected to the corporate network
  - 77% don't know what data is lurking on all of those devices.
  - 33% can track these devices
  - 50% can secure these devices should they be lost or stolen
  - 75% "security headaches" are actually caused by the mobile devices

- http://www.mformation.com/mformation-news/press-releases/cios-raise-security-concerns-around-backdoor-mobile-devices

Cloud security: is it different?

- What's the same
  - can do intrusion detection/monitoring
  - can encrypt stored data
  - availability? Service/network/power - SLA
- What's different
  - AV could be easier
  - pen testing?
  - forensics?
  - personnel security
  - localization

- Privacy
- Large and attractive target
  - What if someone takes over the infrastructure management?

VMWare isn't an additional security layer, it's just another layer to find bugs in [Kostya Kortchinsky]

Outline

- COMSEC versus COMPUSEC
- IT Security threats
- Privacy risks
- e-Business
- Taking a step backwards
- Non-technical dimension
- Conclusions

43

Largest (known) privacy breaches

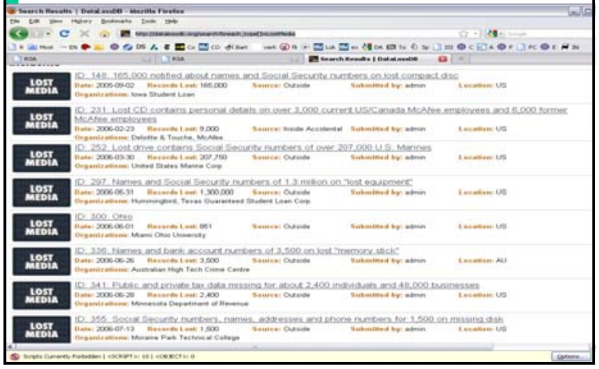
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

152,000,000	2013-09-17	Adobe
145,000,000	2014-02/03	Ebay
130,000,000	2009-01-20	Heartland Payment Systems
94,000,000	2007-01-17	TJX Companies Inc.
90,000,000	1984-06-01	TRW, Sears Roebuck
77,000,000	2011-04-26	Sony Corporation (120 MEURO)
76,000,000	2014-07-??	JP Morgan
76,000,000	2009-10-01	National Archives and Records Administration
70,000,000	2014-12-19	Target credit card data
50,000,000	2013-04-07	LivingSocial (daily deals)
50,000,000	2013-03-02	Evernote
40,000,000	2005-06-19	CardSystems, Visa, MasterCard, Amex
35,000,000	2011-07-28	SK Communications, Nate, Cyworld
32,000,000	2009-12-14	RockYou Inc.
26,500,000	2006-05-22	U.S. Department of Veterans Affairs
25,000,000	2007-11-20	HM Revenue and Customs, TNT (CD)

"only" 10K-500K in individual health care breaches (total a few million)

Data loss: lost media

http://datalossdb.org/search?breach_type[]=LostMedia


Search Results | DataLossDB - Mozilla Firefox
File Edit View History Bookmarks Tools Help
RSA
RSA
Search Results | DataLossDB

LOST MEDIA ID: 148: 165,000 notified about names and Social Security numbers on lost compact disc
Date: 2006-09-02 Records Lost: 165,000 Source: Outside Submitted by: admin Location: US
Organizations: Iowa Student Loan

LOST MEDIA ID: 231: Lost CD contains personal details on over 3,000 current US/Canada McAfee employees and 6,000 former McAfee employees
Date: 2006-02-23 Records Lost: 9,000 Source: Inside Accidental Submitted by: admin Location: US
Organizations: Deloitte & Touche, McAfee

LOST MEDIA ID: 252: Lost drive contains Social Security numbers of over 207,000 U.S. Marines
Date: 2006-03-30 Records Lost: 207,750 Source: Outside Submitted by: admin Location: US
Organizations: United States Marine Corp

LOST MEDIA ID: 297: Names and Social Security numbers of 1.3 million on "lost equipment"
Date: 2006-05-31 Records Lost: 1,300,000 Source: Outside Submitted by: admin Location: US
Organizations: Hummingbird, Texas Guaranteed Student Loan Corp

LOST MEDIA ID: 300: Ohio
Date: 2006-06-01 Records Lost: 851 Source: Outside Submitted by: admin Location: US
Organizations: Miami Ohio University

LOST MEDIA ID: 336: Names and bank account numbers of 3,500 on lost "memory stick"
Date: 2006-06-26 Records Lost: 3,500 Source: Outside Submitted by: admin Location: AU
Organizations: Australian High Tech Crime Centre

LOST MEDIA ID: 341: Public and private tax data missing for about 2,400 individuals and 48,000 businesses
Date: 2006-06-28 Records Lost: 2,400 Source: Outside Submitted by: admin Location: US
Organizations: Minnesota Department of Revenue

LOST MEDIA ID: 355: Social Security numbers, names, addresses and phone numbers for 1,500 on missing disk
Date: 2006-07-13 Records Lost: 1,500 Source: Outside Submitted by: admin Location: US
Organizations: Moraine Park Technical College

Scripts Currently Forbidden | <SCRIPT>: 10 | <OBJECT>: 0 Options

Privacy and technology

- search engines
- XML
- biometry
- location (GSM!!, GPS)
- printers
- DRM
- spyware and cookies
- huge databases
- data mining
- video cameras
- RFID

- PET: Privacy Enhancing Technologies
- proxies
- pseudonyms
- cryptology
- mixes
- credentials

46

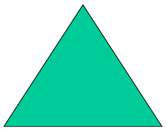
Privacy violations

http://panopticlick.eff.org/

http://wtikay.com/docs/details.html

47

Security for everyone



key escrow
Government

Users
privacy

Industry
DRM

warning: this is an oversimplification – e.g. privacy is a security property

48

The privacy debate

- user: convenience and improved service
- businesses:
  - protect company assets (email, DRM)
  - price discrimination
- law enforcement: fraud, theft, stalking, counterfeiting
- national security

- privacy is essential for a democracy
- legislation
- technology

Business perspective on security

Direct Losses

- theft
  - money
  - confidential information
  - computer resources
- productivity loss
  - data corruption
  - recovery and continuity

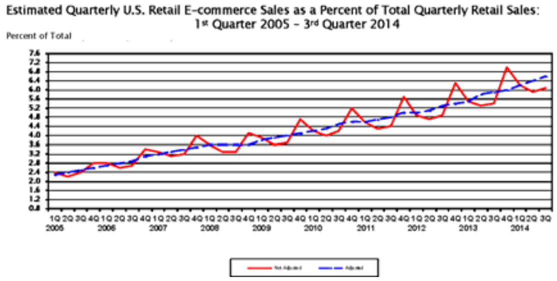
Indirect losses

- secondary loss
  - sales
  - competitive advantage
  - brand
- legal exposure
  - privacy regulations
  - legal obligations
  - contract breach

U.S. E-commerce (retail)

Q3 2014:

- e-commerce (retail): 78 B$
- total (retail) commerce: 1.185 B$


Estimated Quarterly U.S. Retail E-commerce Sales as a Percent of Total Quarterly Retail Sales: 1st Quarter 2005 – 3rd Quarter 2014

Taking a step backwards

- computer security research is about 40 years old
- thousands of researchers, ten thousands of scientific articles, thousands of security products and services
  - Gartner: security services spending 35 B$ in 2011
- increased accountability [Sarbanes-Oxley '02] [Basel II '04]
- critical infrastructure protection

[Adi Shamir '07] We are winning yesterday's information security battles, but we are losing the war. Security gets worse by a factor of 2 every year.

Somehow humanity can deal with imperfect systems

IT environment

Walled fortress

- closed doors, physical isolation
- security as protection
- defend data, networks and systems

Open metropolis

- open, unbounded, interconnected
- trust as an enabler
- share content and resources
- protect data

Feudal system

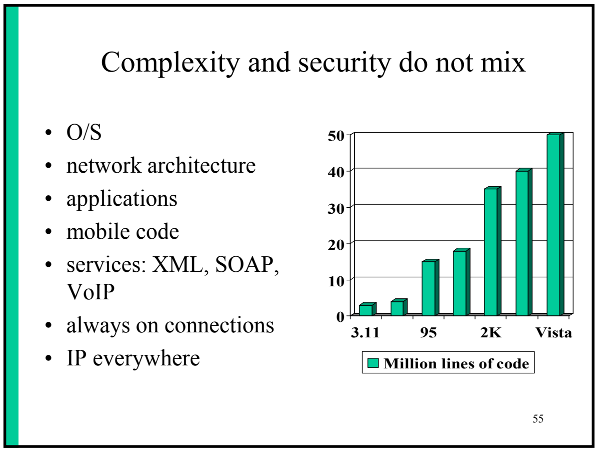
- impose central rules
- data for protection
- loss of control

Complexity of technology

- IC: 2 B transistors
- Windows/Linux: 20-200 M lines of code
- Application: 1-20 M lines of code
- Internet: 3 B computers/tablets
- Mobile phones: 6 B

- Securing a complex system: difficult, expensive and slow

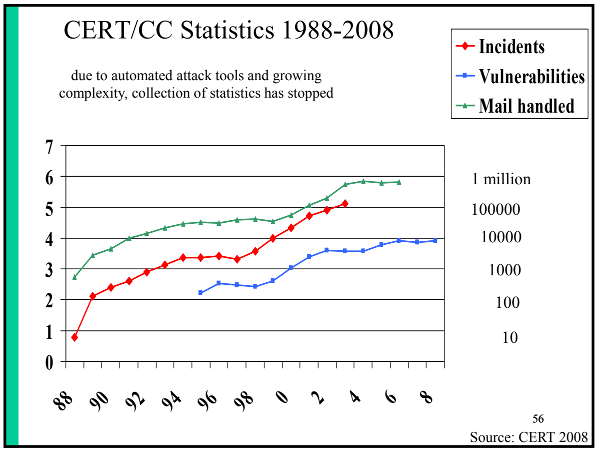
- Fast evolution of ICT world



Complexity and security do not mix

- O/S
- network architecture
- applications
- mobile code
- services: XML, SOAP, VoIP
- always on connections
- IP everywhere

55

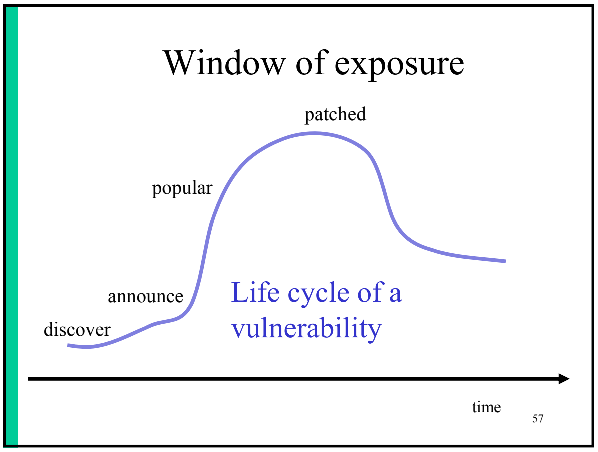


CERT/CC Statistics 1988-2008

due to automated attack tools and growing complexity, collection of statistics has stopped

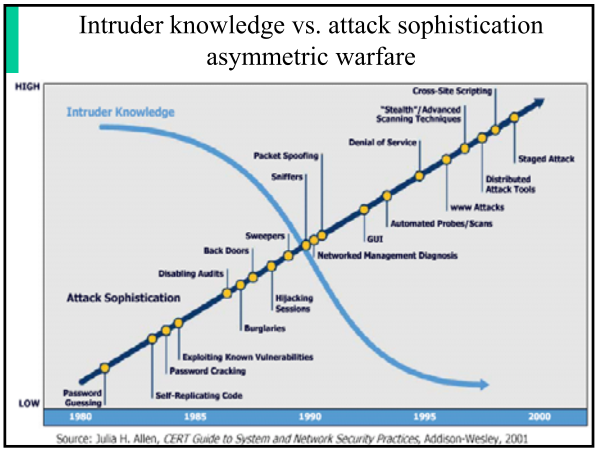
56

Source: CERT 2008



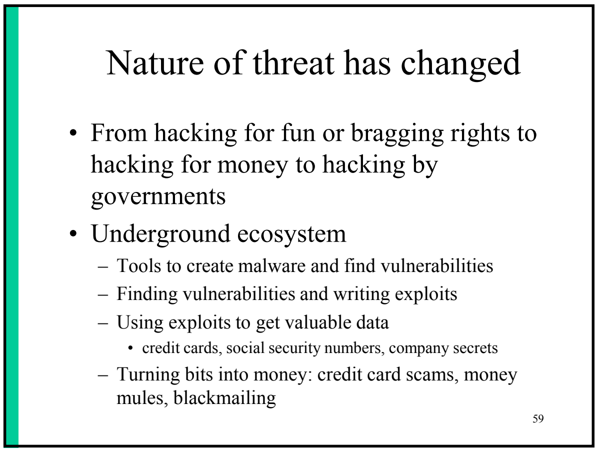
Window of exposure

57



Intruder knowledge vs. attack sophistication asymmetric warfare

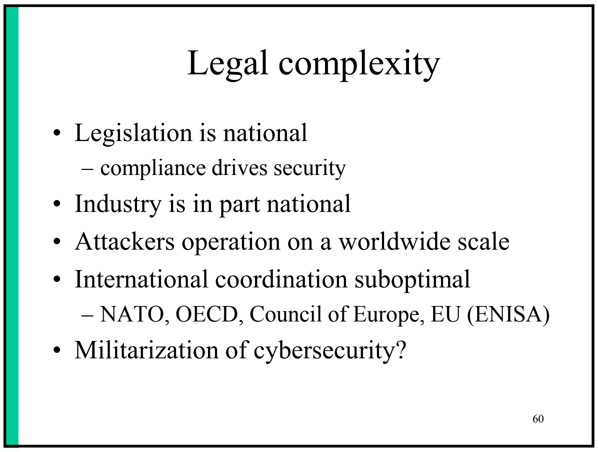
Source: Julia H. Allen, *CERT Guide to System and Network Security Practices*, Addison-Wesley, 2001



Nature of threat has changed

- From hacking for fun or bragging rights to hacking for money to hacking by governments
- Underground ecosystem
  - Tools to create malware and find vulnerabilities
  - Finding vulnerabilities and writing exploits
  - Using exploits to get valuable data
    - credit cards, social security numbers, company secrets
  - Turning bits into money: credit card scams, money mules, blackmailing

59



Legal complexity

- Legislation is national
  - compliance drives security
- Industry is in part national
- Attackers operation on a worldwide scale
- International coordination suboptimal
  - NATO, OECD, Council of Europe, EU (ENISA)
- Militarization of cybersecurity?

60

Economic problems

- in ICT world: market share is more important than security
  - Success requires 40-80% adoption
- market of lemons: user cannot distinguish between secure and insecure products
- players do not want to pay for security or privacy of others (“tragedy of the commons”): market failure
  - botnets
  - payment systems
  - software exploits

R. Anderson: Why Information Security is Hard. An Economic Perspective, 2006, http://www.cl.cam.ac.uk/~rja14/econsec.html
R. Anderson, R. Böhme, R. Clayton, T. Moore, Security Economics and the Internal Market, report for ENISA, 2008

Humans have problems making security decisions

- always a tradeoff
  - Security costs time, memory, effort
- humans are very bad at making e-security decisions
  - our brains have developed to take security decisions in the African highlands about 100,000 years ago
    - “stay or flee” reflex in amygdala (very fast)
    - heuristics in neocortex
- large gap between being secure and feeling secure
  - exploited by politics and marketing

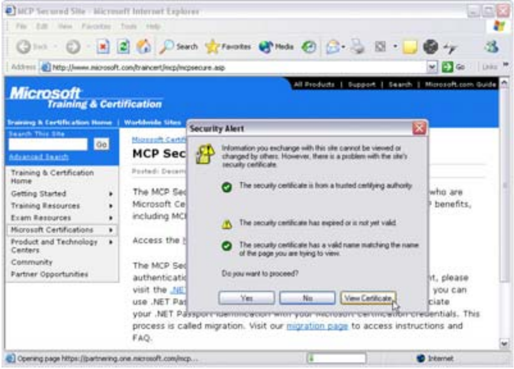
“any sufficiently advanced technology is indistinguishable from magic” [Arthur C Clarke 1961]

B. Schneier, The Psychology of Security, 2008, http://www.schneier.com/essay-155.pdf

How do we judge risks?

overestimate	underestimate
• spectacular	• daily
• rare	• frequent
• personal	• anonymous
• outside our control	• under our control
• in the news	• unmentioned
• intentional	• natural
• Immediate	• long term
• new and unfamiliar	• familiar
• w.r.t. kids and loves ones	• w.r.t. ourselves

Usability issues


MCP Secured Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
All Products | Support | Search | Microsoft.com Guide
Microsoft Training & Certification
Training & Certification Home | Worldwide Sites
Search This Site
Go
Advanced Search
Training & Certification Home
Getting Started
Training Resources
Exam Resources
Microsoft Certifications
Product and Technology Centers
Community
Partner Opportunities
Internet

Address: http://www.microsoft.com/traincert/mcp/mcpsecure.asp

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority

⚠ The security certificate has expired or is not yet valid

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Yes No View Certificate

MCP Sec

The MCP Se ... who are Microsoft Ce ... P benefits, including MC

Access the

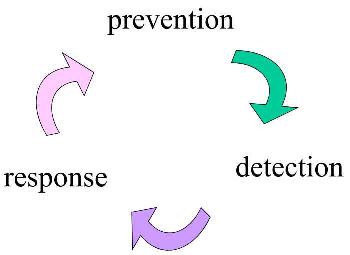
The MCP Se ... authenticati ... t, please visit the .NE ... you can use .NET Pa ... ciate your .NET Passport identification with your Microsoft Certification credentials. This process is called migration. Visit our migration page to access instructions and FAQ.

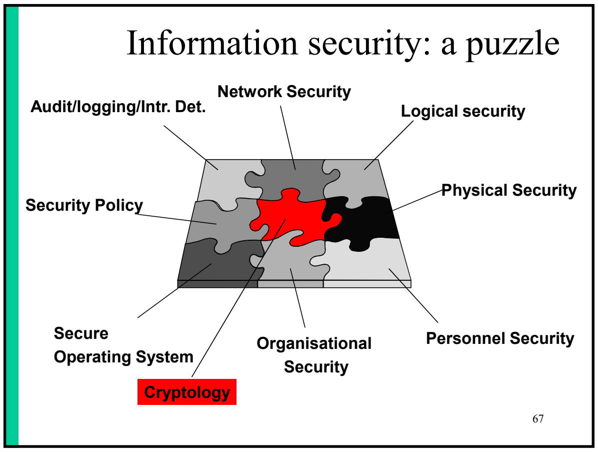
Opening page https://partnering.one.microsoft.com/mcp...

From risk avoidance to risk management

- accept the risk
- reduce risk with technology
- reduce risk with procedures
- reduce risk with insurance
- reduce risk with disclaimers
- transfer the risk

Process approach to security





Information security: a puzzle

Audit/logging/Intr. Det.

Network Security

Logical security

Security Policy

Physical Security

Secure
Operating System

Organisational
Security

Personnel Security

Cryptology

67