

## Trends in Information Security

Prof. Bart Preneel  
COSIC – Kath. Univ. Leuven - Belgium  
Bart.Preneel(at)esat.kuleuven.be  
<http://homes.esat.kuleuven.be/~preneel>

© Bart Preneel. All rights reserved

1

## Outline

- ICT trends
- The changing threat landscape
- Where is crypto going?
- 2020 and beyond

2

## ICT trends

- Cloud
- Social networks
- IPv6
- Consumerization
- Insider attacks

3



4

## 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

5

## Cloud

- Define?
  - private/community/hybrid/public
  - SaaS, PaaS, IaaS
- reduce capital and operational expenses
- scalable and elastic architecture
- Typical organizations have between 15-30 SaaS applications (often without the CIO knowing about it)

6

## Cloud security perceived as a huge issue

- survey commissioned by Microsoft measuring attitudes on cloud computing among business leaders and the general population. while 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, **more than 90 percent of these same people are concerned about the security, access and privacy of their own data in the cloud.**

<http://www.microsoft.com/presspass/press/2010/jan10/1-20BrookingsPR.msp>

7

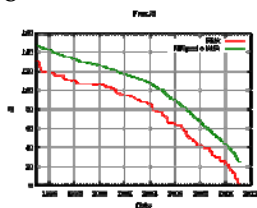
## Cloud security: Is it different?

- 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
  - Virtualization: "VMware isn't an additional security layer, it's just another layer to find bugs in" [Kostya Kortchinsky]
  - Localization
- Privacy
- Large and attractive target!
  - What if someone takes over the infrastructure management?

8

## IPv6

last IPv4 block handed out in Feb 2011 by IANA



- IPv6 is on by default (since Vista, iPhone, iPad) and tunneled across IPv4 (Teredo, MAC OS X, Linux)
- If you haven't planned for IPv6, you have already deployed it
- Your security infrastructure (firewall, IDS) have fewer capabilities for detecting and blocking IPv6

9

## 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

10

## 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>

11

## From closed to open 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

12

### Insider attacks



- Which technology would have stopped them?

13

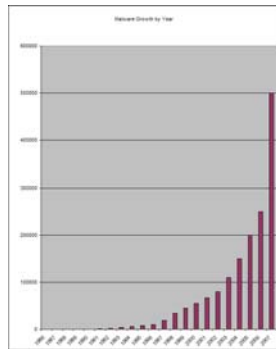
### The changing threat landscape

- Malware – APT
- Web application insecurity (moving up)
- Hardware hacking (moving down)
- Cyberwar
- Privacy

14

### Malware

- Proof of concept virus: 1970s
- First threat: mid 1980s
- Explosion: mid 1990s
- 2008: 1 million
- 2011: 50 million



Source: F-Secure

In 2010, more than 0.5 B attacks detected against the customers of a large AV vendor

Some anti-virus companies have stopped counting in 2009

Others set the count today at 50 million

Item name	Delta	Version
1	New	Trojan-Dropper.Worm.Agent.a
2	New	Trojan-Dropper.Worm.Agent.a
3	New	Downloader.Java.OpenConnection.a
4	New	Downloader.Java.OpenConnection.a
5	New	Exploit.VBA.CVE-2010-1801.ad
6	New	Adware.HTML5.Fastlog.gpl
7	New	Adware.HTML5.Fastlog.gpl
8	New	Trojan.Java.Agent.a
9	New	Exploit.JS.Flash.CVE
10	New	Trojan
11	New	Downloader.Java.OpenConnection.a
12	New	Trojan
13	New	Downloader.Java.OpenConnection.g
14	New	Trojan.HTML.Agent.a
15	New	Exploit.JS.Silverlight.2
16	New	Trojan.JS.Fraud.2.a
17	New	Trojan.Chrome.JS.Agent.a
18	New	Trojan.JS.Fraud.2.a
19	New	Trojan.JS.Fraud.2.a
20	New	Trojan.JS.Fraud.2.a
21	New	Trojan.JS.Fraud.2.a
22	New	Trojan.JS.Fraud.2.a
23	New	Trojan.JS.Fraud.2.a
24	New	Trojan.JS.Fraud.2.a
25	New	Trojan.JS.Fraud.2.a

### Latest malware trends

- Spread via social networks
  - e.g., Koobface worm [December 2008]
    - spreads via Facebook/Twitter message
    - convince user to download Trojan
    - steals credit card numbers
- Moving to mobile devices and WLAN routers

“I have Zeus on 11% of my machines, and that is below the industry average of 18%”

“Don't click on stupid links”  
“Please give me a list of stupid links so that I know which ones to avoid”

### APT – Advanced Persistent Threats

- Targeted theft or damage, but less visible
- Google Aurora Q3/Q4 2009
- Stuxnet – July 2011

18

## 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 centrifuges)
- 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

What's next?

19

## OWASP Top 10 Web Application Security Risks

OWASP Top 10 – 2007 (Previous)	OWASP Top 10 – 2010 (New)
A2 – Injection flaws	↑ A1 – Injection
A1 – Cross Site Scripting (XSS)	↓ A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑ A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	= A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	= A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 Insecure Configuration Management>	+ A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	↑ A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	↑ A8 – Failure to Restrict URL Access
A9 – Insecure Communications	= A9 – Insufficient Transport Layer Protection
<not in T10 2007>	+ A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	- <dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	- <dropped from T10 2010>

20

## Hardware hacking

- Tivo, Kinect, iPhone, PS3, ...
- altering firmware
- bus sniffing
- memory dumps to find crypto keys
- tools: <http://www.arduino.cc/>

21

## “Hacked”



- May 2008: MiFare
- May 2010: Car systems
  - Experimental Security Analysis of a Modern Automobile
  - Update March 2011: via wireless interface
- May 2010: EMV
  - Chip and PIN broken
- July 2010: ATM machines
  - Jackpotting Automated Teller Machines Redux
- Sept 2010: HDCP (High-bandwidth Digital Content Protection)
- Dec 2010: Sony PS3

22

## Cyberwar

- US DoD
  - 2008: DoD infected through thumb drive with Trojan that stole classified data
  - > 100 intelligence agencies have attempted to attack their systems
- DoS: limited impact
- Estonia 2007
- Georgia 2008
- Anonymous: PayPal 2010 (Wikileaks)
- ...

23

## Cyber force?

At the RSA Security Conference (22/02/2011), General Keith Alexander, Commander of U.S. Cyber Command and the director of the National Security Agency (NSA) said that the United States need to create a "cyber force" to be able to withstand attacks targeted at the nation critical infrastructure.

We need to concurrently push STEM (science, technology, engineering, and mathematics) and educate the public about what goes on these networks so that we can fix it as a team. We need your help to do that.

According to Alexander, a cyber force could be a band between government agencies and the private sector, in which early warning signs could be detected and defend the country against "sophisticated adversaries and malicious insiders." He envisions a team-based collaboration to counter trends in a world where "cyber offensive- and defensive operations are the keys to military victory."

Alexander called for a greater focus on education at the elementary and secondary level: "We can't let the advantages we've had in the past erode the future," he said.


24

### Privacy and technology

- search engines
- PET: Privacy Enhancing Technologies
- XML
- proxies
- biometry
- pseudonyms
- location (GSM!!, GPS)
- cryptology
- printers
- mixes
- DRM
- credentials
- spyware and cookies
- huge databases
- data mining
- video cameras
- RFID

25

### Privacy violations

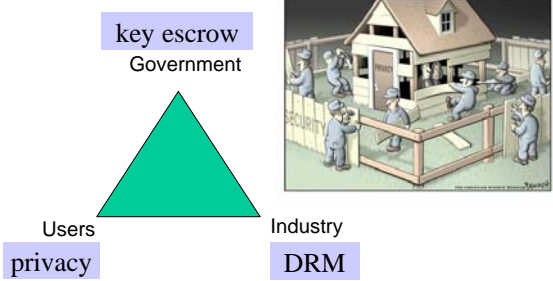


<http://panopticlick.eff.org/>

<http://wikia.com/docs/details.html>

26

### Security for everyone



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

27

### 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

28

### Where is crypto going?

- Successes and failures
- Lightweight crypto
- Advanced protocols
- Quantum crypto

29

### COMSEC

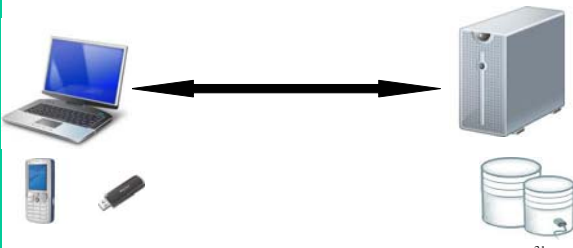
	Confidentiality	Data authentication	Entity authentication
1 G (analog)			
2 G (GSM)	weak		unilateral
3G			
WLAN			
TLS			unilateral
IPsec		optional ☺	
Skype	not open	not open	not open

} Not end to end

30


### Use of crypto: COMPUSEC

- **Data at rest:**
  - Hard disk (Bitlocker)
  - Database
  - Floppy disk/CD/USB
  - Mobile devices
- **Secure execution:**
  - TPM
  - ARM TrustZone
  - Apple DRM



31

### AES (2001)



- FIPS 197 published Dec'01 after 4-year open competition
  - other standards: ISO, IETF, IEEE 802.11,...
- fast adoption in the market
  - except for financial sector
  - NIST validation list: 1601 implementations
    - <http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html>
- 2003: AES-128 also for **classified** information and AES-192/-256 for **secret** and **top secret** information!
- security:
  - algebraic attacks of [Courtois+02] not effective
  - side channel attacks: cache attacks on **unprotected** implementations
- speed:
  - Intel NI instruction in < 1 cycle/byte
  - Software: 7.6 cycles/byte

[Shamir '07] AES may well be the last block cipher

### Lightweight crypto

- Symmetric crypto
  - AES: 3000 gates
  - KATAN/PRESENT: 450-1000 gates
- Public key crypto
  - RSA: 50-250 Kgates
  - ECC: 15-30 Kgates

33

### Bad news: the CA mess

[Eckersley10] "An observatory for the SSLiverse"

- 10.8M servers start SSL handshake
- 4.3M use valid certificate chains
- 1482 CA certs trustable by Windows or Firefox
- 1.4M unique valid leaf certs
  - 300K signed by one GoDaddy cert
- 80 distinct keys used in multiple CA certs
- several CAs sign the IP address 192.168.1.2 (reserved by RFC 1918)
- 2 leaf certs have 508-bit keys
- Debian OpenSSL bug (2006-2008)
  - resulted in 28K vulnerable certs
  - fortunately only 530 validate
  - only 73 revoked


How can we fix this mess?

34

### Advanced protocols

- multi-party computation
- threshold crypto
- privacy protecting data mining
- social and group crypto

decryption based on location and context  
distance bounding



"you can trust it because you don't have to"

stop building databases with policies - go for privacy by design with true data minimization

### Multi-party computation becomes "truly practical"

- Similar to first public key libraries 20 years ago
  - EU: CACE project (Computer Aided Cryptography Engineering), [www.cace-project.eu](http://www.cace-project.eu)
  - US: Brown Univ. + UCSD (Usenix 2010)
- Examples
  - efficient zero-knowledge proofs
  - 2-party computation of AES (Bristol)
  - secure auction of beetroots in Denmark (BRICS)
  - oblivious transfer for road pricing (COSIC)

36

## Anonymous credentials

- Chaum in the 1980s: science fiction
  - Proof knowledge of a signature
  - Rather than possession of a private signing key
  - Can also prove predicates on attributes
  - Verifier gains no additional information
    - Except in case of abuse – judge can intervene
  - Secure even if Issuer and Verifier collude (single/multiple show)
- Concrete protocols
  - Chaum-Pedersen and Brands: Credentialica – U-Prove (Microsoft)
  - Camenish-Lysyanskaya - Idemix (IBM)
  - DAA in TPM

Recent announcement: patents will be freed 37

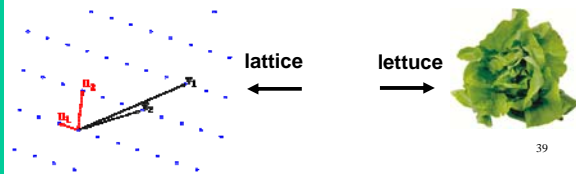
## Internet voting

- Helios [Adida'08] [www.heliosvoting.org](http://www.heliosvoting.org)
  - sophisticated cryptographic protocols: open audit
  - open source
- Spring 2009: rector elections in UC, Belgium
- August 2010: adopted by IACR
- +
  - remote voting
  - as everything is encrypted, log files can be made public so disputes can be resolved easily
- -
  - coercion risk
  - Trojan or virus can easily undermine these elections (proof of concept [Desmedt'09])

not suitable for public sector elections 38

## Fully homomorphic encryption

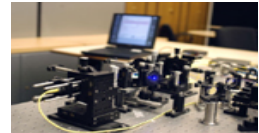
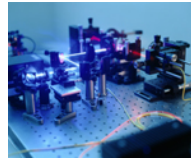
- From  $E(x)$  and  $E(y)$ , you can compute  $E(x+y)$ ,  $E(c.x)$  and  $E(x.y)$  **without decrypting**
- Many cool applications including cloud computing
- [Gentry'09] ideal lattices = breakthrough
- First implementations require only seconds [Vercauteren-Smart'10], [Gentry-Halevi'10]....
  - but to ciphertext for 1 bit is 3 million bits and public key is several Mbyte



39

## Quantum cryptography

- Security based
  - on the assumption that the laws of quantum physics are correct
  - rather than on the assumption that certain mathematical problems are hard



40

## Quantum cryptography

- no solution for entity authentication problem (bootstrapping needed with secret keys)
- no solution (yet) for multicast
- dependent on physical properties of communication channel
- cost
- implementation weaknesses (side channels)

41

## Quantum hacking

<http://www.iet.ntnu.no/groups/optics/qcr/>



42

### Challenges for crypto

- security for 50-100 years
- authenticated encryption of Terabit/s networks
- ultra-low power/footprint

secure software and hardware implementations

algorithm agility



43

### Information storage and transmission

- 2010: digital universe is 1.2 Zettabyte; this corresponds to 600 million hard drives with a capacity of 2 Terabyte (2020: 80 Zettabyte)
- 2014: global internet traffic will grow to 64 Exabyte/month (2009: 15 Exabyte)

Megabyte  $10^6$   
Gigabyte  $10^9$   
Terabyte  $10^{12}$   
Petabyte  $10^{15}$   
Exabyte  $10^{18}$   
Zettabyte  $10^{21}$

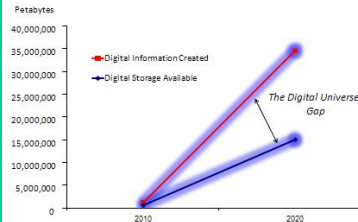


photo 1 Mbyte  
song 50 Mbyte  
movie 4.7 Gbyte  
95 yrs 3.10<sup>9</sup> seconds  
life movie 3 Petabyte

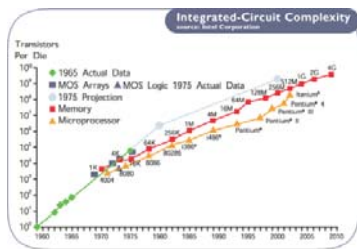
44

### 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\$



45

### 2020 and beyond

- Psychology: humans are very bad at managing and evaluating risks in complex systems
- Economics: information security risks are typically systemic with large market failures in part due to negative externalities (e.g. software, e-commerce)
- Not so different from other areas: deep oil drilling, nuclear energy, finance industry, global warming, – The larger the scale, the larger the risk (too big to fail)

46

### 2020 and beyond: CPUs everywhere:

- merging of physical and cyberworld
- massive memory and processing
- automation of many physical tasks
- computer-brain interfaces
- artificial organs
- social networks



47

### 2020 and beyond

- Total loss of privacy for individual
- Security for society depends on the answer to the following questions:
  1. Are we **technically** able to build robust and secure networked systems
    - with 10 trillion devices
    - that each consist of 100 billion transistors
    - the most complex ones will have 1 billion lines of code
  2. If yes, can our society **understand** and **manage** the risks that are **unlikely to be solvable by market forces**

48