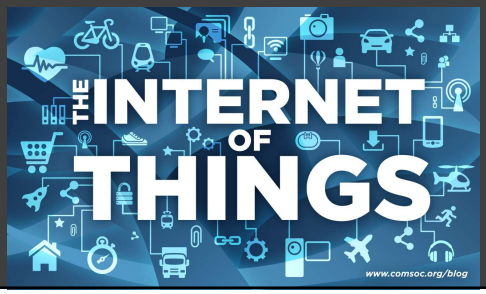
The Future of Security

Bart Preneel
imec-COSIC KU Leuven

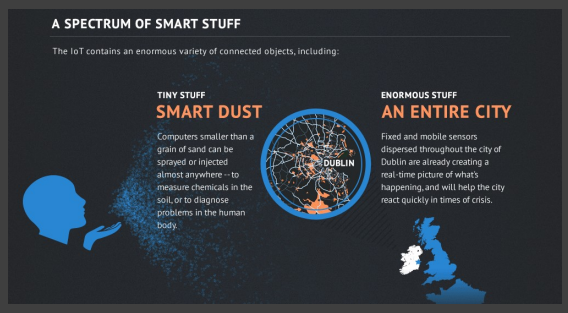
imec embracing a better life
COSIC
KU LEUVEN

Trend 1

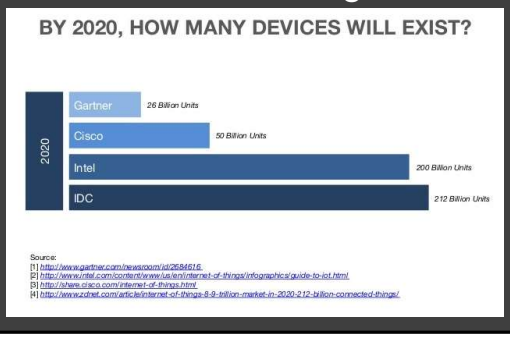
IoT makes IT more intrusive



IoT markets (source: Intel)



How fast will IoT grow?



Intrusive
unavOidable
sTealthy

IoE security risks

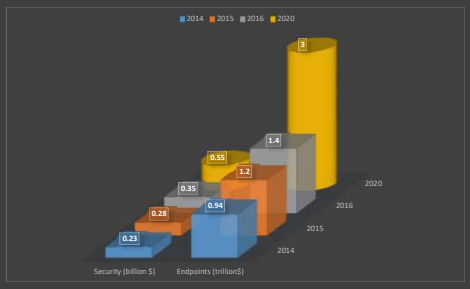
IoE security risks

Low cost
Large attack surface
Hard to update

Market for lemons
Tragedy of the commons
Lack of regulation

IoT: security vs. endpoint spending

[Gartner, Apr 2016]



Trend 2

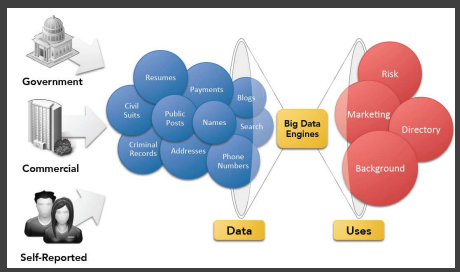
Big Data and Data Analytics for Security

Big data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization.

veracity

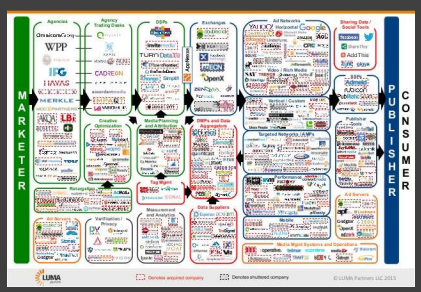
Gartner, 2010

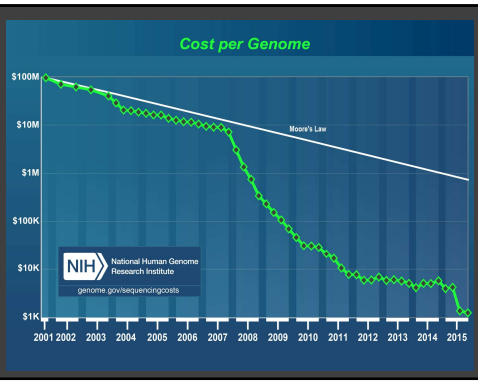
The data supply chain [Jim Adler]



https://www.usenix.org/sites/default/files/conference/protected-files/adler_sec13_slides.pdf

The Internet advertising ecosystem





Big Data for Security

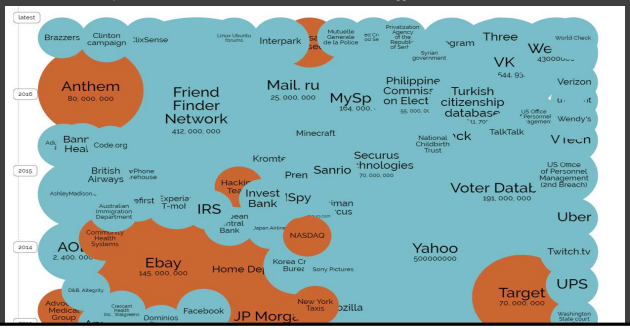
If you have no visibility of your systems, how can you secure them?

Prevention is hopeless: if you detect all incidents, you can stop the bad guys in a cost effective way (read: you can reduce investments in prevention)

By applying analytics to incident data sets, we can learn how the bad guys behave and detect them even faster next time around

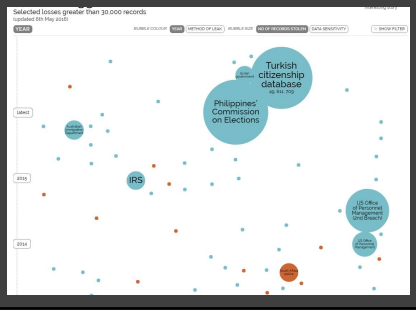
World's Biggest Data Breaches

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



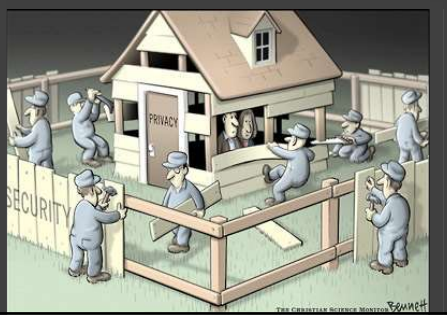
World's Biggest Government Data Breaches

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



OPM – 21 million people
Forms submitted by military and intelligence personal for security clearances
(eye colour, financial history, substance abuse)

Privacy is a security property

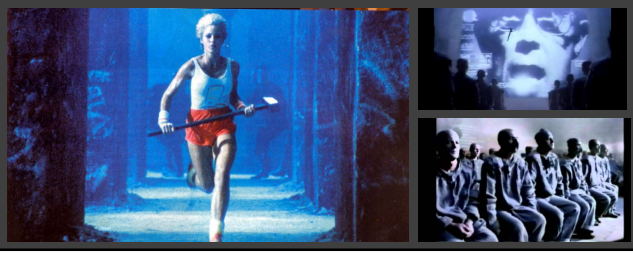


A metafor

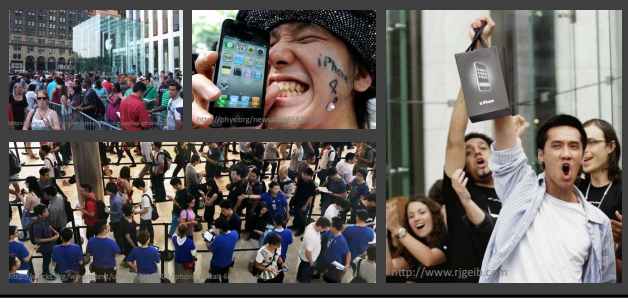
Thinking of
Big Data in terms
of pollution

Trend 4: Big Data for mass surveillance

« Who knew in 1984…



… and the Zombies would be paying customers ? »

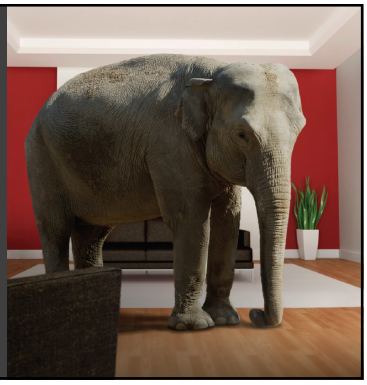


NSA calls the iPhone users public 'zombies' who pay for their own surveillance

It's the

metadata

stupid

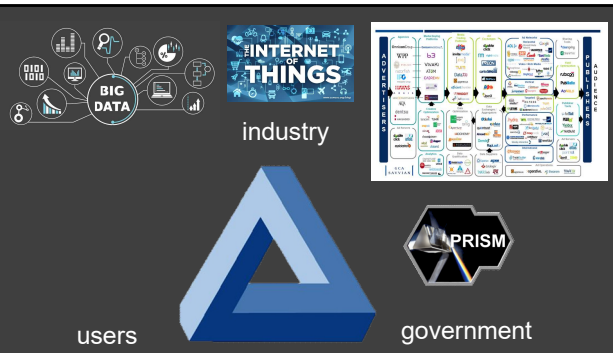


Which questions can one answer with mass surveillance systems/bulk data collection?

Tempora (GCHQ) ~ Deep Dive Xkeyscore (NSA)

- I have one phone number – find all the devices of this person, his surfing behavior, the location where he has travelled to and his closest collaborators
- Find all Microsoft Excel sheets containing MAC addresses in Belgium
- Find all exploitable machines in Panama
- Find everyone in Germany who communicates in French and who use OTR, Signal or Telegraph

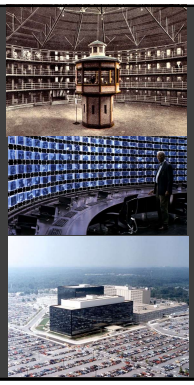
BND has spied on EU (incl. German) companies and targets in exchange for access to these systems



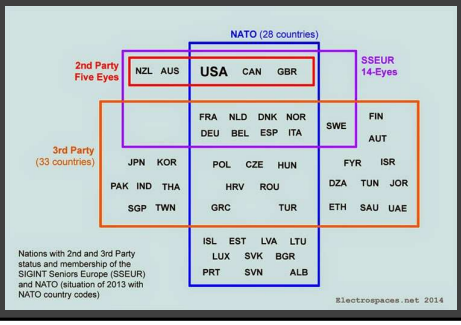
Mass Surveillance

panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse



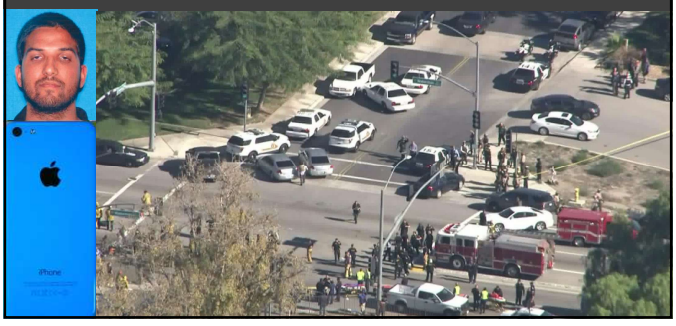
NSA is not alone



Trend 5

The Crypto Wars will ~~return~~ continue

San Bernardino, CA, December 2, 2015



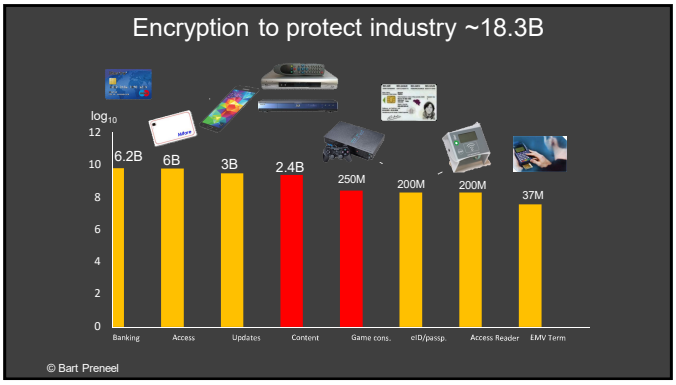
At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone

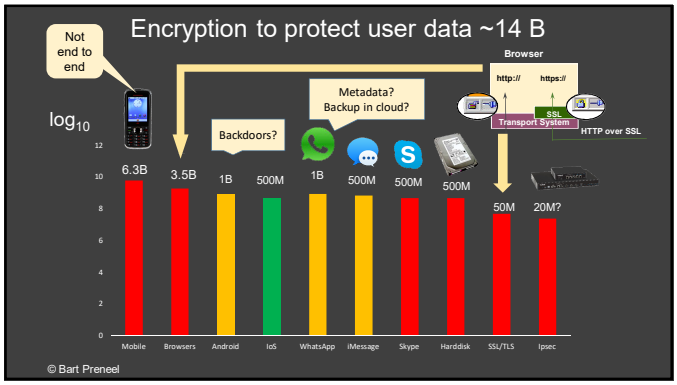
It is an old battle

We are going dark

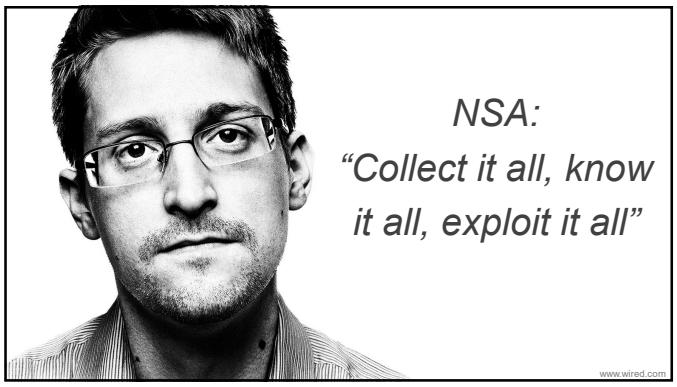
"[I]n our country, do we want to allow a means of communication between people which we cannot read?"

France and Germany push for encryption limits


Encryption to protect industry ~18.3B
log10
12
10
8
6
4
2
0
6.2B
6B
3B
2.4B
250M
200M
200M
37M
Banking
Access
Updates
Content
Game cons.
eID/passp.
Access Reader
EMV Term
© Bart Preneel


Encryption to protect user data ~14 B
Not end to end
Browser
http://
https://
SSL
Transport System
HTTP over SSL
Metadata? Backup in cloud?
Backdoors?
log10
12
10
8
6
4
2
0
6.3B
3.5B
1B
500M
1B
500M
500M
500M
50M
20M?
Mobile
Browsers
Android
IoS
WhatsApp
iMessage
Skype
Harddisk
SSL/TLS
Ipsec
© Bart Preneel


Trend 6
Nation state hacking and cyber arms proliferation


NSA:
"Collect it all, know it all, exploit it all"
www.wired.com

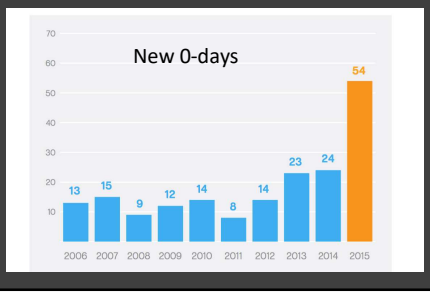

Names and definitions of leaked CIA hacking tools
CENTRAL INTELLIGENCE AGE
www.techcrunch.com

(Part of) government seems to prefer offense over defense

How many 0-days does the FBI and the NSA have?

Are they revealed to vendors?

If so when?



We need a Digital Geneva Convention

Microsoft President Brad Smith:

"Nation states are hacking civilians in peace time"

Architecture is politics [Mitch Kaipor'93]

Avoid single point of trust that becomes single point of failure

COMSEC - Communication Security

Secure channels: still a challenge

- authenticated encryption studied in CAESAR http://competitions.cr.yp.to/caesar.html

Forward secrecy: Diffie-Hellman versus RSA

Denial of service

Simplify internet protocols with security by default: DNS, BGP, TCP, IP, http, SMTP,…

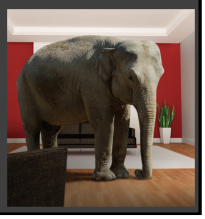
Or start from scratch: Gnunet [Grothoff+], SCION [Perrig+]

COMSEC - Communication Security

meta data

Hiding communicating identities
- few solutions – need more
- largest one is TOR with a few million users
- well managed but known limitations
  - e.g. security limited if user and destination are in same country

- Location privacy: problematic

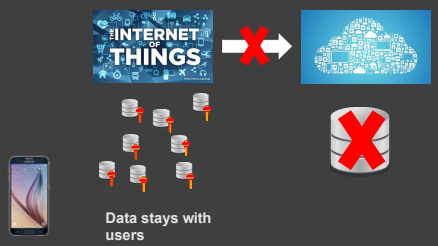


COMPUSEC - Computer Security

Protecting data at rest
- well established solutions for local encryption: Bitlocker, Truecrypt
- infrequently used in cloud
  - Achilles heel is key management
  - Territoriality

Secure execution
- essential to avoid bypassing of security measures

From Big Data to Small Local Data



Distributed solutions work

Root keys of some CAs

Skype (pre -2011)

Cryptocurrencies

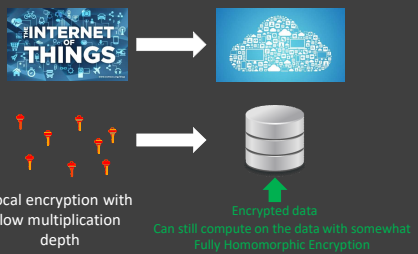
Distributed systems with local data

Many services can be provided based on local information processing
- advertising
- proximity testing
- set intersection
- road pricing and insurance pricing

Cryptographic building blocks: ZK, OT, PIR, MPC, (s)FHE

Almost no deployment:
- massive data collection allows for other uses and more control
- fraud detection may be harder
- lack of understanding and tools

From Big Data to Encrypted Data



Centralization for small data

exceptional cases such as genomic analysis

- pseudonyms
- differential privacy
- searching and processing of encrypted data
- strong governance: access control, distributed logging

fascinating research topic but we should

favor local data

not oversell cryptographic solutions

Open (Source) Solutions

Effective governance

Transparency for service providers

EU-FOSSA **EU Free and Open Source Software Auditing**

Conclusions (research)

Rethink architectures: distributed

Shift from network security to system security

Increase robustness against powerful opponents who can subvert many subsystems during several lifecycle stages

Open technologies and review by open communities

Cryptomagic can help

Conclusions (policy)

Pervasive surveillance needs **pervasive collection** and **active attacks** with massive collateral damage on our ICT infrastructure

Back to targeted surveillance under the rule of law

- avoid cyber-colonialism [Desmedt]
- need industrial policy with innovative technology that can guarantee economic sovereignty
- need to give law enforcement sufficient options

Bart Preneel, imec-COSIC KU Leuven

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
TWITTER: @CosicBe
TELEPHONE: +32 16 321148

ECRYPT CSA

http://www.ecrypt.eu.org

59

Further reading

Books

Glenn Greenwald, No place to hide, Edward Snowden, the NSA, and the U.S. Surveillance State, Metropolitan Books, 2014

Documents:

https://www.eff.org/nsa-spying/nsadocs
https://cjfe.org/snowden

Articles

Philip Rogaway, The moral character of cryptographic work, Cryptology ePrint Archive, Report 2015/1162

Bart Preneel, Phillip Rogaway, Mark D. Ryan, Peter Y. A. Ryan: Privacy and security in an age of surveillance (Dagstuhl perspectives workshop 14401). Dagstuhl Manifestos, 5(1), pp. 25-37, 2015.

More information

Movies

Citizen Four (a movie by Laura Poitras) (2014) https://citizenfourfilm.com/

Edward Snowden - Terminal F (2015) https://www.youtube.com/watch?v=Nd6qN167wKo

John Oliver interviews Edward Snowden https://www.youtube.com/watch?v=XEVlyP4_11M

Snowden (a movie by Oliver Stone) (2016)

Zero Days (a documentary by Alex Gibney) (2016)

Media

https://firstlook.org/theintercept/

http://www.spiegel.de/international/topic/nsa_spying_scandal/

Very short version of this presentation: https://www.youtube.com/watch?v=uYk6yN9eNfc