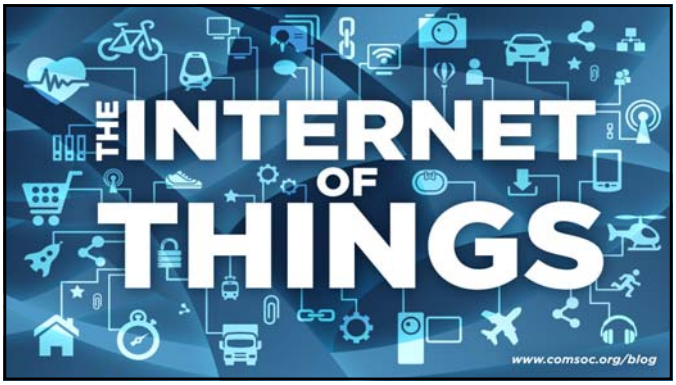
The Future of Security

Bart Preneel
imec-COSIC KU Leuven

imec COSIC KU LEUVEN



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.

Gartner, 2010

Trend 1

Big Data and Data Analytics for Security

Big Data for Security

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

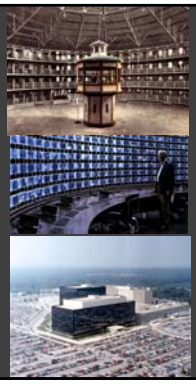
Prevention is hopeless: if you detect all incidents, you can stop the bad guys in a cost effective way (read: you can reduce investments in prevention)

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

Mass Surveillance

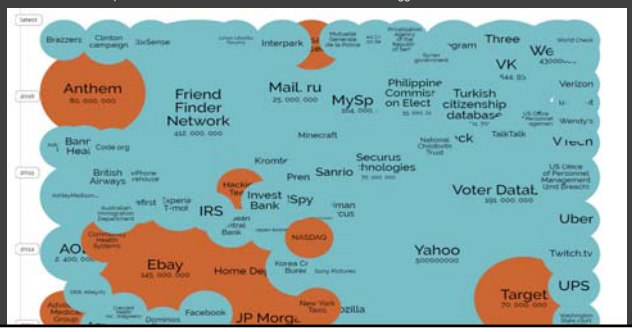
panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse



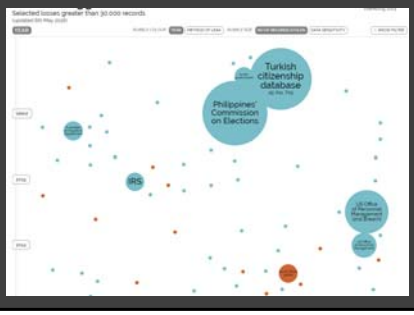
World's Biggest Data Breaches

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



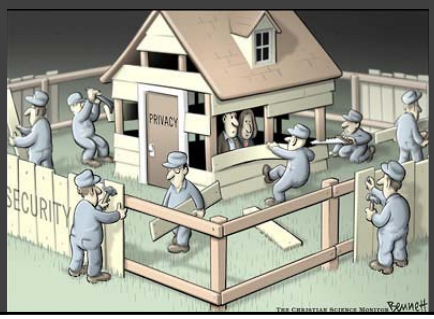
World's Biggest Government Data Breaches

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



Trend 3

Everything will be called "Privacy by Design"

Legal dimension

04/05/2016 General Data Protection Regulation (GDPR) 2016/69 published

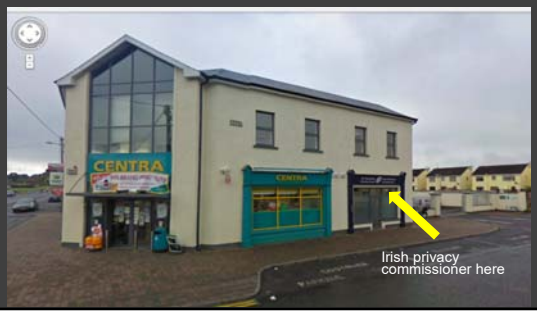
28/05/2018 GDPR comes into force

"Privacy by Design"

Fines up to 4% of global turnover

Excludes national security

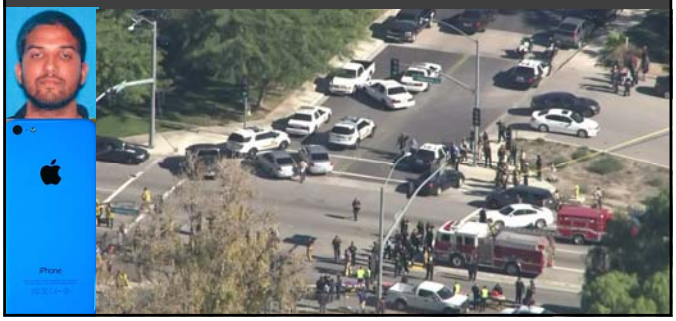
06/10/2015 Court of Justice of the European Union invalidates Safe Harbour US - replacement: Privacy Shield



Trend 4

The Crypto Wars will ~~return~~ continue

San Bernardino, CA, December 2, 2015



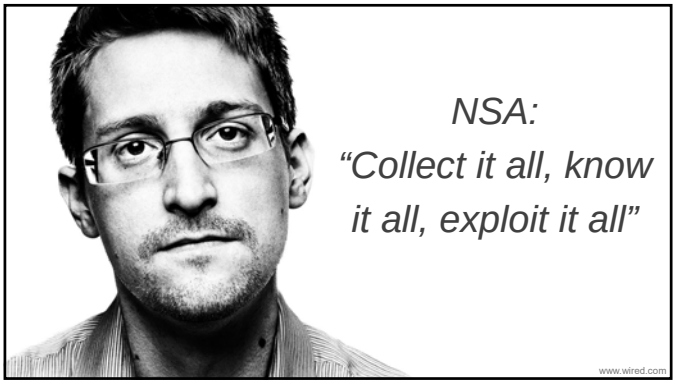
At the request of the FBI, based on an all writs order (1789), a U.S. federal magistrate judge has ordered Apple to break the security of the iPhone

March 28: FBI gets access with help of a hacker at the cost of over US$ 1 million

…yielded almost no useful information

April 22: federal government withdraws from a similar case in NY related to drugs trafficking

Sergei Skorobogatov: The bumpy road towards iPhone 5c NAND mirroring. arXiv:1609.04327, Sept. 2016 (US$ 100 kit)



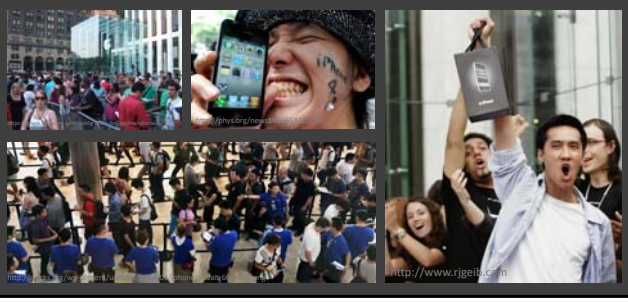
NSA:

"Collect it all, know it all, exploit it all"

« Who knew in 1984…

… that this world would be big Brother … »

… and the Zombies would be paying customers ? »



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

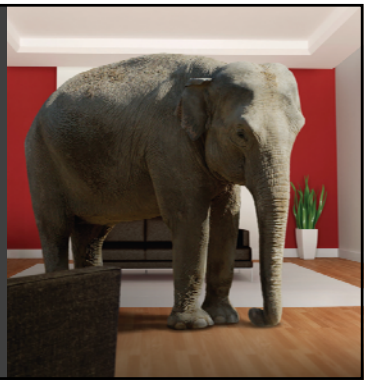
US citizens have protections based on 4th Amendment but Europeans don't

NSA and GCHQ claim that they perform targeted surveillance while they run mass surveillance programs (Tempora and XKeyScore Deep Dive)

It's the

metadata

stupid

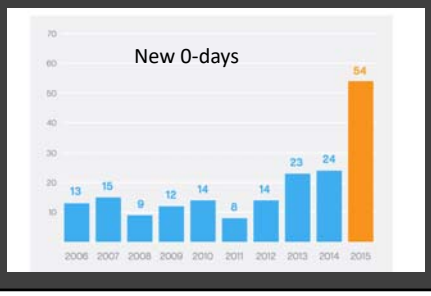


(Part of) government seems to prefer offense over defense

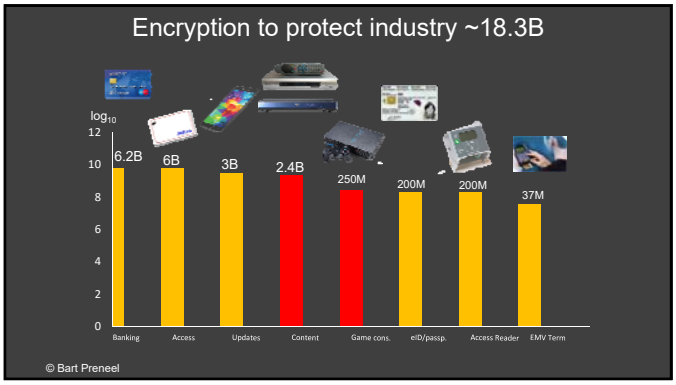
How many 0-days does the FBI and the NSA have?

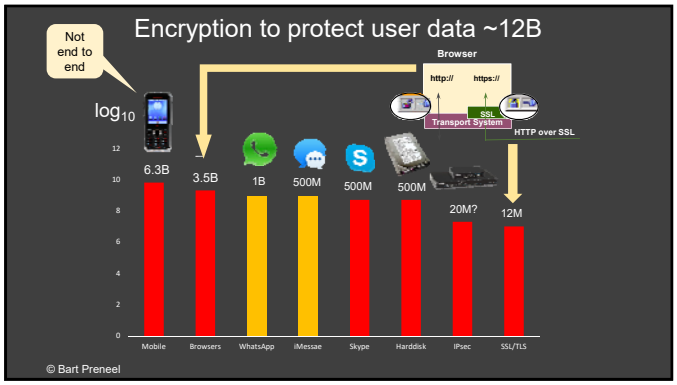
Are they revealed to vendors?

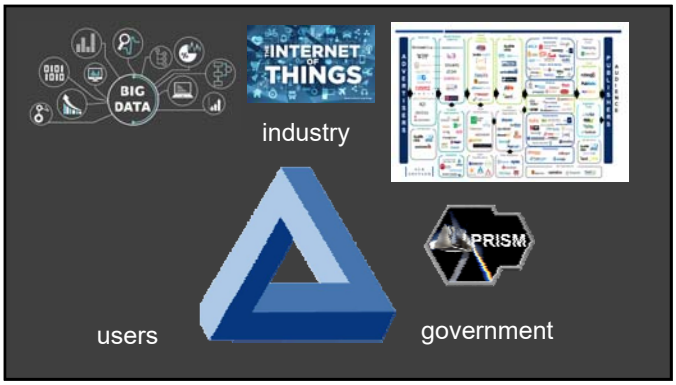
If so when?



It is an old battle


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 ~12B
Not end to end
Browser
http://
https://
SSL
Transport System
HTTP over SSL
log10
12
10
8
6
4
2
0
6.3B
3.5B
1B
500M
500M
500M
20M?
12M
Mobile
Browsers
WhatsApp
iMessae
Skype
Harddisk
IPsec
SSL/TLS
© Bart Preneel


BIG DATA
INTERNET OF THINGS
industry
PRISM
users
government


Optimism is a moral duty


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

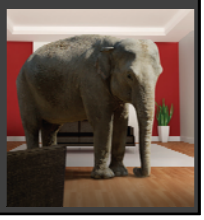
Denial of service

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

From Big Data to Small Local Data

Data stays with users
Local computation

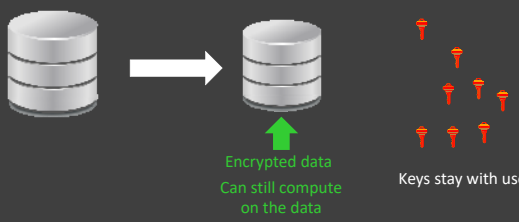
Distributed solutions work

Root keys of some CAs

Skype (pre -2011)

Cryptocurrencies

From Big Data to Encrypted Data



Encrypted data
Can still compute on the data

Keys stay with users

Open (Source) Solutions

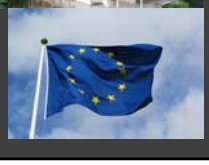
Effective governance

Transparency for service providers

Rearchitect our Infrastructure

Industrial policy

Protecting sovereignty and human rights



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

44