The Future of Identity, Security and Privacy

Bart Preneel
imec-COSIC KU Leuven
Trend 1
IoT makes IT more intrusive
IoT security risks
IoT security risks

- Low cost
- Large attack surface
- Hard to update

Market for lemons
Tragedy of the commons
No regulation
IoT: security vs. endpoint spending

[Gartner, Apr 2016]
Trend 2
Big Data and Data Analytics for Security
Richard Stallman: the cloud is someone else’s computer
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
Trend 3

Big Data means ever bigger breaches
World’s Biggest Data Breaches

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks
Privacy is a security property
Thinking of Big Data in terms of pollution

A metaphor
Prof. Dr. Bart Preneel: THINKING OF BIG DATA IN TERMS OF POLLUTION:

BIG DATA
Trend 4: Big Data for mass surveillance

« 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
It’s the metadata stupid
Mass Surveillance

panopticon
[Jeremy Bentham, 1791]

discrimination
fear
conformism - stifles dissent
oppression and abuse
Trend 5: Big Data for Identity
Identity: common law versus the rest

100+ countries with compulsory national ID cards
15 countries with optional national ID cards
9 countries without national ID cards

but only few have no national register
(including 5 eyes)

but those still have registers for social security, driving licenses, ...
Contracts: US versus Belgium

US

• Acceptable to sneak in nasty clauses in the middle of an 80-page contract
• But a scan of a signature is fine

Belgium

• Still insists on paper copies
Identity Management: back to 2002

Legend:
- Identity of Alice
- Partial Identity of Alice

- Government
- MasterCard
- Diners Club
- Alice
- Telecom
- Leisure
- Work
- MasterCard
- Visa
- Diners Club
- Boyfriend
- Travel
- Shopping
- Payment
- Cellphone Number
- Blood Group
- Income
- Name
- Age
- Health Status
- Address
- Credit Rating
- Birthday
- Foreign Languages
- Phone Number
- Likes & Dislikes
- Tax Status
- Health Care
- Insurances
- Driving Licence
- Interests
- Birthplace
- Good Conduct Certificate
- Diary
- Income
- Birthday
- Birthplace
- Name
- Address
- Credit Rating
- Likes & Dislikes
- Phone Number
- Income
Conflicting views

Ideal world

• User centric
• Privacy: prove properties of attributes using anonymous credentials
• GDPR: “privacy by design”

Real world

• A few large players trace us everywhere on the web and in apps
• Sophisticated privacy settings but real control is unclear
• Major source of advertising income
• Trends: price discrimination, recommendations, banking services
EU focus: entity/data authentication
EU and e-signature

Electronic Signatures Directive 1999/93/EC
- no regulation of CAs (Diginotar!)
- define e-signature, AES, QES

eiDAS Regulation EU 910/2014
- legal framework for mutual recognition by governments
- allows for cloud signing
- 3 levels of security
- crossborder
- electronic seals (legal entities/corporates)
- trust mark for trust services

Divergent implementations
Technology neutral??
Sometimes way too strict
15cm of standards
Does not allow cloud signing
eIDAS: cloud-based trust services

Directive 1999/93/EC
• ‘electronic signature creation data that the signatory can use under his sole control’.

eiDAS
• ‘electronic signature creation data that the signatory can use under his sole control, with a high level of confidence’.
eIDAS: cloud-based trust services

Not secure enough: WYSIWYS

• steal key
• signing Trojan
eIDAS: cloud-based trust services

WYSIWYS?
eIDAS: cloud-based trust services

KISS
Google signs a statement: “user with Gmail account `Bart Preneel’ agrees to contract X” (just need 1 key)

WYSIWYS?
Data/entity authentication requires a secure computer

Is this what the industry calls trusted computing?
Behavioural biometrics for entity authentication

- How you hold phone
- Gait
- Voice (text-dependent and text-independent)
- Keystroke dynamics
- Handwritten signature
- ...

- Easy to use and less intrusive
- Mix of characteristic of individual and device
- Variable-size data streams
- Learning system
- What if person is distressed?
- FAR/FRR worse than for physiological
Google Trust API
Identity management choices

secure local information vs. the surveillance approach
Architecture is politics [Mitch Kaipor’93]

Avoid single point of trust that becomes single point of failure
Secure computing

Trusted by the user
From Big Data to Small Local Data

Data stays with users
From Big Data to Encrypted Data

Local encryption with low multiplication depth

Encrypted data
Can still compute on the data with somewhat Fully Homomorphic Encryption
Open (Source) Solutions

Effective governance

Transparency for service providers

EU Free and Open Source Software Auditing
Control technology to take control of our lives

Industrial policy

European sovereignty and values
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

http://www.ecrypt.eu.org
Credits

Napoleon
By Jacques-Louis David - zQEbF0AA9NhCXQ at Google Cultural Institute, Public Domain, https://commons.wikimedia.org/w/index.php?curid=22174172

Trustmark