Confidentialité et sécurité

Introduction

Dr. Jan Camenisch

Cryptography & Privacy
Principal Research Staff Member
Member, IBM Academy of Technology
33% of cyber crimes, including identity theft, take less time than to make a cup of coffee.
10 Years ago your personal data on the black market was worth $150. Today....
We have an increasing amount of data and many are personal
We use them with different devices, store them anywhere
We use and generate them in interaction with other entities
to make things worse: it's en vogue to let users manage their data :-(

© 2015 IBM Corporation
But how can we protect all these data?
Houston, we have a problem!
Houston, we have a problem!

“Buzz Aldrin's footprints are still up there”
(Robin Wilton)
Computers don't forget

- Data storage ever cheaper → “store by default”
  - also collateral collection, surveillance cameras, Google Street View with wireless traffic, Apple location history,…

- Data mining ever better
  - self-training algorithms cleverer than their designers
  - not just trend detection, even prediction, e.g., flu pandemics, ad clicks, purchases,…
  - what about health insurance, criminal behavior?

- The world as we know it
  - Humans forget most things too quickly
  - Paper collects dust in drawers

We build apps with the paper-based world in mind :-(
  - if it works it works
  - security too often still an afterthought
  - implementors too often have no crypto education
You have no privacy, get over it .....?!

… “I have nothing to hide!”
… “The intelligence agencies have all my data anyway”

- Huge security problem!
  - Millions of hacked passwords (100,000 followers $115 - 2013)

- Difficult to put figures down
  - Credit card fraud
  - Spam & marketing
  - Manipulating stock ratings, etc..
  - (Industrial) espionage

- We know that 3 letter orgs can do it easily, but they are not the only ones
  - however, this is not about homeland security
  - and of course there are limits to the degree of protection that one can achieve

- Last but not least: data are the new money, so they need to be protected!
What does that mean?

- **Apply Data Minimization – Privacy & Security by Design**
  - Require users to reveal only the data that are really needed
  - Do not design with the sandy beach beach in mind

- **Encrypt every bit and attach usage & access control policy**
  - Data should never ever be in the clear
    - process it in the encrypted domain
    - still need to manage keys carefully
  - Needs to support switching of cryptographic algorithms
    - symmetric key crypto gets broken at times
    - beware of quantum computers
Cryptography to the Aid
Privacy Attribute-based credentials

- Service provider tells user what attribute are required
- User transforms credentials into a token with just these attributes
- Service provider can verify token w.r.t. issuers' verification keys

See: idemixdemo.mybluemix.net
Password-based cryptography
- Off-line vs on-line attacks
- Solution: distributed password verification
- Done s.t. no info depends solely on password
- Must work even for short passwords (mobile)

Various operations possible
- Secure password verification
- Strong authentication (client certificates, two factor authentication)
- Digital signatures, decryption
- Password vault

→ Virtual Smartcard/Security Token
Securing the Cloud

First of all: cloud is (also) a deployment model

- "Fully homomorphic encryption" – works only for rather small computation
- Multiparty computation
  - secret share data
  - distributed computation
  - can compile programs

Secure computation in the cloud (and your servers)
(Personal) data → allows us to learn lots of new and important things

- Marketing, Medical data, traffic control, ....
- How can we have the benefits without all the cons?
  → Anonymization of data
Let engage in some rocket science!

- Much of the needed technology exists
- … need to use them & build apps “for the moon”
- … and make apps usable & secure for end users

Thank you!