Cryptographic dimensions of Privacy

Dr. Jan Camenisch
Principle RSM; Member, IBM Academy of Technology
IBM Research – Zurich

@JanCamenisch
ibm.biz/jancamenisch
We all increasingly conduct our daily tasks electronically

....are becoming increasingly vulnerable to cybercrimes
33% of cyber crimes, including identity theft, take less time than to make a cup of tea.
10 Years ago, your identity information on the black market was worth $150. Today….
$4,500,000,000 cost of identity theft worldwide
Houston, we have a problem!
Houston, we have a problem!

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

- Apps built to use & generate (too much) data
- Data is stored by default
- Data mining gets ever better
- New (ways of) businesses using personal data

- Humans forget most things too quickly
- Paper collects dust in drawers
Where's all my data?

The ways of data are hard to understand

- Devices, operating systems, & apps are getting more complex and intertwined
  - Mashups, Ad networks
  - Machines virtual and realtime configured
  - Not visible to users, and experts
  - Data processing changes constantly

→ No control over data and far too easy to lose them
"Applications are designed with the sandy beach in mind but are then built on the moon"

- Feature creep, security comes last, if at all
- Everyone can do apps and sell them
- Networks and systems hard not (well) protected
Security & Privacy is not a lost cause!

We need paradigm shift & build stuff for the moon rather than the sandy beach!
That means:

- Reveal only minimal data necessary
- Encrypt every bit
- Attach usage policies to each bit

Cryptography can do that!
The case of authentication

IBM Identity Mixer

authentication without identification
Alice wants to watch a movie at Movie Streaming Service

I wish to see Alice in Wonderland

Alice

Movie Streaming Service
Alice wants to watch a movie at Movie Streaming Service

You need:
- subscription
- be older than 12
Watching the movie with the traditional solution

Using digital equivalent of paper world, e.g., with X.509 Certificates

ok, here's
- my eID
- my subscription

Alice

Movie Streaming Service
Watching the movie with the traditional solution

...with X.509 Certificates

Aha, you are
- Alice Doe
- born on Dec 12, 1975
- 7 Waterdrive
- CH 8003 Zurich
- Married
- Expires Aug 4, 2018

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Watching the movie with the traditional solution

This is a privacy and security problem!

- identity theft
- discrimination
- profiling, possibly in connection with other services

Aha, you are
- Alice Doe
- born on Dec 12, 1975
- 7 Waterdrive
- CH 8003 Zurich
- Married
- Expires Aug 4, 2018

Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Watching the movie with the traditional solution

With OpenID (similar protocols), e.g., log-in with Facebook

ok, I'm Alice@facebook.com

Alice

Movie Streaming Service
Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook

Aha, Alice is watching a 12+ movie
Watching the movie with the traditional solution

With OpenID and similar solution, e.g., log-in with Facebook

Aha, Alice is watching a 12+ movie

Aha, you are
- Alice@facebook.com
- 12+
Mplex Customer
- #1029347
- Premium Subscription
- Expires Jan 13, 2016

Movie Streaming Service
Identity Mixer solves this.

When Alice authenticates to the Movie Streaming Service with Identity Mixer, all the services learns is that Alice

has a subscription

is older than 12

and no more!
Privacy-protecting authentication with Privacy ABCs

Users' Keys:

- One secret Identity (secret key)
- Many Public Pseudonyms (public keys)

→ use a different identity for each communication partner or even transaction
Privacy-protecting authentication with Privacy ABCs

Certified attributes from Identity provider

- Issuing a credential

Name = Alice Doe
Birth date = April 3, 1997
Privacy-protecting authentication with Privacy ABCs

Certified attributes from purchasing department

- Issuing a credential
Privacy-protecting authentication with Privacy ABCs

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12
Proving identity claims

- but does \textit{not} send credentials
- only minimal disclosure
Proving Identity Claims: Minimal Disclosure

Alice Doe
Dec 12, 1998
Hauptstr. 7, Zurich
CH
single
Exp. Aug 4, 2018

 verifies ID

Age: 12+
Exp. Valid

 verifies ID
Privacy-protecting authentication with Privacy ABCs

Proving identity claims

- but does not send credential
- only minimal disclosure

Transaction is not linkable to any other of Alice's transactions!

Aha, you are
- older than 12
- have a subscription

(Public Verification Key of issuer)
Try Identity Mixer for yourself

Try yourself:
Build your app:
Source code:
Info:
idemixdemo.mybluemix.net
github.com/IBM-Bluemix/idemix-issuer-verifier
github.com/github.com/p2abcengine/p2abcengine
ibm.biz/identity_mixer
You might already have Identity Mixer on your devices

Identity Mixer (and related protocols) in standards

- FIDO Alliance authentication is standardizing this as well (w/ and w/out chip)

TPMs allow one to store secret key in a secure place!
Other examples: secure and privacy access to databases

Who accesses *which data* at which time can reveal sensitive information about the users (their research strategy, location, habits, etc.)

- DNA databases
- News/Journals/Magazines
- Patent database

Cryptography access protocol s.t. database provider has *no* information about

- which user accesses
- which data
Let engage in some rocket science!

- Much of the needed technology exists
- … need to use them & build apps “for the moon”
- … get crypto experts on your design team

Thank you!