Authentication without Identification
How to Protect On-Line Identity

Dr. Jan Camenisch

Principle Research Staff Member
Member, IBM Academy of Technology
IBM Research – Zurich

@JanCamenisch
jca@zurich.ibm.com
ibm.biz/jancamenisch
33% of cyber crimes, including identity theft, take less time than to make a cup of tea.
10 Years ago, your personal data on the black market was worth $150. Today....
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
  - 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!
Privacy is not a lost cause!

we need paradigm shift & build stuff for the moon rather than the sandy beach!
Private Credentials
The paradigm shift for authentication
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
With OpenID and similar solution, e.g., log-in with Facebook

ok, I'm Alice@facebook.com
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

Alice

Movie Streaming Service
Private Credentials (Privacy- ABC) solve 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)
Certified attributes from Identity provider

- Issuing a credential

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

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Movie Streaming Service

Alice
Privacy-protecting authentication with Privacy ABCs

Alice

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Alice

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service

Concept: presentation policy
Proving identity claims

- but does not send credential
- only minimal disclosure

Privacy-protecting authentication with Privacy ABCs

Alice

- valid subscription
- eID with age ≥ 12

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Proving identity claims
- but does not send credential
- only minimal disclosure

Alice

Movie Streaming Service

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

(Public Verification Key of issuer)
Alice Doe
Dec 12, 1998
Hauptstr. 7, Zurich
CH
single
Exp. Aug 4, 2018

verified
ID

Age: 12+
Exp. Valid

verified
ID
Try yourself at www.ibm.biz/identitymixer
IBM's Privacy ABCs: Identity Mixer

- Scientific foundation laid 15 years ago, well studied & award winning
- Successful real-world pilots in series of EU projects

- You can have identity mixer, too!
  - Open-source implementation: https://github.com/p2abcengine
  - Idemix-as-a-Service on IBM Bluemix
  - Web-based demo to try for everyone
  - Coming soon: Idemix on mobile
Some Use Cases
Subscriptions, membership

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

- Patent databases
- DNA databases
- News/Journals/Magazines
- Transportation: tickets, toll roads
- Loyalty programs
Anonymous consultations with specialists

- online chat with a psychologist
- online consultation with IBM Watson

1. Alice proves she has insurance
2. Alice describes symptoms
3. Alice gets credential that she is allowed to get treatment
4. Alice gets treatment from physician, hospital, etc
5. Alice sends bill to insurance and proves that she had gotten the necessary permission for the treatment.
Polls, recommendation platforms

Providing anonymous, but at the same time legitimate feedback

- **Online polls**
  - applying different restrictions on the poll participants: location, citizenship

- **Rating and feedback platforms**
  - anonymous feedback for a course only from the students who attended it
  - wikis
  - recommendation platforms
Conclusion – Let's Engage in Some Rocket Science

- Personal data are the oil of the information society

  Still, we hardly protect these data

- Need to protect our infrastructure much better
  - encrypt every bit
  - data parsimony
  - strong authentication, but only to the level necessary

- Necessary technology exists but is not used!
  - and is it not hard to use it
Thank you!

- eMail: idemix@zurich.ibm.com
- twitter: @IdentityMixer
- Links:
  - www.zurich.ibm.com/idemix
  - idemixdemo.zurich.ibm.com
  - github.com/p2abcengine & abc4trust.eu/idemix
  - console.ng.bluemix.net/catalog/services/ibm-identity-mixer/