Cryptography for People

Dr. Jan Camenisch

Cryptography & Privacy
Principal Research Staff Member
Member, IBM Academy of Technology

jca@zurich.ibm.com
@JanCamenisch
ibm.biz/jancamenisch
33% of cyber crimes, including identity theft, take less time than making a cup of coffee.
10 Years ago your personal data on the black market was worth $150. Today…. 
We all increasing amount of data and many are personal

1$ for much more data
use them with different devices, store them anywhere
use and generate them in interaction with other entities

leave collateral data while doing so
to make things worse: it's en vogue to let users manage their data :-(
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
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
  - Not visible to users, and experts
  - Data processing changes constantly

- And the cloud makes it worse...
  - Processing machines can be moved around w/out borders

Far too easy to lose (control over) data and to collect data!
You have zero 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!
Privacy is not a lost cause!

We need paradigm shift &
build stuff for the moon
rather than the sandy beach!
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**
  - 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

- **Attach usage & access control policy to every bit**
  - enforce need to know
  - honest but curious probably good enough
What does it mean: the electronic gap

- Strong security requires strong cryptographic authentication
- Humans rarely can remember cryptographic keys let alone compute with them
- From Humans to Keys – the electronic gap
  - Smart cards, HW tokens: a nuisance!
  - Passwords: … are dead ?!
  - Biometrics: cannot change them, too easily fooled
The Privacy & Security Paradox

We do have the technology/crypto, but it is hardly used
- Deemed too expensive
- Too hard to manage all the keys, fear of loosing keys
- Protecting data is considered futile
- Often required by law, but these are w/out teeth
- Debate about legality of encryption V2.0

On the positive side
- Importance of security and privacy increasingly recognized
- Laws are revised
Cryptography to the Aid
I. Human-Computer authentication
Password-based security: from humans to cryptographic keys

II. Authentication in the Internet without identification
Identity mixer: privacy protecting authentication
Cryptography to the Aid

III. Protecting data by encryption

- **User to User**
  - technology here, used to some extend (storage, email, instant msg)

- **User to Service Provider**
  - technology here, hardly used

- **Between Devices**
  - technology here, somewhat used (VPNs, TLS), missing for IoT

- Biggest Issue: key & access management (cf Diginotar, IoT)

IV. Securing the cloud

- **Deployment Model**

- **Working with encrypted data**
Password-based Security
Password are insecure, aren't they?

username-password the most prominent form of user authentication

Passwords inherently insecure?
No! We're just using them incorrectly
Problem 1: passwords are useless against offline attacks
The problem with passwords

Problem 1: passwords are useless against offline attacks

- NIST: 16 chars ≈ 30 bits entropy ≈ 1 billion possibilities
- $150 GPUs test several billions/second
- More expensive hash functions provide little help

Problem 2: single-server solutions inherently vulnerable to offline attacks
The solution: distributed password verification

Setup: Open account w/ password p

\[ p = p_1 \rightarrow p_2 \]

\[ p = p_1 \rightarrow p_2 \]
The solution: distributed password verification

Login to account with password $p'$

- no server alone can test password
- passwords safe as long as not all servers are hacked
  - off-line attacks no longer possible
  - on-line attacks can be throttled
- pro-active re-sharing possible
- First server
  - web-server $\rightarrow$ replaces hash-data files
  - user's computer $\rightarrow$ secure against loss or theft of user device
How it works in a nutshell

- Servers share encryption secret key $x_1$ and $x_2$ for PK X for homomorphic scheme
- At setup: user encrypts $p$ under X: $E = \text{Enc}_X(p)$
- Password verification: check for encryption of 1

$E' = \left(\text{Enc}_X\left(\frac{1}{p'}\right) \right) \odot \left(E\right)^r$

$= \text{Enc}_X\left(\frac{p}{p'}\right)^r$

- Servers do not learn anything
  - 1 if passwords match, random number otherwise
- User could even be talking to the wrong servers...
One of the servers could be your smart phone, laptop, …
Get key share from if password check succeeded
Decrypt all your files on phone (or stored in the cloud, etc)
From password to cryptographic keys

[CLN12, CLLN14, CEN15]

- One of the servers could be your smart phone, laptop, …
- Get key share from if password check succeeded
- Decrypt all your files on phone (or stored in the cloud, etc)
Identity Mixer
Alice wants to watch a movie at Movie Streaming Service

I wish to see Alice in Wonderland
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
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 and similar solution, 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)
Getting a Credential

- issued on one of the public keys
- by induction on all public keys

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

Alice says: I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Alice

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Concept: presentation policy

I wish to see Alice in Wonderland

You need:
- subscription
- be older than 12

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Like PKI

- but does not send credential
- only minimal disclosure

Alice

- valid subscription
- eID with age $\geq 12$

Movie Streaming Service
Privacy-protecting authentication with Privacy ABCs

Like PKI
- but does not send credential
- only minimal disclosure

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

Movie Streaming Service

(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
So, let's watch a movie!

idemixdemo.mybluemix.net
idemixdemo.zurich.ibm.com
Identity Mixer status

- 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
Further Research Needed!

- **Securing the infrastructure & IoT**
  - “ad-hoc” establishment of secure authentication and communication
  - audit-ability & privacy (where is my information, crime traces)
  - security services, e.g., better CA, oblivious TTPs, anon. routing, …

- **Usability**
  - HCI
  - Infrastructure (setup, use, changes by end users)

- **Provably secure protocols**
  - Properly modeling protocols (UC, realistic attacks models, …)
  - Verifiable security proofs
  - Retaining efficiency
Further Research Needed!

- **Quantum Computers**
  - Lots of new crypto needed still
  - Build apps algorithm agnostic

- **Towards a secure information society**
  - Society gets shaped by quickly changing technology
  - Consequences are hard to grasp yet
  - We must inform and engage in a dialog
Conclusion

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!

Joint work w/ Maria Dubovitskaya, Anja Lehmann, Anna Lysyanskaya, Gregory Neven, and many many more.

jca@zurich.ibm.com @JanCamenisch ibm.biz/jancamenisch