Identity is so overrated

Hogan Lovells Vrouwennetwerk

Bart Jacobs
bart@cs.ru.nl
8 Oct. 2015

Outline

Where we are, sofar

Identities are highly overrated (they are so 2010s)

Ask yourself:

- In how many situations in daily life do you really need to know someone's identity?
  - when do you check someone's identity card / passport?
- Often it is much more useful to know certain properties (here: attributes) of people
  - when you're ill, you care about the *doctor* attribute
  - in public transport, having a *ticket* counts, not who you are
  - when buying a (violent) game, what matters is that you are over 16 or 18

Identities versus attributes

- Identity management seems to revolve around identities
  - In practice this means uniquely identifying numbers, like social security number, or passport number
  - high-value targets for profiling & identity fraud
    (this also holds for pseudonyms)
- But a more flexible identity ecosystem uses attributes
  - 'over 18', 'over 21', 'over 65', 'under 15', 'female', 'male'
  - 'student', 'doctor', 'lawyer', 'top secret clearance'
  - 'NL-citizen', 'resident of Nijmegen'
  - 'home address', 'owner of bankaccount nr. ...'
- Attributes may be identifying (like social security number, bank account, phone number) or non-identifying

Your **identity** is the collection of attributes that hold for you

Key idea in attribute-based IdM

- Each transaction only requires a **subset** of your attributes for authentication
  - the subset should be small & proportional: data minimisation
  - this also offers some protection against identity fraud
- Typical transactions involve a combination of attributes
  - address + bank account, for online shopping
  - minimal age + bank account for online gambling / XXX / ...
  - "doctor" status + medical registration number for write-access to medical record

Attribute-based authentication & authorisation

- Non-identifying attributes are good enough for many transations:
  - a cheaper hair-cut for a student, or cheaper public transport for senior citizens
  - participation in local referendum for locals
  - buying games/books/videos online (over 16, or over 18)
  - participation in chatbox for minors (under 12, or 15)
- Attribute-based extends role-based access control
  - the captain of the ship can turn the ship's wheel
  - very relevant in the medical sector (access to files)
  - in the military (or elswhere): hierarchies/compartments/roles

Where we are, sofar

Essentials of IRMA = I Reveal My Attributes

- An IRMA user can selectively disclose different attributes about him/her self, depending on the situation
  - privacy-by-design, via data minimalisation and user-control
- Attributes are issued by (different, relevant) authorities, and are verified by service providers
- Attributes are reliable via a digital signature of the issuer
  - they also carry a validity date
- Attributes are stored locally, under direct control of the user
  - storage on mobile phone is most convenient
  - attributes are cryptographically bound to the user, and are non-transferrable

Where we are, sofar

iCIS | Digital Security
Radboud University

Privacy essentials

- We naturally live in different contexts
  - home, work, sports club, in church, with friends ...
- We naturally want to keep information in context
  - what we tell to our doctor should not end up in a supermarket
- People get upset when contextual integrity is broken
  - recall anger: about selling customer financial data (ING), about speeding data ending up at the police (TomTom), about school children's performances in online tests ending up at publishers
- When explained like this, almost everybody cares about privacy
  - "I've got nothing to hide" is utter nonsense
  - often promoted by companies/authorities with clear interests

iCIS | Digital Security
Radboud University

Privacy and attributes

- Attributes support **contextual privacy**
  - reveal different aspects of yourself in different contexts
  - attributes support such "partial identities" or "personas"
  - they enable proportional authentication
- Identities support **profiling**
  - the Google's of this world make us use the same identifier everywhere
  - they break-up contexts, and destroy our basic privacy intuitions
  - that's why such companies don't like attribute-based approaches

iCIS | Digital Security
Radboud University

Is IRMA a dead-end project?

- If the giants of the information society don't support attributes, who will?
- The national government is fragmented, without vision/steering
  - EZ only does what companies want, doesn't care about citizens
  - BZK "does not do innovation"
  - Fin, RDW develop their own ad hoc methods
- More enlightened companies, like KPN, are supportive
  - experiments are planned with different user groups
- Regulators (CBP's in EU, FTC in US) may step in and demand use of available privacy-friendly technology.
- European judges — the new heros — may one day forbid ubiquitous identification

In the end, it's all about power

- **Follow the money!**
  - traditional way to understand power structure in society
- **Follow the data!**
  - this is what counts now
  - one big problem is that data flows are hardly transparent

The authentication infrastructure reflects power relations in society

Where we are, sofar

Main points

- Identities are old-skool, attributes are hot
  - basis for flexible, proportional authentication
  - privacy-friendly, and close to our intuitions
- IRMA is an academic demonstration project
  - the technology is open source, and freely available
  - Radboud University has no commercial interests
  - it demonstrates what can be done, and thus raises standards
- IRMA open functionality test will start next week
  - see irmacard.org
  - everyone can participate (with Android phone)
  - this includes easy, cheap self-enrolment (with passports)
  - if interested, do join!

There are privacy-friendly alternatives! We do have a choice!

Demo