Attributes in Action: Next Generation of Electronic Identity Management

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen, The Netherlands

TSCP Workshop, Washington, 25 sept. 2014

Outline

Smart card research @Nijmegen, NL

- Vulnerabilities uncovered in many smart cards:
  - Mifare Classic
  - iClass
  - Secure/Crypto-Memory
  - Hitag2
  - Megamos
- But also more constructive research on secure, attribute-based authentication

What this presentation is about

- Presenting latest technology
  - attribute-based authentication via smart cards

  - IRMA = "I Reveal My Attributes"
  - it uses advanced crypto (so-called zero-knowledge proofs)
- What this technology can do
  - unprecedented privacy protection
  - in combination with security, flexibility and enablement
  - great functionality, not only for privacy fundamentalists

Background: who did what?

- The underlying crypto was developed by IBM Zürich
  - called Idemix; published openly, some 15 years ago
- At Nijmegen University a fast smart card implementation was developed, called IRMA, together with
  - Idemix protocol extensions, like tunnels, revocation
  - an ecosystem for attribute-based identity management
- All based on open source (and open standards)
  - no commercial, only academic, interests
  - independent of government activities in this area

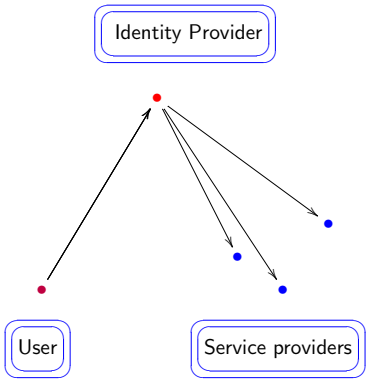
Identities and attributes

- In many situations (online) it is important to know with certainty "who is on the other side of the line"
- But in many situation only partial information is sufficient
  - eg. age verification for buying certain games/movies online
  - access to local government facilities (eg. referendum, disposal)
  - participation in online discussion groups (eg. medical)
  - when someone's identity needs to be shielded
- Attributes support contextual privacy, or different personas

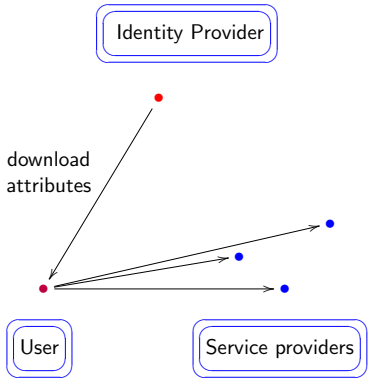
Two main selling points

- Flexibility of attributes (versus inflexibility of identities)
  - selective disclosure of attributes, depending on context
  - eg. for roles (nurse, doctor) or ranks (sergeant, captain)
  - usable for identifying (like: SSN) or non-identifying attributes (like: over 21).
  - the sky-is-the-limit in applications
- Decentralised architecture
  - attributes are stored on-card, not centrally
  - no vulnerable or privacy-unfriendly central hub is needed for verification
  - ideal for international contexts/collaborations (like passports)

Centralised architecture



Decentralised architecture



Security & privacy properties

- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to my private cryptographic key in the card
- Issuer-unlinkability: the issuers should not be able to track where I use which attribute
  - realised via blind signatures
- Multi-show unlinkability: service providers should not be able to connect usage (at different providers)
  - realised via zero-knowledge proofs
- Revocation: rogue attributes (via stolen/lost cards) should be blockable.
  - realised via clever use of "epochs"

What is in it for the military?

- The military organisation has many attributes: ranks, roles, capabilities, clearances, ...
- They like robust, decentralised infrastructure that does not depend on vulnerable hubs
  - (and in their volatile international cooperations such shared hubs may not exist)
- Anonimity can be important, eg. for special forces, intelligence folks, pilot, ...
- but in other cases someone's identity is relevant: flexibility via selective disclosure is required.

Ongoing IRMA pilots

- Chip-company NXP is developing IRMA support in its high-end smart cards ("SmartMX")
- National telecom provider KPN is doing a pilot with Nijmegen to support IRMA on smart phones/tablets
  - via a prototype implementation on SIM-cards
  - but also via a trusted execution enironment (TEE, like TPM)
- Two dozen Redhat developers worldwide are experimentally using IRMA cards for authentication and authorisation
- The computer science student association at Nijmegen is introducing IRMA cards as membership cards
  - used for age verification for drinks, and for event registration
  - also, Nijmegen university as a whole is looking at IRMA cards, both for students and staff (strong authentication)

Conclusions

- Attribute-based identity management is hot
  - privacy-friendly, secure, flexible, ...
- Advanced crypto offers amazing functionality
  - that can actually be implemented on smart cards (IRMA)
  - (and in principle on secured smart phones too)
- This approach fits in privacy/security-by-design strategies
  - our demos lead to higher requirements for privacy protection
  - this may be demanded, at some stage, by regulators
- IRMA is an academic, open project, but it is ready for practical pilots and up-take by industry
  - who seizes the opportunities?
  - more info at `irmacard.org`