FACULTY OF SCIENCE

Bart Jacobs

Privacy and Computer Security, very briefly

Radboud University Nijmegen

Contents

I. Background & main issues

Who is this guy?

- Computer security professor at Nijmegen (NL)
- Apart from academic abstract nonsense, involved in e-government / identity management, like biometric passports, voting, public transport cards, road pricing . . .
- Engaged security community in NL and greater awareness that information security can make or break large ICT-projects
- Occasional role in media

Ongoing change (partly wishful)

From: Database-centric / centralised approach:

- traditional focus of PET
- low-tech crypto, if any
- incidents are structural

To: User-centric / decentralised approach:

- data/credentials stored at user-side
- attributed-based instead of identity-based authorisation (for privacy, against identity-fraud)
- high-tech crypto (eg. zero-knowledge proofs)

Intermediate version

- Storage not with user, but with user control
- Used eg. in Dutch Medical Patient Dossier:
  - storage at caretaker, but central pointer structure
  - user can see access log & set permissions

Underlying societal issues

- Information is power
- Architecture is politics (Mitch Kapor, EFF)
- Those in power typically choose architecture
- Citizen privacy & autonomy needs protection and regulation, more than ever.

II. What went wrong: public transport chipcard

What happened?

- Bumpy, ongoing introduction of national (!) smart card for all public transport in NL
- Card uses Mifare Classic chip, with proprietary weak crypto (48 bits)
- Completely broken in 2008;
  card is “open wallet”, without data protection
- Same cards used in public transport in London, Moscow, Beijing, Boston, . . .
  (and for much more sensitive access control too)

Privacy disaster

- ***Cards***
  - fixed identifier allows individual tracing
  - everyone can see/modify contents
- ***Database***
  - contains travel movements of all citizens (*Stasi* would be jealous)
  - Data protection authority imposes
    - opt-in for marketing, in general
    - opt-out for abstract profiling, for traffic spreading
  - Only procedural limitations

III. What could go right: road pricing

What is happening?

- Replacement of flat road tax by fairer, use-based fees
- also for congestion & pollution reduction/spreading
- Cars will get special box, with GPS and GSM
- Big issue: where will location data be stored:

(1). “**Thin**” box: data are stored centrally

(2). “**Fat**” box: data & fee calculations happen in car

(3). Alternative (joint work with Wiebren de Jonge)

Road pricing via commits

- Main idea: don't send traffic data, but ***hashes of*** traffic data, to central office
- Do this daily; commits drivers to trajectories, without revealing anything
- After photo spot check, ask driver's box for pre-image of hash
- Fee submission also possibly in privacy-friendly and fraud-resistant manner
- Further details in paper on own webpage (more applications possible)

IV. Conclusions

Main points

- Much is possible, leaving people
  - responsible
  - autonomous
  - in control . . .
- . . . but requires:
  - political will
  - and technical skill

(and individual desire to remain responsible/autonomous/in control)