Electronic Identities in Europe

Royal Institution, London
Feb. 21, 2019

Bart Jacobs — Radboud University, Nijmegen, NL
bart@cs.ru.nl

Where we are, so far

Outline

Introduction
Computer security
Identities
Attributes, in theory & practice
Intermediaries & platforms
Privacy
Conclusions

Nijmegen’s Roman history — as Noviomagus
Nijmegen’s landmark bridge over the river *Waal*

The audacious WWII airborne plan of Sept. 1944

The British 1st Airborne Division landed at *Arnhem*, to capture its bridge, but had to withdraw after a week, with heavy losses.

From the movie: *A Bridge Too Far* (© MGM, 1977)

Nijmegen was liberated by ‘Robert Redford’

British tanks crossing Nijmegen bridge — too late

The first Grenadier Guard tank’s commander was Lord Peter Carrington
Where we are, so far

Introduction

Computer security

Identities

Attributes, in theory & practice

Intermediaries & platforms

Privacy

Conclusions

My main area is computer security

Computer Security is about regulating access to (digital) assets

Key issues

- **Assets**: the valuables that need protection
  - Eg. company/government secrets, or personal data (privacy)

- **Regulating access**: involves making sure that the **good guys** can get to the assets, but not the **bad guys**
  - who are we dealing with? who is on the other end of the line?
  - identity is very much part of the area

- Implicitly there is a malicious **attacker** that is trying to get unintended access
Security management summary

```
Assets
  Threats
    Controls
```

Computer security is hot topic

- Modern societies are highly dependent on digital technology
  - it offers great benefits, convenience, connectivity, etc.
- But this also makes us vulnerable
  - via unintended and intended (malicious) failures
  - clearly, the bad guys have gone digital
  - e.g. via cyber crime / espionage / warfare
  - but also via commercial and/or political manipulation
- Defence is typically more difficult than attack
  - esp. if the main focus is on functionality, not on security
  - see the Internet of Things, with all sorts of devices connected, monitoring, poorly designed, and not being maintained

Big question today: can we protect what we build?

Security@Nijmegen’s claim-to-fame, wrt. vulnerabilities

1. 2008: security flaws discovered in Mifare Classic chipcard
   - used in public transport in NL, but also in London’s Oyster card
   - around 1 Billion copies sold; used worldwide
   - card producer NXP took university to court, for publication ban
   - worldwide attention, including e.g. on BBC World’s Click

2. 2013: weaknesses in Megamos Crypto in car immobilisers
   - more than 100 car models affected
   - Volkswagen managed to get a publication ban in London!!
   - the ban lasted two years; then the scientific paper appeared

3. 2018: vulnerabilities in Solid State Drives (SSDs)
   - storage chips that offer built-in “hardware” encryption
   - implementation mistakes in 100M+ devices, of several models/manufacturers — also covered by BBC Click
   - the world (and producers) got used to security flaws

A news snippet, from the Guardian (18 aug. 2015)

One of the 3 researchers had moved from Nijmegen to Birmingham, and was mentioned explicitly. The other two were from ‘a Dutch University’
Warfare is going digital

Wars and Sciences

- WWI was the chemists’ war, with the use of poisonous gases
- WWII was the physicists’ war, with the atomic bomb
- WWIII, if ever, will be the computer scientists’ war

Broader, societal perspective

Follow the data!

- Traditionally, one should “follow the money” in order to understand power relations in society.
- Nowadays one needs to follow the data

- Big IT-companies have understood this like no other
- Recall: computer security is about regulating access to assets
- There are many laws and rules to regulate and monitor financial flows. Regulation of data flows is still in its infancy

The role of computer scientists

- Traditionally, computer scientists are seen as the architects of the digital world
- In fact, they have become architects of the social world

This social role & responsibility is especially prominent in the area of digital identity.
Where we are, so far

- Introduction
- Computer security
- Identities
- Attributes, in theory & practice
- Intermediaries & platforms
- Privacy
- Conclusions

When is your identity needed? Some examples

- For online banking
  - when you login, you authenticate: you prove who you are
  - in principle, each transaction/transfer needs to be signed by you
- For buying alcohol, you need to show identification
  - “if you look under 25” is typical supermarket’s policy
  - what if you buy online, and the website asks you to upload a copy of our ID-document?
  - really, you only need to prove that your age is $\geq 18$
- When you open an account on Facebook
  - Facebook has a “real name policy”: they demand that you’re truthful about your identity (name, date-of-birth etc)
  - can they check? Why do they care at all?
- GOV.UK Verify provides you with an eID, for public services
  - How is it established who you are, when you open an account?
  - Which attributes are revealed when you login?

Real-world and virtual-world authentication

- In daily life we rely on context for many forms of (implicit) authentication
  - uniforms / places / behaviour / etc
- In the online world such contexts are either lacking, or easy to manipulate (fake e-banking site)

“On the internet nobody knows you’re a dog.”
(Peter Steiner, New Yorker, 1993)

Correction, from 2010

In the age of profiling this anonymity suggestion is completely outdated!
Napoleon’s heritage: completely different mindsets

- It was Napoleon who started registering people’s identities in the countries that he conquered.
- He needed these registers to draft people into his huge armies.
- This never happened in Anglo-Saxon countries — which typically have no citizen administration.
- People in continental Europe, in contrast, see the government as the primary source of (administrative) identities.
- In the Anglo-Saxon world there is much more identity anarchy:
  - you need energy & phone bills etc. to prove who you are
  - in the US a driver’s licence is the best government registration

National differences/traditions/sensitivities

- GB & DE have no national identification number.
- NL has a national identification number — for public use only.
- Scandinavian countries have such numbers — for both public and private usage.

Where we are, so far

Introduction

Computer security

Identities

Attributes, in theory & practice

Intermediaries & platforms

Privacy

Conclusions

Attributes

Attributes are properties of people with some level of stability.

- **Examples**: given name, family name, physical address, e-mail address, date-of-birth, phone number, nationality, etc.
  - attributes are typically “small” pieces of information
  - they are distinguished from larger “records” and “dossiers”
- An attribute can be:
  - (uniquely) identifying, like a student number — in a context
  - non-identifying, like gender, or "older than 18"
- Attributes have a certain **validity period**, after which they expire
  - Example: "younger than 15", or address
Identities & attributes

**Definition**

The (complete) identity of a person is the set of all attributes that hold for that person — at a particular point in time.

Basic ideas behind using attributes:

- **Authorisation** can be done based on attributes
  - You can participate in this discussion group because you are younger than 15, or because you are a student of this course, etc.
  - Knowing your passport/citizen number does not help here
- The selection of attributes asked for authentication should be minimal, for privacy protection, in line with the GDPR
- Different attributes are shown in different contexts: contextual authentication

The IRMA app as everyone’s personal hub

**Attribute sources**

- Municipalities
- Banks
- Edu-registers
- Healthcare registers

**Attribute receivers**

- E-government
- Webshops
- Schools
- Healthcare portals

IRMA history, in two phases

- **2008 — now**: Scientific research project at Radboud University
  - Active research line on attribute-based authentication
  - 3 PhD theses so far, postdocs too, many publications
  - Prototype implementations on:
    - Smart card — at first, but no longer supported
    - Smart phone — for Android only

- **2016 — now**: Technology deployment via non-profit foundation
  - [https://privacybydesign.foundation](https://privacybydesign.foundation) set up in fall 2016
  - Foundation runs infrastructure, and issues some attributes
  - Both Android and iOS apps, with common code-base in Go
  - Attribute verification pilots are now emerging
**Why a foundation — and not a company?**

(1) To avoid conflicts of interests and vulnerabilities to accusations
- there is some overlap between my IRMA-related research, and work for the foundation
- by keeping the foundation non-for-profit, there is no tension

(2) User acceptance in this area works best without commercial agenda
- very concretely in work with city of Nijmegen, but also others
- but also: people in NL will not accept having to login at the tax office with, say, Facebook

(3) Foundation cannot be acquired so easily by "big-IT"
- widely-used strategy to buy possible competitors early on
- (and kill their technology if it threatens established interests)

---

**Prizes for IRMA (in 2018 en 2019)**

- Privacy award from Privacy First
- Brouwer prize from KHMW
- Internet Innovation award from ISOC

Juries appreciate the combination of a solid scientific basis and potentially big societal impact.

---

**Starting a new approach, like IRMA**

**Chick and egg problem to get off the ground**

- as long as there are no IRMA users, websites will not offer/require it
- as long as websites don’t offer IRMA, users will not install it

- The Privacy by Design Foundation decided to concentrate on the chicken problem first: IRMA app + attribute content
- This part is now (mostly) done; attention has shifted to the eggs.

---

**Which sectors are leading?**

- **Municipalities**, i.e. local, not national, government
  - Nijmegen issues 20-some attributes from official citizen administration (BRP), to everyone in NL
  - this goes national: dozens of other cities in NL are joining
  - strategic breakthrough that others can build on

- **Healthcare**, esp. via new data portals
  - both for patients and for medical staff
  - digital signatures are useful for consent and for recipes etc.
  - several health care pilots with IRMA are now emerging

- **Education**, esp. together with SURFnet in NL and EduGain internationally

- **Webshops**: slower uptake
  - extremely pragmatic and focused on user-friendliness
Citizens can login, and then obtain IRMA attributes from the government’s citizen administration. This is available for everyone in NL.

Several e-health companies in NL are joining forces to set-up an open standard, including IRMA-based authentication & signing. This consortium nuts.nl issues special IRMA attributes to health care professionals — contributing to an IRMA ecosystem.

Login to patient portal with IRMA.

Where we are, so far

- Introduction
- Computer security
- Identities
- Attributes, in theory & practice
- Intermediaries & platforms
- Privacy
- Conclusions
Another dimension

- So far, attributes have been discussed
  - attributes work better than "identities"
  - this is widely accepted now, and uncontroversial

- What is actually controversial are issues like:
  - where should these attributes be stored?
  - who should provide them? What are the data flows? This will be discussed next.

Centralised versus decentralised, schematically

**Centralised**: everything goes via the Attribute Provider (think Facebook)

**Decentralised**: everything goes via the User (think IRMA)

All this is highly politically sensitive!

- Information flows and authentication requirements determine power relations in modern societies

- The choice of authentication architecture is extremely sensitive
  - substantial differences exist between central and decentral
  - power and (financial) control are key in the central approach
  - privacy and autonomy are leading values in the decentral one

- What kind of society do we prefer to live in?
  - it's an urgent question
  - who makes these choices?
  - recall: computer scientists as architects of the social world

The world's platforms

<table>
<thead>
<tr>
<th>US</th>
<th>Europe</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>Amazon</td>
<td>Alibaba.com</td>
</tr>
<tr>
<td>Facebook</td>
<td>Netflix</td>
<td>Tencent</td>
</tr>
<tr>
<td>Spotify</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The shared US-CN agenda

- Both US and CN platforms wish to control digital identities
  - they wish to precisely register who is doing what & when online
  - goal: build up detailed profiles
- The US platforms have mostly commercial motives
  - but they have been used for political manipulation too
- The CN platforms are instrumental in maintaining state control
  - see e.g. their role in ‘social credit scores’

These systems work on the basis of a unique identifier (number), per individual, that is used everywhere — very unlike attributes

After the Cambridge Analytica scandal...

- Widely shared sentiment: we need another kind of IT-infrastructure
  - one in which European values are embedded
    - arising through “value-driven design”
  - ultimately this is a geopolitical matter
    - developments are driven by the commercial sector in the US
    - by the state in China
    - by civil society in Europe?

International dimension of IRMA

IRMA is globally available, with now ≥90% of > 5200 registrations in NL

The decentralised set-up makes IRMA ideal for international usage
- only public keys needed for verification — and open source software
- attributes can reflect existing national authentication cultures

International expansion of IRMA

- Expansion will go step-by-step, since national trust anchors are needed, per country, as reliable sources of attributes
- Internationally available IRMA attributes, at this stage:
  - e-mail address,
  - social media basics (Facebook, Twitter, LinkedIn)
  - mobile phone number (EU only)
  - EduGain (selected educational institutes)

But no high assurance attributes; they will have to be issued locally

- Still, this can be useful already, e.g. using e-mail attribute for:
  - IRMA login on your website — without need for passwords
  - signing (e-mail) messages, with e-mail attribute
- IRMA has contacts in the UK with companies digi.me and yoti.com
  - IRMA works well for combining several (consistent) attributes to get to a higher assurance level — where no registrations exist
Where we are, so far

Introduction

Computer security

Identities

Attributes, in theory & practice

Intermediaries & platforms

Privacy

Conclusions

Privacy is keeping information in context (Helen Nissenbaum)

- 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
  - e.g. when banks try to monetise customer financial data
- When explained like this, almost everybody cares about privacy
- The Google/Facebook/Baidu’s of this world make us use the same identifier everywhere or track us via Like and cookies
  - they break-up contexts, and destroy our basic privacy intuitions
  - Mark Zuckerberg: “Having two identities for yourself is a lack of integrity” 😞😞

GDPR & IRMA

GDPR = General Data Protection Regulation, in force since May’18.

(1) Authentication via IRMA, for right of access (art. 15)
  - authentication can be focused on how the data subject is known to the data controller — with relevant attributes only

(2) Digital signing via IRMA, for consent (art. 7)
  - also such signing is attribute-based / contextual
  - superior to box ticking, with transferrable proof

(3) IRMA has been designed for data minimisation
  - via selective disclosure of relevant attributes, i.e. via contextual authentication
  - also minimisation of the number of parties involved — no unnecessary intermediaries / privacy hotspots

Where we are, so far

Introduction

Computer security

Identities

Attributes, in theory & practice

Intermediaries & platforms

Privacy

Conclusions
Concluding remarks I

- When the internet was designed in the 1980s, no protocols for
  securely establishing the identities of communicating parties were
  included in its design.
- While understandable from a historical perspective, it created lot’s of
  serious problems down the road: fraud, threats etc.
- Getting “identity” right is a really big thing:
  - it’s of geopolitical nature: power relations between states
  - inside states too, between government, private sector, civil society
  - Europe should act, now that the situation is still open
- Governments are unsuccessful in this area, and businesses fail too,
  because of issues with monopolisation, lock-in’s, backdoors
  - maybe a non-profit, community-driven, bottom-up approach can
    work.

Concluding remarks II

- Information flows and authentication requirements determine power
  relations in modern societies
  - what kind of society do we wish to live in?

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>Europe</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- IRMA is a decentralised, open source, non-profit, flexible identity
  platform that is up and running, and being tested by various parties
  - it integrates attribute-based authentication and signing
  - it provides privacy-friendly empowerment of users
  - it’s well on the way, on a long road
  - it’s a community effort, not aiming to monopolise

Is IRMA a naive attempt, bound to fail?

- Some public authorities are beginning to realise that they have a
  task to protect/strengthen public values also in the digital world
- Data protection authorities may become tougher
  - GDPR, art. 25 requires: data protection by design and by default
  - “Taking into account the state of the art . . . the controller shall
    . . . implement appropriate technical and organisational measures . . . to
    implement data-protection principles, such as data minimisation . . .”
  - DPA’s could say: the technology is there, thou shalt use it!
- Some companies are beginning to realise that collecting and storing
  personal data forms a serious liability
  - IRMA allows them to ask users to disclose whatever is needed, per transaction

Curious, interested, or even inspired?

- install the IRMA app yourself & collect some of your attributes
- try out some IRMA demo’s
- or integrate IRMA into your own products/services
- spread the word: IRMA does not have a lobby / advertisement budget

See website: privacybydesign.foundation

See for up-to-date info: twitter.com/IRMA_privacy
Thanks for your attention. Questions/remarks?