Privacy by Design

Marc Langheinrich
University of Lugano (USI)
Switzerland
Example 1

NON PRIVACY BY NON DESIGN
Speed through checkout.
Get $10
20 cards

no encryption
<table>
<thead>
<tr>
<th>Cardholder's Name</th>
<th>Card Number</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
69 ft
Non Privacy By Non Design
Example 2

NON PRIVACY BY BAD DESIGN
Protection from Forgery!!
Digital Signature
‘Fakeproof’ e-passport is cloned in minutes

New microchipped passports designed to be foolproof against identity theft can be cloned and manipulated in minutes and accepted as genuine by the computer software.

„...cloned and manipulated...“
Broken?
Mustermann Christian
0000000000000

Proof of Genuine Passport

Broken!

Mustermann Christian
0000000000000

Proof of Genuine Passport
(US)
Non Privacy By Bad Design
Example 3

PRIVACY BY DESIGN?
Smart Stove
Receiptless Returns
Fast Checkout
Threats
Tiger Tanga
Maker: Aldi (Suisse)
Last washed: 5 days ago

Viagra
Maker: Pfitzer
Size: Maxi (60 pills)
Solution
Information on Smart Chip

Deactivate Smart Chip?

Do you want to deactivate the information on the Smart Chip?

Yes
Working Hypothesis
People don’t want privacy tools
People want to get things done!
The more secure, private, safe, the better
Getting Things Done?
Vision
Hands Free Privacy

The more secure, private, safe, the better
Example: The Shamir Tag

Example: The Shamir Tag

- Unsolicited read-outs take **long time**
  - Difficult (but not impossible) to track or identify

- **Instant Identification** for known tags
  - Owner uses tags without restrictions

---

RFID-Tag contains encrypted ID + Key, but cut in many small pieces. All pieces are needed to decrypt Tag ID.
Shamir Tags Illustrated

Original RFID-Tag: RFID-Tag contains *encrypted ID* + Key, but cut in many small pieces. **All** pieces are needed to decrypt Tag ID.

Unknown Reader sees:
- Only few shares disclosed
- A few more shares disclosed
- Still not enough shares...

*Time*
Shamir Tags Illustrated

Original RFID-Tag:

RFID-Tag contains encrypted ID + Key, but cut in many small pieces. All pieces are needed to decrypt Tag ID.

Unknown Reader sees:

- Only few shares disclosed
- A few more shares disclosed
- Still not enough shares...

Owner’s Reader sees:

- Only few shares disclosed
- Owner checks for known (cached) tag

Instant Identification
Consumers receive **basic** protection for **all** tagged goods.

**Additional** security mechanism can be **layered** above Shamir Tags.
Summary
Privacy by Design

• **Difficult** to do even for technology experts
  – **Industrial** (RFID Credit Cards)
  – **Government** (ePassport)

• Difficult if **wrong user model**
  – People want to **get things done**
  – Privacy, security often **gets in the way**

• We need **usable** security and privacy
  – Sometimes **less** security may mean **more** privacy