Threats in future AmI Applications: First evidence

Michael Friedewald

More and/or new threats in a World of AmI?

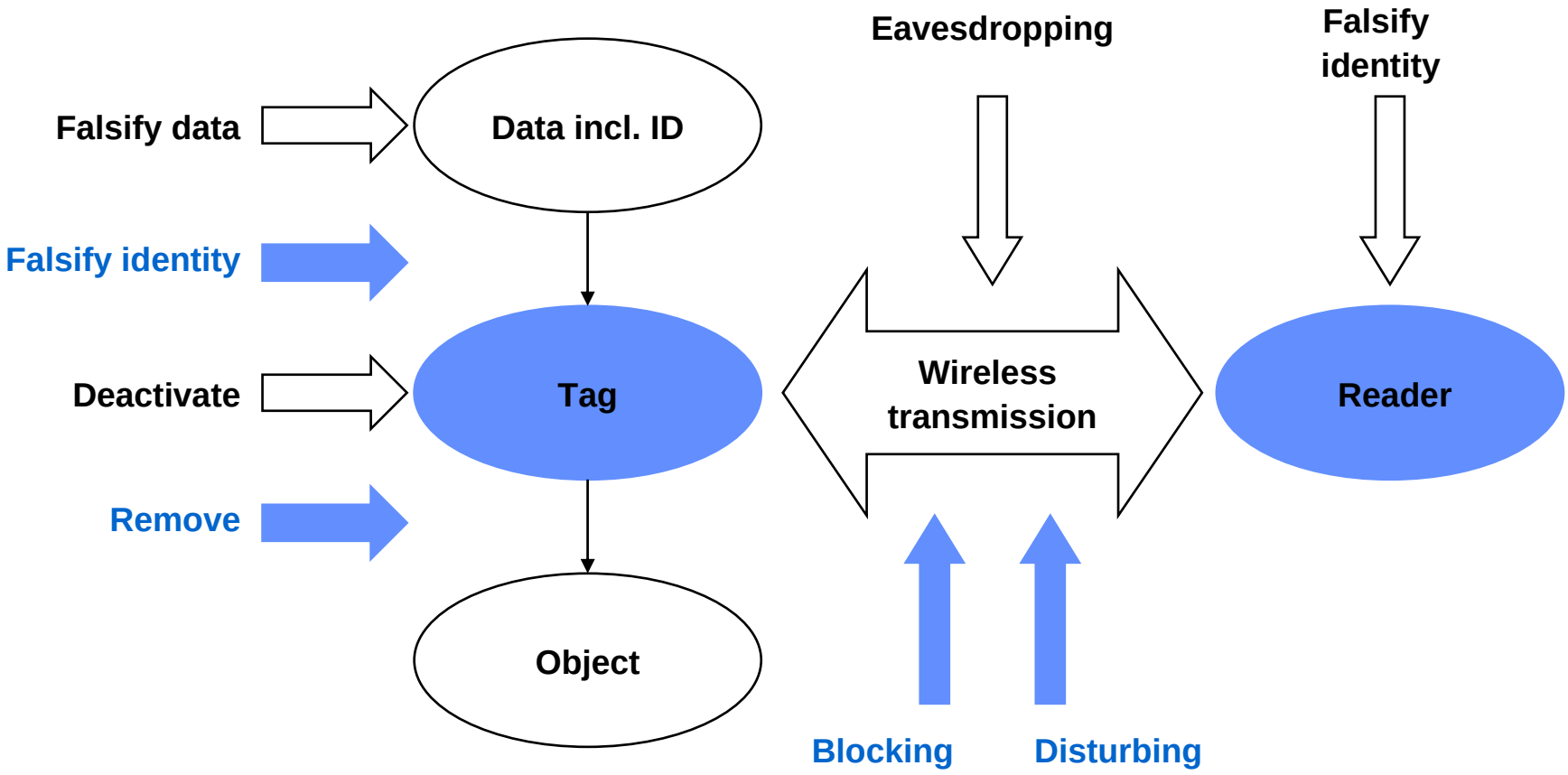
Threats stem from two necessary innovations for the success of Ambient Intelligence

- enhanced ability to collect data on people's everyday interactions (in multiple modalities and over large spans of time and space)
- enhanced ability to quickly search large databases of collected data, greater possibilities for personal profiling, and other forms of data mining

Resulting generic privacy threats

- Sheer quantity of personal information in circulation will increase greatly
- Introduction of perceptual and biometric interfaces will transform the qualitative nature of personal information in circulation
- Personalised services require the tracking and collection of significant portions of users' everyday activities

Possible vulnerabilities of technical system



Source: BSI 2004

Five types of threats

1. Surveillance of users
2. Spamming
3. Identity theft
4. Malicious attacks
5. Digital divide

Surveillance of users

Availability of personal data can provoke desires to access and use them legally, semi-legally or even illegally

The spheres and activities where data is collected increases - even where privacy is considered sacrosanct as in the home

- Disclosure of health information, personal preferences, habit and lifestyles
  ➲ can lead to discrimination by insurances, at the workplace, etc.
- Disclosure of personal information to service providers/retailers ➲ rebound effect („transparent customer“) may overcompensate positive effects for the citizen
- Disclosure of location information ➲ rebound effects (harm of privacy, enabling of robbery and terrorist attacks) may overcompensate convenience of location-based services
- Even seemingly unproblematic surveillance may enable unwanted misuse

Spamming

Building of personal profiles is at the core of personalised services, but

- How much personalised information does the average citizen need?
- How much information can the average citizen process?
- Must personalised information be „pushed“?

Profiles may become a valuable „trading good“ – as in the case of the Internet

- New source of income for data collectors
- Personal profiles will be used to send unwanted information, advertisement etc
- Customers may lose interest in personalised (push) services

Identity theft

Identity theft = unjustified obtaining data needed for identification in the AmI system

Stolen identity can be used for fraud, robbery, kidnapping even terrorist attacks

Different risk depending of type of storage

- Local (personal device): may get lost, stolen and easily used, but only one identity at a time
- Remote (server, grid of servers): may be better protected, but „successful attack“ may cause bigger damage; risk grows with number of places where identity is stored

Theft and illegal use may be online or offline – the list of means for stealing ID online is continously growing

Especially online theft may remain unnoticed for some time

Malicious attacks

Attacks may be active or passive:

- deliberate alteration or destruction of the contents of an AmI system, creation of false information and messages, viruses, denial of service (blocking and disturbing)
- unauthorized monitoring of data without altering them (wiretapping) ➲ surveillance

Disruption of AmI system operation may have a variety of effects

- Loss of convenience because service is not available
- Disrupted emergency and health systems are a risk for health and life
- Manipulated home systems may cause malfunction of household appliances, even ignite fires
- Businesses based on AmI may be ruined if not able to provide services or if back office systems are manipulated

Who is responsible in a highly distributed AmI system?

What does the dependence on an AmI system mean for citizens‘ autonomy?

Digital divide

Pervasiveness of the technology may result in social pressure and digital divide

- People may be forced to use the technology (using predefined procedures and routines) in order to use services (even those that were available „offline“ before) ➲ *limiting personal freedom and self determination*
- Growing automation *limits social contacts* especially with elderly and handicapped people
- Too much reliance on the AmI system may frustrate people, *hinder their personal development, limit creativity and self-confidence*
- AmI visions are often extremely individualistic, not recognising people as members of a family and social groups
- Ami will challenge relations between actors: parents-children, customers-retailers, etc-
- AmI will not be free of charge – who can afford which services? Is privacy a value that only the better off can afford?