RFID Privacy Risks & Countermeasures

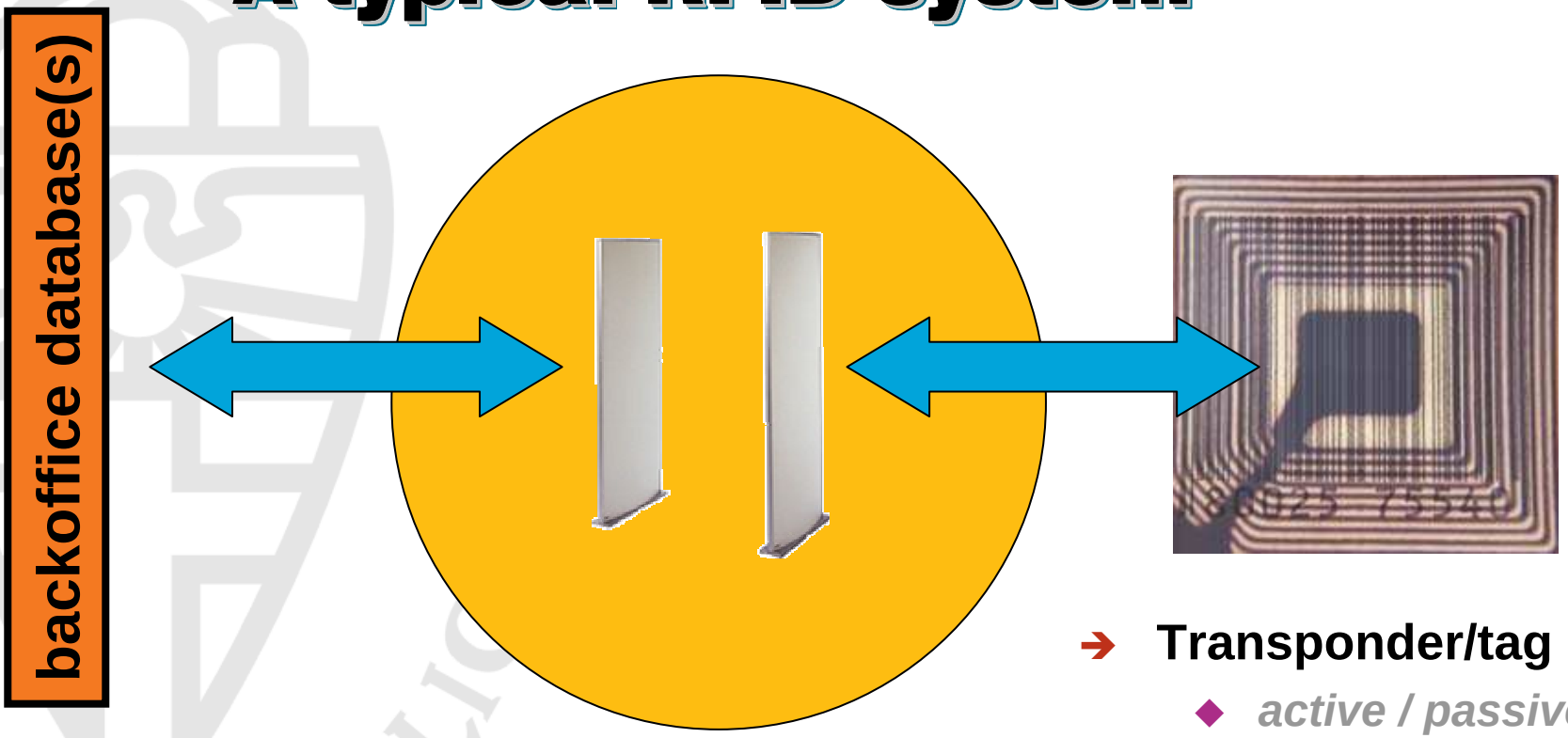
Technical issues

Jaap-Henk Hoepman
Security of Systems (SoS) group
Nijmegen Institute for Computing and Information Sciences (NIII)
Radboud University Nijmegen, the Netherlands
jhh@cs.ru.nl
www.cs.ru.nl/~jhh

Contents

- A typical RFID system
- The privacy problem
- Possible solutions

A typical RFID system



- **Reader**
  - *LF / UHF*
  - *Communication range*
  - *Coupling*

- **Transponder/tag**
  - *active / passive*
  - *1 bit – 64 kB (EEPROM/SRAM)*
  - *controller / CPU*
  - *read-only / read-write*

Reading distance

Limited by power consumption of controller/CPU on tag

- ➔ For passive tags
  - *Low frequency (LF)*
    - ~ 1.2 meter
    - *better penetration of objects*
  - *Ultra High Frequency (UHF)*
    - mostly: ~ 2 meter
    - latest product: ~ 3.3 meter
    - in the labs: ~ 4.5 m (EU) / ~ 9 m (US)
- ➔ Higher for active tags

The issue

We now face the imminent expansion of cyberspace into physical space in the form of

- networked cameras,
- biometric identification devices,
- RFID tags on consumer goods,
- and a wide variety of sensors.

Current RFID systems unsafe

- No authentication
  - *No friend/foe distinction*
- No access control
  - *Rogue reader can link to tag*
  - *Rogue tag can mess up reader*
- No encryption
  - *Eavesdropping possible*
- Predictable responses
  - *Traffic analysis, linkability*
- No GUI…
  - *… and "distance" not enforced by tag*

RFID Risks: Consumers

- **User profiling**
  - *Possible robbery target*
  - *Possible street-marketing target*
  - *Personalised loyalty/discounts*
  - *Refuse/grant access to shop/building*
    - **Even for tags without serial no#**
  - *Loss of location privacy*
    - **By tracking same user profile**
- **Fake transactions / Identity theft**

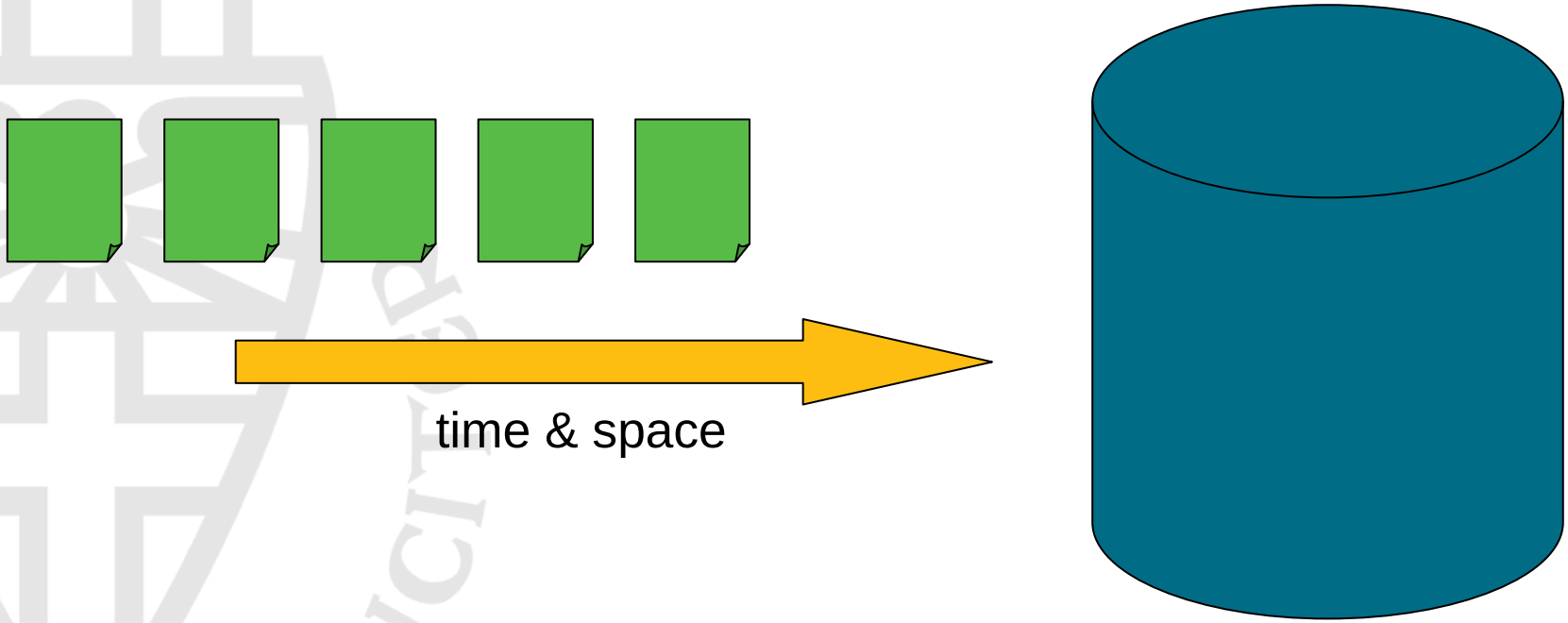
RFID Risks: Companies

- **Corporate espionage**
  - *Scanning competitors inventory (or customer base)*
    - Eavesdropping tags
    - Querying tags
  - *Unauthorised access*
    - Fake RFIDs
- **Derived/competing services**
  - *Using competitors installed base*
- **Denial of service attacks**
  - *Supply chain failure*
    - Jamming signals
    - Fake RFIDs

Example: “What-is-this”

- **With RFID**
  - *Not only immovables (**GPS**)*
    - **Including billboards**
  - *RFID (U**ph**ID) → URL*
  - *Conditional access*
    - **“Sowing seeds” vs “1 UphID for all”**
    - **1 RFID = n UphID**

Aggregate data



➔ **Maybe too big to analyse/datamine….**

- ***…. but easily searched for 1 person***

Me and my DATABODY

- This is / is not me!
  - *Plausible deniability*
  - *"Proof of ownership"*
- Selective disclosure
  - *Dressing up your databody*
- Hygiene…
  - *Cleaning…*
  - *Protecting…*
  - *Keeping in shape…*

http://www.cs.kun.nl/perfide

Privacy Enhanced
RFID Environment

jhh@cs.kun.nl