Privacy Challenges in RFID-Systems

RESEARCH GROUP FOR

Distributed Systems

Marc Langheinrich

ETH Zurich, Switzerland

http://www.inf.ethz.ch/~langhein/

joint work with Chris Floerkemeier and Roland Schneider

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

The Ubicomp Vision

„The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.“

Mark Weiser (1952 – 1999), Xerox PARC

- The computer as an everyday tool
- Networking all things
- Embedding computers into intuitive UI's

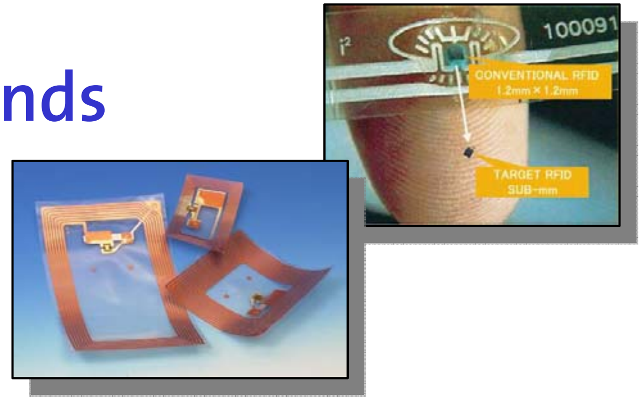
Data Collection in Ubicomp

- High Potential for…
  - Unprecedented collection size
  - Unprecedented collection detail
  - Large public unawareness

What?	How?
Coll. Scale	Everywhere, Anytime
Coll. Manner	Unobtrusive, Invisible
Data Types	Detailed, Mundane, Close-Up & Personal
Motivation	Everything is Important (Context!)
Accessibility	Machine-to-Machine Interactions

Radio Frequency Identification

- "Barcode++"
  - Stores (potentially very detailed) IDs
  - Provides link between real and virtual
- Unobtrusive
  - Tags can be read without line-of-sight
  - Tags need no batteries (reader provides power)
- Efficient
  - Dozens of tags can be read in seconds
- Cheap
  - Price range: 5-10 Cents



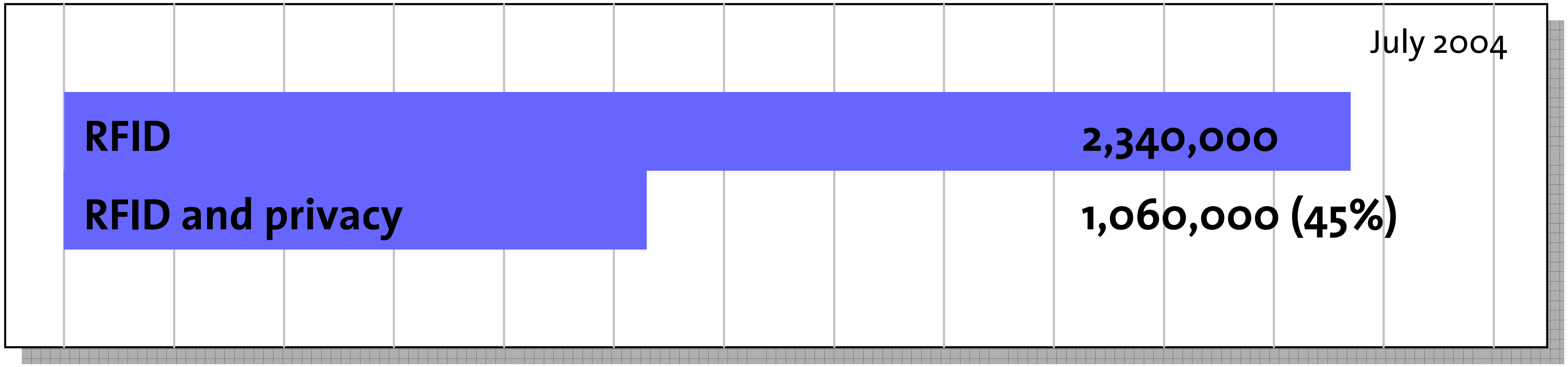
RFID Privacy

WAL★MART ALWAYS LOW PRICES. Always

UNITED COLORS OF BENETTON.

- Ubiquitous Technology?
  - WalMart, US DoD, Benetton, Metro, ...
- Ubiquitous Reading?
  - Anything, anytime, anywhere?
- Public Concern (measured by Google*)

C.A.S.P.I.A.N.
Consumers Against Supermarket Privacy Invasion and Numbering

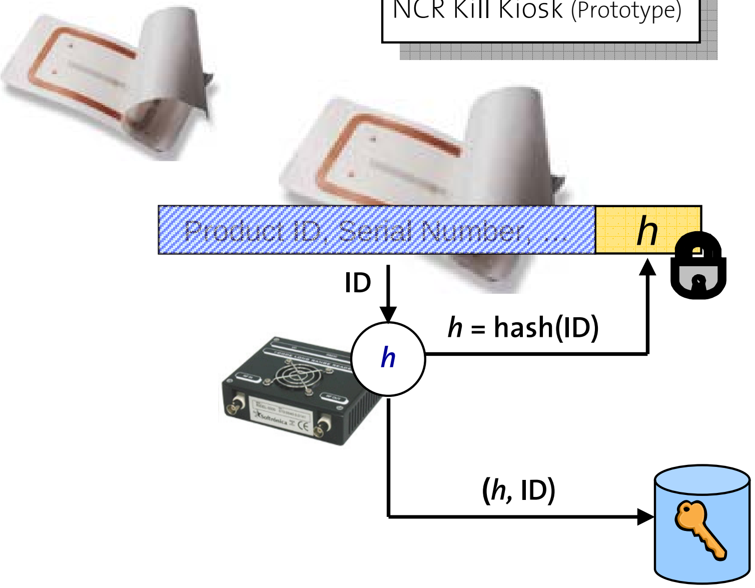


* Original numbers by Ravi Pappu, RFID Privacy Workshop @ MIT: November 15, 2003

Current Solutions

- Tag Deactivation (Kill Tag)
  - Cumbersome
  - Expensive training / equipment
  - Prevents post point-of-sales applications
- Communication Block (Blocker Tag)
  - Unreliable
  - Interferes with 3rd party tags
- Access Control (Hash Locks)
  - Expensive chip design
  - Impractical key management

NCR Kill Kiosk (Prototype)



Threat Models

- What are We Trying to Protect?
  - ~~Secret surveillance networks?~~
  - ~~Pickpockets and burglars?~~
  - Staying in control of personal data flows!

unlikely (expensive, unreliable)

impractical (expensive, unreliable)

ubiquitous! (everywhere, anytime, unnoticed)

- Goal: Transparency Protocols
  - Use machines to monitor plethora of interactions
  - Support for privacy laws & regulation (see P3P)
- RFID Approach
  - Embed support for the *Fair Information Principles* in RFID-protocols (reader-to-tag communication)

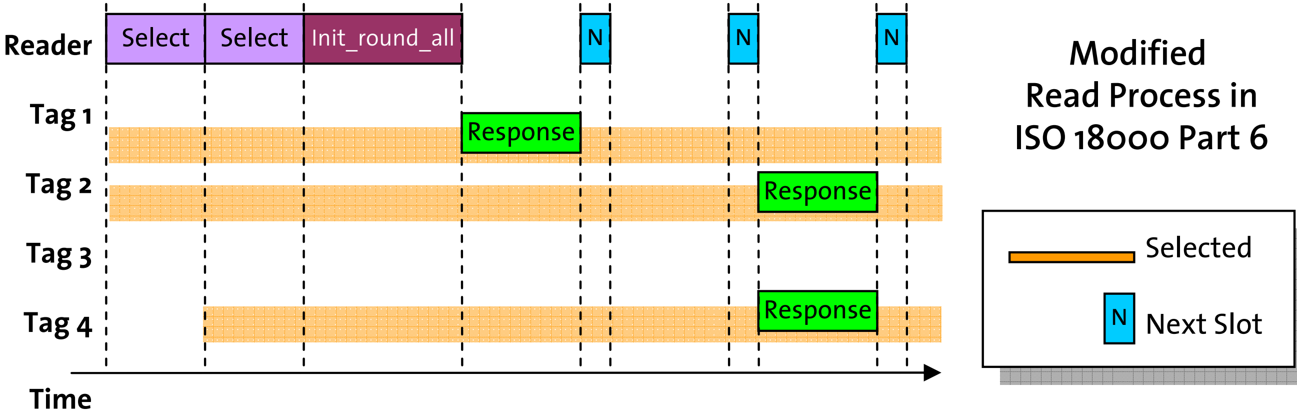
RFID FIP-Support

Principle	Support through...
Collection Limitation	Tag Selection Mask
Consent	Watchdog-Tag (optional)
Data Quality	n/a (with „privacy-aware database/PawDB“)
Purpose Specification	Purpose Declaration, Collection Type
Use Limitation	n/a (Leveraging from Purpose Specification)
Security Safeguards	Encryption/Authentication (?)
Openness	Reader-Policy ID
Participation	n/a (using PawDB)
Accountability	Reader-Policy ID

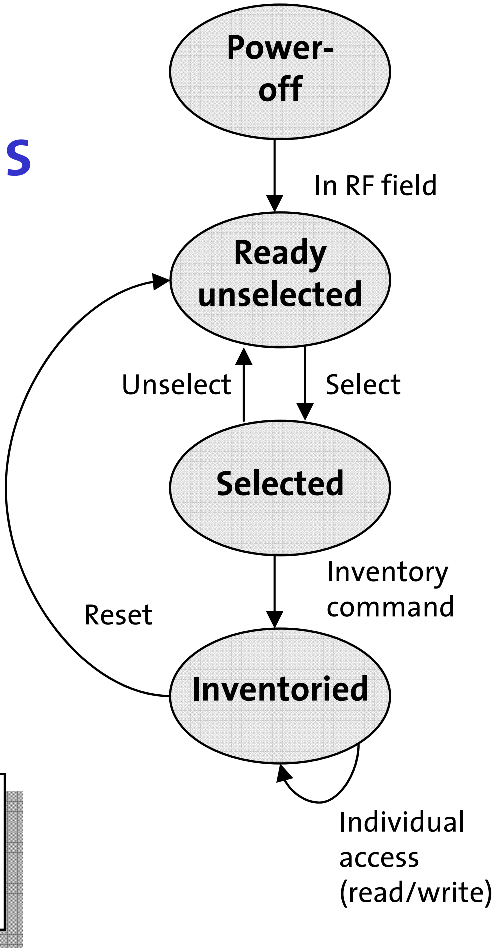
Fair Information Practices, OECD 1980

Collection Limitation

- Targeted Read Commands
  - Smart shelf only reads razorblades
  - Smart checkout reads only store items
- Selection Mask (e.g., “*.E32B*.*”)
  - Only selected tags reply
  - Requires hierarchical IDs (e.g., EPC)



Modified Read Process in ISO 18000 Part 6

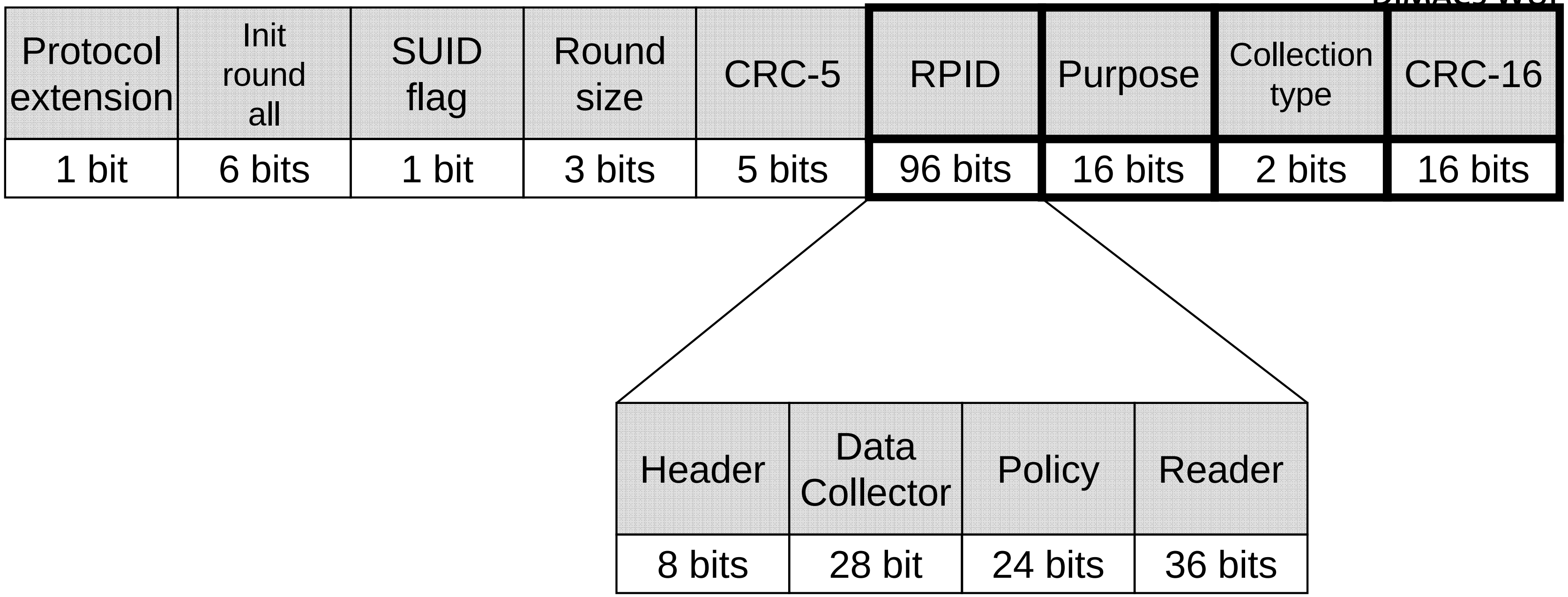


Openness

Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

- `Init_Round` Command in ISO 18000 Part 6
  - Begins read-round (Aloha-based anti-collision)
  - Contains anti-collision protocol parameters
- 130 Bits „Privacy-Header“ Extension

ReaderPolicyID



Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

Header	Data Collector	Policy	Reader
8 bits	28 bit	24 bits	36 bits

5F.4A886EC.8EC947.24A68E4F6

- All read-request uniquely identified
  - Data collector, reader, and policy identifiable
  - Format follows EPC standard (allows code reuse)

Collection Type

Protocol extension	Init round all	SUID flag	Round size	CRC-5	RPID	Purpose	Collection type	CRC-16
1 bit	6 bits	1 bit	3 bits	5 bits	96 bits	16 bits	2 bits	16 bits

1) Anonymous Monitoring
2) Local Identification
3) Item Tracking
4) Person Tracking

Declaration of Intent

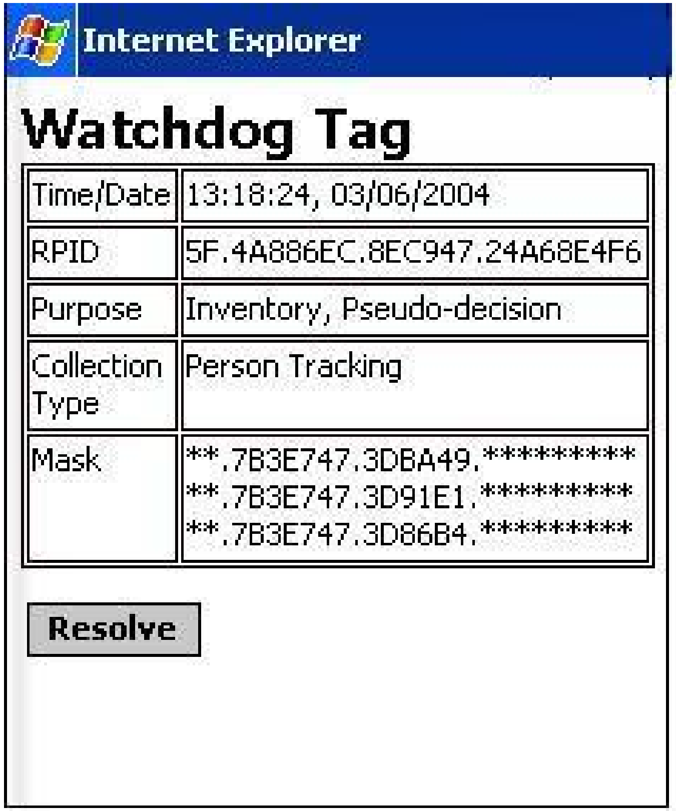
- Typical RFID usage w/o identification
  - personally identifiable data is collected but only used anonymously (needs audits)

Purpose Specification

1) Access Control
2) Anti-Counterfeiting
3) Anti-Theft
4) Asset Management
5) Contact
6) Current
7) Development
8) Emergency Services
9) Inventory

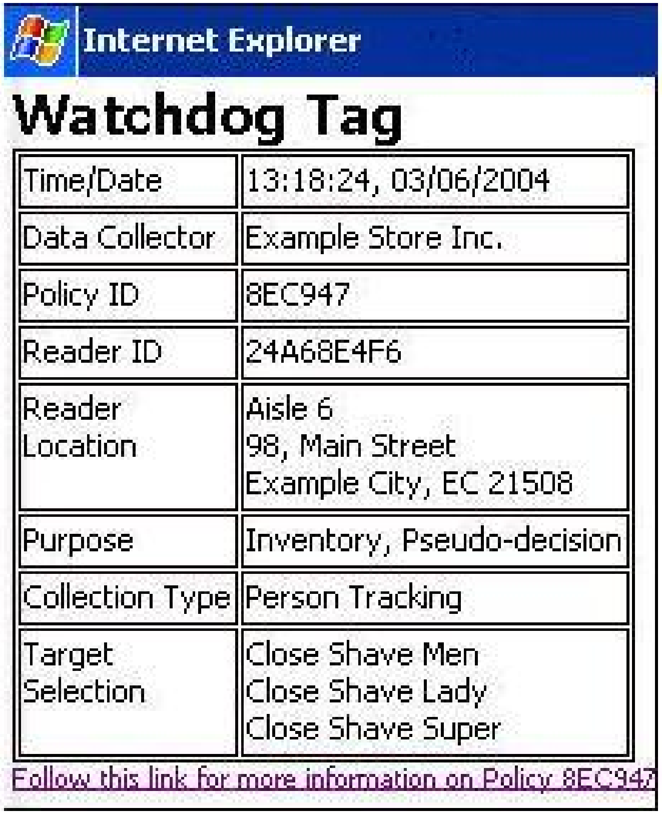
10) Legal
11) Payment
12) Profiling
    a. Ad-Hoc Tailoring
    b. Pseudo Analysis
    c. Pseudo Decision
    d. Individual Analysis
    e. Individual Decision
13) Repairs & Returns
14) Other Purpose

Transparency: Watchdog Tag


Internet Explorer

Watchdog Tag

Time/Date	13:18:24, 03/06/2004
RPID	5F.4A886EC.8EC947.24A68E4F6
Purpose	Inventory, Pseudo-decision
Collection Type	Person Tracking
Mask	**.7B3E747.3DBA49.********* **.7B3E747.3D91E1.********* **.7B3E747.3D86B4.*********


Internet Explorer

Watchdog Tag

Time/Date	13:18:24, 03/06/2004
Data Collector	Example Store Inc.
Policy ID	8EC947
Reader ID	24A68E4F6
Reader Location	Aisle 6 98, Main Street Example City, EC 21508
Purpose	Inventory, Pseudo-decision
Collection Type	Person Tracking
Target Selection	Close Shave Men Close Shave Lady Close Shave Super

Follow this link for more information on Policy 8EC947

Feasibility?

- Extending Reader Devices
  - Software-update
  - Integrates with enterprise solutions (“Privacy-DB”)
- Extending Tags
  - Needs protocol-level standardization (EPC, P3P, ...)
  - No new hardware (program logic only)
  - Good performance (only about 1% loss in speed)
- Reliability?
  - No tag configuration necessary
  - “Reliable” like a public announcement (poster, etc)
    - can be ignored by consumer, but lacking it can be noticed

Summary

- Ubicomp brings privacy challenges
  - Large-scale, unnoticed data collections
  - RFID-technology most prominent example
- Current RFID privacy solutions fall short
  - Too complicated, expensive
- Proposal: Put Transparency into RFID
  - Readers identify themselves, purpose, etc…
  - Support for laws & regulations

For more information...

- Ch. Flörkemeier, R. Schneider, M. Langheinrich, *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols*. Submitted for publication
- M. Langheinrich, *A Privacy Awareness System for Ubiquitous Computing Environments*. Proceedings of Ubicomp 2002
- M. Langheinrich, *Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie*. Appears in 2004 (German)

http://www.vs.inf.ethz.ch/publ/