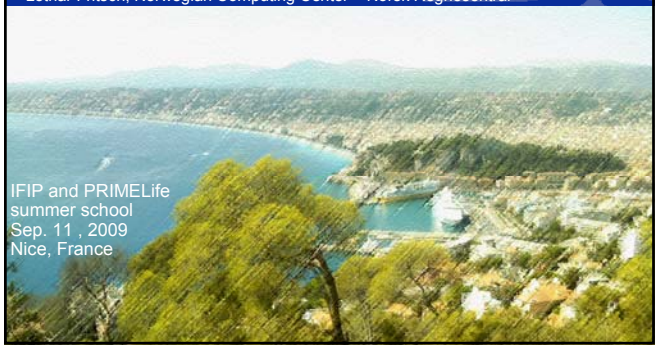
www.nr.no

Business risks from RFID in tracking, tracing and logistics

Lothar Fritsch, Norwegian Computing Center – Norsk Regnesentral



IFIP and PRIMELife summer school
Sep. 11 , 2009
Nice, France

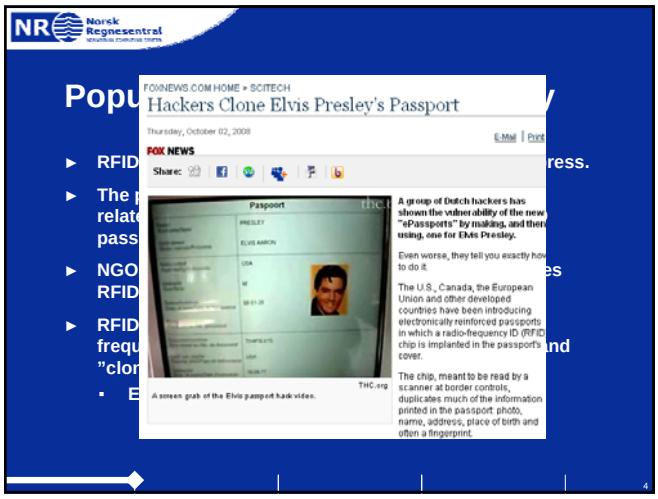
Lothar Fritsch

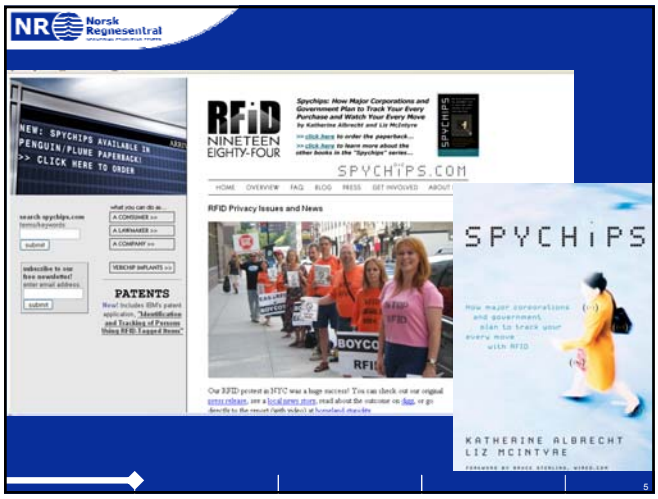
- Research Scientist in IT Security & Privacy in Norsk Regnesentral's ICT research department
- Master degree in Computer Science, specialist on information security & privacy
- Product manager for a German e-business-security firm
- PhD at Frankfurt's Goethe University's Information Systems department in m-commerce security, privacy and business models
- Participant in EU privacy technology research, e.g. SEMPER, PRIME, FIDIS projects

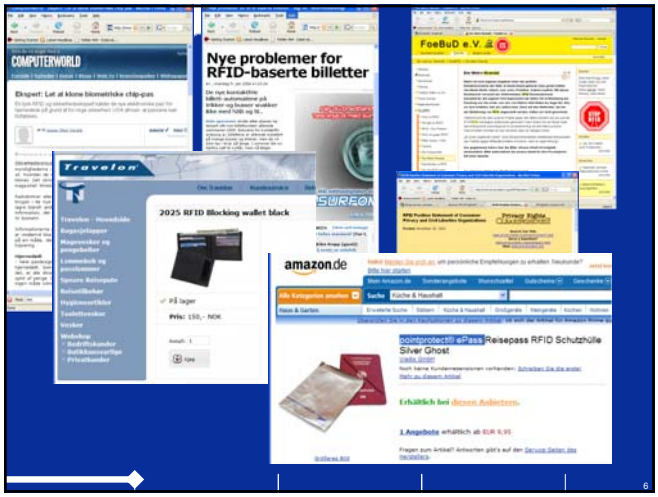
Web: *http://www.nr.no/ ~lothar*

Agenda

1. The popular view on RFID security and privacy
   - Privacy issues
   - Business risks
2. RFID applications are larger than tags & readers
   - Analysis of information in the whole system
3. Case studies: Business risks with RFID
   - Boycott phone
   - Retail espionage
   - Fisheries information chain
   - The RFID future through the looking glass
4. Approaches and solutions for secure RFID applications
   - Risk analysis & evaluation
   - Identifier management schemes
   - Access control & information flow design
   - Checklist for RFID risks


Norsk Regnesentral
Popu
RFID
ress.
The
relat
pass
NGO
es
RFID
RFID
frequ
nd
"clon
E
FOXNEWS.COM HOME > SCITECH
Hackers Clone Elvis Presley's Passport
Thursday, October 02, 2008
E-Mail | Print
FOX NEWS
Share:
Passport
A screen grab of the Elvis passport hack video.
THC.org
A group of Dutch hackers has shown the vulnerability of the new "ePassports" by making, and then using, one for Elvis Presley.
Even worse, they tell you exactly how to do it.
The U.S., Canada, the European Union and other developed countries have been introducing electronically reinforced passports in which a radio-frequency ID (RFID) chip is implanted in the passport's cover.
The chip, meant to be read by a scanner at border controls, duplicates much of the information printed in the passport: photo, name, address, place of birth and often a fingerprint.
4


Norsk Regnesentral
NEW: SPYCHIPS AVAILABLE IN PENGUIN/PLUME PAPERBACK! >> CLICK HERE TO ORDER
RFID NINETEEN EIGHTY-FOUR
Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move
by Katherine Albrecht and Liz McIntyre
SPYCHIPS.COM
RFID Privacy Issues and News
PATENTS
SPYCHIPS
How major corporations and government plan to track your every move with RFID
KATHERINE ALBRECHT
LIZ MCINTYRE
5


COMPUTERWORLD
Eksport: Let at klone biometriske chip-pas
Nye problemer for RFID-baserte billetter
FoeBuD e.V.
Travelon
2025 RFID Blocking wallet black
amazon.de
pointprotect® ePass Reisepass RFID Schutzhülle Silver Ghost
6

EPCglobal Guidelines on EPC for Consumer Products

1. Consumer Notice
Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer Choice
Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer Education
Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarise consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record Use, Retention and Security
The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

Revised September 2005, Source: http://www.epcglobalinc.org/public/ppsc_guide

7

Ontario's RFID privacy guide lines

- **Focus on RFID information systems, not technologies:** The problem does not lie with RFID technologies themselves, but rather, the way in which they are deployed that can have privacy implications. The *Guidelines* should be applied to RFID information systems as a whole, rather than to any single technology component or function;
- **Build in privacy and security from the outset – at the design stage:** Just as privacy concerns must be identified in a broad and systemic manner, so, too, must the technological *solutions* be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID data; and
- **Maximize individual participation and consent**: Use of RFID information systems should be as open and transparent as possible, and afford individuals with as much opportunity as possible to participate and make informed decisions.

Ontario's privacy commissioner, Ann Cavoukian, 2006-2008
http://www.ipc.on.ca/images/Resources/up-2006_06_19rfid.pdf
http://www.ipc.on.ca/images/Resources/up-1rfid_HealthCare.pdf

8

EU draft recommendations

1. **RFID operators shall conduct privacy risk assessment!**
2. **Risk assessments should honor stakes, and cover all stakeholders!**
3. **Take appropriate technical and organizational measures to mitigate the privacy risks!**
4. **Assign a responsible person for audit and adaption of the above!**
5. **Privacy & security risk management shall be aligned.**
6. **The privacy risk assessment summary must be published latest upon deployment of the RFID application.**

9

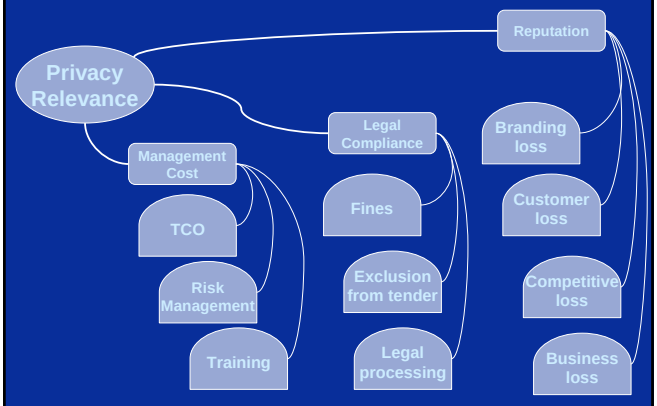
Norwegian Regulation

- General rules in "personopplysningsloven" (personal data law) apply to RFID applications. No specific regulation has been implemented.
- BUT: Data protection authority has already commented several RFID-based projects and formulated stringent requirements, e.g. in the case of passports:
  - The Police shall assess privacy risks of biometric passport handling with repsect to §13 personopplysningsloven (POL) og §2-4 personopplysningsforskriften.
  - The Police shall provide all necessary information to applicants and holders of biometric passports acc. to §19 POL.
  - The Police must design and implement an internal privacy controlling system according to §14 POL. The system must not be outsourced.

►http://www.datatilsynet.no/upload/Dokumenter/saker/2006/passflvarsel.pdf

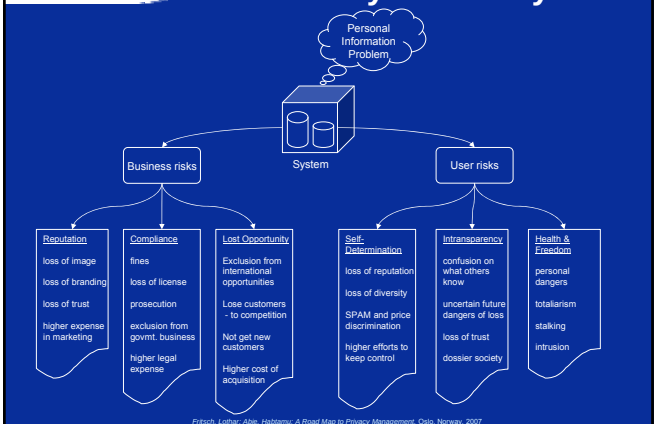
10

Privacy Protection matters.



11

Duality of Privacy Risks



Fritsch, Lothar; Abie, Habtamu: A Road Map to Privacy Management, Oslo, Norway, 2007

12

Return-on-Investment depends on security & privacy

- ROI of RFID infrastructure investments can be at risk
- Surprises (e.g. unplanned for data protection or privacy requirements)
- Malicious players take advantage (espionage, sabotage, hacking, exposure)

Security and privacy analysis provides to sustainability of investments & to the business propects!

13

Agenda

1. The popular view on RFID security and privacy
   - Privacy issues
   - Business risks
2. RFID applications are larger than tags & readers
   - Analysis of information in the whole system
3. Case studies: Business risks with RFID
   - Boycott phone
   - Retail espionage
   - Fisheries information chain
   - The RFID future through the looking glass
4. Approaches and solutions for secure RFID applications
   - Risk analysis & evaluation
   - Identifier management schemes
   - Access control & information flow design
   - checklist

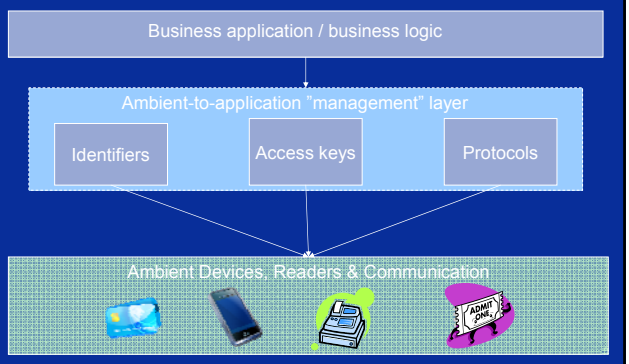
14

RFID applications: Beyond privacy, tags & readers

- Much research has been puyblished on RFID tag security, reader protocols, and access control to the tag's data fields.
- However, the privacy and business intelligence risks are created by a link between tags and a particular context:
  - a person
  - a product
  - a vendor
- Thus, both the middleware and the application context are critical inputs to risk analysis.
- Unfortunately, most technical descriptions describe tag & reader products detached from the application context.

15

Scenario assumption: RFID applications



16

Agenda

1. The popular view on RFID security and privacy
   - Privacy issues
   - Business risks
2. RFID applications are larger than tags & readers
   - Analysis of information in the whole system
3. Case studies: Business risks with RFID
   - Boycott phone
   - Retail espionage
   - Fisheries information chain
   - The RFID future through the looking glass
4. Approaches and solutions for secure RFID applications
   - Risk analysis & evaluation
   - Identifier management schemes
   - Access control & information flow design
   - checklist

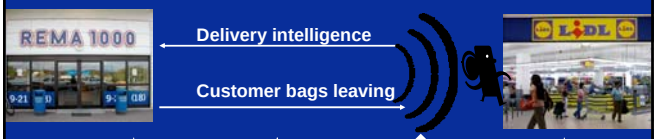
17

Case 1: The Boy e

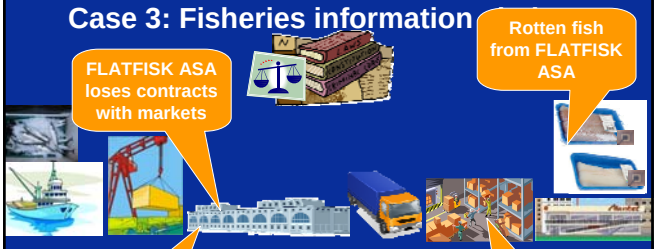
18

Case 2: Retail espionage

- What if a new market player could obtain intelligence about delivery, and carry-out of tagged items from competition?
- Targeted special offers & location-optimized sortiment.
- *AC Nielsen* creates vast profits with such information.



Case 3: Fisheries information



FLATFISK ASA loses contracts with markets

Rotten fish from FLATFISK ASA

- Many erent stakeholders involved – ere is tion stored?
  l see which part of the inf
  held liable for damages
  ature information dissemin

5 weeks later: FLATFISK ASA out of business due to credit problems

3 weeks later: Mattilsynet confirms warehouse problem

Case 4: RFID future uses – the two-edged sword

Imagine a world where…

- A vendor's trash (packages, products) will be tracked around the globe, even 20 years after production, until it turns up on a polluted site in Africa – and on some NGO's agenda;
- The city trash removal facilities read RFIDs on package waste to bill the producers for the trash processed;
- Corporate tax & toll is adjusted based on scanners at borders, ware houses and waste dumps.
- Does the "kill" function kill TID?

Agenda

1. The popular view on RFID security and privacy
   - Privacy issues
   - Business risks
2. RFID applications are larger than tags & readers
   - Analysis of information in the whole system
3. Case studies: Business risks with RFID
   - Boycott phone
   - Retail espionage
   - Fisheries information chain
   - The RFID future through the looking glass
4. Approaches and solutions for secure RFID applications
   - Risk analysis & evaluation
   - Identifier management schemes
   - Access control & information flow design
   - checklist

22

Risk Analysis & Evaluation

- Risk assessment is an integral part of security management, e.g. in ISO 27000 or ISO 17799.
- Risk assessment analyses and evaluates risks to information security, and suggests control measures to contain the risks.
- Risk assessment has to be done regularly, e.g. as audits, within the risk management methodology. Updates of the security and privacy measures must be in the annual IT budget!

23

Identifier Management

- Tag identifiers can tell many stories.
- The most simple approach is a tag serial number indexed in a data base.
  BUT: Who owns the data base, and how will it be protected from unauthorized use?
- Tag data standards move some of the data to a tag. But now, the tag is out of the security perimeter of the vendor.
- The use of anonymizing schemes, cryptographic methods, randomized numbering schemes and zero-knowledge-protocols for identifier management should be considered.
- Identifiers should be analyzed for information leakage and possible risks.

24

Access Control & Information Flow

- Multi-level and role-based access control models are used in server & mainframe computing for more than three decades.
- Security models implemented on a ”need to know” basis.
- But today’s RFID approaches aim for maximum transparency, efficient data access, and global standardization.
- Information flow analysis and access control models are essential to protect business secrets.

Privacy & Security Checklist

- Are you aware of all contextual information that can be correlated to your tags?
  - delivery frequency & destinations
  - return quotas & retail rates
  - predictable identifiers (e.g. serial number sequences)
- Countermeasures:
  - Identifier management
  - Encryption from tag to application level
  - Use tags without individual numbers

Checklist

- Do your tags contain interpretable information?
  - product keys
  - receivers or customer information
  - indications of object value
  - origin information
- Countermeasures:
  - Identifier management
  - Encryption & Access control
  - Tag self-destruct / deactivation or self-sealing

Checklist

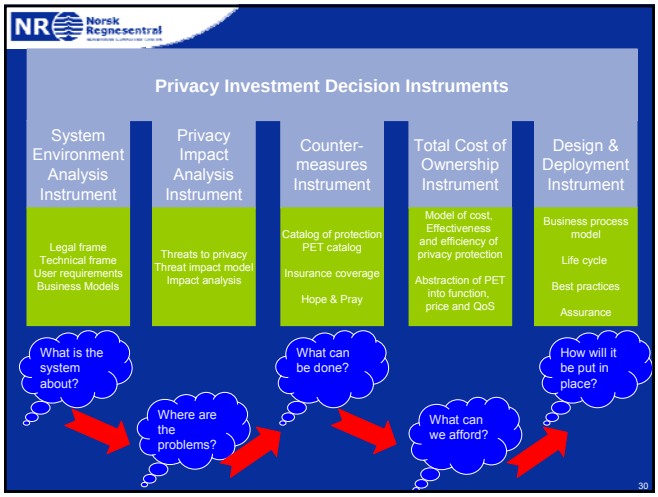
- Are your tags person-relateable?
  - Equipment check-out
  - e-tickets
  - consumer items
  - ID cards, door cards, passports, bank cards
- Countermeasures
  - De-activation (including chip serial number!)
  - Identity management
  - Privacy risk assessment & audits
  - Privacy-enhancing technology (PET)

28

Checklist

- Are your tags securely bound to the tagged objects?
  - Tag-switching destroys food tracing ROI (e.g. rotten meat with "good" tag
  - Fraudulent customers switch product tags to shop cheaper
- Countermeasures
  - Redundant information on tag & object
  - "Biometrics" derived from the object stored on tag
  - Fingerprinting techniques based on secrets

29



30

What can Norsk Regnesentral provide to your RFID project?

- Scientific research & consulting in security concepts
- Evaluation of security systems, properties & privacy impact
- Preparation of IT certification or audit
- *Industry-* or *publicly funded* research
- Open or confidential cooperation

31

Questions & discussion

32

Contact

Lothar Fritsch

forsker · research scientist
DART · department of applied research in information technology

dir. phone: (+47) 22 85 26 03
mob. phone: (+47) 968 85 758
Lothar.Fritsch@nr.no

Norsk Regnesentral · Norwegian Computing Center
Gaustadalléen 23, P.O. Box 114, Blindern
NO-0314 Oslo, Norway
www.nr.no · nr@nr.no

phone: (+47) 22 85 25 00
fax: (+47) 22 69 76 60

33