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
Popular view on RFID & privacy

► RFID's are presented as “Spychips” in the popular press.
► The press has a preference on tracking, tracing, and related privacy invasions, visible in debates on RFID passports, drivers licenses, e-tickets, etc.
► NGOs are forming wherever a major player introduces RFID to a consumer value chain.
► RFID is perceived insecure and immature (e.g. with frequent reporting of hacked transportation tickets and “cloned” RFID ID-cards.

Elvis is alive!
RFID Privacy Issues and News

Our RFID protest in NYC was a huge success! You can check out our original press release, see a local news story, read about the outcome on digg, or go directly to the report (with video) at homeland.stupidity.
Nye problemer for RFID-baserte billetter

Av, mandag 9. jan 2006 kl. 10:04

De nye kontaktfrie billett-automatene på skilte og busser snakker ikke med NSB og SL.

Oslo spesialister skulle etter planen ha ferdigstilt nye billetsystemet allerede sommeren 2006. Balkene for kontaktfri avtak av billettene er allerede installert på mange busser og skilte, men de er ikke klar i bruk på tunge. I sommer ble nyndring startet med utbyggingen.

2025 RFID Blocking wallet black

Pris: 150,- NOK

På lager

Antall: 1

Kjøp

Reisepass RFID Schutzhülle

Erhältlich bei diesen Anbietern.

1 Angebote erhältlich ab EUR 9,95

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.

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
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.
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 respect 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.

Privacy Protection matters.

- Privacy Relevance
  - Management Cost
  - TCO
  - Risk Management
  - Training
  - Legal Compliance
  - Fines
  - Exclusion from tender
  - Legal processing
  - Reputation
  - Branding loss
  - Customer loss
  - Competitive loss
  - Business loss

- Fines
- Exclusion from tender
- Legal processing
- Training
- Risk Management
- TCO
- Management Cost
- Privacy Relevance
- Reputation
- Branding loss
- Customer loss
- Competitive loss
- Business loss

TCO
Risk Management
Training
Legal Compliance
Fines
Exclusion from tender
Legal processing
Reputation
Branding loss
Customer loss
Competitive loss
Business loss
Duality of Privacy Risks

- **Personal Information Problem**

  - **Business risks**
    - **Reputation**
      - loss of image
      - loss of branding
      - loss of trust
      - higher expense in marketing
    - **Compliance**
      - fines
      - loss of license
      - prosecution
      - exclusion from govmt. business
      - higher legal expense
    - **Lost Opportunity**
      - Exclusion from international opportunities
      - Lose customers - to competition
      - Not get new customers
      - Higher cost of acquisition
    - **Self-Determination**
      - loss of reputation
      - loss of diversity
      - SPAM and price discrimination
      - higher efforts to keep control
  - **User risks**
    - **Intransparency**
      - confusion on what others know
      - uncertain future dangers of loss
      - loss of trust
dossier society
    - **Health & Freedom**
      - personal dangers
      - totalitarianism
      - stalking
      - intrusion

*Fritsch, Lothar; Abie, Habtamu: A Road Map to Privacy Management, Oslo, Norway, 2007*
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 prospects!
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
RFID applications: Beyond privacy, tags & readers

- Much research has been published 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.
Scenario assumption: RFID applications

Business application / business logic

Ambient-to-application "management" layer

- Identifiers
- Access keys
- Protocols

Ambient Devices, Readers & Communication
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
Case 1: The Boycott Case

Web community

3G data connection

Boycott FLATFISK ASA!

Boycott all farmed salmon!

Get 2 for the price of 1 at FJORDFISK!

Supermarket cart
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 chain

Many different stakeholders involved – where is the information stored?

► Who should see which part of the information?

► Who will be held liable for damages resulting from premature information dissemination?

FLATFISK ASA loses contracts with markets

3 weeks later: Mattilsynset confirms warehouse problem

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

Rotten fish from FLATFISK ASA
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
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!
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.
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)
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
Privacy Investment Decision Instruments

System Environment Analysis Instrument
- Legal frame
- Technical frame
- User requirements
- Business Models

Privacy Impact Analysis Instrument
- Threats to privacy
- Threat impact model
- Impact analysis

Countermeasures Instrument
- Catalog of protection
- PET catalog
- Insurance coverage
- Hope & Pray

Total Cost of Ownership Instrument
- Model of cost, effectiveness and efficiency of privacy protection
- Abstraction of PET into function, price and QoS

Design & Deployment Instrument
- Business process model
- Life cycle
- Best practices
- Assurance

What is the system about?
What can be done?
What can we afford?
How will it be put in place?
Where are the problems?
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
Questions & discussion