SPIEKERMANN, S., ZIEKOW, H., "RFID: A SYSTEMATIC ANALYSIS OF PRIVACY THREATS & A 7-POINT PLAN TO ADDRESS THEM", JOURNAL OF INFORMATION SYSTEMS SECURITY, VOL. 1, NR. 3, 2006

RFID: A SYSTEMATIC ANALYSIS OF PRIVACY THREATS & A 7-POINT PLAN TO ADRESS THEM[1]

Sarah Spiekermann
Humboldt-University of Berlin
Spandauer Straße 1
10178 Berlin
Germany
Tel.: +49 39 2093-5742
Fax.: +49 39 2093-5742
E-Mail: sspiek@wiwi.hu-berlin.de

Holger Ziekow
Humboldt-University of Berlin
Spandauer Straße 1
10178 Berlin
Germany
Tel.: +49 39 2093-5742
Fax.: +49 39 2093-5742
E-Mail: ziekow@wiwi.hu-berlin.de

[1] Presented in May 2005 on the 13th European Conference on Information Systems in Regensburg

RFID: A 7-POINT PLAN TO ENSURE PRIVACY

Sarah Spiekermann

Sarah Spiekermann completed her Ph.D. at the Institute of Information Systems at Humboldt University Berlin in 2002 on the subject of "Online information search with electronic agents". Today she is director of the Berlin Research Centre on Internet Economics (InterVal) and Assistant Professor at the Institute of Information Systems. Sarah (born in 1973) studied business and management at the University of Passau and at the European School of Management (ESCP-EAP) in Paris, Oxford and Berlin. Before joining Humboldt she worked as a strategy consultant for A.T. Kearney and later headed EMEA Business Intelligence for Mobile Internet inventor, Openwave Systems, based in Redwood City, California.

Holger Ziekow

Holger Ziekow studied computer science at the Humboldt-University of Berlin and is currently finalising his thesis at SAP Research Labs in Palo Alto, California on “Semantical Support for Embedding Smart Items in Business Applications”. In 2003 he joined the Institute of Information Systems as a a research assistant at the Berlin Research Centre on Internet Economics (InterVal).

RFID: A 7-POINT PLAN TO ENSURE PRIVACY

Abstract

This paper gives an overview of consumer fears associated with the introduction of RFID technology. It analyses the motivation and technical viability of these fears and derives suggestions for privacy-friendly technology design. The analysis shows that all consumer fears currently debated are essentially justified, because from a technical perspective they can all be implemented in the short- or mid-term. A 7-point plan of technological measures is presented that should be taken into consideration and developed further by standardization bodies, researchers and governments in order to impede potential abuses of the technology in the long term.

Keywords: RFID, Privacy, Security,

RFID: A 7-POINT PLAN TO ENSURE PRIVACY

Introduction

Radio frequency identification, short RFID, is a technology strongly debated in the information systems world of today. Next to other wireless technologies like Bluetooth or Wireless LAN it represents a major building block of the 'intelligent infrastructure' or 'ubiquitous computing environment' envisioned by IS researchers (Weiser 1991). RFID allows objects to be read out simultanously, through optical barriers and from a distance. Consequently, a strong driver of RFID adoption is its current deployment in worldwide retail and logistics operations. Major players like Walmart, the Metro Group or the US Department of Defense have set ambitious roadmaps for tagging products with RFID chips ('tags'). The goals are, for example, increased efficiency and control of supply chains, reduction of counterfeits, decrease of loss and waste of objects, etc.. In addition, new information systems and business models are being developed for RFID use beyond supply chain applications. Here, new forms of recycling, warranty management, intelligent home applications and infotainment systems have been discussed.

To make these services and business models come true RFID technology is complemented with an infrastructure called the EPC Network. This network is envisioned to serve as a backend service domain in which information on each object is accumulated and managed, can be searched for and accessed. The *key* between RFID at the front-end and this back-end infrastructure is the so called Electronic Product Code, EPC, which uniquely identifies each object (Engel 2003). Using the EPC in conjunction with services such as the Object Name Service (ONS) (Mealling 2004) or the EPC Discovery Service (VeriSign 2004) information about the history and state of objects can be found.

Seen this vision and first standards of the intelligent infrastructure to come, privacy advocates and researchers have pointed at the technology's strong impact on privacy and security. In the German and international press potential threats to consumer's privacy and security are now representing around 1/3 of all media messages on the subject (Spiekermann and Guenther 2004). Investigations of consumer fears and public campaigns of protest (e.g. demonstrations of the FoeBuD e.V. in front of the Metro Future Store or CASPIAN's "Boycott Benetton"-Campaign) show that the issue of privacy and security needs to be addressed for successful introduction of RFID – technology. However, so far, the discussion of privacy in the context of RFID has been very emotional, fragmented and focused on single, isolated problems. Consequently, a holistic and systematic analysis of the technology and potential ways of misusing it is required. The purpose of this paper is to fill this gap. Based on the major consumer threats associated with RFID introduction, the authors use strategies from security analysis to explore the technical feasibility of these threats. An attack-tree methodology based on Schneier (1999) is used for this purpose. Privacy threats or 'goals of attacks' are being hierarchically dissembled into sub-goals which need to be achieved in combination or alternatively. These sub-goals are then analyzed to systematically identify critical aspects of the technology. On this basis, a 7-point plan to ensure privacy with RFID is being developed.

Structured Models of RFID Threats for Privacy

For quite some time scholars have been discussing the impact of ubiquitous computing on peoples' lives. It has been pointed out that the permanent presence and registration of objects and people and the long-term saving of such data lead to an intrusion of privacy on multiple levels. Bohn et al. (Bohn, Coroama et al. 2004) in particular show how ambient intelligence possesses the ability to pull down peoples' natural, social, temporal and ephemeral privacy borders. Besides this fundamental research in

the societal impacts of ubiqutious computing some user-studies have been conducted at the AutoID Labs (Duce 2003) and at Humboldt University Berlin (Spiekermann and Guenther 2004). Here consumers have been observed discussing the technology in focus groups. In this way, a number of immediate and key threats could be identified. These include:

1. Unauthorised assessment of one's belongings by others
2. Tracking of persons via their objects
3. Retrieving social networks
4. Technology paternalism
5. Making people responsible for their objects

The following chapters will delve into the details of these threats, examine their technical feasibility and propose some means of prohibiting their realization. To keep the terminology of security analysis the realisation of an analysed scenario is referred to as an 'attack' and the proceeding instances as 'attackers'.

Unauthorised Assessment of One's Belongings by Others

A very basic attack is the unrecognized and unauthorised assessment of one's belongings. For example, criminals might be interested in some person's items. By scanning inventories of flats and houses or baggage at airports promising targets for theft or burglary might be identified. In addition, seizing objects can be a part of other threat-scenarios discussed below like tracking people's movements and social networks. Apart from these examples, economic interests may evolve around the possibility to send personalized advertising messages to people based on the objects they carry.

These examples and the attacks described in the following chapters show that the assessment of objects marks a core privacy problem of RFID technology. The way objects can be assessed is visualised by the attack-tree displayed in figure 1.

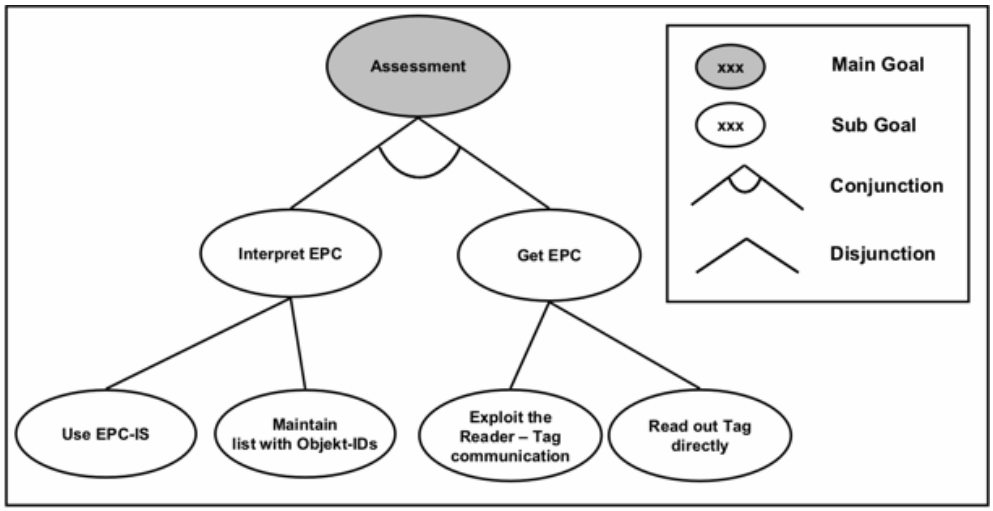

Figure 1. Attack-tree: Assessing objects

Two properties need to be fullfilled in order to seize objects unnoticed (and potentially unauthorized): 1. The Electronic Product Code (EPC) which is stored on an RFID tag must be read out unnoticed and 2. it needs to be interpreted.

Reading out is easily done. The retail industry is propagating the use of passive tags class 1 operating in the ultrahigh frequency band between 860-930 MHz (EPCglobal 2004). These tags currently

implement no protection against unauthorised access to the EPC. Hence the EPC can be read out directly by any RFID-reader from a six to eight meters distance. This range is big enough for attackers to scan objects unnoticed or track objects reliably at entry postes to public buildings and places.

If the attacker is too far away from an object he might alternatively eavesdrop the reader-tag communication. As the readers transmissions spread much further than the ones of the tags, this communication channel is highly vulnerable to eavesdroppers. As pointed out by Weiss (2003) insecure protocols holding information about the tags are of a high risk in the context. For example the deterministic collision handling[2] that was used in the first generation of class 1 tags (Auto-ID Center 2002) could reveal EPC codes to an attacker.

Once the desired EPC is known it needs to be interpreted to determine what kind of object it labels. Figure 2 shows how the EPC is assembled (Brock 2001). The part referred to as object class, is used for numbering a manufacturer's products. What the attacker needs to know is the link between these object class numbers and the *types* of products associated with them.

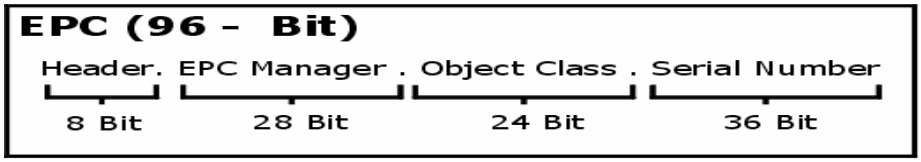

Figure 2. The structure of the Electronic Product Code.

To learn about this mapping one possible way could be to use an EPC Information Service (EPC-IS) (Harrison 2003; Global Commerce Initiative 2003). These services are planned to be part of the EPC Network (Harrison 2003; Global Commerce Initiative 2003; VeriSign 2004) and meant to provide item-related information such as the product catalogue information (Floerkemeier, Anarkat et al. 2003). Therefore they can be used to learn about the nature of a product labelled with a certain EPC.

Alternatively, databases for looking up product information on the basis of EPCs may be established independently from the EPC Network and the retail industry. For instance, Greenpeace could provide additional information on gene-food or rating agencies could publish the nature and quality of certain products based on the EPC.

The ease of reading out an EPC unnoticed and decoding its meaning shows how realistic such a basic attack is. Anybody with a low-cost reader and an Internet connection might be able to read out someone's belongings without notice. It therefore cannot be excluded that an investment in such an infrastructure makes sense in quite a few circumstances. Neither technical nor economic barriers are present to prevent such a scenario from happening. Hence, finding means to protect RFID tags from unauthorised assessment is essential to protect privacy.

Potential Approaches to Prevention

Seen the ease of seizing one's objects the industries' standards bodies should have an interest to protect RFID tags' content more rigorously. One proposal is to kill tags at store exits. For the tags class 1 a kill-function has therefore been specified which can be used to permanently deactivate a tag. Yet, while the killing of tags at the store would solve probably most privacy problems outside the store, the this solution also has some technical and economic drawbacks. Most important, many

[2] Anti-collusion describes the mechanism by which readers handle the presence of multiple tags at the same time.

industry bodies furthermore oppose the killing of tags, because this would equally kill any post-purchase intelligent infrastructure services, including the management of returnable itms, warranty checks, etc.

As a way out of this dilemma hash-lock and password protection schemes (Engels, Rivest et al. 2003; Inoue 2004; Spiekermann and Berthold 2004) have been proposed that put object control into the hands of object owners. Here, tags are deactivited at store exits per default. Yet, if people want to use a tag again they can switch it on via an authentication protocol. These solutions obviously drive tag cost and therefore are not willingly embraced by the industry up to now for mass-market solutions.

Tracking of Persons Via Their Objects

RFID-technology is believed to enhance logistics by enabling item-level tracking of objects. Once these objects are owned by persons, though, the ability of tracking objects becomes an ability to track individuals.

Using RFID-technology retailers might track customers within their shops in order to create profiles of movement which can be used to improve marketing strategies at the point of sale (Jannasch and Spiekermann 2004). In shopping malls several shops might interlink tracks and analyse the popularity of different aisles. The state could have an interest in tracking in the context of criminal proceedings. Other purposes of tracking might be a company's interest in monitoring employees' whereabouts and working habits.

How tracking of persons can possibly be done, is displayed in figure 3.

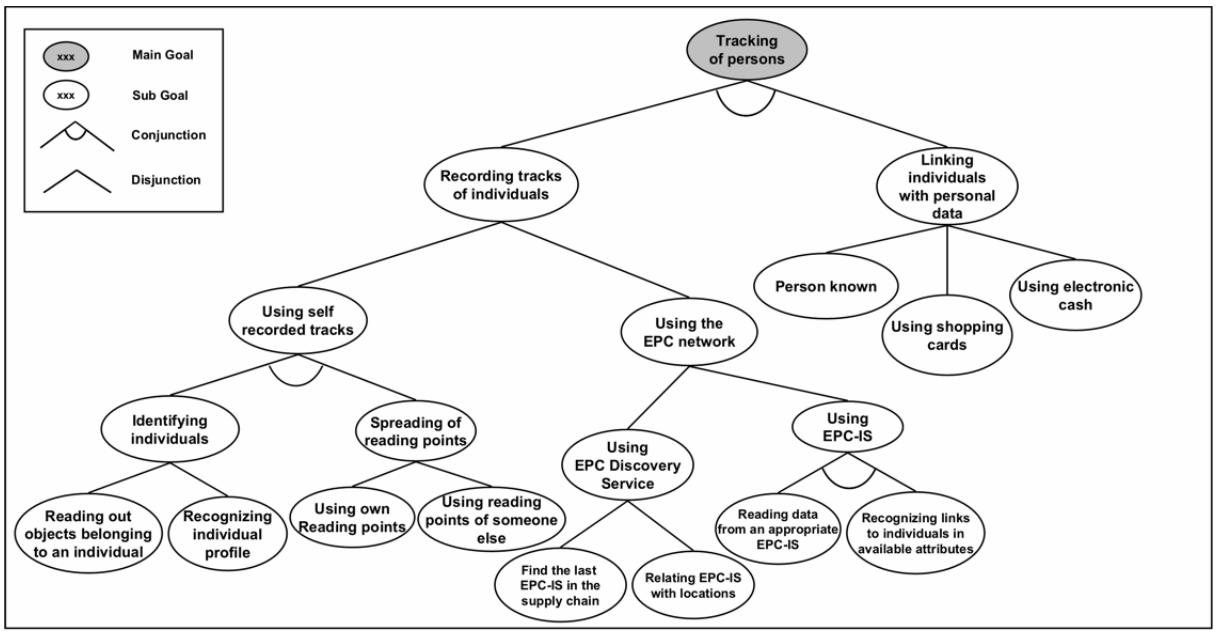

Figure 3. Attack-tree: Tracking persons

To track people, identification data has to be linked with individual tracks of movement. Identification data is collected when customers pay with electronic cash or use loyalty cards. Alternatively, the person might already be known to the attacker.

The second general objective necessary to track people is to automatically record individual tracks of movement. Due to the unique numbering scheme of the EPC and the easy seizing of this identifier (see above) RFID-technology readily supports the recording of tracks. In various documents of the Auto-ID Centre data structures and information systems to maintain the readout of items together with the referring timestamp and location are described (Harrison, Moran et al. 2003; Harrison 2003;

Floerkemeier, Anarkat et al. 2003). The purpose of this infrastructure is to generate and exchange EPC based tracking information.

Tracking of persons can be done best by using EPCs of products regularly carried by a person over a longer period of time, e.g. wristwatches or purses. The EPC would then serve as a kind of cookie. Alternatively, profiles assembled by various products could be created and used for a highly probable recognition of individuals.

When tracking is desired on a regional or even global scale, the EPC Network could possibly be used to gain a geographically wider spread of data points for tracking. Dependent on the access rights of an attacker read points and times of readers from diverse locations could be retrieved from the EPC Network by querying for a product's last position. Verisign already announced the launch of a so called EPC Discovery Servie which could be used to serve this very purpose (VeriSign 2004).

Potential Approaches to Prevention

If tracking is done within stores and shopping malls tags and readers are fully controlled by retailers. Hence, mechanisms for protection could be regulated by law or be based on retailer's voluntary self-limitations.

Ways to preserve the privacy of people could take several forms: The first one may be to only save reading data for a very limited time span, e.g. during the shopping period, and second to not share this local tracking data with the EPC Network. In this way, peoples' movements would not be trackable for a longer period of time and not be centrally accessible. Furthermore, personal identification data (if available) could generally not be saved after the shopping trip, so that *personal* tracks cannot be recapitulated in the aftermath.

Furthermore, retailers could refrain from saving the full serial number of an object with an owner's name. In this way, the ling between people and their objects would be broken.

Finally, the timestamps saved together with EPC readouts could be saved with limited accuracy leading to less granular tracks.

While all of theses measures are straight forward technical designs that do not require peoples' participaton to ensure privacy there have also been some other privacy proposals that involve people in the tracking decision. One is to use privacy profiles as it is already being done on the Internet on the base of P3P (Cranor 2003). Here peoples' privacy preferences are recorded by an identity mangement tool, e.g. a Privacy Watchdog-Tag (Langheinrich 2003; Floerkemeier, Schneider et al. 2004). The privacy preferences application defines, for example, how tracking-data needs to be handled by retailers, but also under what circumstances it may at all be collected. Readers would have to obey to the privacy preferences of users or will not be allowed to access personal object IDs. The challenge with this 'P3P-for-RFID' approach is not only that P3P has been little successful even in the Internet context where user interface control is much bigger than in the RFID context, but it also takes final privacy control away from users (Cranor and Reidenberg 2002). There may be circumstances under which readers do not obey to the privacy preferences specified by users. And generally there may be quite a few ways to define the purpose and extend of read-outs in accordance with the P3P protocol while these are actually far from what the user acutally wants. This lack of P3P to fully reflect purpose and context has been cirticised elsewhere.

For tracking after product purchase, another promising way to put control into the hands of people is to use one of the hash-lock models described above (Engels, Rivest et al. 2003; Spiekermann and Berthold 2004). In such a scenario all RFID-tags would be turned off by default. If commercial or institutional services are at a person's disposition though he or she gets the possiblity to 'turn on' her object's chip again with the help of a personal password. In this way, unauthorized seizing and tracking is generally prohibited and under full user control. Unnoticed or unauthorized tracking would not be possible under these circumstances.

Retrieving Social Networks

Using data mining techniques, additional information can be gained from registered tracks. For instance analysing information about movement can be used to deduct social links between persons. This may be of potential interest for governmental agencies in the context of law enforcement. Figure 4 visualizes how tracks of movement could be used to ascertain social networks.

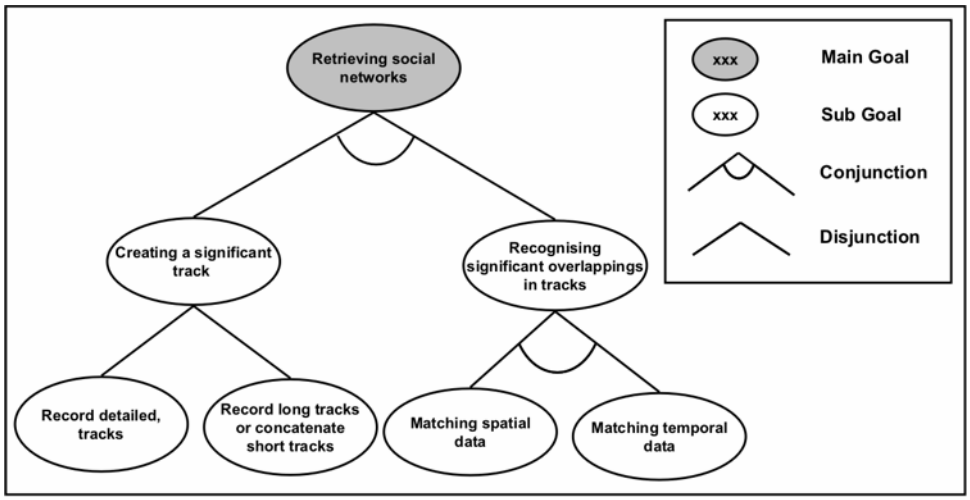

Figure 4. Attack-tree: Retrieving social networks

It is reasonable to assume that people who are often at the same location at the same time or repeatedly walk close to each other, are socially linked. On this assumption social networks may be hypothesized. Personal tracks of movement are then compared with each other in order to find significant matches. This means, similarities in spatial and temporal data of tracks would need to be compared. To be significant, the matching would need to be done on a very finely grained level or over a longer period of time. For example, two tracks of persons moving at the same time through various shops in a mall with just two meters distance are significant enough to conclude a social link between them.

If data points are sparse, because few readers are set up, then longer tracks are needed. For example, known that two persons have been in the same store at the same time is not sufficient to reasonably assume a social relationship between them. But if these people happen to be tracked in the shop at exactly the same time over a period of several months, a social link between them is likely.

Potential approaches to prevention

The approaches to prevention are generally the same as those outlined above for tracking. However, in this context the special role of reading granularity becomes apparent. If read-out timestamps set by readers are precise, social networks can be retrieved. If the timestamps registered are, however, condensed to time intervals, let's say every 5 minutes, then the movement of objects and people becomes blurred and the retrieval of social networks would not be possible any more.

Technology Paternalism

Technology paternalism refers to a fear expressed in the focus groups of uncontrolled autonomous action of machines that cannot be overruled by object owners. Examples include smart shelves in supermarkets which cause an alarm when a wrong product is placed in them, or cinema entries which

automatically check visitors for drinks, snack foods or cameras brought with them, cars that force people to wear seatbelts by emitting noise, CD players that refuse to play records the copyright of which is unclear or paper-garbage that starts to emit noise when a battery is by hazard put into it. RFID has the potential to overrule or punish people instantly for a myriad minor incidents of misconduct and by this intrude heavily on peoples' life. What is more, using RFID-technology in this way can be in the interest of governmental and commercial institutions to reduce cost (e.g. for sorting garbage) or to automatize financial penalties. How RFID-technology can be used to implement this type of automated control is shown in figure 5.

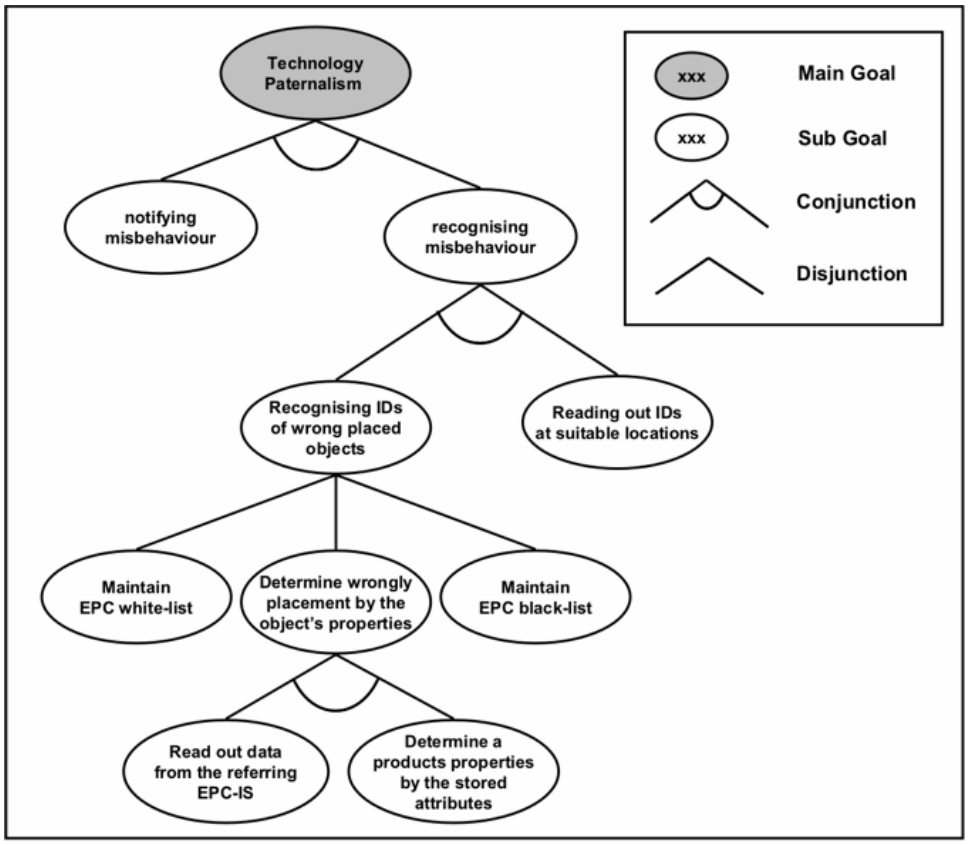

Figure 5.Attack-tree: Implementing technology paternalism on the base of RFID-labelled items

RFID-technology can be used to detect misbehaviour by simply detecting wrongly placed objects. To do this, readers need to be installed at the locations desired to control. Furthermore, misplaced objects must be recognised by their EPC. To do so different approaches can be taken:

A possibility to identify misplaced objects is to compare them with a black-list containing significant parts of EPCs referring to products which are not to be placed at the location of read-out. Alternatively, a white-list could be used, containing patterns of EPCs allowed at the monitored location.

If such lists are not suitable, the EPC could be used to find out about an object's attributes to determine whether or not it is allowed at the controlled location. To do this, PML data potentially provided by EPC Information Services in the EPC Network may be available (Floerkemeier and Koh 2002; Engel 2003). Here, however, a connection to the Internet, and access rights to the referring EPC Information Services would be needed, a rather costly solution that may not be feasible economically in most situations.

Realizing this scenario is, in any case, only reasonable if the investments are justified by the expected benefits. Therefore only those scenarios are likely to be realized where reasonably maintainable black-lists or white-lists can be used to decide whether or not an object is placed correctly. Furthermore, the

cost of RFID-readers has to be taken into account. Hence, in a reasonable scenario the number of readers required is either limited or readers are already available for other purposes (e.g. on smart shelves).

Potential Approaches to Prevention

Generally two ways exist for preventing the described attack. One approach is to avoid that objects can be identified as wrongly placed by reading out their EPC. This means, automatic interpretation of numbers must be prevented. Yet, this seems unlikely.

If the EPC Network is needed to determine an object as wrongly placed, limited access rights to EPC Information Services could stop some attackers. But most likely scenarios can be expected to use black-lists or white-lists for the identification of wrongly placed objects. This, however, cannot be prevented in technical ways. Consequently, laws may need to be passed that prohibit the use of the technology in such a way or put major restrictions on its widespread deployment.

The other way of protection is to make sure that objects can't be read out at the monitored location. Killing tags, protecting them with a password or even using blocker tags would be a good approach to protect people from this type of attack.

Making People Responsible for Objects

The scenario that people might be held responsible for objects they own or owned has frequently been cited in press articles to criticize RFID-technology. Public institutions could have interest in identifying owners of objects, e.g. in the case of criminal investigations. Or, alternatively, if waste was found outside rubbish bins, those who pay for cleaning up might have an interest to fine the responsible person. Below the attack-tree model is shown where this attack is visualized.

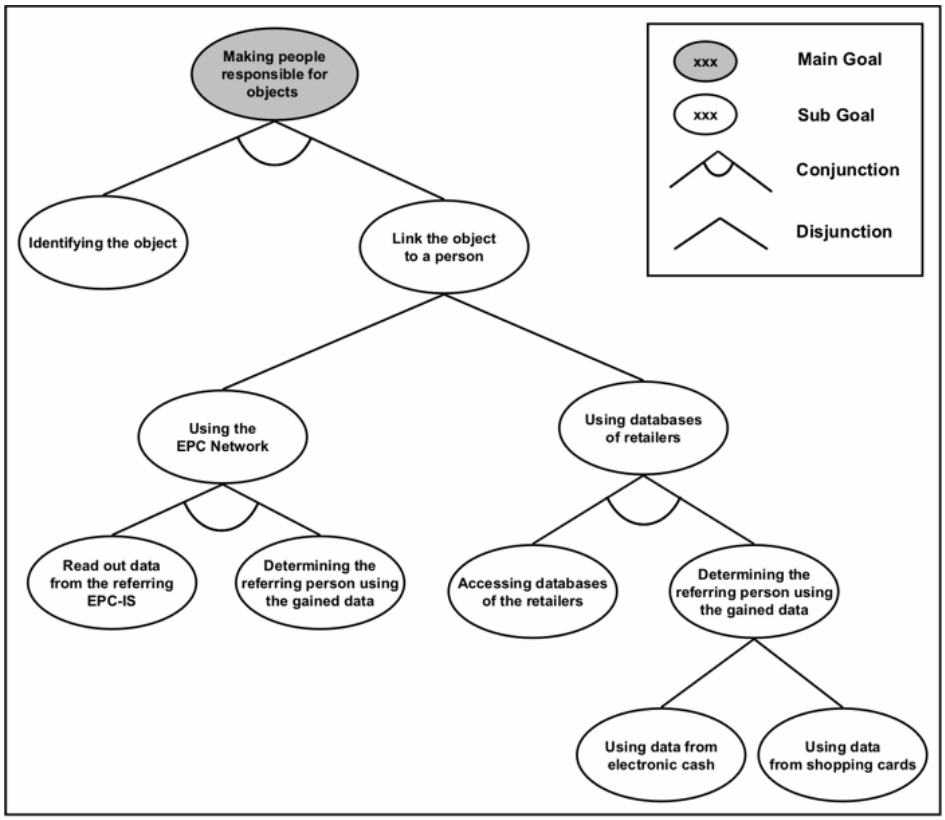

Figure 6. The general attack tree to make people responsible for objects.

In order to hold people responsible for objects it is necessary to *uniquely* identify an object and associate it with a person. As RFID-labelled objects are uniquely numbered with the EPC and increasingly people use loyalty cards revealing their identities such a link is easily made. Typically, an EPC would be stored with the object owner's name in a retailer database. In the context of law enforcement governmental agencies would most likely be allowed access to these databases.

Reading out an EPC is, as was shown above, trivial for tags which are not deactivated. But even for those that are deactivated the EPC may potentially still be determined by disassembling the chip and reading out its memory manually. This requires advanced technical skills though and may therefore only be feasibly in serious cases of criminal investigation.

Potential Approaches to Prevention

As has been stressed in the previous discussion, governmental agencies can realize this scenario if objects are labelled with an EPC and these numbers are linked with consumer identification data in retailer databases. Consequently, protection has to address at least one of these aspects assuming that governmental agencies should *not* be given this type of investigation right.

To ensure that objects are not labelled with an EPC the tags memory needs to be deleted. However, permanent disabling has economic drawbacks. Therefore hash-lock or other strong encryption of the EPC on the tag may help. These however rise tag costs considerably.

Instead of preventing the EPC from getting known links of EPCs to customers could therefore be avoided in retailer databases. As data necessary for marketing research or bonus systems do not need product information on an item-level and thus do not need to use the full serial number part of an EPC, a reasonable habit could be to store EPCs by default without their serial number part or only parts of this serial number. In some countries, joint storage of uniquely identified purchases and persons' names is already prohibited by the law.

Conclusion

This paper gives an overview of consumer fears associated with the introduction of RFID technology. It systematically analyses the motivation and technical viability of these fears and derives suggestions for privacy-friendly technology design. The analysis shows that all consumer fears currently debated are essentially justified, because from a technical perspective they can all be implemented in the short- or mid-term. Once objects are owned by persons, the ability of tracking and sizing objects becomes an ability to track and size individuals. Not all attacks are economically feasible, though, for the institutions that may be interested in the data. The paper thus shows that the extent of technology abuse will partly be limited by market forces. Still, a number of technological measures could be taken into consideration and developed further by standardization bodies, researchers and governments in oder to impede potential abuses of the technology in the long term. These include:

1. Default killing of RFID tags at store exits OR password protection of RFID tag content
2. No sharing of local tracking data (times and places) with the EPC Network beyond logistics
3. Minimal granulariy: Limited timestamp information
4. Partial or no saving of the full EPC serial number
5. Rigorous controls and transparency of EPC Network access rights
6. Deletion of all object data after a certain period of time
7. Owner control over personal information on sold objects available on the EPC Network

The first listed measure addresses a very basic security risk by stopping unauthorised read outs. As shown in the analysis, nearly every considered attack includes read out as a sub goal. Hence, controlling access to tags is the most important step to preserve privacy.

Furthermore the envisioned IT-backend infrastructure coming along with RFID plays an important role in most attacks. These are EPC Network services and RFID related databases. The attack-tree analysis points out a number of ways how this infrastructure might be abused. The listed means from number two to six can be applied to set up privacy friendly information handling in this context.

The final point in the list is to ensure basic privacy rights as stated by the OECD. This issue is not directly linked to a specific attack scenario but may heavily influence how privacy is perceived by consumers.

Applying the listed measures would help to make RFID technology more privacy friendly since many scenarios of misuse could be prevented. Future research Even though this list may not be complete, it can serve as a good basis for a structured research approach and debate the goal of which should be to get a positive start on a new technology dimension in our lives.

References

Auto-ID Center (2002), '860MHz–930MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1', Technical Report, Auto-ID Center, MIT, Cambridge, USA.

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F. and Rohs, M. (2004), 'Living in a World of Smart Everyday Objects – Social, Economic, and Ethical Implications', *Journal of Human and Ecological Risk Assessment*, 10 (5): 763-785.

Brock, D. (2001). The Electronic Product Code (EPC) - A Naming Scheme for Physical Objects. Auto-ID Center. Cambridge, USA, Massachusetts Institute of Technology

Cranor, L. F. (2003). P3P: Making Privacy Policies More Useful. *IEEE Security & Privacy*. 1: 50-55.

Cranor, L. F. and J. Reidenberg (2002). Can user agents accurately represent privacy notices? *The 30th Research Conference on Information, Communication, and Internet Policy (TPRC 2002)*, Alexandria, Virginia, USA.

Duce, H. (2003). Public Policy: Understanding Public Opinion. Auto-ID Center. Cambridge, UK, University of Cambridge, UK.

Engel, D. (2003), 'The Use of the Electronic Product Code', Technical Report, Auto-ID Center, MIT, Cambridge, USA.

Engels, D., R. Rivest, et al. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. *First International Conference on Security in Pervasive Computing (SPC 2003)*, Boppard, USA, Springer Verlag.

EPCglobal (2004), Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9, www.epcglobalinc.org

Floerkemeier, C., Anarkat, D., Osinski, T. and Harrison, M. (2003), 'PML Core Specification 1.0', Auto-ID Center Recommendation, Auto-ID Center, MIT, Cambridge, USA.

Floerkemeier, C. and Koh, R. (2002), 'Physical Mark-Up Language Update', Technical Memo No. TM-006, Auto-ID Center, MIT, Cambridge, USA.

Floerkemeier, C., R. Schneider, et al. (2004). Scanning with a Purpose - Supporting the Fair Information Principles in RFID Protocols. *2nd International Symposium on Ubiquitous Computing Systems*, Tokyo,Japan.

Global Commerce Initiative (2003), 'Global Commerce Initiative EPC Roadmap', http://www-1.ibm.com/industries/wireless/doc/content/bin/EPCRoadmap.pdf, Global Commerce Initiative (GCI) and IBM

Harrison, M., H. Moran, et al. (2003). White Paper - PML Server Developments. Cambridge, University of Cambridge.

Harrison, M. (2003), 'EPC Information Service – Data Model and Queries', White Paper No. WH-025, Auto-ID Centre, University of Cambridge, Cambridge, UK.

Inoue, Y. (2004). RFID Privacy Using User-controllable Uniqueness. RFID Privacy Workshop, Massachusetts Institute of Technology, Cambridge, MA, USA.

Jannasch, U. and S. Spiekermann (2004). RFID Technologie im Einzelhandel der Zukunft: Datenentstehung, Marketing Potentiale und Auswirkungen auf die Privatheit des Kunden. Berlin, Lehrstuhl für Wirtschaftsinformatik, Humboldt Universität zu Berlin.

Langheinrich, M. (2003). A Privacy Awareness System for Ubiquitous Computing Environments. *4th International Conference on Ubiquitous Computing*, UbiComp2002, Göteborg, Sweden, Springer.

Mealling, M. (2004), 'EPCglobal Object Name Service (ONS) 1.0', Working Draft Version, EPCglobal.

OECD (1980). Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.

Schneier, B. (1999). Attack Trees. *Dr. Dobb's Journal*.

Spiekermann, S. and O. Berthold (2004). Maintaining privacy in RFID enabled environments - Proposal for a disable-model. Pervasive 2004, *2nd International Conference on Pervasive Computing*, Vienna, Austria.

Spiekermann, S. and O. Guenther (2004). RFID & Privacy: Consumer Perspective & Technology Insights. M.-L. St.Gallen. St.Gallen, CH.

Spiekermann, S. and H. Ziekow (2004). Technische Analyse RFID-bezogener Angstszenarien. Berlin, Lehrstuhl für Wirtschaftsinformatik, Humboldt Universität zu Berlin.

VeriSign (2004). The EPC Network: Enhancing the Supply Chain. VeriSign.

Weiser, M. (1991), 'The Computer for the 21st Century', *Scientific American*, 265: 94-104.

Weis, S. A. (2003). Security and Privacy in Radio-Frequency Identification Devices. Cambridge, Massachusetts Institute of Technology.