

TECHNISCHE UNIVERSITÄT DRESDEN

FACULTY OF COMPUTER SCIENCE
INSTITUTE OF SYSTEMS ARCHITECTURE
CHAIR OF PRIVACY AND DATA SECURITY

Master Thesis

Protection of the Users' Privacy in Ubiquitous RFID
Systems

Ivan Gudymenko
(Born 15. December 1986 in Nikolaev)

Advisor: Dr. Katrin Borcea-Pfitzmann

Dresden, November 29, 2011

Master's Thesis Application

Name, First Name Gudymenko, Ivan

Course: Computational Engineering Student ID: 3|5|2|9|1|3|5

Subject: Protection of the Users' Privacy in Ubiquitous RFID Systems

Objective :

Privacy and Security issues are gaining importance in modern UbiComp systems due to the constant increase of collection and processing of personal information, which raises the users' concern over this problem.

This Master thesis focuses on developing a framework for designing privacy-respecting RFID-based systems (as being part of UbiComp). This implies exploration of the inherent privacy threats in such environments and development of suggestions for solutions.

The following issues should be covered within the Master thesis:

1. A survey on related work in the field of privacy in UbiComp with the respective conclusions.
2. Development of suggestions for design principles of UbiComp, RFID-based systems with regard to privacy.
3. Focus on privacy modelling as one of the ways of reflecting privacy requirements of the users.
4. Developing an approach to obtaining implementable privacy requirements from the model.
5. Validation of the concept based on selected use cases.


Supervisor: Dr.-Ing. Katrin Borcea-Pfitzmann

Teacher in Charge: Dr.-Ing. Katrin Borcea-Pfitzmann

Institute: Chair of Privacy and Data Security

Start date : 01.06.2011

The thesis must be submitted on : 30.11.2011



Signature of the Teacher in Charge:

Declaration

Herewith I declare that this submission is my own work and that, to the best of my knowledge, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher education, except where due acknowledgement has been made in the text.

Dresden, November 29, 2011

Ivan Gudymenko

Abstract

This master thesis considers the privacy-respecting ubiquitous RFID systems and the possible ways of their development. In order to perform that, the notion of privacy is structured and classified, which enables its holistic consideration. Afterwards, the specific privacy threats and the ways of its enforcement in the RFID domain are structured. This forms the necessary basis for privacy requirements engineering, which can be performed according to the concepts described in the specifically developed framework.

Contents

1	Introduction	3
2	Related work on privacy in UbiComp	5
2.1	UbiComp: an outline	5
2.2	RFID as the enabler of UbiComp	6
2.3	Privacy concerns inherent in UbiComp systems	7
2.3.1	Transparent accessibility and self-governance	8
2.3.2	Existing approaches to privacy management in UbiComp and their assessment	9
2.3.3	The problems of transparent accessibility and self-governance in RFID systems	12
2.4	Chapter summary	14
3	Privacy implications of RFID systems	15
3.1	Main components of RFID systems	15
3.1.1	RFID tags	15
3.1.2	RFID readers	18
3.1.3	RFID back-end	19
3.2	Classification of RFID systems	20
3.3	Privacy issues in RFID systems	23
3.3.1	Defining privacy	23
3.3.2	Privacy facets	25
3.3.3	Peculiarities of privacy management in RFID systems	27
3.4	Privacy enforcement	40
3.4.1	Privacy enforcement mechanisms	41
3.5	Security peculiarities in RFID	47
3.5.1	A CIA triangle in RFID	48
3.5.2	Attacking an RFID system	50
3.5.3	Security management in RFID	53
3.5.4	Summary on security peculiarities of RFID	57
3.6	Chapter summary	58
4	Designing a privacy-respecting RFID system	59
4.1	Motivation for designing RFID systems in a privacy-preserving way	59
4.2	Making privacy inherently built into the functionality of an RFID system	60
4.3	Considering privacy and security in a joint fashion	61
4.4	Chapter summary	65
5	Privacy modeling: motivation and suggestions	67
5.1	Privacy modeling: motivation	67
5.2	Privacy modeling in a privacy management system	68
5.3	Existing privacy models and their assessment	70
5.3.1	A sociological perspective: Crossing "Personal Borders"	70
5.3.2	A legal perspective: A Taxonomy of Privacy-invading Activities	73
5.3.3	Privacy modeling from the technical perspective	75
5.3.4	Privacy models: a short summary	82
5.4	Chapter summary	84
6	Privacy requirements inference	85
6.1	A framework outline	85
6.2	A framework elaboration	87
6.2.1	Step 1: An abstract privacy model	87
6.2.2	Step 2: System-specific privacy requirements	87

6.2.3	Step 3: Implementation	96
6.2.4	A short summary	97
6.3	Use case validation	97
6.3.1	Use case 1: RFID tags woven into garments	97
6.3.2	Use case 2: RFID-enabled keys in the enterprise	101
6.3.3	Use case 3: contactless payment cards	103
6.3.4	A short summary	105
6.4	Chapter summary	105
7	Conclusion	107
	Bibliography	109
A	Implementation attacks on RFID tags	115
B	Privacy modeling: a legal taxonomy of privacy-invading activities	117

1 Introduction

Rapid evolution of Information Systems opens new opportunities for business and enables companies to deliver services hardly imaginable a decade ago. The so-called "Ubiquitous Computing" (UbiComp) is one of the main enablers of this process and therefore has attracted a lot of attention from academia and become a hot topic in scientific discussions.

The notion of UbiComp incorporates a big variety of systems and different kinds of underlying technologies. Among them, the systems exploiting Radio Frequency Identification Technology (RFID) are one of the most widespread due the relative simplicity of end devices (RFID tags) and the ability to integrate them into the surrounding environment in a pervasive manner.

Along with numerous advantages that ubiquitous RFID systems provide for their users, concerns over privacy and security arise, which might eventually impede the adoption of such systems and consequently have a negative impact on their commercial success.

This master thesis focuses on developing approaches to designing privacy-respecting RFID-based systems. In order to perform this, the following issues were covered. In Chapter 2, a concise description of UbiComp is carried out leading to RFID systems as one of its main enablers. Privacy concerns of UbiComp systems in general influence privacy management in every concrete ubiquitous system that comprise UbiComp, including the RFID-based one. For this reason a short discussion on main privacy concerns imposed by UbiComp are provided in Chapter 2 as well.

Chapter 3 focuses on privacy implications of RFID systems highlighting specific issues which should be considered while designing solutions for privacy management in the RFID domain. The general notion of privacy is also discussed together with its possible classification and motivation for considering privacy in an interdisciplinary manner. Since security provides for the necessary basis for implementing and ensuring privacy and is, therefore, an integral part of the underlying mechanisms of privacy management, security peculiarities of RFID are considered as well. RFID systems have a specific structure which should also be considered while protecting the privacy of the users. That is why the main components of RFID systems are briefly discussed in Section 3.1 with the focus on capabilities of end devices – the RFID tags.

Chapter 4 develops recommendations for designing RFID systems in a privacy-respecting way.

Having specified the general recommendations for developing privacy-preserving RFID systems, the thesis focuses on privacy requirements engineering for RFID systems. The motivation for using privacy modeling in order to achieve this together with the review and assessment of several existing privacy models is covered in Chapter 5. Suggestions for further utilization of privacy models in the underlying privacy-preserving systems are considered as well.

In order to provide for an efficient process of obtaining privacy requirements from a privacy model, a special framework was developed and presented in Chapter 6 along with the respective validation against several use-cases.

2 Related work on privacy in UbiComp

This chapter starts with a brief description of the UbiComp paradigm, discusses its main properties and focuses on their influence on privacy. The connection between UbiComp and RFID is then highlighted together with the privacy implications of UbiComp and their impact on privacy of the users of RFID systems.

2.1 UbiComp: an outline

Computing has made a giant leap forward over the last 20 years. Computers have become an integral part of our everyday life, and already now it is hardly possible to perform our daily routines without their assistance. The technological advance has made it feasible to shift a substantial part of computing from desktop machines to mobile devices making it *pervasive*. This also implies a dramatic increase in background computing and results in the fact that a substantial part of overall computing processes has become invisible to the end users. That introduces a qualitatively new scenario where the human beings are *unconsciously* using the benefits of mobile computing without having to explicitly concentrate themselves on "how" but rather on "what" they want to perform¹.

A notion of "[...] integrating computers seamlessly into the world at large [...]" was envisioned by Marc Weiser in his seminal paper [Wei91] as "ubiquitous computing" (or shortly "UbiComp"). Frank Stajano further elaborated on this idea and described UbiComp as "[...] a scenario in which computing is *omnipresent*, and particularly in which devices that do not look like computers are endowed with computing capabilities." [Sta02]. According to him, UbiComp does not imply "the computer on every desk" but rather embodying the computational power into different parts of the surrounding environment (clothes, household appliances, etc.) that are not supposed to be equipped with it in the conventional sense.

¹For example, a user is near the supermarket and a system notifies him/her that there is not enough milk in the fridge and advising which bottle of milk at which shelf of the supermarket should be taken utilizing unobtrusive computing devices attached to every item in the store. In this case, the computing is *omnipresent*, or *pervasive*, i.e. is accompanying the individual throughout the day.

UbiComp has a number of core properties that distinguish it from conventional computing. They are listed below (adapted from [Pos09]):

1. Computers are pervasively networked and transparently accessible.
2. Human-computer interaction (HCI) is rather seamless and implicit.
3. Computers are context-aware in order to optimize their operation in the environment.
4. Computers can operate autonomously, i.e., without human intervention and be self-governed (in contrast to the case of conventional HCI, which implies a step-by-step process of user control).
5. Computers can handle a multiplicity of dynamic actions and interactions, governed by intelligent decision-making and intelligent organizational interaction (mainly computer-computer interaction, CCI). This might entail some form of artificial intelligence in order to handle:
 - a) incomplete and non-deterministic interactions (both HCI and CCI);
 - b) cooperation and competition between members of organizations;
 - c) richer interaction (in general) through context sharing, semantics, and goals.
6. Interoperability of solutions is going to determine the pervasiveness of UbiComp.

Different technologies provide for realization of certain properties of UbiComp therefore partially enabling its implementation. The solutions having been developed so far are rather tailor-made and designed without interoperability in mind exemplifying the "first stage" of UbiComp development described in [Pet06]. The transition from numerous "isolated solutions" to a unified one enabling the interconnection of heterogeneously designed applications and hardware should mark the begin of the "second stage" of UbiComp. This will satisfy the interoperability property of UbiComp and provide for a qualitatively new degree of pervasiveness.

2.2 RFID as the enabler of UbiComp

UbiComp encompasses a big variety of underlying technological solutions each of them having their own benefits and shortcomings. The possible spectrum of existing technologies that have a potential of enabling the UbiComp paradigm are mainly concentrated in the area of lightweight communications. The latter should provide for interconnection of resource-constrained and unobtrusive

devices, which eventually comprise the front-end of a UbiComp system as opposed to the back-end maintaining the support of background processes like heavy computation, global interconnection (e.g. via the Internet), billing, etc.

Having conducted a survey on communication technologies which can be seen as the enablers of UbiComp, the most prospective of them from my point of view are presented in Figure 2.1 together with the IP stack (to depict the completeness of each solution with respect to the layering concept¹).

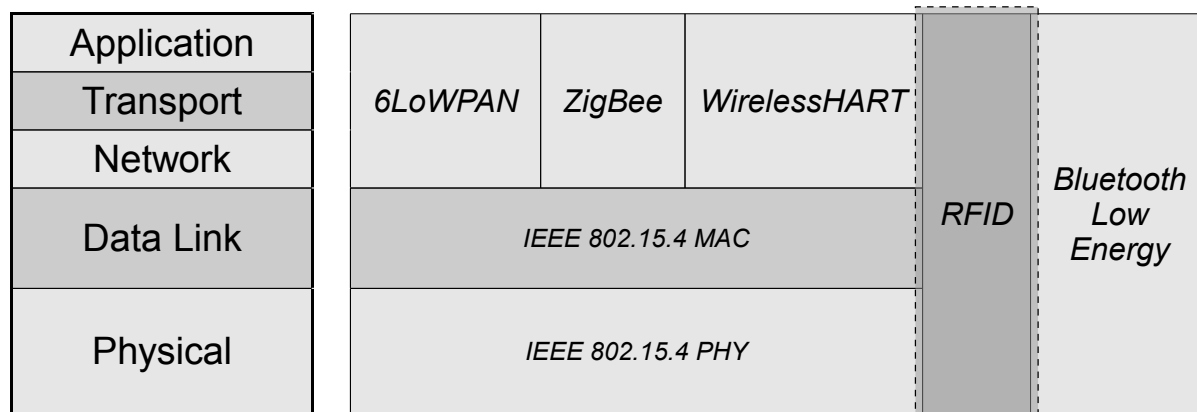


Figure 2.1: The IP stack layering scheme and the most promising communication technologies for UbiComp.

Remark: RFID in this case implies not only the underlying physical principles of tag–reader communication but also readers interconnection via the backbone network, i.e. an RFID system in general (including the back-end).

One of the key technologies which can be seen as enablers of UbiComp is Radio Frequency Identification (RFID) highlighted in Figure 2.1. This technology deserves special attention for several reasons. RFID end devices (RFID tags) can be mass-produced and therefore are relatively cheap (an order of several cents). RFID technology has existed for several decades and has become established and mature in such fields as logistics, supply chain management, retail industry, etc. The inherent pervasiveness of RFID, the small size and low cost of end devices make it one of the main technological enablers of UbiComp for the nearest future.

2.3 Privacy concerns inherent in UbiComp systems

Privacy concerns inherent in UbiComp influence privacy management in every specific system that can be regarded as a ubiquitous one, including the main focus of the thesis – the RFID systems. This section discusses the main problems of privacy management in the UbiComp domain and surveys several solutions.

¹Layers in terms of IP layering or more generally, the OSI layers, see [DZ83].

The connection between privacy- and security-related problems inherent in UbiComp and RFID systems is considered as well.

2.3.1 The problems of transparent accessibility and self-governance

Whereas UbiComp introduces a set of tangible benefits for the user¹, it also raises serious privacy concerns. The core properties of UbiComp systems described in the Section 2.1 determine several privacy- and security-related problems inherent in this domain. The main ones are the problems of transparent accessibility and self-governance.

Transparent accessibility

Transparency in context of UbiComp² is a useful property which enables hiding the unnecessary (with regard to the current operation) information from the entities in order to facilitate their cooperation and avoid overloading the user with irrelevant information. Despite having a number of tangible advantages, transparency introduces a serious security and privacy challenge. The reason for this is that, having executed an access procedure in a transparent fashion, the user either does not see *what* is being accessed or by *which means* it has been accessed. Moreover, it might not be clear *which entity* performs an access procedure. This leads to a dramatic loss of control of security and, as a consequence, endangers the privacy of an individual.

One of the ways to mitigate the problem is to implement transparency as an optional feature instead of an inherent built-in system property: only if the user allows, may the corresponding access procedure be executed in a transparent way. If not, the system is to provide all the necessary details to the user, which enables him/her to examine all the otherwise hidden details of the transparent access procedure at any time. In order to avoid overloading the user with information, a software agent can be utilized, which is authorized to manage privacy and security settings of an individual acting as a privacy and security guard.

Thereby, transparency as an option is a positive feature of UbiComp but transparency implemented as a design principle without the ability to check the details of background processes on demand is *incompatible* with security and privacy. For this reason, it is worth distinguishing the transparency property for the end user (to enable the desired seamless interaction but always having an opportunity to explore all the details when needed) and transparent access as an

¹For example, unobtrusiveness of devices with respect to their size and operation mode, the ability of the user to concentrate on the specific (business) tasks without having to pay much attention to the management of the underlying technical system, etc.

²In contrast to the definition of transparency as exposing all the details of underlying background processes.

inherent system property (when a user *is not able* to check the necessary details even if he wanted). A possible option could be providing transparency for the end user (to enable comfortable interaction), but ensuring that all the details are exposed to the corresponding user agent (acting as a user proxy).

The problem of self-governance

The problem of self-governance is a side-effect of the desired automation of a UbiComp system, which aims at providing comfort and easiness of use to the end user, i.e. not distracting him/her with technical details of system management and allowing to focus on specific tasks. This can, however, lead to the loss of control over the system and paves the way for the unrecognized hacking of the whole UbiComp system. The fact that devices are ubiquitously networked aggravates the situation because it is not possible to physically isolate parts of the UbiComp system and to hinder the adversary in performing the attack. Moreover, in UbiComp environments it is much harder to provide for physical protection of the system due to their pervasive nature and wide distribution of end devices.

Thus, with respect to UbiComp, the self-governance property is to be considered with particular attention when introducing the transition of computing power to the background. The desired automation property should be implemented in such a way that the stage of ensuring the required privacy and security mechanisms is integrated during the system design stage (in contrast to the run time). This enables the proper privacy and security precautions to be *inherently* built into the UbiComp system's functionality.

2.3.2 Existing approaches to privacy management in UbiComp and their assessment

Privacy management in UbiComp is a challenging task due to the volatility of its environment, context-awareness and therefore context-dependency, and its pervasive nature. The advances of sensing technology and memory amplification enable the development of qualitatively new scenarios of privacy violation in UbiComp. Marc Langheinrich claimed in [Lan01] that "ubiquitous devices will per definition be ideally suited for covert operation and illegal surveillance, no matter how much disclosure protocols are being developed".

Depending on the specific tasks of UbiComp applications, appropriate privacy regulations should be applied in conjunction with the privacy requirements of the user. It is important to consider that solely implementing security does not necessarily imply that privacy is going to be also protected by default (i.e.

is a by-product of security). Privacy issues should be considered in their own right. The authors of [Kru10] give the following example: a high level of security does not at all guarantee privacy in case of the surveillance state¹. Or the other way around: it is possible to have privacy along with moderate security management in case of a private table conversation in a busy restaurant.²

Similarly to technological solutions partially implementing the UbiComp paradigm (see Section 2.2), the solutions for privacy management in this domain are also rather tailor-made.

For example, in [Lan01] it was suggested that privacy is regulated in a declarative way with the aid of an announcement system, e.g. an announcement on entering the building that the talks inside might be recorded: "An office building could collectively declare that audio recording is done in all of its room, even if not all of them actually had sensors equipped" [Lan01]. The author claims that this helps "to form the bottom line for any privacy-aware ubiquitous system" and aims at a coarse-grained privacy regulation.³ This approach, however, has a number of side-effects. Firstly, it is important that it is *explicitly known* whether the recording has taken place or not. The reason for this is that for some situations voice recording is desirable, for others not. Thus, an announcement that within a certain building voice recording takes place can be very misleading. Imagine the situation when after an interesting conversation a request to obtain the respective recording fails because the meeting room where the conversation took place was either not equipped with the respective sensors or the recording of this particular talk was turned off for privacy reasons. This consequently leads to the second side-effect – *an information availability problem*.

Another approach to privacy management in ubiquitous environments was mentioned in [DC05]: the video data from a smart room was made available only to the participants of the meeting using cryptographic techniques. The content was encrypted with a randomly generated secret key (a symmetric cryptography procedure), which was in turn encrypted by the public keys of file owners (participants of the meeting), so that only the persons who had been present at the meeting were able to access the content. By doing so, the authors claim that their scheme embeds access rights in the data and makes them "safe by themselves": "Even if an adversary gains access to the data, he cannot take ad-

¹In the surveillance state the authorities claim that a widespread surveillance is aimed at preventing crime or terrorism and ensuring security of citizens. However, that might lead to a so-called over-surveillance and threaten individual's privacy and civil liberties.

²Of course, it depends on the kind of attacker as well as on his attacking goals. Nevertheless, in general such a case is possible under certain assumptions.

³The concept of a `robots.txt` file on the World Wide Web servers works in a similar way.

vantage of them because they are encrypted and are not different from random data to those who don't have access rights" [DC05].

The authors of [JL02] suggested that in a context-aware UbiComp system, privacy is managed using the abstraction of information spaces which helps to organize information, resources and services around "important relevant contextual factors". Privacy policy settings are reflected in so-called "privacy tags" attached to every data item, which are effectively the privacy metadata. It is then used by the privacy-respecting access control system to ensure that access to data items is granted only to the authorized users. This approach is similar to the "sticky policy" paradigm discussed in [KSW03] where it was used within the Platform for Enterprise Privacy Practices (E-P3P) by an authorization scheme that defines how collected data may be used.

None of the aforementioned approaches, however, explicitly considers the problems of transparent accessibility and self-governance. The reasons may be the following. Firstly, at the current stage of UbiComp systems development ("the first stage" introducing a big variety of different tailor-made solutions, see Section 2.1) the degree to which transparency and self-governance are implemented (if implemented at all) is not large enough to raise major privacy concerns, which arise through other factors, for example, pervasive networking. This consequently leads to the second reason: most of the solutions tackle the problem of privacy management from a single perspective treating the most significant issues relevant to each concrete system (like the problem of tracking due to the pervasive networking environment).

However, with the advances in UbiComp systems engineering (leading to the "second stage" of UbiComp systems development with the features of transparent accessibility and self governance decently implemented) these problems are very likely to have a significant influence on privacy management in the real world systems already in the nearest future.

For UbiComp systems based on RFID, it is already possible to implement the properties of self-governance and transparent accessibility in the supporting back-end system. For example, if an employee possesses an RFID-enabled ID badge, it is possible to track his location within the office building. Suppose some personal things of the employee, which he always carries back home with him, are also equipped with RFID tags (e.g. a wallet). When the employee walks out of the main entrance and heads back home after work, the system can check if any of his personal belongings have been left in the office and if that is the case, inform him of that. In this scenario, the RFID infrastructure is constantly interrogating the RFID-enabled ID badge and the employee's personal belongings by *transparently* accessing the respective RFID devices. Therefore,

it can determine when the employee has left the office building (e.g. is walking out the main entrance) without having taken his belongings from the office. By constantly monitoring the location of the respective RFID tags (attached to the ID badge and personal belongings) and using other relevant contextual information (e.g. time when the employee usually leaves the work), the system is able to *automatically* infer that something has been forgotten and perform the respective actions (e.g. notify the person of that). The procedure of constant interrogation of RFID tags refers to the transparent accessibility property of a UbiComp system. The inference with the subsequent actions (user notification in this scenario) exemplifies the self-governance property. In both cases, the user does not have control over the background processes and should rely on trustworthiness of the RFID infrastructure in protecting his privacy.

For this reason, I consider it important to carefully take the threats imposed by the properties of transparent accessibility and self-governance into account while designing a UbiComp system. Moreover, it should be done already at the system design time. Otherwise, it might be impossible to implement privacy-respecting mechanisms later as an add-on because the user may have a limited access to the background information (or no access at all), which might be critical especially if considering UbiComp systems as "[...] the last step before we begin implanting computational devices into our body or even our consciousness" [Lan01].

2.3.3 The problems of transparent accessibility and self-governance in RFID systems

As it was already mentioned above, the problems of transparent accessibility and self-governance have their implications in RFID systems. Figure 2.2 depicts the parts of a typical RFID system which are directly affected by them. As it can be seen, the problem of transparent accessibility influences both the back-end (the RFID infrastructure) and the front-end (the deployed end devices – RFID tags) of an RFID system. The situation is aggravated by the fact that RFID tags are usually extremely resource-constrained (both in terms of computation and energy) which results in the fact that most of them are not able to perform any security-related operations¹ (e.g. encryption). That means that in many cases the access procedure (a query from an RFID reader) is performed in a transparent way by default.

The problem of self-governance, which is caused by background informa-

¹Recent research has demonstrated the feasibility of implementing cryptographic procedures on an RFID chip, see for instance, [Hut11]. This, however, increases the overall cost of a tag and therefore stimulates the companies to use more simple and cheap tags for their systems.

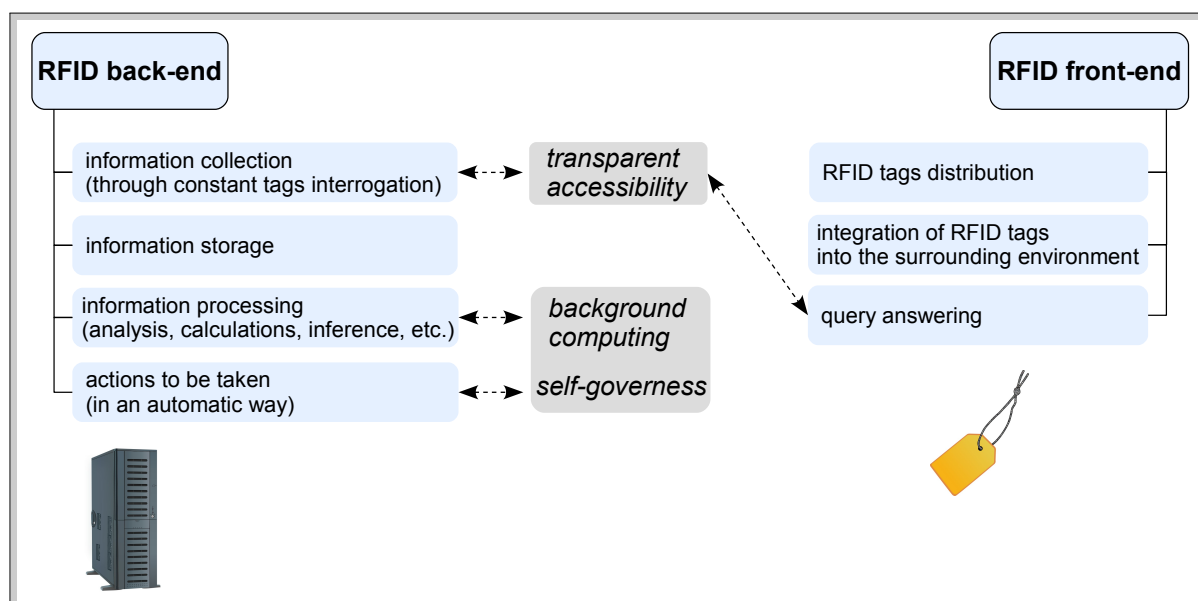


Figure 2.2: The problems of transparent accessibility and self-governance in RFID systems.

tion processing and subsequent actions performed in an automatic way, mainly affects the back-end of an RFID system (the left part of Figure 2.2) where the information collected from RFID tags is stored and processed. The RFID infrastructure can then perform automatic actions based on the result of information analysis. The end user of RFID systems (e.g. the employee owing an RFID-enabled badge or a customer wearing clothes with RFID tags woven into them) has no control over these processes happening in the back-end.

Many privacy experts target their research at the end devices of RFID systems developing mechanisms for protection from clandestine reading, resistance of tags to tracking, etc. (see, for example, [LM07]). Whereas it helps to protect the privacy¹ of RFID tags being the "weakest link" in RFID systems, it does not take into account the processes happening in the underlying RFID infrastructure after the information has already been collected from the end devices. This, however, should be carefully considered by the developers of a privacy-respecting RFID system along with privacy-enhancing technologies for the tags, and that is why the problems of transparent accessibility and self-governance are explicitly discussed here.

As it can be seen, in order to be able to effectively analyze the peculiarities of privacy management in RFID systems, the main structure and underlying technological principles thereof should be additionally considered. For example, in Figure 2.2, the problems of transparent accessibility and self-governance were discussed with respect to different components of RFID systems. That

¹Here, the term "privacy" is used in the broad sense meaning the privacy of the person possessing the RFID tag or to whom it can be linked. Further in the master thesis, the privacy of the devices is treated separately and called the M2M privacy.

requires the knowledge of basic principles of RFID systems, i.e. the main components, their interaction with each other, etc. For this reason, to explore privacy implications of RFID systems in the next chapter, it starts with a concise description of RFID basics.

2.4 Chapter summary

The general notion of UbiComp was discussed in this chapter. It was shown why the RFID technology is regarded as one of its main enablers. Privacy concerns inherent in every UbiComp system were presented and their peculiarities with respect to RFID systems were discussed.

The next chapter considers privacy issues peculiar to the RFID domain, which form the necessary basis for developing the respective privacy management solutions.

3 Privacy implications of RFID systems

This chapter focuses on privacy implications of RFID systems exploring the privacy threats specific to this domain and the ways of mitigating the problems caused by them in order to provide for a privacy-respecting RFID system. Due to the fact that the notion of privacy is vaguely defined and therefore fairly ambiguous, the chapter also discusses the ways of its definition and classification together with the motivation of considering privacy in an interdisciplinary manner.

Since security provides for the necessary basis for implementing and ensuring privacy and is, therefore, an integral part of the underlying mechanisms of privacy management, security peculiarities of RFID are considered as well.

In order to provide for a detailed assessment of privacy issues of RFID systems, the knowledge of their specific structure is required. For this reason, the chapter begins with a brief description of the main components of RFID systems, focusing on capabilities of their end devices – RFID tags, and concisely describes different classes of RFID systems.

3.1 Main components of RFID systems

As it was already partially mentioned before, RFID systems have a special structure comprising of RFID front-end, RFID back-end and the bridging component, which enables the interaction between the front-end and the back-end. End devices of the RFID systems called tags form its front-end. Information is gathered from the tags using the so-called RFID readers, which subsequently forward it to the RFID back-end system. In the back-end, the information processing is performed and the necessary commands are sent to the tags (via the readers). Figure 3.1 depicts the general structure of a typical RFID system.

3.1.1 RFID tags

End devices of RFID systems are called RFID tags. A conventional RFID tag consists of the following components (adapted from [Hen08]):

- antenna;
- microchip;
- encapsulation/packaging;
- a power supply [optional] (in case a tag is active or semi-active, see further).

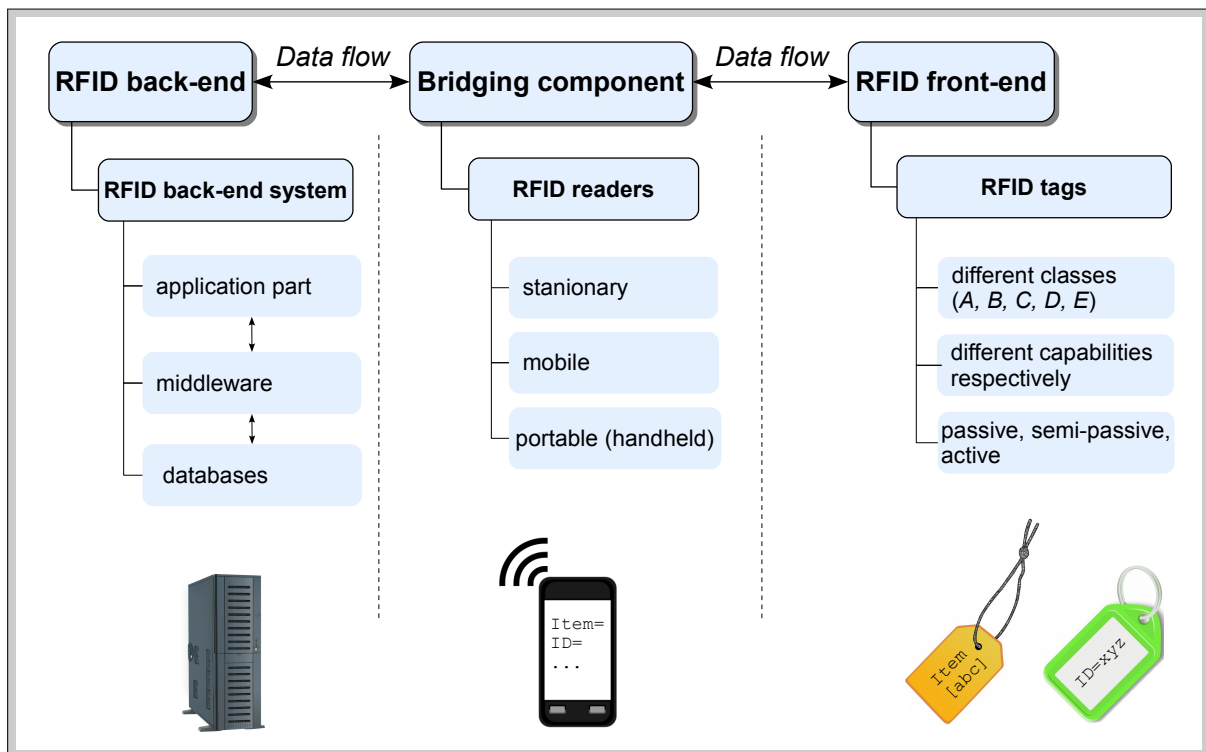


Figure 3.1: The general structure of a typical RFID system.

An example of a simple RFID Tag (with no power supply) is depicted in Figure 3.2.

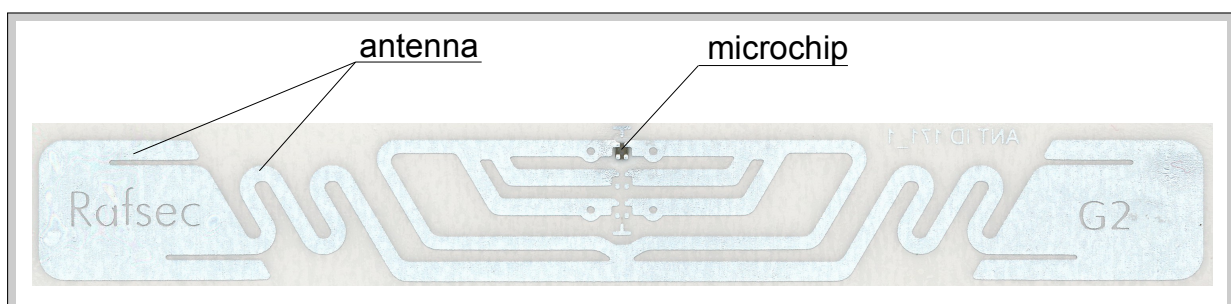


Figure 3.2: An example of a passive RFID Tag.

Depending on the power source, there exist three types of RFID tags: passive, semi-passive and active (see Figure 3.1). An RFID tag is considered to be passive if it has no own power supply (i.e. no battery) and uses the power of a reading device (a reader) to generate the response to it. For example, the tag

depicted in Figure 3.2 is passive. If a tag has an internal power source to supply the circuitry in order to perform its specific functions (e.g. to monitor the environment, etc.) but still uses the power of a reading device to answer a query, it is called semi-passive. An RFID tag is considered to be active¹ if it possesses an internal power source to supply its functions and perform communication with a reading device.

RFID tags can be further divided into 5 classes depending on their functional capabilities (see Table 3.1). The class *A* devices are the simplest and the cheapest ones. They have no memory, contain no unique identifying information and do not possess any built-in power source (i.e. are passive): "They simply announce their presence to a reader [to a reading device]" [Wei08]. This kind of tags has been used for a long time to prevent shoplifting from the stores by attaching the tags to the goods and by this making it possible to monitor them (in the so-called Electronic Article Surveillance (EAS) systems).

The class *B* devices are passive as well and contain certain identifying information that can be written only once during the manufacturing process of a tag. It is theoretically possible to equip them with a battery. However, the cost of it could outweigh the price of the tag itself and therefore would dramatically increase the production expenses.

The tags of class *C* (Electronic Product Code – EPC) are used to uniquely identify and track the object (usually a certain product) and to provide for data logging. These tags possess re-writable memory [Wei08] which enables them to support setting the identifier (e.g. writing some specific information to the tag) by the end user in contrast to performing it at manufacture time. In practice, the class *C* tags are usually passive, which allows to keep the production costs down.

Sensor tags (the class *D* devices) possess relatively profound processing and communication capabilities, and are more expensive due to the built-in power source (they are mainly semi-passive) and sensor functionality.

The class *E* devices ("Motes", or "Smart Dust") are the most advanced of all and are already able to perform peer-to-peer communication, organize themselves in an ad-hoc way and therefore act as conventional sensor nodes. They are necessarily active.

If required, the functionality of RFID tags can be additionally extended by utilizing other technologies. For example, passive RFID tags can be additionally equipped with plain displays, which are based on the electronic paper (ePaper) technology and require power only to change the displayed information, not to hold it [Hen08]. The information residing in the tag can then be read by hu-

¹The price of an active RFID tag is substantially higher than of a passive one, around tens of €.

mans without having to use readers, which is convenient in case the tag, for instance, identifies a certain product and represents its price. Moreover, according to [AP10, Hen07], RFID tags can be used in conjunction with the Global Positioning System (GPS), which further extends tracking capabilities of such a hybrid RFID-based system and makes it ubiquitous in a much wider sense.

Table 3.1: RFID classes. Adapted from [Wei08].

Class	Name	Memory	Power Source	Applications
A	EAS ^a	None	Passive	Article Surveillance
B	Read-only EPC ^b	Read-Only	Passive	Identification Only
C	EPC	Read/Write	Passive	Data Logging
D	Sensor Tags	Read/Write	Semi-Passive	Environmental Sensors
E	Motes	Read/Wite	Active	Ad Hoc Networking

^aElectronic Article Surveillance

^bElectronic Product Code

3.1.2 RFID readers

In order to read the information contained in RFID tags, special reading devices called RFID readers are used. They query the tags in their vicinity and forward the gathered information to the back-end system for further processing. RFID readers are effectively the bridging component between the front-end and the back-end of an RFID system enabling their interaction.

A typical RFID reader consists of the following parts [Hen08]:

- an antenna along with the required electronics for communication;
- a microprocessor for controlling the device;
- an interface for forwarding the data to the processing back-end system.

In case the communicated RFID tags are passive, the readers provide them with power to process the request and send an answer.

As is depicted in Figure 3.1, the readers can be stationary, mobile or portable. An RFID reader is considered to be *stationary* if it is affixed to a certain place and its location does not change (e.g. the readers deployed in a warehouse). A *mobile* reader can be attached to a vehicle or used by an employee when mobility is required, for example in case it is economically unreasonable to cover the whole area of a warehouse with stationary readers. A *portable* reader is in essence very similar to a mobile reader with an exception that it is explicitly produced to be portable (handheld). Its functionality (e.g. the ability of concurrent reading from multiple tags, etc.) may be limited compared to mobile

or stationary readers but in this case it is not the main requirement. Many researchers do not make a distinction between mobile and portable readers due to the subtle difference between the two. The reason why it has been made in the master thesis is that the portable readers represent the advent of small and unobtrusive handheld devices capable of querying RFID tags. That in turn raises concerns over privacy of the users of RFID systems because it paves the way to clandestine reading, which can be performed from virtually any location to where the adversary has access (see [GBPT11]).

The speed of the information flow between the tags and the reader has implications for privacy of the users as well. The faster the speed, the more pieces of information can be obtained from the tags by adversary during a short session (e.g. passing by the victim). The achievable data rate may vary substantially and depends on the RFID standard and operating frequency¹.

3.1.3 RFID back-end

The RFID back-system performs processing of the information obtained from tags by readers. Unlike the RFID-front end, it does not have similar resource constraints. RFID back-end can be divided into several parts (see also Figure 3.1):

- databases;
- middleware;
- application part.

The *databases* are used for storing the aggregated data and data logging.

Middleware is used for aggregation of the queried data, its subsequent filtering, and provides a common interface for the applications [Hen08]. Furthermore, high level applications need not be aware of the exact types of RFID tags, which are currently in operation, because this task is encapsulated in middleware. Therefore, middleware provides for decoupling and flexibility.

The *application part* is responsible for providing specific functionality for the user by, for example, making use of the previously queried and filtered data to enable various user-defined tasks. Processing of information encompassing information analysis, the necessary calculation and subsequent inference, etc. is performed in the applications part as well. Furthermore, depending on the functionality of applications, the necessary commands to the RFID tags can be initiated (e.g. update the price field or even kill the tag).

¹For example, in ISO/IEC 18000-6:2004 the data rate of the forward link (reader → tag) is up to 128kbit/s and the one of the return link can reach 320 kbit/s, see http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=34117. In experimental set ups, however, it was shown that a read capability can be significantly higher, namely up to 4 Mbit/s in [PJDD08].

3.2 Classification of RFID systems

This section discusses different classes of RFID systems, which determine their system-level capabilities that in turn influence privacy management in each particular RFID deployment.

RFID systems are characterized by a number of properties. Among them, the physical principles of communication between a reader and a tag (the physical coupling method) together with the operating frequency are the most important ones. They determine further characteristics of RFID systems such as operating range, robustness, efficiency and costs, etc.

According to the two core parameters mentioned above, the following types of RFID systems can be distinguished [Fin10]:

1. *Close coupled systems.* The communication is carried out with passive transponders (tags) at frequencies between several Hz to 30 MHz through the procedure of inductive or electric coupling [CT01]. It results in a very small operating range (around 1 cm) and requires extremely low power levels to function.

Main applications in this case are the systems with stringent security requirements. For example, electronic door locking systems, contactless payment, etc.

2. *Remote coupled systems.* They are based on inductive coupling [CT01], have an operating range around 1 m and are the most widespread of all. The main operating frequencies are 100 –135 kHz, 6.75 MHz, 13.56 MHz and 27.125 MHz.

Typical applications are the so called "smart labels" used for animal identification, industrial automation, etc. Contactless chipcards fall within this category as well.

3. *Long range systems.* This kind of RFID systems operate utilizing a concept of electromagnetic waves propagation and backscatter effect (see e.g. [GD09] for more information). Typical frequency range is UHF¹ (868 MHz in Europe and 915 MHz in the USA) and the microwave range (2.5 GHz and 5.8 GHz). If a passive transponder is used, a typical operating range is around 3 m. In case of an active one, the achieved operating range can be 15 m or more.

RFID systems working in UHF range can be used for asset tracking. For example, in hospitals they can be utilized for protecting capital equipment, efficient use of crash carts, diagnostic equipment, etc.²

¹The ITU Radio frequency range of electromagnetic waves between 300 MHz and 3 GHz.

²For more details, see <http://www.aliantechnology.com/docs/applications/SBAssetTracking.pdf>.

The aforementioned classes of RFID and their properties are put in Table 3.2.

RFID systems can be additionally classified by the ability to perform data processing at the tag side. According to [Fin10], there are so-called low-end, middle-class and high-end RFID systems (see Table 3.3).

1. *Low-end systems*:
 - a) The simplest case. The reader plainly checks the possible presence of a tag in the interrogation zone, such as in Electronic Article Surveillance (EAS) or other anti-theft systems. The tag transmits a single "presence" bit.
 - b) Read-only tags. A data set is permanently encoded into the tag during the manufacturing time and therefore is immutable. Usually it is a unique serial number, which can be interpreted as a barcode (in barcode systems), a container number (logistics) or a cattle number (animal identification systems).
2. *Middle-class systems*. Information can be remotely written into the tags, which are already capable of processing simple reader commands. Anticollision algorithms are also supported (e.g. slotted ALOHA [Hua06], etc.). Moreover, simple authentication and encryption procedures between a tag and a reader are possible.
3. *High-end systems*. Microprocessors in conjunction with a smart card operating system are used to advance on-tag processing (such as cryptographic and authentication procedures). Most of these systems are operated at 13.56 MHz.

Data management in an RFID system

General capabilities of RFID tags (see Table 3.1) and the ability to perform processing at the tag side (see Table 3.3), determine the possible options of data management in an RFID system. The data associated with an RFID tag can be either stored directly on it or in the back-end database [Hen08]. For example, in case of low-end systems (see Table 3.3), the tag carries an immutable ID which can be associated with a certain object (e.g. a product in logistics). The information which enables this kind of linking is stored in the back-end database. If it is possible to rewrite the information residing in the tag (middle-class and high-end RFID systems), then there is an option of storing certain pieces of information directly on a tag. It can facilitate the implementation of mobile applications, which can query the tag directly without having to send request to

Table 3.2: RFID systems classification based on physical coupling method and operating frequency.

RFID Class	Operating frequency	Communic. principle	Power Supply	Operating range	Data storage capacity	Main applications area
<i>Close coupled</i>	100...135 kHz	inductive or electric coupling	passive	~1 cm	<100 kB, read/write	Systems subject to strict security requirements: Electronic door locking, contactless payment
<i>Remote coupled</i>	100...135 kHz 6.75 MHz 13.56 MHz 27.125 MHz	inductive coupling	passive	~1 m	<100 kB, read/write	The most widespread of all, various applications e.g. supply chain management, logistics, etc.
<i>Long range</i>	868 MHz and 2.5 GHz in Europe; 915 MHz and 5.6 GHz in USA	radio frequency backscatter effect	passive, semi-passive, active	>3 m	high bandwidth, read/write	Toll collection, logistics.

Table 3.3: RFID systems classification based on the ability to perform processing at the tag side.

RFID class	Data processing on the tag	Applications
<i>Low-end</i>	a) none, a "presence bit" transmission b) none, a hard-coded data set	anti-theft systems, EAS; barcode systems, animal identification.
<i>Middle-class</i>	remote write, simple processing incl. authentication and encryption	RFID-enabled passports, access control systems.
<i>High-end</i>	relatively advanced, microprocessors and embedded OS are used	smart cards.

the back-end system to obtain the needed information. Furthermore, the data can be stored in a distributed manner, which in some cases may be preferable (see further).

On the other hand, storing the data associated with the tag in the back-end database simplifies the general process of data management and keeps the costs of data storage and maintenance down. Moreover, the data can be secured more easily by applying mature access control mechanisms, encryption and anonymization techniques (if necessary). Furthermore, it is usually easier to provide for physical security of the back-end database¹ (e.g. physically isolating the server room of a data center, etc.).

However, in some cases storing data on the tag may be preferable. For ex-

¹The advent of cloud computing may render the term "physical security" inapplicable to the data residing in the cloud. In this case, nevertheless, the database administrator is inclined to have mature mechanisms to ensure that data is secured at the logical level (e.g. encryption).

ample, many countries have already begun to issue RFID-enabled passports¹, where privacy-critical information resides. In order to protect sensitive data from clandestine scanning and unauthorized modification, the high-end RFID systems are usually utilized. The initial purpose of such an RFID-enabled passport, as well as the conventional one, is to provide for worldwide available means of person identification. Every time when passport check is performed (e.g. during international border crossings), it would be extremely difficult to query the necessary personal information from a distributed database in a secure and reliable way. Some countries may even have no appropriate equipment for that. Moreover, management of such an international, concurrently operated distributed database might become a serious bottleneck. Thus, in such a case it would be beneficial to store personal data solely on a tag (and to back it up in a special security database of a country, which issued the passport, with strict and well-enforceable access control policies).

3.3 Privacy issues in RFID systems

This section describes the notion of privacy, discusses common delusions about it and focuses on peculiarities of privacy management in RFID systems.

3.3.1 Defining privacy

Defining privacy is a difficult task because for different individuals perception of privacy differs substantially. Privacy is to a large extent a highly subjective issue. That greatly impedes the process of designing generic mechanisms for privacy management and imposes the need to reconsider privacy issues for each specific system. Furthermore, the author of [Hen08] claims that "[...] people's privacy perception is not objective so that the perception of threats for their privacy resulting from the current development is also not objective". That is why it is important to consider the underlying factors that influence privacy perception and hence the respective privacy solutions: "Without understanding of what the privacy problems are, how can privacy be addressed in a meaningful way?" [Sol06].

It is critical to understand *why* there is a desire for privacy as well; how an individual decides that in certain situations a privacy violation has taken place and in others not. Marc Langheinrich claims in [Lan02] that in order to provide for privacy solutions, it is "crucial to understand *when* it is exactly

¹See, for example, http://www.bmi.bund.de/cln_156/DE/Themen/Sicherheit/PaesseAusweise/eReisepass/eReisepass_node.html.

that people feel that their privacy has been violated". From a law perspective, for example, if an individual has previously consented to some actions, which are generally considered as privacy-violating, the subsequent events involving them are going to be treated as privacy non-violating with regard to him/her [Sol06]. The question is, however, what happens if the individual changes his mind afterwards and would like to withdraw his consent and possibly eliminate all the consequences of a committed privacy violation (e.g. delete all copies of private photos published in a social network). Most of the laymen are not aware of how technical devices work and what the possible risks to their privacy are. Moreover, moving along with technology, people simply get used to giving away their data and "usually only the advantages of doing so [giving away a personal data] are communicated to them" [Hen08].

Furthermore, privacy cannot be addressed without considering its tight connection to society, which has a profound influence on privacy perception and determines the need for privacy as such.

The common misunderstanding of privacy is plainly regarding it as "the right to be let alone" [WB90], "an individual's desire for seclusion" [Hen08] or "the right to be forgotten"^{1,2}. The aforementioned characteristics of privacy can be fairly considered as facets of the privacy notion, which provide for its partial description. Privacy, however, is a far more complex issue. One of the common delusions about it is that privacy is quantifiable and therefore the "more" privacy the individual has, the better his identity is protected [GBP11a]. However, privacy does not have a monotonic behavior. The optimum is situated in the vicinity of the "golden middle" because individuals live in society and hence experience the need for social interaction. This implies exchanging of certain pieces of private information between communicating entities. Individuals, without fully realizing it, need *adequate* and *appropriate* privacy. In each situation an individual is constantly performing reasoning about what he/she is willing to disclose to get which kind of service. Managing privacy implies constant processes of negotiation between communicating entities (along with the aforementioned reasoning process) with regard to which personal information is given out in which situation and enforcing that the privacy policy of each entity is being followed.

Moreover, privacy is a context-dependent issue. For example, the information communicated to the boss and to a friend is substantially different (communication partner context, *with whom*). The location of communication partners

¹Internet privacy and the "right to be forgotten":
<http://www.reuters.com/article/2011/03/17/us-eu-internet-privacy-idUSTRE72G48Z20110317>

²EU proposes online right "to be forgotten":
<http://www.telegraph.co.uk/technology/internet/8112702/EU-proposes-online-right-to-be-forgotten.html>

(i.e. location context, *where*) also plays an important role in privacy management: conversations held in the office and in the pub are surely going to have different privacy implications.

In order to take the aforementioned issues into account, the following definition of privacy, elaborated in [BBP11] with an addition of purpose binding, can be adhered to:

Definition 1. *Privacy of an entity is the result of negotiating and enforcing when, how, to what extent, and in which context which data of this entity is disclosed to whom and for which purpose.*

This definition takes into account the communication partner, the context, in which the communication takes place, and the negotiation processes, which are needed to flexibly manage privacy. This is necessary to reason which personal information an individual is willing to disclose to get which kind of service and to solve possible conflicts, which might arise due to the contradiction of privacy goals of different individuals. Moreover, which personal data is disclosed, its granularity¹, and the enforcement of the individual privacy requirements are also considered in Definition 1. Last but not least, the initial purpose for which personal data have been communicated should be preserved. This is called purpose binding and is mentioned in the definition as well. The importance of considering purpose binding is stated in the European Data Protection Directive [Eur95], which allows processing of personal data only for a clearly defined and legitimate purpose. In order to technically enforce this, the authors of [FHO98] developed a privacy-respecting system with the requirement of purpose binding being of the core ones. They additionally claim that "[...] personal data cannot be classified accurately by its sensitivity per se, because the sensitivity of personal data is related to the purpose and context of its use." This further underlines the importance of considering purpose binding in privacy management and stimulates its explicit inclusion in Definition 1.

3.3.2 Privacy facets

Despite much research effort in the privacy field² and hence numerous attempts to describe and define privacy, its perception by individuals is still substantially different. The notion of privacy is therefore considered to be fairly vague, which complicates the development of "proper"³ mechanisms of privacy management.

¹Consider exposing the information about a birth date: one can reveal the sign of the zodiac only (e.g. Sagittarius) or the exact date (e.g. the 15th of December), or provide the year as well (e.g. 15.12.1986).

²A lot of research on privacy and its implications for society and technology is being carried out in various fields of both social and natural sciences.

³It is difficult to define what the "proper" mechanisms of privacy management are because of the vagueness of the privacy notion itself.

I nevertheless believe that the previously discussed Definition 1 to a large extent provides for a disambiguation of the privacy notion and can be the basis for developing privacy management mechanisms. It would be helpful, however, to further classify privacy by introducing the so-called privacy facets, which represent different parts the notion of privacy is comprised of. Since privacy perception is strongly influenced by society (e.g. societal norms, traditions, etc.), it has evolved over time along with society evolution introducing new dimensions of privacy, referred to as privacy facets in the master thesis.

The notions of "the public" and "the private" were already raised in ancient times. For example, Aristotle introduced a distinction between the public sphere of political activity and the private sphere associated with family and domestic life [DeC08]. Much later, in medieval England, the law was issued which forbid peeping or eavesdropping recognizing the concerns over so-called behavioral, or *media privacy* [Lan01]. The right to seclusion while being at home, which is widely known as "my home as my castle" saying, brings in another privacy facet – *territorial privacy*.

Back to 1890, Warren and Brandeis in their essay "The Right to Privacy" [WB90] laid the foundation for a modern concept of privacy (known as control over information about oneself) and highlighted the importance of explicitly considering privacy in the age of technological advance [DeC08]. One of the examples is the evolution of telecommunications, which revolutionized the conventional ways the people communicate to each other and at the same time raised concerns over *communication privacy*¹. Furthermore, the advent of electronic data processing in the digital age raised serious concerns over *information privacy* (see, for example, [MBSK95]), which nowadays has resulted in data protection frameworks around the world.

Availability of numerous location-aware services, such as the ones based on GPS (Global Positioning System), together with mass produced navigation devices raise concerns over illegitimate tracking and profiling therefore violating the *location privacy*. Location data is hence quite sensitive and is subject to careful protection.

Privacy is often referred to as a basic human right [Bea62]. Than introduces another facet of privacy called *bodily privacy* (see, for example, [LA77]), which represents physical inviolability as an inalienable right of an individual in every democratic society. Furthermore, the right of individual to freely decide on personal matters concerning private life, family, etc. without any interference

¹One of the prominent examples of raising the question of communication privacy can be the legal case of *Katz v. United States* in 1967, which considered electronic wiretapping performed by FBI agents without the necessary warrant as violation of privacy "[...] upon which petitioner justifiably relied while using the telephone booth [...]" [Ins67].

from governmental authorities is often referred to as *decisional privacy* [All88].

Evolution of communication technologies together with the advent of qualitatively new solutions for social interaction (e.g. social networking, messaging and video telephony systems, etc.) have defined the need to extend the conventional ways of privacy management in social groups to virtual spaces and therefore raised additional concerns over *interpersonal privacy* (see, for example, [RM09]).

The aforementioned facets of privacy complement Definition 1 and are depicted in Figure 3.3.

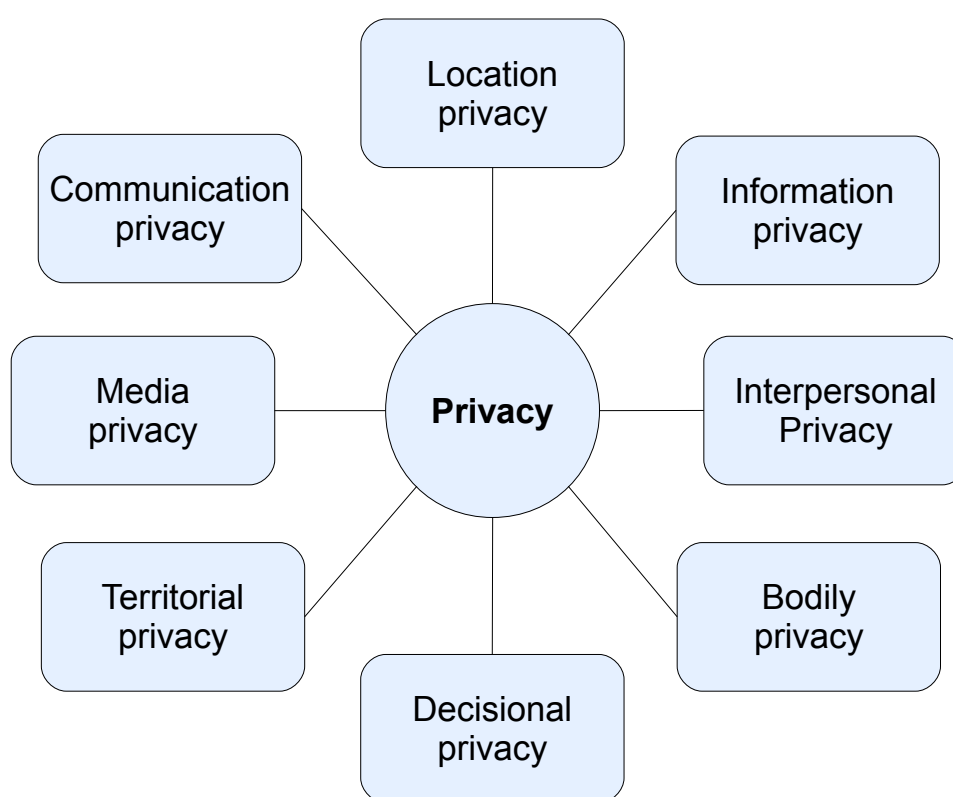


Figure 3.3: Privacy facets.

3.3.3 Peculiarities of privacy management in RFID systems

Generic privacy concerns of UbiComp have their implications in RFID systems as discussed in Section 2.3. Although the problems of transparent accessibility and self-governance are important to consider during the development of RFID systems (see Figure 2.2), there is a number of other issues peculiar to this domain affecting privacy of the users as well. They are discussed below.

Privacy implications through a subtle use of an RFID system

The factors which determine RFID as one of the main enablers of UbiComp may have a negative side-effect on privacy of the users. Mass production, low prices and unobtrusiveness of RFID tags make it possible to integrate them into almost every artefact, which is required to possess a certain degree of intelligence. That demonstrates the solid potential of RFID systems to extensively penetrate our daily lives. What raises privacy concerns in this case is that individuals might be unconsciously involved in the use of an RFID system being unaware of the fact that they are "passive" users, i.e. are using a system *in a subtle way*.

The possible scenario which exemplifies the aforementioned problem is represented by integration of RFID tags into clothes^{1,2}. For logistic purposes and returns tracking, tags can be sewn into garments during the manufacturing process and remain in operation even *once the item has been sold*. Thus, the customers, who have never given their explicit consent to have their garments equipped with RFID tags woven into material, happen to *passively use* the RFID system. In the worst case scenario, it might happen that all the clothes of the individual are equipped with RFID tags and are hence enabled for remote tracking. That paves the way to illegal profiling and consequently introduces a clear case of privacy violation.

That is why in [Web10], it was mentioned that the EU Commission is going to seriously consider the "right to silence of the chips [RFID tags]". That should guarantee that individuals³ are provided with an opportunity of either to leave the tags which were integrated into the artefacts (e.g garments or other goods) in operating mode or to have them deactivated at any time since the purchase has been made.

In order to avoid the case of individuals unconsciously using an RFID system and therefore paving the way to violation of their own privacy, the affected users should be properly informed of the fact that the clothes they buy, for example, is going to stay RFID-enabled after the purchase. Only if explicit consent to this is obtained, can the respective RFID tags be left in operating mode after the purchase has been made.

¹"Benetton to Tag 15 Million Items": <http://www.rfidjournal.com/article/view/344>

²"Privacy concerns hinder RFID rollout": <http://www.itnews.com.au/News/11417,privacy-concerns-hinder-rfid-rollout.aspx>

³It is especially important that the individuals who happen to use the system in a subtle way, i.e. "passive" users, are properly informed and given the choice of whether to continue using the RFID system or have the respective tags deactivated.

The disability to opt-out

Having consented to leave the RFID-enabled garments in operating mode after the purchase, the customer should have an opportunity to *withdraw* his consent at any time and have the respective tags deactivated. It might be the case, however, that it is either technologically not foreseen to provide for a standard procedure of tags deactivation or it is likely to cause much inconvenience for the customer (e.g. bringing a big amount of RFID-items to a service point to have them deactivated) and hence hinder him in doing so. This exemplifies the problem when a user can not easily refuse to use an RFID system, which is more formally called "the disability to opt-out" in [GBP11a]. The problem is aggravated by the fact that RFID technology is widely penetrating our everyday lives and the number of RFID-enabled artefacts is constantly growing¹. Furthermore, according to [Hen08], if opt-out is nevertheless made possible, the following problems might arise:

- much inconvenience caused by opt-out (e.g. postal mail of a check instead of a credit card payment);
- opt-out can look suspicious (a denial to give away certain data in particular situations may look suspicious, e.g. switching the location sensor off during the time when a crime was committed, etc.)

Furthermore, Weber in [Web10] underlines the importance of generally providing the individuals with the opportunity "to disconnect from their networked environment at any time". Therefore, one of the key requirements which should be considered during the development of a privacy-respecting RFID system is to provide for the support of opt-in/opt-out according to the users' preferences hence carefully taking their explicit consent into account.

Pervasive availability of PII

In an RFID system, personally identifiable information (PII) may reside not only in the back-end but in the end devices as well. In the latter case, PII can be either directly stored on a tag (an RFID-enabled ID card) or be associated with an individual (the purchased item with an RFID tag woven into it together with the customer's name: a tuple [tag ID, person name]). Given the wide distribution and ubiquity of RFID tags, the number of PII exposure scenarios raises dramatically. This problem is called "pervasive availability of PII" within this master thesis. There are several major factors that comprise this problem:

¹Consider an example of affixing RFID tags to bank notes, ID cards, electronic locking systems or almost every item, which can be purchased in a store.

- the ability to perform clandestine reading of RFID tags in a ubiquitous way utilizing handheld devices, e.g. portable readers;
- the possibility of making the queried PII worldwide available through the Internet (e.g. connecting the reader to the Internet gateway);
- physical layer identification of RFID tags with subsequent profiling (bypassing the privacy-preserving mechanisms of higher layers, e.g. access control, pseudonyms, etc.).

In order to query a conventional RFID tag, it is not necessary to possess a standard reader device. It was reported in [ZSC11] that it is possible to initiate communication with a tag using low cost, self-configured USRP¹ device attached to a general purpose computer. Therefore, an adversary is provided with the customizable means of illegitimate scanning of RFID tags in his vicinity. Moreover, the advent of highly portable reading devices (see, for example, [K⁺07b]) is going to aggravate this problem. As a consequence, PII can be easily disseminated not only to the established infrastructure (where control of privacy policies can be ensured) but also to numerous unobtrusive handheld devices, even in a clandestine way. If they are further equipped with the function of transforming the RFID-specific data (obtained from the query) into an IP-compatible format (i.e. acting as a gateway) and have access to the Internet, then the queried PII can be made worldwide available without necessarily allowing the affected individuals to have any control over this, or not even informing them of such data dissemination.

There is a number of mechanisms available to mitigate the problem, for example using lightweight implementations of data encryption and reader authentication. However, it might not be enough. The authors of [ZSC11] raise concerns over the possibility of the physical-layer identification of RFID tags, which can bypass the privacy-preserving mechanisms carried out at the higher layers of the OSI² model, such as access control, pseudonyms, encryption, etc. That paves the way to clandestine scanning with subsequent identification of RFID tags, which enables the illegal profiling of the users utilizing the RFID-enabled artefacts.

Whereas it is possible to utilize such privacy-preserving solutions as physical destruction of a tag, Faraday cages³, active jammers or "clipped" tags⁴, they are not always applicable, for example in case RFID tags are woven into clothes.

¹Universal Software Radio Peripheral

²Open Systems Interconnection [DZ83]

³Protecting an RFID tag by enclosing it in a conducting material and thereby preventing it from external communication via electromagnetic field.

⁴"Clipped" tags allow for a removal of an RFID antenna in a user-controlled and reversible way. See [KM05] for more details.

In [ZSC11], it was demonstrated how RFID tags can be identified by their physical layer fingerprint that renders the privacy-preserving techniques of higher layers ineffective. The fact that users might possess several RFID-enabled artefacts aggravates the situation and makes such a low-level profiling more accurate. The problem is likely to become especially serious for privacy-critical applications, such as RFID-enabled passports, which rely on encryption and access control procedures. Moreover, in contrast to, for example, video surveillance systems, where recorded information should be firstly analyzed to perform any reasoning about the tracked individuals, RFID profiling can be carried out in an automatized way without the need for subsequent data processing [ZK09].

Physical layer identification still remains an open issue and should be specifically addressed and carefully considered during the design of a privacy-respecting RFID system.

Confidentiality of intimate communications and context-awareness

The above mentioned problem of the pervasive availability of PII may endanger the confidentiality of intimate communications by raising the likelihood of their public exposure. In [Hen08], this problem is referred to as "the loss of ephemeral communication". Similarly, Schneider states: "The moral is clear: If you type it and send it, prepare to explain it in public later"¹. Moreover, taking into account that privacy is context dependent (see Definition 1) and the inherent context-awareness of UbiComp systems² in general, including the ones based on RFID, additional concerns over contextual integrity arise. The latter was described in [BPPB11] as "falsifying the context in which information has been communicated" by "putting it into a wrong context"³. Therefore, despite the fact that the problems of confidentiality of intimate communications and contextual integrity are not peculiar to RFID systems, they have their own specifics in RFID environments, which in turn influences privacy management in such systems.

Moreover, privacy management mechanisms of every UbiComp system should be able to dynamically react to context changes and adapt themselves accordingly. That in turn raises the question of understanding context and its

¹Bruce Schneider, "Casual Conversation, R.I.P", http://www.forbes.com/2006/10/18/nsa-im-foley-tech-security-cx_bs_1018security.html.

²See the core properties of UbiComp systems, Section 2.1.

³Consider an example of a debating club when one of its members is asked to state arguments in favour of a rather controversial historic event (e.g. the construction of the Berlin Wall). If his speech is put into another context later on (e.g. shown on TV) *without specifying the original context*, the speaker's reputation might be dramatically spoiled, i.e. the "decontextualization of communicated information" has turned "innocuous" information into the "mortifying" one [BPPB11].

implications for individual privacy in ubiquitous RFID systems.

The following paragraphs elaborate on this issue considering the notion of context with regard to UbiComp, which therefore pertains to RFID systems as well.

Structuring and classifying context

Context could be described using so-called context facets, or dimensions of context, alongside with a layering concept (see Figure 3.4). The basic constituents of context are situated at the lower layers. They represent a subtle but important part of the context notion without which the utilization of the upper layers is doubtful, if not impossible. This approach is similar to Maslow's hierarchy of needs which sets up a hierarchy of five levels of basic human needs: "In the levels of the five basic needs, the person does not feel the second need until the demands of the first have been satisfied, nor the third until the second has been satisfied, and so on" [DBID87]. This idea could be used for structuring and prioritization of various context constituents. As it can be seen in Figure 3.4, at the lowest layer resides a computing context, such as computing resources, battery life, etc. It determines the operation of the contexts at upper layers and is a precondition for the existence of a UbiComp system as such. The second basic layer is a physical context that encompasses such factors as lighting, noise level, temperature, etc. At this layer, proper environmental conditions for both end devices and human beings using them are considered.

The upper layer (namely, the third one in Figure 3.4) consists of many facets, which represent the types of context which are conventionally used. For example, the ones mentioned in [Kru10]: identity (who), location (where), activity (what), etc.

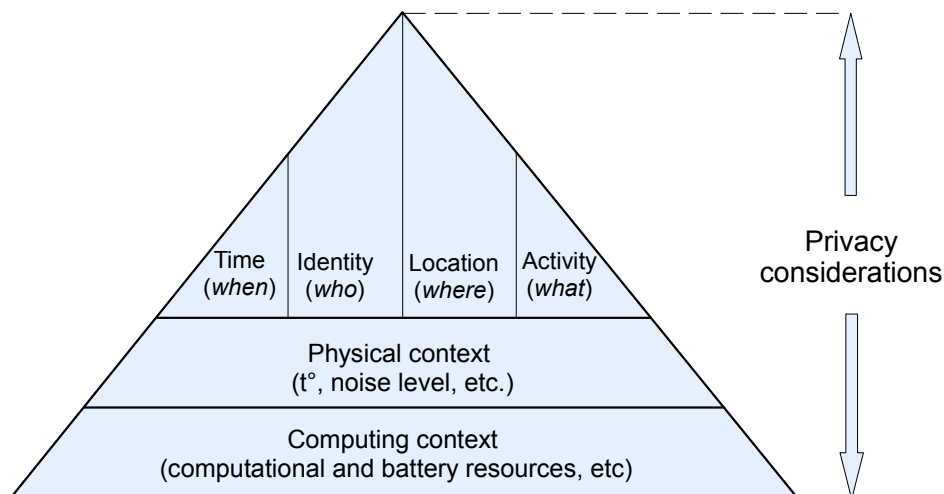


Figure 3.4: Context classification layering scheme with facets.

In recent years, context itself has become a target of data collection and hence a subject to protection, which is especially critical in context-aware Ubi-Comp systems. This affects the PII of the users of UbiComp systems and is aggravated by the implications of mosaic theory of data protection suggesting that the data which by themselves reveal no information about the individual can do so if combined with other data [Poz05]. For example, the pieces of information about the noise level, temperature, time and location gathered by ubiquitous sensors, may be used for illegal profiling if combined. That is why, in order to protect individual privacy in such environment, privacy issues are considered in a cross-layered approach in Figure 3.4.

Context pyramid in different context-aware scenarios

This classification can be applied to real-world scenarios of context-aware applications, such as smart house, location-based service delivery and privacy respecting IoT¹ services.

As an example of a smart house environment, The Georgia Tech Aware Home can be used [KPJ⁺08]. The authors developed a context-aware system which supports several scenarios for families or individuals living at home, namely assisted living for elderly people, applications for busy families, and facilities for children with special needs. In order to provide for this, the means of capturing and interpreting human activity in physical environment are needed, which were developed leveraging various technologies, such as RFID and sensor networks (specified objects tracking), power line positioning (indoor localization), video capturing (activity characterization), etc. According to the context classification described in the previous paragraph, various facets of context can be recognized cross-cutting the tree layers (see Table 3.4). At the first layer, networking context is explicitly used to locally interconnect the artefacts and to enable event notification to external services (e.g. to call an emergency). At the second layer, the lighting context is represented by the respective event detection (sensing if the light is turned on or off). Although not explicitly mentioned, the other facets of physical context are utilized as well, for example through temperature and noise sensing (temperature and noise level facets respectively). The main goal of the Georgia Tech Aware Home system is ensuring well being of a person at home. That is achieved through activity sensing (the activity facet) of a supervised person (the identity facet) together with the information on his/her position in the house (the location facet) combined with timing (the time facet). Therefore, the context facets of the uppermost level of our context classification are fully covered.

¹The Internet of Things, see [AIM10].

Table 3.4: Context pyramid used in different context-aware scenarios

		The Georgia Smart Home	The GUIDE Project (location-based)	RFID Ecosystem	
Contexts directly in use	THIRD LAYER	<i>Time</i>	✓	✓	✓
		<i>Identity</i>	✓		✓
		<i>Location</i>	✓	✓	✓
		<i>Activity</i>	✓	✓	✓
	SECOND LAYER (Physical context)	<i>Lighting</i>	✓		
		<i>Noise level</i>	✓		
		<i>Temperature</i>	✓		
	FIRST LAYER (Computing context)	<i>Battery Life</i>		✓	
		<i>Networking</i>	✓	✓	✓

Another context-aware application can be represented by a Context-aware Tourist Guide, which provides for location-based service delivery [CDMF00]. The system was developed in order to provide tourists with a customizable context-aware electronic guide, which displays the list of attractions in their vicinity based on location information and taking into account user's preferences (e.g. which types of tourist attractions are preferable), time of the day in conjunction with the sights' opening hours, etc. The guide was installed on a tablet PC equipped with a wireless 802.11 module. Therefore, the first-layer networking and battery life contexts were important for such a system (see Table 3.4). To the contrary, context facets of the second layer (lighting, noise level and temperature) were irrelevant for this application. At the uppermost layer, the location facet was used in order to provide tourists with information about the attractions in their vicinity. Similarly, to flexibly inform users about the opening hours of nearby attractions with respect to time of the day, the time facet of context was considered. The users' preferences are taken into account utilizing the activity facet. The system does not need any information about the user identity to operate. Therefore, the identity facet of context is not explicitly considered.

Lastly, context-aware and privacy-respecting IoT services are described in [WBC⁺09], where a so-called RFID Ecosystem was developed. Within this system, the users can have RFID tags embedded into their badges or attached to personal objects. The RFID readers deployed throughout the building can then interrogate the tags and report the respective data to the central server. Privacy was ensured in the back-end through enforcing access-control policies¹.

¹A rather superficial approach to privacy management in RFID environments since the front-end was not considered at all together with a number of specific privacy threats. In this example, however, the focus is shifted to the context-awareness of RFID Ecosystem and its relation to our context classification.

RFID Ecosystem enables to develop several Web-based applications in order to offer various IoT services, for example a search engine for things letting users view the last recorded location of their tagged objects or search for a particular object's location. The more profound applications provide for creation of a user profile, e.g. users' trends in their activities – a Digital Diary application. In this system, similarly to the Georgia Smart Home, the network facet of context was considered at the lowest layer. However, the whole second layer was irrelevant to RFID Ecosystem. In contrast, the facets of the third layer were extensively used since time, identity, location and activity were directly considered in, for example, a Digital Diary application.

Table 3.4 summarizes the context classification for the three above mentioned scenarios.

Private and shared context

The notion of context in computer science was adopted from human-to-human interaction processes. They implicitly use context in a shared way, which provides for an increase of conversational bandwidth. This type of context can be called a "shared context" with a notion of a "private one" being complementary to it (see Figure 3.5). Therefore, in addition to the aforementioned context pyramid, a further division to private and shared contexts can be made. This differentiation is *objective* dependent, which means that the same context can appear as private or shared depending on the situation. The objective in this case is individual privacy management, i.e. privacy goals determine if a certain context in each particular situation is private or shared and, as a consequence, whether it should be exposed to the others or not. As a consequence, privacy management mechanisms in a UbiComp system should additionally consider a process of transition from a private context to a shared one (and vice versa) and be able to react accordingly in response to such context changes.

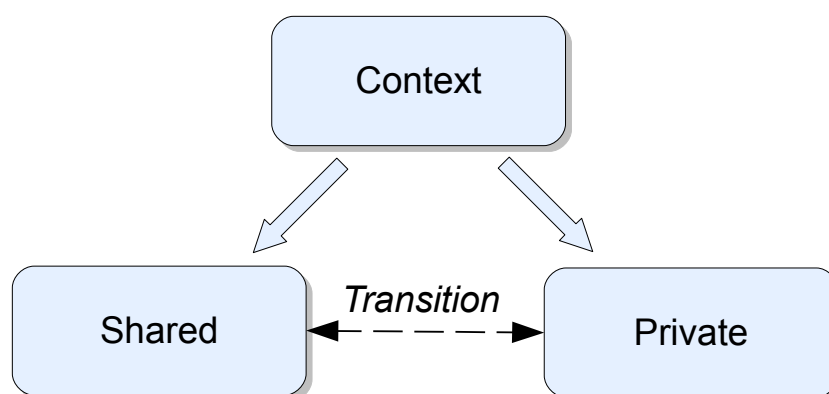


Figure 3.5: Private and shared context.

Using context classification for privacy management

The aforementioned classification may be utilized for dynamic context-based privacy management in UbiComp systems. For example, a context sensing subsystem (or middleware) can provide for continuous context updates, which may be used by a special context-reasoning entity (e.g. a software agent) to dynamically manage individual privacy. Context monitoring can be carried out, for example, via a publish/subscribe scheme as described in [EPS10]. In this case, a context-reasoning entity can subscribe only to those contexts (or/and context facets, see Figure 3.4) which are relevant for each particular application of a UbiComp system (as it is depicted in Table 3.4, for example).

M2M privacy concerns

The technological evolution enables not only properly equipped humans to communicate with end devices of an RFID system (i.e. query tags) but also smart artefacts themselves to initiate direct communication with each other without human intervention. The latter is called machine-to-machine (M2M) communication [WTJ⁺11a]. Despite a solid potential of bringing in new services and consequently enhancing the quality of life, M2M communication raises privacy concerns. With the advent of M2M, intelligence-enabled artefacts in many cases can be directly associated with their owners or even with other individuals in their vicinity [GBPT11], which may lead to the scenario of "things having identities and virtual personalities [...]" [AIM10]. This results into such artefacts possessing their own privacy derived from that of an individual, which in [GBPT11] is referred to as M2M privacy. However, current EU Directives only consider natural persons as objects of privacy laws hence not taking M2M privacy issues into account [Eur02]. Given the ubiquitous presence of RFID-enabled artefacts, it is important to recognize that M2M privacy may influence the privacy of humans and therefore to take this issue into consideration while developing an RFID system.

RFID tags and their influence on privacy

End devices, which are fairly considered to be the "weakest link" of an RFID system due to their constrained computational and energy resources as well as the pervasive physical presence¹, to a large extent determine the peculiar threats to privacy of the users utilizing such systems. Tags' influence on privacy management in RFID environment is determined by several major factors:

¹It is extremely difficult to ensure physical integrity of RFID tags (as well as the integrity of the on-tag data) and to prevent the adversary from having physical access to the tags in case of their pervasive distribution. For example, RFID tags attached to artefacts like clothes, equipment, etc.

1. privacy implications of the different types of RFID tags according to their functional capabilities;
2. physical principles of RFID tags operation;
3. tag-side security issues.

1. Firstly, different classes of RFID tags possess different functional capabilities (see Section 3.1.1, Table 3.1), which directly influence the ability to implement privacy preserving mechanisms¹ on a tag. The requirements of direct functionality of an RFID system determine the "lower-bound" of the capabilities the RFID devices should have, e.g. an operation range, amount of memory required (if any), size, reliability, etc. Privacy and security concerns impose further constraints on end devices and therefore introduce new requirements for the capability range of RFID tags. Consider the following examples.

Example 3.1.

If an RFID system is intended for a proprietary use in a closed environment, such as an assembly line or other industrial applications, it could be sufficient that only requirements of direct functionality are implemented. Security and privacy concerns can be carried out by auxiliary systems (environment shielding, video surveillance, strict access control, etc.) because the environment in which the system operates is closed and only a limited number of authorized persons have access to it. In this case, relatively simple RFID devices can be chosen, e.g. plainly storing the ID number of the component at the assembly line and communicating this information to *any* reader in its vicinity upon request without carrying out an authentication procedure.

Example 3.2.

In case of a public use of an RFID system, the question of privacy and security should be very carefully considered. The reason for that is that the number of potential attackers is virtually unlimited, the environment where the system operates is open and no strict access control to the end devices is possible. An example of such a system can be a contactless ticketing system for public transport. Thus, despite the fact that relatively simple devices can be used to provide for direct functionality of the system (as in the previous example), the more profound ones should be utilized in order to provide for authentication and encryption (e.g. middle-class or high-end devices, see Table 3.3).

¹For example, authentication, encryption, etc.

2. Furthermore, physical principles of RFID tags operation have their own privacy implications in RFID systems as they determine the ability to (permanently) deactivate the tag, reactivate it later on (e.g. after the purchase of an RFID-enabled artefact), etc. For example, the main operating principle of the tags used in electromagnetic RFID systems¹ is based on the reversible process of magnetic hysteresis [Fin10]. This allows for *reactivating* the previously deactivated RFID tags at any time by demagnetizing their magnetic strips, which paves the way to violation of consumers' privacy through the subtle use of an RFID system (see Section 3.3.3). Therefore, while developing a privacy-respecting RFID system, it is advisable to adhere to the RFID technology utilizing the tags which can be physically deactivated in a permanent way.

3. Last but not least, security issues of the RFID front-end play an important role in implementing privacy-preserving mechanisms in such systems. There is a number of specific attacks targeted at RFID tags, which directly endanger privacy, namely tag spoofing and cloning, manipulating the data stored on a tag as well as the attacks to obtain the cypher keys used for encryption, authorization, etc. (side-channels attacks, fault analysis, and reverse engineering). The security-related issues in the RFID domain are covered in more detail in Section 3.5.

A short summary

Table 3.5 summarizes the list of privacy peculiarities of RFID systems. Privacy issues discussed above substantially influence the process of privacy management in RFID systems. In order to effectively protect privacy, it is not enough to solely realize the specific privacy threats peculiar to RFID and develop the respective privacy requirements. It is of paramount importance that the proper mechanisms of privacy enforcement are available as well. Therefore, the next section discusses this issue with regard to RFID systems.

¹Such systems are usually used in anti-theft applications and are fairly simple, i.e. a tag simply announces its presence to a reading device. However, even in this case the location privacy of customers can be endangered.

Table 3.5: Privacy issues peculiar to RFID systems.

RFID privacy concerns	Description	Ways of mitigation
<i>Subtle use of an RFID system</i>	Users are unconsciously involved in the use of an RFID system without being informed about it.	Enforcement of “the right to silence to chips”.
<i>The disability to opt-out</i>	A hindrance to refusing to use an RFID system.	Explicit support of opt-in/opt-out decisions according to the user’s preferences.
<i>Pervasive availability of PII</i>	Dramatic increase in the number of PII exposure scenarios due to the wide distribution and ubiquity of RFID tags: (a) clandestine reading using handheld readers; (b) worldwide availability through the Internet; (c) physical layer identification with subsequent profiling.	Lightweight implementations of encryption and authentication, tags shielding.
<i>Confidentiality of intimate communications and context awareness</i>	Raising likelihood of intimate communications exposure; implications of contextual integrity.	Encrypting privacy-critical data; context-binding; context-aware privacy management through context-sensing middleware.
<i>M2M privacy concerns</i>	M2M privacy and its implications for privacy of individuals in RFID environments.	Recognizing M2M privacy in legislation; utilization of lightweight implementations of privacy-preserving mechanisms in M2M communication (e.g. encryption, authentication, etc.).
<i>Influence of RFID tags on privacy</i>	RFID tags being “the weakest link” in RFID systems introduce additional privacy concerns: (a) privacy implications of the different types of RFID tags according to their functional capabilities; (b) physical principles of RFID tags operation; (c) tag-side security issues.	Carefully choosing the class of RFID tags before system deployment; adhering to the RFID technology utilizing the tags which can be physically deactivated in a permanent way; carefully considering specific attacks at RFID tags and the respective security countermeasures.

3.4 Privacy enforcement

Privacy enforcement is an important procedure which ensures that the defined and deployed privacy policy is being adhered to. Quite often privacy policies are defined in a declarative way without considering underlying solutions to enforce them. For example, the Platform for Privacy Preferences (P3P)¹ is a well-known and widely used protocol that allows websites to declare their privacy policies, i.e. processing the users data, intended use, etc. However, no mechanism for enforcing the declared privacy policies was specifically considered. To the best of my knowledge, neither websites nor users are under obligation of using P3P. That makes P3P more an optional feature than a default setting, which contradicts with the principles of Privacy by Design, see [Cav09, Sha09] and hence only partially covers the privacy management problem.

Therefore, privacy enforcement is an important part of any privacy management solution. The process of developing, deploying and enforcing privacy policies described in [APS02] can be used for RFID systems as well². Figure 3.6 summarizes the idea and shows the place of privacy enforcement in the process of privacy management. According to this approach, within the first two steps a privacy policy is created and deployed respectively. Having performed this, at the third step it is further ensured that end users' consent to the deployed privacy policy is registered on submitting their privacy sensitive data to the system. That can be a part of the "Sticky-policy Paradigm" [APS02], which associates the customer-consented policies with their data containing PII. Important is that the data is linked to the privacy policy being actual at the time of their submission and should be managed accordingly even in case of further policy updates. Only if explicit user consent to processing personal data according to a new privacy policy is obtained, can the "sticky policy" be updated. The control module 5 makes sure that this condition is satisfied (e.g. keeps track of time stamps of "sticky policies" and their updates).

The enforcement of the privacy policy is carried out at the forth step. This implies various technical and non-technical measures of ensuring the deployed privacy policy is adhered to. An audit trail of access to data containing PII can be further performed. This will provide for accountability and can be used by the module of control (step 5) to perform constant checks that data access procedures conform to the deployed privacy policy.

¹Platform for Privacy Preferences (P3P Project). Enabling smarter Privacy Tools for the Web, <http://www.w3.org/P3P/>

²The approach presented in [APS02] can be adopted for privacy management in RFID systems provided that privacy enforcement mechanisms are considered both in the RFID back-end as well as in the front-end.

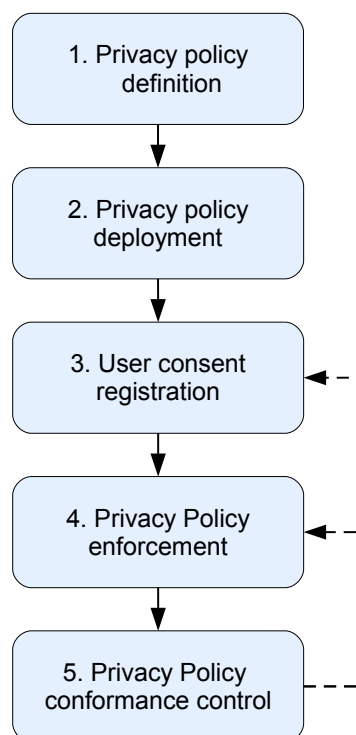


Figure 3.6: Privacy management process. Based on the structure presented in [APS02].

3.4.1 Privacy enforcement mechanisms

As it was mentioned above, privacy enforcement implies the combination of technical and non-technical measures, represented by the step 4 in Figure 3.6. The latter is mainly comprised of the means of legal privacy enforcement. Depending on each specific case, other constituents may be added, for example, the social mechanisms of privacy enforcement¹.

The next paragraphs cover the issues of technical and legal privacy enforcement with regard to RFID systems in more detail.

Technical privacy enforcement

Technical measures of privacy enforcement should be an integral part of any privacy-respecting RFID system because of their direct influence on privacy protection (as opposed to legal enforcement and regulatory approaches). They include implementation of privacy guards, software agents, etc., which utilize various privacy preserving techniques such as:

¹Social privacy enforcement is to a large extent based on social ethics and interpersonal relations. For example, if a certain piece of private information is publicly disclosed by a close friend of an individual without consent of the former, friendship may be broken. Therefore, friendship in this case enforces that private information stays confidential being known only to the certain persons.

- *Anonymization.* This technique is targeted at providing anonymity and can be used against data linking and profiling¹. For example in [CKK07], a scheme was described which allows an RFID tag to answer with a different ID to each new request of the reader. It is based on the randomization procedure² implemented in a special circuit within the tag. A legitimate reader is connected to a system database where the possible combinations of IDs for each particular tag are stored. This enables to identify the tag for legitimate parties and should prevent an attacker from doing so.
- *Encryption.* In order to provide for protection of the tag data containing PII, lightweight implementation of encryption can be utilized (see, for instance, [FWR05]). In [HFW11, HJS11], it was shown that AES³ and ECC⁴ are already feasible for RFID and it is just a matter of costs whether to implement cryptographic algorithms in RFID tags. Moreover, there exists a set of lightweight cryptographic algorithms specifically designed for the domain of resource-constrained devices, such as PRESENT, HIGHT, TEA, etc. (see [EK07] for more details).
- *Hash functions.* This technique may be used, for example, to ensure that an RFID tag offers its functionality only to a legitimate reader, which possesses a special unlock key (see [WSRE03] for more details).
- *Tamper-resistant modules.* Tamper resistance can be used to protect critical data, which should reside in protected memory areas of a tag (e.g. encryption and authentication keys, etc.).
- *Disabling a tag.* A very straightforward but effective approach: physically shielding a tag when not in use (e.g. Faraday cage), temporarily disconnecting RFID antenna (by using, for instance, the "clipped" tags principle described in [KM05]) or plainly killing a tag by permanently destroying its antenna.

The authors of [Hen08] claimed that implementing technical safeguards in practise is a non-trivial task for the following reasons:

- individual privacy requirements are highly subjective, elusive and difficult to specify;
- existence of conflicting goals of different parties involved (e.g. citizens/consumers against companies/governments);

¹It is important to consider anonymity in a cross-layered fashion. Otherwise, it can be compromised by, for example, utilization of physical layer identification discussed Section 3.3.3

²Randomization is performed using an internal pseudo random generator and used to update the tag's ID.

³Advanced Encryption Standard [NIS01].

⁴Elliptic Curve Cryptography [Kob87].

- implementing safeguards increases overall costs, which might deter their integration into the design process of RFID systems.

Taking into account the specific structure of RFID systems, privacy enforcement should be implemented both in the back-end and in the front-end. Whereas in the first case this can be done using well-known and standardized techniques, such as full-fledged access control mechanisms, mature encryption, etc., it may introduce a serious bottleneck in the front-end part of a systems due to the limited resources and pervasive distribution of end devices. Inherent privacy concerns in the RFID domain (mainly pertaining to the tags) summarized in Table 3.5 determine specific issues which need to be covered to enforce privacy. To a large extent, this can be done by the technical means of privacy enforcement targeted specifically at the RFID domain and discussed above.

Legal privacy enforcement

Technology alone will not be able to provide for full-fledged privacy protection mechanisms. Additionally, legal issues should be considered [GBPT11]. Legal privacy enforcement encompasses a spectrum of legal regulation activities, e.g. privacy laws, acts, etc. It is a powerful measure to tackle privacy management problems from a legislative perspective, which has, however, a number of connotations:

1. *Violator detection.* Legislative restrictions are effective when a violator can be detected and brought to justice accordingly. In IT systems, it is often extremely difficult to spot an attacker acting in violation of privacy laws. The situation is especially critical in RFID systems, where wide distribution and quantity of end devices pose an additional challenge to the legal enforcement of privacy.
2. *International interoperability.* There can be substantial differences in privacy legislation across countries. For example, the EU legal frameworks use a cross-sector approach¹ to privacy legislation [Eur95]. Canada and Australia adhere to the similar principle [APS02]. In contrast, privacy legislation in the US has a rather sectoral approach with separate regulations for the finance sector, health care, etc. [Lan05, APS02]. Moreover, legal enforcement of privacy rights in countries of the Third World is in question as such. That introduces the problem of international interoperability concerning legal privacy regulation between different countries².

¹Cross-sector approach to privacy management implies considering privacy across several industrial domains, e.g. health care, finance, etc. It is arguably regarded to be more comprehensive than the sectorial one, which enacts separate regulations for different sectors [APS02].

²For example, protection of PII residing in a biometric RFID-enabled passport crossing several borders.

3. *The outsourcing problem.* The problem of international interoperability of privacy legislation fosters a favourable environment for further cases of law bypassing. For example, processing of PII in third countries without specific privacy regulation laws, which is referred to as the outsourcing problem within this master thesis.
4. *Inherent inflexibility.* Privacy laws are fairly inflexible¹ in certain cases [GBP11a]. Firstly, it is extremely difficult to develop a legal framework which would be both generic (i.e. applicable to a wide area of use cases) and detailed enough to cover the peculiarities of each use case. Therefore, quite often privacy laws are coarse-grained and hence inflexible. Moreover, the process of bringing in a new law (or introducing new amendments) requires time. That impedes the ability of legal enforcement to rapidly react to technological changes, which might introduce new privacy implications uncovered by previous laws. For example, the need to consider M2M privacy implications discussed in Section 3.3.3.
5. *Vagueness of definitions.* Many definitions used in legal frameworks are vague and ambiguous. In some cases it might be difficult to map them to the technology area and provide for unambiguous interpretation. For example, in [Kos11], it has been stated that the terms "electronic communications services" and "to provide an electronic communications network" of Directive 2002/58/EC (ePrivacy) are not clear and should be explained in more detail.

In the EU, the data protection framework is based on several directives [Kos11]:

- *Directive 1995/46/EC* – Data protection directive, defines basic principles with respect to data protection [Eur95].
- *Directive 2002/58/EC* – ePrivacy directive: regulation of processing of personal data in public communication networks [Eur02].
- *Directive 2006/24/EC* – Data retention directive: who can retain which data and for how long [Eur06].

Directive 1995/46/EC provides for the necessary legal basis for privacy protection. It clearly defines what personal and sensitive data are, what is understood under processing of personal data and which are the main actors in this area. The basic principles and rules for data processing, main obligations, etc. are defined as well. For example, according to Eleni Kosta [Kos11], the transfer

¹The coarse-grained and inflexible nature of privacy laws was claimed by Weber in [Web10]: "[...] only "extreme" warranties are legally guaranteed [...]".

of data from EU to other countries, which do not guarantee an adequate level of protection, is prohibited. This should mitigate the outsourcing problem, see point 3 of the list of privacy enforcement connotations. In order to bridge the differences between privacy legislation systems of the EU and the USA and by this solve the problem of international interoperability (see point 2), a "Safe Harbor" legal framework¹ has been established, which according to [Kos11] encompasses the following principles:

- Notice;
- Choice;
- Onward Transfer;
- Access;
- Security;
- Data integrity;
- Enforcement.

"Safe Harbor" was developed by the U.S. Department of Commerce in consultation with the European Commission. It should enable international commercial activities which are compliant with the privacy regulating frameworks of both the EU and the USA.

As it can be seen, there is a number of mechanisms for legal privacy regulation and enforcement. However, a lot of work should be done in order to improve existing legal frameworks and provide for necessary amendments in order to keep up with technological advance.

Privacy Impact Assessment Framework (PIA)

One of the initiatives to address privacy issues in the EU has resulted in the creation of a so-called Framework for Privacy and Data Protection Impact Assessments (PIA), which was developed to ensure privacy compliance of an RFID system being deployed [Rep11]. This framework is targeted at facilitating the process of establishment and maintenance of compliance with the privacy and data protection laws and regulations as well as risk management in RFID systems. It also provides for privacy assessments at early stages of RFID system development, which contributes to the process of RFID systems development according to the Privacy by Design paradigm [Cav09].

PIA creation is a decent step towards a competent and widely acceptable privacy assessment of an RFID system in a way that can be understood by all business parties involved. When the appropriate legal basis is created, it might

¹The US Department of Commerce in consultation with the European Commission: U.S.–EU Safe Harbor, http://export.gov/safeharbor/eu/eg_main_018476.asp

be possible to oblige organizations to carry out PIA assessment with, for example, subsequent certification. PIA report can be provided for an external review by the respective authorities. That should not only promote privacy in RFID systems but also additionally enforce the observance of privacy laws in the EU.

Privacy enforcement in a compound way

In order to provide for a full-fledged solution for privacy management in the RFID domain, both technical and legal privacy enforcement should be considered. The former ensures that an adversary is substantially¹ hindered in his attempts to violate privacy utilizing technical measures like clandestine reading, illegal profiling, etc. Legal regulations should be supporting this and consider the issues uncovered by the means of technical privacy enforcement. For example, introducing a legal responsibility for the actions considered to be privacy violating or contributory to them and therefore rendering them unprofitable for an adversary (risks of being brought to account outweigh the possible benefits).

Moreover, in order to increase efficiency of the compound privacy enforcement, a cooperation between legislators and IT specialists is needed. The latter possess the necessary technological basis and can highlight the peculiar privacy threats inherent in the RFID domain, which, for example, can not be fully covered by technology² and need to be protected by law, therefore fine-tuning the legal privacy-regulations [GBPT11].

Furthermore, different facets of privacy discussed in Section 3.3.2 require that this complex notion is considered in a cross-disciplinary approach. For instance, bodily and decisional privacy can not be enforced by applying technological means. To the contrary, in order to enforce communication privacy, for example, technical privacy enforcement should be utilized in the first place since it is extremely difficult to spot the adversary, who is simply eavesdropping³ and make him accountable. Therefore, the other facets require both technology and law to provide for an optimal privacy management solution (see Figure 3.7).

¹The degree to which an adversary is prevented from committing privacy violation highly depends on the attacker model and consequently on the capabilities he has.

²For example, the implications of M2M privacy, etc.

³See the problem of violator detection discussed within legal privacy enforcement on page 43.

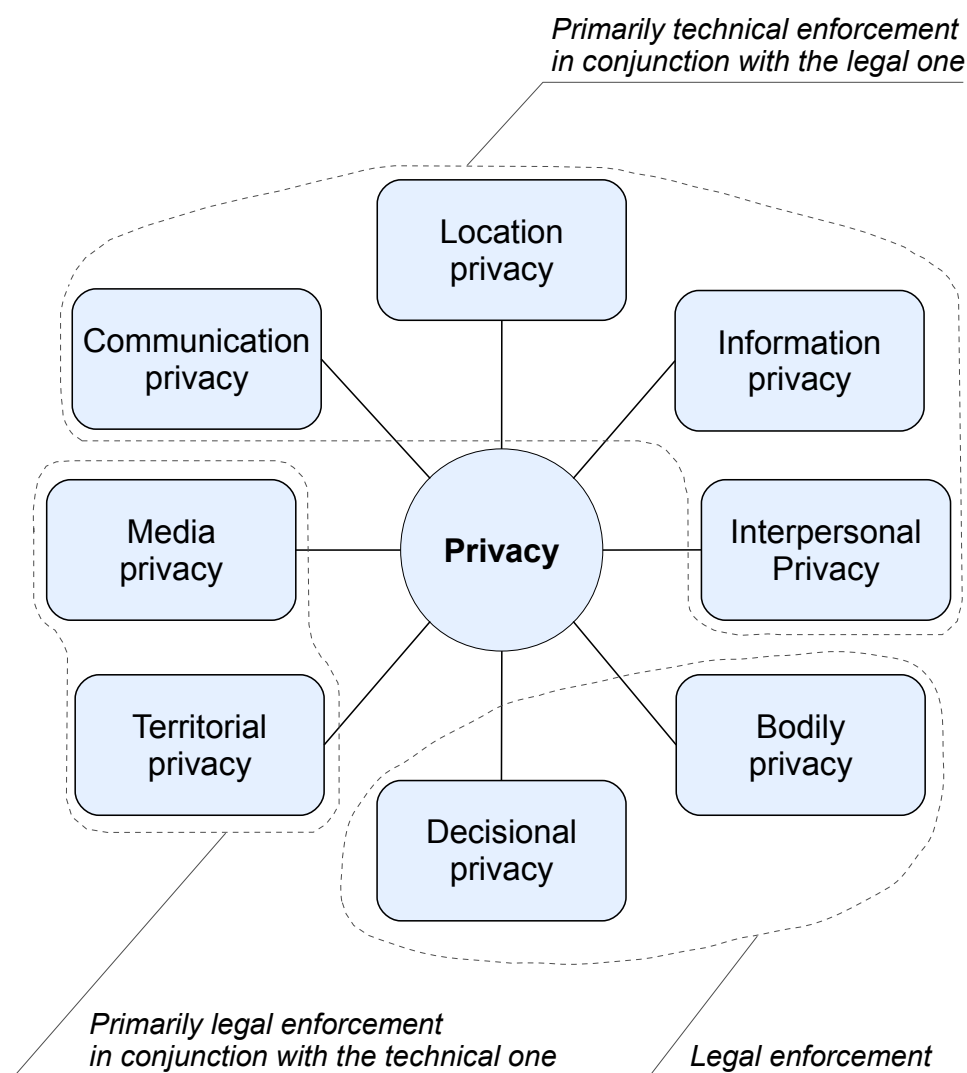


Figure 3.7: Privacy facets and privacy enforcement.

3.5 Security peculiarities in RFID

Security provides for the necessary basis for implementing and enforcing privacy and is, therefore, an integral part of the underlying mechanisms of privacy management. In this section, security issues peculiar to the RFID domain are discussed. The main components of RFID systems (the back-end, the bridging component, and the front-end) possess different functional capabilities, which further distinguishes security peculiarities pertaining to this domain and is therefore considered in this section as well.

Considering security implies taking into account certain protection goals, which are classically represented by a so-called CIA triangle: confidentiality, integrity and availability. Each of these goals has a set of its own distinguished features in the RFID environment.

3.5.1 A CIA triangle in RFID

Confidentiality

In RFID systems, the information exchange between readers and tags is performed over the wireless interface. This raises concerns over confidentiality of information transmitted over an inherently insecure radio channel, especially for security- and privacy-critical applications. One of the main threats in this case is eavesdropping because of its clandestine nature and difficulty of detection. Lightweight implementations of encryption algorithms combined with tamper-resistant modules, which store keys on a tag with enhanced reliability, should mitigate the problem. The authors of [HFW11, HJS11] demonstrated that it is already possible to efficiently implement AES¹ and ECC² encryption algorithms on an RFID tag. This raises the costs, though, and introduces a computational overhead which otherwise could be used for fulfilment of direct functionality requirements. That is why quite often security mechanisms are traded off for functionality of the system, especially if it is considered to be "security uncritical" by, for example, company management or customers.

Exchange, storage and protection of cryptographic keys are further issues to be considered. The procedure of key exchange (and constant update thereof) should be performed over a secure channel, which might become a bottleneck in case it has to be carried out for numerous constrained devices. Storing the key on an RFID tag is a costly operation itself since it requires a relatively considerable amount of gates³ [Pre11]. Even if this problem has been solved,⁴ the stored keys have to be properly protected. Tamper-resistant memory areas might be used in this case, which, however, raises the production costs. Moreover, the size of these areas is usually quite limited.

Furthermore, it is usually very difficult to provide for physical protection of ubiquitously deployed RFID tags. This paves the way to so-called implementation attacks⁵, which are targeted at obtaining the cryptographic keys using physical properties of encryption hardware and can bypass the conventional key protection mechanisms.

¹Advanced Encryption Standard [NIS01].

²Elliptic Curve Cryptography [Kob87].

³A logic gate is an idealized or physical device implementing a Boolean function [Jae97].

⁴For example, using ECC, where the key is shorter, or by introducing more gates, which should be easier in the future according to Moor's law.

⁵Namely, side-channel attacks, fault analysis and reverse engineering, which are further discussed in Section 3.5.2 and Appendix A.

Integrity

Unsolicited data modification which stays unnoticed may have disastrous consequences in RFID applications. Direct manipulation of data residing in the RFID tag's memory (e.g. using small charged needle probes) can bypass protection mechanisms of higher layers (like encryption) [MBPL09]. Integrity of the exchanged messages can be also violated utilizing the vulnerabilities of radio-frequency communication. In [HB11], it was shown that by altering the modulated signal at the physical layer it is possible to invert the correct bit in a signal sequence under certain conditions (depending on types and level of modulation used).

Similarly to the confidentiality problem, integrity can be ensured as long as the authentication procedure has been successfully carried out and key distribution has been performed. Energy concerns may impose a severe burden in this case as well. Moreover, according to Bart Preneel [Pre11], the problems of confidentiality and integrity (as well as authenticity) are *shifted* to the one of keeping the respective keys secret. For example, securing the keys in software is extremely difficult and can be broken by performing instant memory dump and searching for random patterns, which are very likely to be the keys. Tamper-resistant hardware may be utilized to mitigate the problem of secure keys storage. The cost of it, however, might impede its adoption to the area of RFID because even storing the key is very costly and requires a considerable number of gates [Pre11]. Furthermore, the actual implementation of a cryptographic algorithm determines its resistance to real attacks since many of them are rather targeted at each specific implementation thereof than at the algorithm itself.

Availability

In RFID networks, the devices are pervasively distributed, which makes it extremely hard if not impossible to physically isolate them from potential attackers. Physical destruction, jamming or simply enclosing a tag into conductive material (see Section 3.5.2 for more details) can violate availability of a tag or even render it inoperable.

Without special measures (e.g. wake password), any reading device can query a tag and therefore introduce collisions, which might comprise a DoS attack in case communication is initiated concurrently by several readers.

Summarizing, the CIA triangle is an inalienable part of the security notion and therefore, it is important to realize and consider its specifics in RFID sys-

tems to be able to efficiently perform privacy management, which is to a large extent based on the available security mechanisms.

In the next section, specific attacks on RFID systems are considered in more detail since they determine the specific security threats inherent in the RFID domain.

3.5.2 Attacking an RFID system

In RFID environments, the attacker is unlikely to experience the same limitations in computational, memory, and energy resources as the end device. For example, most of the cryptographic techniques, which are currently feasible to implement on constrained devices, are succumb to violation by a resource-powerful attacker [PT11]. This raises the problem of power imbalance between the attacker and the victim, which in turn greatly restricts the set of available countermeasures.

RFID systems consist of three main parts: the back-end, the bridging element (readers) and the front-end. The attacks targeted on the back-end system can be considered as non-specific to the RFID domain since in this case the computational and power resources enable the implementation of mature and well-established classic security mechanisms in the back-end . To the contrary, the two other components of RFID systems determine the characteristic attacks in this domain. They fall into a number of categories depending on their target [Fin10]:

- Attacks on an RFID tag;
- Attacks on a radio-frequency (RF) interface (radio channel between the tag and the reader);
- Attacks on a reader.

The categorized attacks on an RFID system are listed below in more detail¹ and summarized in Figure 3.8.

Attacks on an RFID tag:

- Permanent destruction of a tag (affects availability):
 - due to exposure to a relatively strong electromagnetic field (e.g. putting a tag into a microwave oven);
 - mechanical destruction (e.g. cutting the antenna off);
 - chemical destruction.

¹Most of them are presented according to [Fin10] with several additions, like implementation attacks and data manipulation, see attacks on an RFID tag.

- Tag shielding/tuning (preventing the reader's signal from reaching the tag by e.g. wrapping aluminium foil around it; affects availability);
- Tag spoofing and cloning (pretending to be a genuine tag by creating its clone, tag impersonation; affects confidentiality);
- Manipulating the data stored on a tag [ZK09] (affects integrity);
- Implementation attacks (attacks on cypher keys residing in tag's memory, listed in more detail in Appendix A; affect confidentiality and integrity):
 - side-channel attacks (timing analysis, power analysis, electromagnetic analysis, and acoustic attacks)
 - fault analysis;
 - reverse engineering.

Whereas it is extremely difficult to protect an RFID tag against destruction and shielding, tag spoofing and cloning can be mitigated by the utilization of lightweight implementations of cryptographic techniques, such as encryption and authentication. In order to provide for protection against data manipulation, passive¹ and active² shielding of a tag can be used. The possible countermeasures against the implementation attacks are described in Appendix A.

Attacks on an RF interface:

- Eavesdropping (interception of the communication between the reader and the tag; affects confidentiality);
- Jamming (interruption of the communication between the reader and the tag; affects availability);
- Extension of the reading range beyond the norms defined in the respective standard (in order to covertly skim a remote tag; affects confidentiality);
- DoS attack using the blocker tags (preventing the anticollision algorithm from working properly by introducing a so-called blocker tag, which simulates collision³; affects availability);
- Relay attack (an undetected use of a remote tag in order to simulate the fact that it is situated in the proximity of a reader⁴; affects confidentiality and integrity).

¹An additional protective surface on top of the circuitry.

²Integration of sensors to detect the attempts of intrusion and act accordingly, e.g. reset the chip's configuration, delete sensitive data, etc.

³The simulation of collision depends on the anticollision algorithm used. According to [Fin10], there are two established anticollision algorithms in RFID systems: the binary search tree algorithm and the slotted ALOHA. In the first case, the blocker tag misleads the reader by simultaneously sending "0" and "1", thus simulating a collision at each bit location of its serial number. In case of ALOHA, the blocker tag keeps sending its serial number in each available time slot and therefore preventing the other tags from answering the reader's query.

⁴Relay attack can be used to attack the tag carrying out the transactions that are subject to charges (e.g. RFID tickets, RFID-enabled paying cards, etc.).

The possible countermeasures in this case would be the utilization of lightweight encryption (against eavesdropping) and authentication (against, for example, relay attacks).

It is, however, extremely difficult to provide for protection against jamming attacks. Klaus Finkenzeller, for instance, states that there are practically no countermeasures available¹.

Attacks on a reader

The reader's performance can be compromised by faking the tags in its interrogation area, which can be done either by direct cloning of a tag or even by mimicking the tag's behavior using a powerful computing device with additional RFID-specific hardware². This can compromise confidentiality and furthermore violate integrity of the data associated with the faked tag (e.g. if a reader forwards an update to the back-end database that the item associated with a faked tag has arrived in the warehouse, even though in reality it has not.).

Lightweight implementations of encryption and authentication can be used to mitigate this problem.

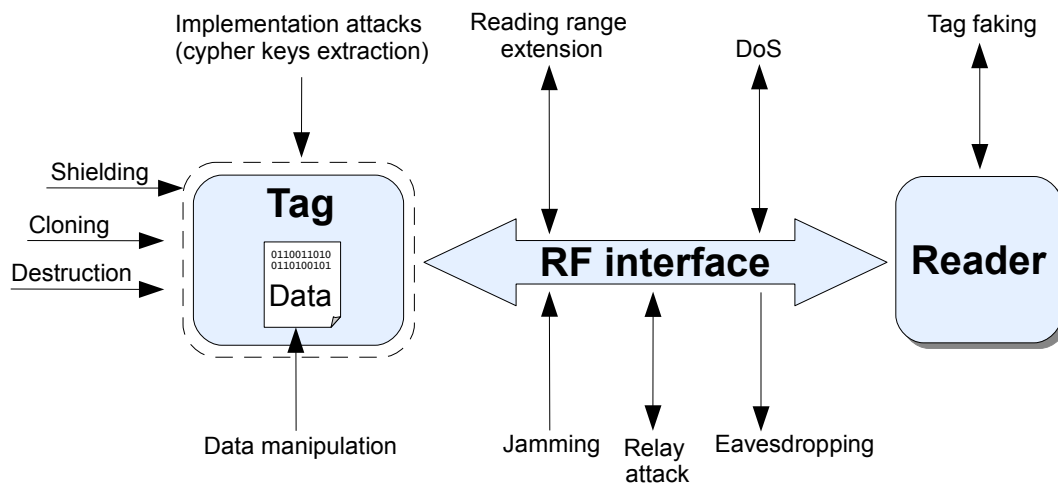


Figure 3.8: Basic attacks on RFID systems.

Having discussed the specific attacks on RFID systems along with possible countermeasures, peculiarities of security management in the RFID domain are considered in the next section.

¹Klaus Finkenzeller. Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities, http://www.rfid-handbook.de/downloads/Finkenzeller_Systemtech-Bremen-2009_v1.0.pdf

²This can be made possible if the RFID interface is well-standardized, which is quite often the case. If, however, the details of the RFID communication stack are unknown to the attacker (consider proprietary systems), then it is much harder to mimic the tag's behavior and perform the attack.

3.5.3 Security management in RFID

Security management in the RFID domain has a number of distinguished features determined by several factors:

- The specific structure of RFID systems;
- Wide distribution and heterogeneity of end devices;
- Scalability requirements.
- Inherent context-awareness;
- M2M (machine-to-machine) security considerations;

The resource constrained end devices comprising the front-end of RFID are not able to fully manage their security requirements due to resource limitations. Moreover, different classes of RFID tags possess substantially different functional capabilities (see Table 3.1), which raises the problem of managing security in the RFID environment with heterogeneous end devices. The quantity of the deployed RFID tags and their wide distribution further aggravate the problem since it is extremely difficult to perform, for example, key exchange with numerous ubiquitously distributed end devices in a secure manner. This introduces the need to explicitly consider scalability for security management in RFID systems. Context-awareness is another issue to be taken into account since, similarly to privacy management, security requirements should be dynamically managed in response to context changes. Last but not least, it is important to explicitly address the M2M security considerations as they have a profound influence on M2M privacy (see Section 3.3.3).

Therefore, in order to mitigate the aforementioned problems, the following approaches are suggested.

Middleware and gateway approaches

Since constrained end devices are not able to fully manage their security requirements, the notion of an intermediate layer helping to perform security management can be utilized. This in turn can be achieved by applying the concept of middleware (implemented in the RFID back-end and on the readers side) or introducing a special gateway (an RFID reader with an extended functionality) which provide for:

- Domain-specific adaptation of security requirements;
- Security management for heterogeneous devices;
- Outsourcing of performance-demanding tasks and their execution in a secure manner;
- Secure remote administration of an RFID system.

In order to illustrate the domain specific adaptation of security requirements, the following example can be considered.

Example 3.3.

Let an RFID system be used for several applications, namely room access control (RFID-enabled keys), automatic payment services (e.g. the "Ambient Coffee Machine" – a service providing hot beverages, which can be paid by an RFID-enabled pay card for convenience purposes), and health monitoring utilizing RFID sensor nodes (see Table 3.1). For each of these applications, the security requirements are substantially different as well as the capabilities of the utilized RFID tags. In order to properly perform security management in each case and handle the heterogeneity issue, a special gateway can be used. Moreover, the interoperability with the Internet can be provided enabling, for example, the remote administration of an RFID system. Figure 3.9 depicts the idea.

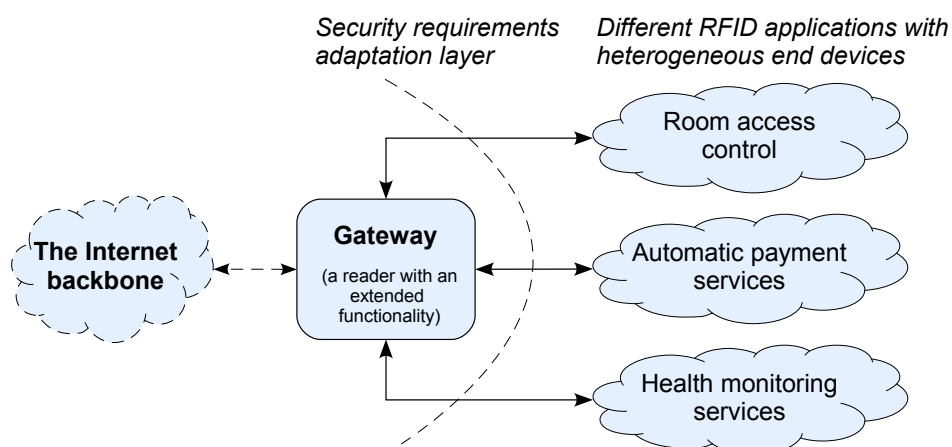


Figure 3.9: A gateway is used for the adaptation of security requirements of different RFID applications as well as for providing interoperability with the Internet.

Moreover, middleware enables end devices to operate in their native manner [GH07]. Therefore, the communication protocols specifically designed and optimized for different classes of end devices (e.g. the protocols of reader-to-tag communication in the front-end) can be used in conjunction with the standard ones (e.g. IPv6 in the Internet backbone). Furthermore, according to [HHW11], the computationally expensive tasks may be performed at the gateway side, so that only the result is communicated to the domain of constrained devices.

In order to provide for a secure remote administration of an RFID system, additional issues need to be considered, namely the trustworthiness of middleware. In case middleware (and the corresponding gateway) is treated as a distrusted system component, it should be ensured that end-to-end security is not

compromised at the gateway during the adaptation phase between the specific RFID protocol and IPv6 of the Internet backbone. In order to ensure that, the authors of [DAK10] suggest that the RFID front-end system being manipulated (the target RFID tags) and the administrating node (e.g. a desktop station) agree on the security suite to build up a secure end-to-end connection. The reader, therefore, solely passes the content of the messages and can only disturb but not compromise the end-to-end connection security. Security suits in this case define the security mechanism used (e.g. encryption or authentication) and also specify particular requirements for the tag (e.g. the ability to perform AES or SHA-1, key exchange mechanism, etc.).

However, it in order to enhance the security management process substantially influenced by the resource-constrained end devices, trusted middleware can be involved. In [SHT10], for example, the authors present a security architecture, which enables heterogeneous embedded devices with different capabilities and therefore different security mechanisms implemented to share information in a controlled manner. A key element in this approach is the information broker¹, which is used to measure the security capabilities² of the embedded device and to control information access and information exchange accordingly. The measurements are performed in different categories (e.g. encryption, authentication, key exchange, etc.), the results of which are further profiled to several security levels. Afterwards, the security levels for each category undergo the union operation and the "weakest link" determines the final security level of the device's security capabilities. Therefore, if a certain constrained device joins the system, its security capabilities are measured and assigned a certain security level. The information broker is required to keep track of information produced by this device, store it "with a particular security level" and "protect information accordingly" [SHT10]. Whereas the authors claim that their leveling scheme "provides sufficient control over security" and at the same time "is also usable enough for end-users to understand", the *individual* security requirements (the specific protection goals of an individual comprising the CIA triangle, see 3.5.1) are not explicitly considered. This is likely to *level out* the specific security requirements of the individuals and result in an inadequate protection of critical information.

Along with the advantages, the gateway approach to security management has several side-effects, which may negatively influence the performance of the system. For example, the authors of [VD10] claim that gateways should be

¹The information broker acts similar to the Object Request Broker in CORBA architecture [OMG08] in that all the communication is carried out via a special mediator entity – the "broker".

²The term "security capabilities" represents which security techniques (cryptographic algorithms, authentication mechanisms, etc.) the particular embedded device possesses and is capable of executing at all.

avoided because of their inherent complexity, inflexibility and lack of scalability. According to them, gateways impede management and troubleshooting of underlying networks and might negatively affect such parameters as Quality of Service (QoS), error recovery, routing, etc. This happens because of unavoidable inaccuracies of protocol translations, which take place at the gateway side. Moreover, protocol translation gateways might become networking bottlenecks because they inherently do not scale. They may also introduce a single point of failure and therefore negatively affect the reliability of an RFID system.

In the specific case of RFID, however, a gateway being implemented as the reader with extended functionality can be considered an inherent part of the system (the bridging element, see Figure 3.1). Therefore, the gateway approach to security management in RFID systems (with the additional support by security middleware) has a decent potential for covering the specific security issues of the RFID domain (see the list at the beginning of the section, p. 53).

Moreover, the scalability requirements and the necessity to perform security management in the context-aware environment can be covered by applying the middleware concept as well. The task of managing security requirements for many heterogeneous end devices (RFID tags with different functional capabilities) according to context information (and in response to context changes) can be encapsulated in security middleware as it was demonstrated in [SHT10, EPS10]. For context monitoring, a publish/subscribe scheme was used, where the module responsible for the determination of security requirements is subscribed to the results of context monitoring and in that can be informed of the context changes. In [EPS10], it was claimed that such security adaptation mechanism acts proactively, i.e. the likelihoods of threats are being constantly analyzed in order to provide for the necessary reasoning about the proper security mechanisms to be used. That is, "threats appear before attacks" [EPS10]. On the contrary, the reactive approach implies that the adaptation of security mechanisms is triggered by the fact that attacks are already taking place. The problem in the latter case is that adaptation might be performed too late and let the attack finish successfully.

M2M security considerations

The issues of M2M (machine-to-machine) communication raise additional security concerns and need to be specifically addressed. M2M communication is referred to as the process of autonomous communication¹ between various end devices, which may be only infrequently interfered by humans for management

¹Moreover, such autonomous communication additionally enables the implementation of transparency and self-governance to a certain extent, which are among the main properties of any UbiComp system, including the RFID domain. See Section 2.1.

and configuration properties. M2M communication has several implications for security management. Firstly, the end devices typically possess only limited computational capabilities and have scarce energy resource. For this reason, complex cryptographic procedures are not an optimal solution. Moreover, physical integrity of numerous end devices (RFID tags) deployed over a large area is of serious concern. They are for the most part left unattended (in public or rural areas) and it is quite often impossible to provide for their physical protection. This paves the way to various attacking scenarios, see Section 3.5.2.

In [WTJ⁺11b], it was underscored that security is of paramount concern in M2M communications. It is expected that advanced security solutions for end devices are going to emerge, such as "security-on-chip". The authors of [CSS⁺09], for example, describe a concept of the trusted environment (TRE), which is a logically separate entity within an M2M device. It can be used for the execution of software and other critical operations, such as storage of sensitive data. With the use of TRE, verification of trustworthiness of an M2M device can be carried out. For example, using autonomous validation (not relying on external entities and hence on network connectivity) and/or remote validation.

Moreover, according to [CSS⁺09], the following two factors determine the peculiarities of M2M security: intermittent connectivity to the core network and the demand for high configurability and flexibility. This denotes the two specific goals [CSS⁺09]: the ensurance that end devices operate in a secure state without network connectivity (e.g. locally assured secure booting) and the ability to assess the trustworthiness of the end device remotely (e.g. using remote validation).

The authors of [WTJ⁺11b] additionally claim that M2M systems should be able to detect unusual events (e.g. unconventional and suspicious behavior of particular end devices, violation of their physical integrity, etc.) and provide for the authentication between end devices as well as between end devices and gateways (alternatively, edge routers in IPv6).

3.5.4 Summary on security peculiarities of RFID

Addressing security issues in the RFID domain is a complex task, which needs to be considered in a cross-layered fashion in every part of an RFID system (in the back-end, front-end as well as in the bridging element). In this section, the peculiarities of security management were approached by firstly considering the specifics of RFID systems with respect to the CIA triangle. Then, the attacks peculiar to the RFID domain together with the possible countermeasures were discussed. The aforementioned issues enable to consider the general process of

security management in RFID, which needs to take into account: *a)* the specific structure of RFID systems; *b)* wide distribution and heterogeneity of end devices; *c)* scalability requirements; *d)* context-awareness and *e)* M2M security considerations.

In order to address these requirements, the middleware and gateway approaches can be utilized. They enable to encapsulate the task of managing the security requirements in security middleware (implemented in the back-end and on the readers side), which provides for: *a)* domain-specific adaptation of security requirements; *b)* security management for heterogeneous end devices; *c)* demanding-tasks outsourcing and their secure execution; *d)* secure remote administration of an RFID system.

The task of communicating the security middleware instructions to the domain of the constrained end devices is performed by gateways, which are RFID readers with extended functionality. The latter implies that a gateway unlike the conventional RFID reader is additionally responsible for the execution of protocol translation tasks (e.g. between IPv6 and the specific RFID interface) and directly carrying out the security management instructions (received from security middleware) between (possibly heterogeneous) RFID tags.

The issues regarding M2M security were considered within this section as well since they introduce a set of security peculiarities pertaining to the domain of constrained devices and have a profound influence on M2M privacy.

3.6 Chapter summary

Privacy implications of RFID systems were discussed in this chapter. In order to approach this issue, the specific structure of RFID systems (Section 3.1) was described together with their classification (Section 3.2), which have a profound influence on privacy management in this domain. The general notion of privacy and privacy peculiarities of RFID systems were presented and discussed in Section 3.3. Since it is of high importance to be able to enforce privacy, the means of privacy enforcement with respect to the RFID domain were considered in Section 3.4.

Security is an inalienable part of any mature privacy-management solution. Therefore, the security peculiarities of RFID systems were considered as well in Section 3.5.

The aforementioned issues form the underlying basis for developing a privacy-respecting RFID system. The recommendations for enabling the development of an RFID system in a privacy-preserving way are presented in the next chapter.

4 Designing a privacy-respecting RFID system

This chapter presents the recommendations for developing a privacy-respecting RFID system, which are based on the RFID specifics considered in the previous parts of the thesis.

Firstly, the reasons to invest in privacy during the development process are discussed within Section 4.1. In Section 4.2, the approach to making privacy inherently built into the functionality of an RFID system is considered. Mutual interdependence between privacy and security leading to the necessity of considering these notions in a joint fashion is discussed in Section 4.3.

4.1 Motivation for designing RFID systems in a privacy-preserving way

The process of any IT system development, including the RFID one, is complex, time-consuming and costly. For this reason, the developers at the beginning concentrate themselves on primary issues of system functionality and quite often leave security and privacy mechanisms to be implemented afterwards as an add-on. From the management perspective, the perception of privacy and security is generally associated with the "necessary evil" at best. Therefore, it is extremely difficult to convince management to additionally invest in these issues. That is why the necessary mechanisms concerning privacy and security are usually implemented "on demand" only after the design process is complete, which too often results in immaturity of privacy compliance of the end product. This might become one of the main burdens on the way to acceptance of such systems among potential users and to commercial success thereof as a consequence.

The authors of [GBP11a] explicitly addressed this problem and claimed that privacy concerns of the users can impede the development and especially the deployment of UbiComp systems. For example, there has been a big number of complaints about Smart Grid systems which alongside their intended purpose paved the way to privacy violation scenarios^{1,2,3}. The emerged public outcry

¹"Why Smart People Are Suspicious of Smart Meters", <http://blogs.forbes.com/williampentland/2010/12/10/why-smart-people-are-suspicious-of-smart-meters>

²Smart Grid Privacy Concerns, http://www.privacyguidance.com/files/SmartGridPrivacyConcernsTableHeroldSept_2009.pdf

³"Smart energy meter will not be compulsory", http://vorige.nrc.nl/international/article2207260.ece/Smart_energy_meter_will_not_be_compulsory

stopped the roll-outs of Smart Meter system in the Netherlands and put its future in question.

For this reason, developing a ubiquitous RFID system in a privacy-respecting manner will increase the likelihood of its acceptance among potential users and broaden the target audience. Furthermore, having created a secure and privacy-respecting infrastructure, it is relatively easy to deliver the end product to customers (to deploy the system, e.g. accompany individuals with the respective end devices) since "individual investments pay off immediately" [Pfi10]. Due to this fact and because of the higher acceptance among customers, a system with decent privacy management mechanisms is more likely to be commercially successful, which further motivates to invest in the privacy-oriented development process [GBP11a].

4.2 Making privacy inherently built into the functionality of an RFID system

In order to develop a secure and privacy-compliant RFID system, it is important to consider privacy and security from the outset. A general approach to development of inherently secure and privacy-respecting UbiComp systems, which holds true for RFID systems as well, was outlined in [GBP11a, GBP11b]. According to it, the process of ensuring privacy and security should begin already at the system design stage, the concept known as "Privacy by Design"¹, and it should continue throughout all the other steps of system development.

It is clearly impossible to predict the security and privacy requirements of all potential users as well as the variations thereof in response to future context changes already during the system design stage. In order to provide for flexibility and extensibility, a concept of special extension/variation points (so-called hooks) for unforeseeable extensions/variations of privacy and security requirements can be utilized. Therefore, the process of "weaving" privacy and security mechanisms into the functionality of an RFID system can be divided into the following steps, depicted in Figure 4.1:

1. During the system design stage, generic (i.e. foreseeable) privacy and security requirements are considered. In order to provide for flexibility in future, a concept of extension/variation hooks with respect to privacy and security requirements is used.
2. At initialization time, an instantiation of generic requirements considered

¹See, for example, [Cav09, Sha09].

during the first step is carried out. Also, the so-called *binding*¹ of extension/variation hooks is performed.

3. At run-time, the previously implemented privacy and security management mechanisms are used. In order to provide for *dynamic* adaptation (e.g. in response to context changes), the concept of dynamic extension/variation hooks may be exploited.

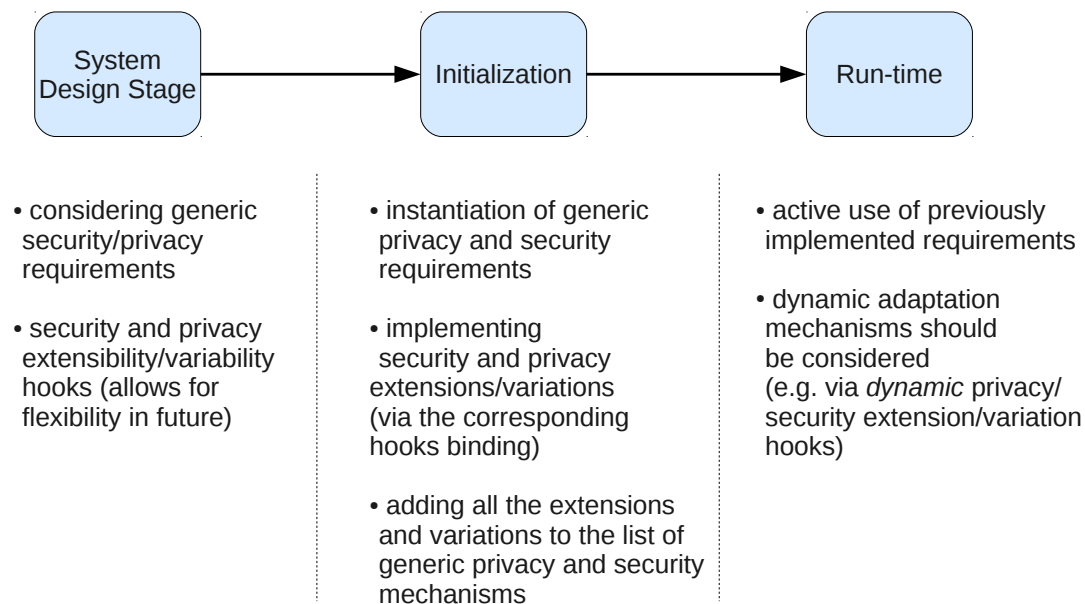


Figure 4.1: The process of "weaving" privacy and security mechanisms into the functionality of an RFID system.

The aforementioned approach should enable the developers to design an *inherently* privacy-respecting RFID system. It is hardly possible to provide for a full-fledged support of privacy management, having considered this issue only after designing and implementing the functional part of a system, i.e. building privacy on top of it (as an add-on). That is why we advocate that the process of ensuring privacy and security has to begin at the *system design stage* and it should continue throughout all the other steps of system development.

4.3 Considering privacy and security in a joint fashion

Ubiquitous RFID systems are likely to introduce a qualitatively new challenge to individual privacy, which stimulates to carefully consider this issue during the system development process. In order to comprehensively address this problem, security mechanisms are needed as well since they are an important part of any

¹The term is adopted from programming. It basically means that the corresponding hooks are being directly used, i.e. extension/variation has taken place via the hook.

privacy management solution. Security threats, specific attacks and vulnerabilities as well as the availability of security mechanisms and their implementation in the constrained environment of RFID systems affect privacy regulation and determine the necessary technical basis for privacy enforcement (see Section 3.4.1).

The tight connection between privacy and security leads to the fact that the processes of designing and managing privacy and security policies are closely intertwined with each other. Important is to recognize that neither of them is a by-product of the other one. Only if having considered both, privacy and security, can the developed ubiquitous RFID system be regarded as privacy-respecting and secure [GBP11a].

Therefore, we advocate considering privacy and security in a joint fashion during the process of RFID systems development. Our approach is inspired by the one mentioned in [KSW03, KS02], where the duties of managing privacy and security are divided between the Privacy Officer (PO) and the Security Officer (SO). Access to privacy-sensitive data is granted to a user u_1 if:

1. The Security Officer (SO) authorizes u_1 to perform a certain task t_2 .
2. The Privacy Officer (PO) certifies t_2 for a purpose p_3 .
3. The PO authorizes p_3 to perform the desired access to the particular privacy-sensitive data ($data_item_2$).

Figure 4.2 depicts the concept.

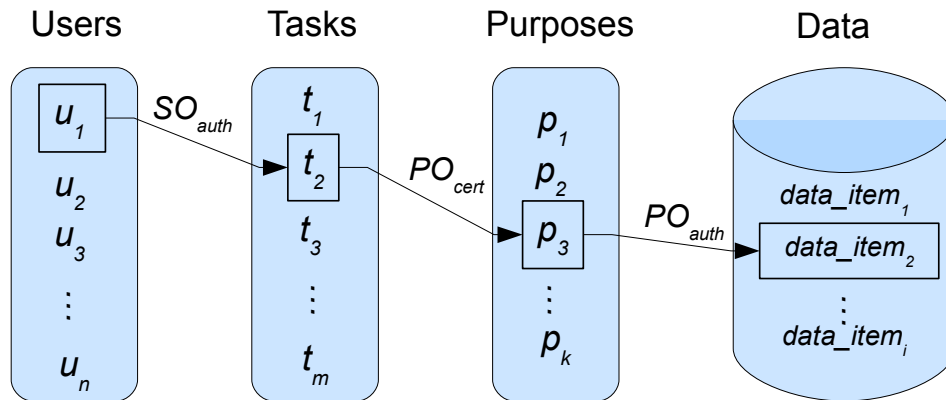


Figure 4.2: Distributed administration performed by the SO and the PO.

SO_{auth} – authorization performed by the SO.

PO_{cert}, PO_{auth} – certification and authorization performed by the PO.

Granting access rights according to such a distributed access control policy can be expressed using a high-level notation:

```
ALLOW [user]
PERFORM [task] on [data_item]
for [purpose] provided [condition].
```

However, according to the approach described above, the privacy and security policies, followed by the SO and the PO, are *already designed and specified*. We suggest that these entities (the SO and the PO) not only control security and privacy in the already deployed system but *design* the policies in a joint fashion as well. The joint design process should be carried out in such a way that security and privacy mechanisms are "woven" into the UbiComp system's functionality already at the system design stage (see Figure 4.1 in the previous Section), which enables proper privacy and security precautions to be *inherently* built into the functionality of the system. That implies that privacy and security requirements are developed in conjunction with the requirements of direct functionality of the system.

Therefore, by analogy with the SO and PO concept, the entities¹ of the Security Engineer (SE) and the Privacy Engineer (PE) can be considered. The SE and the PE, along with administrating and managing security and privacy in the deployed system, are also responsible for the *whole design process* of the respective policies.

In Figure 4.3, a general collaborative approach to designing policies for a privacy-respecting system is depicted. It considers, in the first place, two cooperative entities: the Privacy Engineer (PE) and the Security Engineer (SE). These entities are responsible for the whole design process of privacy and security policies respectively as well as for administrating and managing privacy and security in the deployed system.

The process of designing policies for a privacy-respecting and secure RFID system is therefore performed in the presence of tight collaboration between the PE and the SE, which is aimed at mirroring the interdependence between security and privacy in the design process. Further negotiation with the Functionality Engineer (FE), who is responsible for the design of the direct functionality of the system, is of high importance as well. The reason for this is that it is expected that the requirements elaborated by the PE and the SE along with the ones of the FE may not be free of conflicts. That is why conflict resolution mechanisms are considered during the process of merging the requirements. In order to ensure that the requirements are consolidated in a consistent way (i.e. after the merging, the specific requirements of each area conform to the ones before the merging), consistency checks are performed.

Moreover, the PE and the SE are responsible for carefully considering, respectively, the specifics of privacy (Section 3.3.3) and security (Section 3.5.3) management in the RFID domain including the analysis of inherent threats and

¹The term "entity" implies that there may be several security and privacy experts behind the SE and PE entities respectively. It is possible as well that the tasks of the SE and PE are performed by one expert (e.g. in case of a relatively small RFID system).

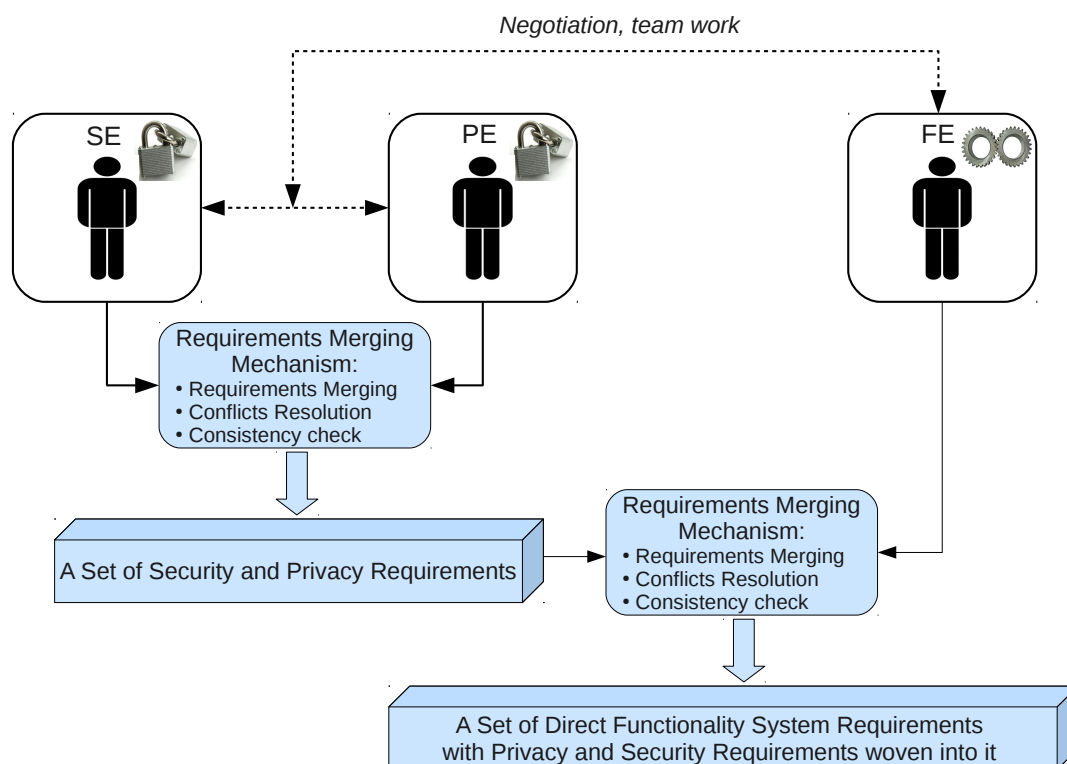


Figure 4.3: A process of joint development of privacy and security requirements.

SE = Security Engineer.

PE = Privacy Engineer.

FE = Direct Functionality System Engineer.

possible countermeasures. The capability range of end devices (see Table 3.1), which are going to comprise the front-end of a future RFID system, needs to be considered by these entities as well since it determines the extent to which privacy (as well as security) can be enforced (see Section 3.4). For example, the PE the SE can impose additional requirements for implementing privacy- and security-enhancing middleware, which utilizes readers as special gateways for dynamic management of privacy and security policies (see Section 3.5.3). These requirements are further communicated to the Direct Functionality Engineer (FE) who is responsible for merging them with the requirements of direct functionality (with subsequent conflicts resolution and consistency checks).

The PE can additionally carry out preliminary privacy assessment according to the PIA framework (see Section 3.4.1) in order to ensure that the developed RFID system complies with the recognized privacy norms, which in turn is going to positively affect its acceptance among users and consequently raise the likelihood of the eventual commercial success.

4.4 Chapter summary

Within this chapter, the recommendations for developing a privacy-respecting RFID system were presented. The focus was made on the method of designing inherently privacy-respecting and secure RFID systems together with the approach to considering privacy and security in a joint fashion during the development process. The former implies the existence of implementable privacy and security requirements, which are engineered during the steps covered in the latter approach. According to it, the process of developing privacy requirements is encapsulated in the tasks of the Privacy Engineer (PE) entity. In order to perform requirements engineering, privacy modeling can be utilized, which is discussed within the next chapter together with the review and assessment of several existing privacy models.

5 Privacy modeling: motivation and suggestions

This chapter presents and discusses the privacy modeling approach which can be used for enhancing and fine-tuning the process of privacy requirements engineering. Firstly, the motivation for privacy modeling is provided in Section 5.1. Section 5.2 describes how this concept can be utilized for privacy management in the underlying system. In Section 5.3, the existing privacy models are reviewed together with their assessment and applicability to RFID systems. As a conclusion, the recommendations for developing a holistic privacy model targeted at the RFID domain are provided.

5.1 Privacy modeling: motivation

Privacy is a complex notion which needs to be addressed in an interdisciplinary manner. Moreover, it is a highly subjective issue by its nature, which means that its perception may substantially differ from individual to individual. Therefore, it is very difficult to provide for a generic privacy management solution.

In order to develop a holistic approach to privacy management, many aspects need to be taken into account, namely technical, legal and even social ones. This corresponds to the different facets of privacy discussed in Section 3.3.2 (see Figure 3.3) highlighting its complex nature and specifying which aspects should be covered in a decent solution for privacy management. Moreover, privacy enforcement is performed across several domains as well, primarily in the technical and in the legal ones (see Section 3.4.1, Figure 3.7).

Therefore, it is highly desirable that all privacy constituents are considered during the process of requirements engineering since it is the necessary basis for the implementation and maintenance of a decent privacy posture of the developed system.

In this context, privacy modeling enables to consider the privacy notion in an interdisciplinary fashion encompassing its facets and therefore taking into account the necessary technical, legal, and social issues. A privacy model can be decoupled from the actual implementation of privacy requirements and is rather focused on *what* should be implemented than on *how* it is going to be done therefore enabling a high-level and holistic view on the problem of privacy management in the system. Moreover, the ability to consider various privacy

facets lets the Privacy Engineer (PE) (see Figure 4.3) perform a combination of privacy issues from different fields in an interdisciplinary fashion, which makes the approximation to the real world scenario more accurate [GBP11a].

In case the developed system is complex enough and needs, for instance, to be deployed in different countries with possibly different privacy regulations and/or different levels of technological advance (may affect the technical enforcement of privacy), different strategies for privacy requirements engineering may be required in each deployment scenario. This results in the fact that the developed privacy requirements for different countries may vary substantially. In order to support flexibility in this case, several privacy models can be designed, which have the same "core" but different additional features reflecting the peculiarities of privacy management according to each country¹.

Moreover, in case a new set of privacy requirements is to be appended to the existing one for certain reasons, it can be performed using privacy modeling as well by either directly adding the new requirements to the existing model or by introducing a new one. This provides the PE with extensibility during the process of privacy requirements engineering.

Furthermore, flexibility and extensibility let the PE perform the necessary updates in response to the recently discovered privacy breaches, advances in technology, and changes in privacy regulations.

Summarizing the aforementioned, privacy modeling enables:

- A holistic approach to privacy requirements engineering (considering privacy facets);
- Decoupling from the underlying implementation of privacy requirements;
- Better approximation to the real-world scenario;
- Flexibility and extensibility.

5.2 Privacy modeling in a privacy management system

The developed privacy model is further utilized for obtaining privacy requirements, which are subsequently exploited for privacy management. In order to demonstrate this, the following approach² can be considered. According to it, the decisions of granting or denying access to a data item (residing in the back-end database or directly on a tag) are controlled by the underlying privacy-

¹This example can be generalized for other cases as well. For instance, RFID systems spanning different price categories with respect to their privacy-awareness (e.g. the most expensive ones possess more mature mechanisms for technical privacy enforcement), which consequently affects the eventual fulfilment of privacy requirements and therefore may result in different privacy models.

²This approach was inspired by the concepts presented in [FHO98].

respecting access control subsystem (which is implemented in the RFID backend) according to the privacy requirements inferred from the respective privacy model. This subsystem consists of two main parts: a Privacy-respecting Reference Monitor¹ and a Privacy Rules Module (see Figure 5.1).

The former acts as a trusted mediator and is the main hub for all data access requests from user entities. Based on the respective privacy requirements (residing in the Privacy Rules Module), the Privacy-respecting Reference Monitor makes decisions whether a user entity is granted access to a certain data item. Suppose a user U_i is willing to access a data item n . The underlying system forwards the request to the Reference Monitor (step 1 in Figure 5.1), which checks if this request is compliant to privacy requirements (step 2). This results in granting or denying access to a data item n (step 3-a, 3-b).

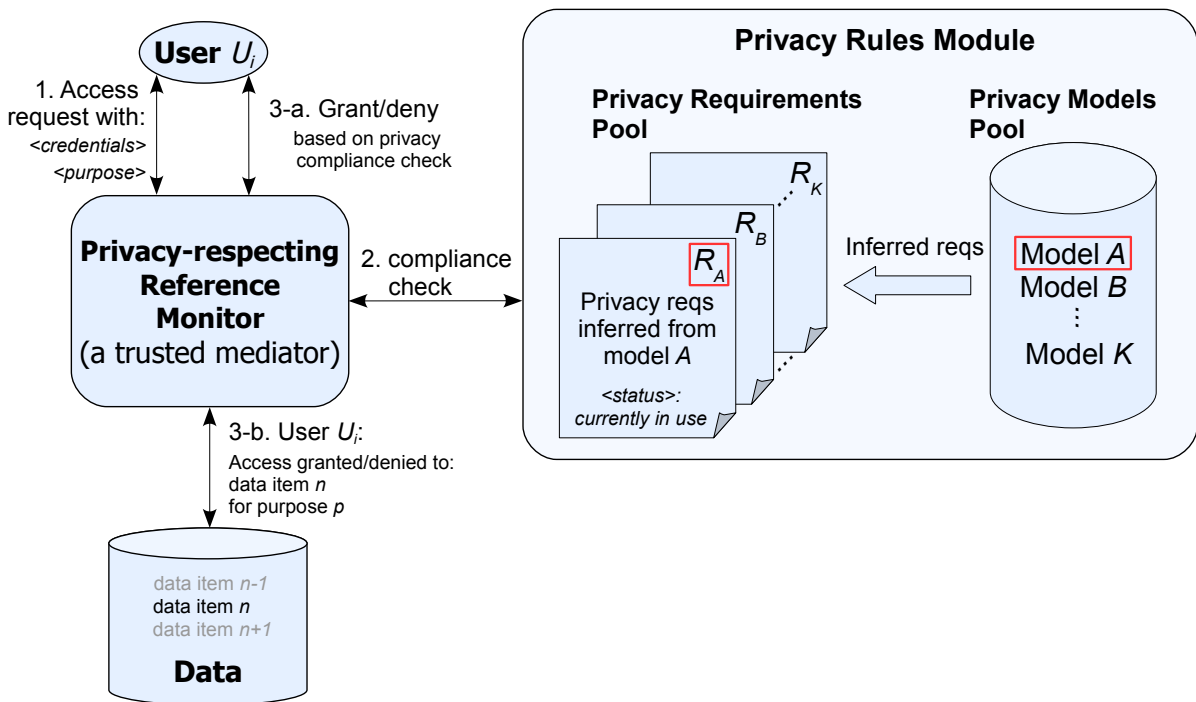


Figure 5.1: Privacy-respecting access control using privacy models.

The Privacy Rules Module encompasses the Privacy Models Pool, where various privacy models reside, and the Privacy Requirements Pool possessing the sets of privacy requirements obtained² from the corresponding privacy model. For example, privacy requirements R_A are obtained from the privacy model A and are subsequently used for privacy compliance check of every request to a data item.

¹The concept is analogous to a reference monitor for runtime security enforcement in operating systems, see, for example, [UE04].

²The process of requirements inference is performed according to the principles of the framework outlined in [GBP11a] and is discussed in more detail in the next chapter.

In case privacy management needs to change the strategy it has been adhering to (e.g. deploying the system in another country with different privacy regulation), the privacy model can be changed respectively (flexibility, see the previous section) or a new privacy model can be added to the Privacy Models Pool providing extensibility. Moreover, the latter enables to adequately respond to such important factors as the recently discovered privacy breaches, advances in technology introducing additional challenges to privacy, etc.

5.3 Existing privacy models and their assessment

Privacy modeling is a demanding and challenging task for several reasons. Firstly, it requires an interdisciplinary approach which introduces complexity since a lot of effort is required for carefully considering all privacy facets (see Figure 3.3). Secondly, the existing privacy models describe this notion mainly from a single perspective (e.g. a sociological, legal or technical one) only partially treating the issues originating from other fields. Moreover, privacy as a research issue was initially addressed in humanitarian sciences (especially in law, sociology, and philosophy) since the technological advance at that time was not mature enough to raise serious privacy concerns. Therefore, there is not much experience in considering privacy implications with respect to technology (bridging privacy issues from humanitarian sciences with technology, i.e. applying the interdisciplinary approach) and consequently there are no established common practice recommendations available.

Technological innovations, however, pose a serious challenge to individual privacy and therefore require that privacy issues are carefully considered during the development process. We advocate that privacy modeling is a promising way to tackle the problem. There have been several attempts to model privacy in technical systems and in this section, the related work on this issue is surveyed and discussed. Since the notion of privacy has been extensively researched in humanitarian sciences, many privacy management solutions in the technical domain utilize the concepts elaborated in other scientific fields (namely, the humanitarian ones). Therefore, the first two reviewed models originate from sociology and law providing the next models from the technical domain with the necessary background for considering privacy.

5.3.1 A sociological perspective: Crossing "Personal Borders"

The model introduced by Gary T. Marx in [Mar01] deals with the concept of "crossing personal borders", i.e. privacy violation occurs when "personal

borders” of an individual are crossed. The author provides a classification of privacy-violating scenarios, analyzes the privacy concerns of individuals and considers the impact of technological advance on privacy as well.

The core idea of the model is depicted in Figure 5.2 and consists of "personal borders crossings", which can happen under the following conditions [Mar01]:

- *Crossing a "natural" border.* The threat is imposed by "[...] tools that extend the senses and make the imperceptible or meaningless perceptible [...]". There exist several "subtypes" of "natural border crossing":
 - clothes that protect parts of the body from being revealed ("nakedness");
 - observable facial expressions, statements or behavior, as against inner thoughts and feelings ("masks");
 - covert surveillance in private places – the assumed non-observability of behavior behind walls, closed doors, etc.;
 - communication privacy violation – when the content of "directed communications" such as a sealed letter, telephone and e-mail messages, which are sent to a particular person with physical protections to exclude consumption by other than the addressee ("wrappers"), is exposed to a third party.
- *Crossing a "social" border* – erroneous expectations of faithful adherence to a certain social role, violation of confidentiality in social interactions, e.g. a doctor or a priest revealing personal information that is supposed to be known only to them.
- *Crossing a "temporal" border* – separation of information pieces referring to various periods or aspects of one's life. For instance, the isolation of elements of personal biography (including the past and the future).
- *Crossing a "spatial" border* – separation of information pieces referring to different locations (e.g. activities in two different cities), as well as their individual visibility.
- *Loss of ephemeral communication* – a personal border can be crossed in case when the individual's assumption about the transitive and ephemeral nature of interaction and communication does not hold true, i.e. concealed surveillance takes place (e.g. hidden video or audio devices are present).

In his paper [Mar01], Marx claims that "[...] the technology may create new opportunities for each of these border crossings". He argues that with the current pace of technological development, privacy concepts of the past are rapidly becoming outdated, which *blurs the boundary* between the "public" and the

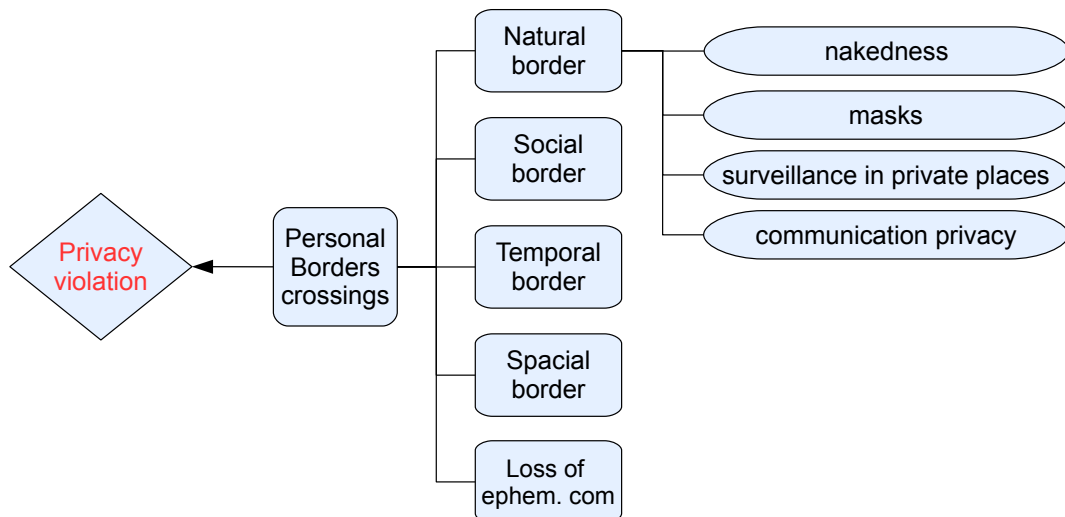


Figure 5.2: Personal borders crossings and privacy violation according to Gary T. Marx [Mar01].

”private” and paves the way to privacy violation scenarios. He also stresses that ”New technologies can be an important factor in altering the structural conditions and contexts within which individuals make their interpretations [of individual privacy]”.

This is related to the idea mentioned in [JA03]: ”Pervasive computing technologies challenge those [social] norms because they often access information that has long been deemed to fall within the scope of individual privacy”.

Marx’s model can be generalized by an abstract societal concept of privacy perception outlined in [Hen08]. It describes a general scenario when individual privacy is violated, see Figure 5.3.

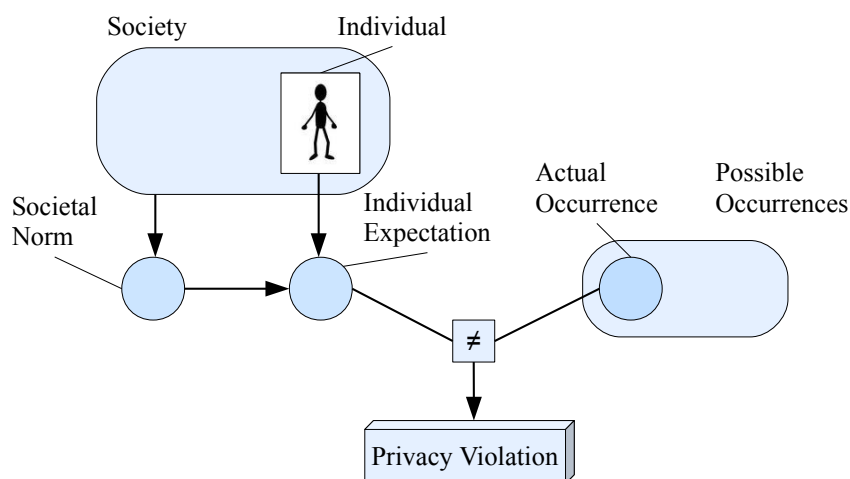


Figure 5.3: Privacy violations take place when occurrence and expectation do not match. Based on [Hen08].

The individual’s expectation of privacy is highly influenced by social norms, specific traditions within the individual’s social environment as well as his/her

value system. "A person's individual expectation is the measurement scale for privacy violation: under all the things that could happen ("possible occurrences" in Figure 5.3), the actual event is rated using the individual expectation". Therefore, a privacy violation in a general sense occurs when an individual expectation of a certain privacy-critical event does not match its actual occurrence (represented by the \neq sign in Figure 5.3).

A short summary

The presented concept of "personal borders crossings" considers privacy modeling from a sociological perspective. This approach can be used for covering privacy issues in a technical system, see privacy modeling from a technical perspective in Section 5.3.3.

A sociological privacy model, like the one created by Marx, elaborates on the issues of privacy perception in society, which needs to be considered in a full-fledged privacy management solution. However, it is unlikely to cover an important question of privacy compliance of a future system (i.e. if the developed system is going to be compliant with current privacy regulation). Therefore, in order to consider privacy in a holistic way, a legal perspective needs to be taken into account as well, which is presented in the next section.

5.3.2 A legal perspective: A Taxonomy of Privacy-invading Activities

As an example of privacy modeling in the legal domain, a Taxonomy of Privacy-invading Activities developed by Solove can be taken [Sol06]. It provides for a taxonomy of privacy and focuses on various activities that invade privacy of an individual: information collection, information processing, information dissemination, and invasion. The model consists of a data subject (an individual) and data holders (who collect, process and disseminate private information), see Figure 5.4. Similarly to Marx (see the sociological privacy model, Section 5.3.1), the author recognizes the influence of technological advance on privacy as well and states that "[...] a new taxonomy to address privacy violations for contemporary times is sorely needed" [Sol06]. A detailed list of privacy-invading activities according to Solove can be found in Appendix B.

This taxonomy enables to consider the notion of privacy from the perspective of law and can be utilized in legal processes involving privacy violation.

While considering legal cases, it is important as well to take various technical details into account, which are a part of a technical testimony¹. In [JA03],

¹The means of computer forensics are typically used in this case.

the following factors were listed, which help to determine whether privacy violation has happened or not:

- The physical nature of the input stimulus, i.e. which physical phenomena (like sound and radio waves propagation) might have contributed to privacy violation¹ (e.g. radio waves are succumb to tapping);
- The location from which the input stimulus originates (i.e. does the stimulus come from a public place, e.g. a store, or it comes from a private place, e.g. from home);
- The location of the sensing device (i.e. the place of the sensing device's deployment);
- How the system detects the input stimulus (i.e. the mechanism of input stimulus detection, e.g. sensor's passive waiting for a stimuli or sending out an excitation signal that might cross into a private space);
- The granularity of the information produced (does the obtained information provide details about the private event or just a basis from which an inference can be made).

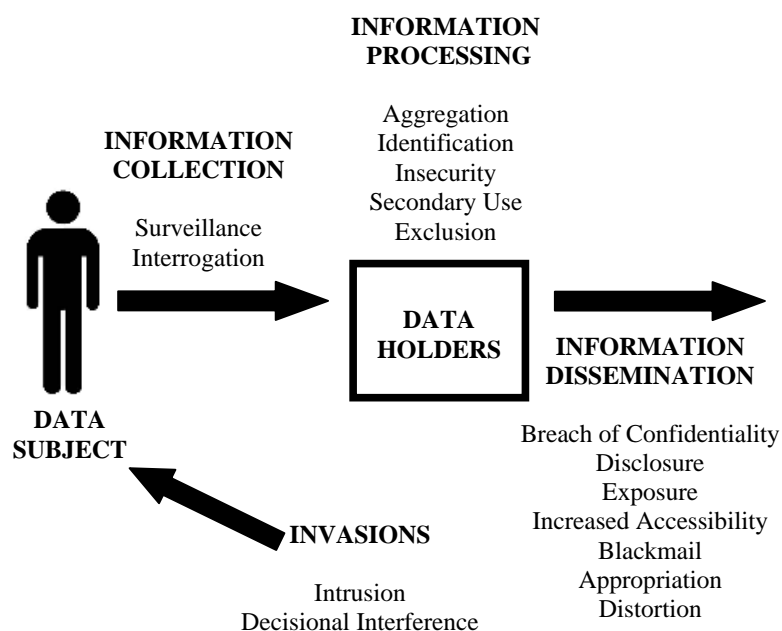


Figure 5.4: Privacy invading activities (described in more detail in Appendix B). Taken from [Sol06].

Privacy modeling in the legal domain covers the important issues of privacy regulation and its legal enforcement (see Section 3.4.1), which consequently affect eventual privacy compliance of the developed system. It is, however, difficult to incorporate legal privacy models into the holistic process of privacy

¹For example, in *Katz v. United States* case [Ins67], the court decided that there was a privacy interest in the sound waves produced by speech [JA03]. That influenced the ultimate decision of recognizing that communication privacy (see Section 3.3.2) of Katz had been violated.

modeling performed by the Privacy Engineer (PE) since most of the legal definitions are often vague and need disambiguation¹. Moreover, privacy laws, which are the basis of legal privacy enforcement, are well specified and documented but quite often coarse-grained, inflexible, and failing to keep up with the technological advance.

Nevertheless, it is of high importance to consider privacy from a legal perspective since it determines privacy compliance of the developed system, which in turn affects its possible certification (e.g. through the utilization of the PIA framework, see Section 3.4.1) and consequently determines its acceptance among users.

Therefore, the PE has to be aware of the current legal regulation and develop privacy requirements accordingly. The next section discusses privacy modeling from the technical perspective, which often utilizes the concepts encapsulated in privacy models originating from sociology (Section 5.3.1) and law (the current section) for approaching the problem of privacy management in the underlying technical system.

5.3.3 Privacy modeling from the technical perspective

Privacy models developed in the technical domain aim at reflecting certain privacy aspects relevant to the specific system² in the underlying privacy management mechanisms (implementing the respective privacy requirements). For example, enabling the support of legal obligations fulfilment, such as obtaining the explicit user consent before forwarding the previously collected personal data to a third party (e.g. for additional processing) and rendering it impossible to bypass this measure unless a special case arises (e.g. police investigation with a warrant).

Within this section, a review of several privacy models developed from a technical perspective is provided together with assessment and discussion of their applicability to RFID.

Information Spaces

The sociological concept of "personal borders crossing" discussed in Section 5.3.1 can be utilized for privacy modeling in the technical domain. For

¹The definitions of privacy-invading activities in Solove's model listed in Appendix B can be ambiguous in some cases. For example, it is not clear which government actions towards an individual can be regarded as "decisional interference" (incursion into individual's private affairs causing privacy violation) and which should be treated as legally justified due to e.g. national security reasons.

²Since privacy is a broad notion requiring an interdisciplinary approach for its holistic consideration, a palliative solution is often used, which solely considers the most important privacy aspects prescribed, for example, by law (without which the developed system is simply not going to be certified for public use).

example, the authors of [JL02] developed a theoretical model for privacy management in context-aware systems, which is based on the core abstraction of *information spaces*. The boundaries of information spaces are related to the "border crossings" of Marx. According to [JL02], an information space provides for organizing information, resources and services around "important privacy-relevant contextual factors" in context-aware systems. It is "a semantic construct around which you can formulate a privacy control policy". The concept of a *boundary* delimits an information space and resembles the notion of the border in Marx's model. The authors describe several types of boundaries:

- *A physical boundary* – demarks an information space using physical limits, e.g. an information space of a private office.
- *A social boundary* – delimits an information space between different social groups, e.g. an information space for family members.
- *An activity-based boundary* – delimits an information space by including only the information relevant to a certain activity, e.g. a meeting being attended by the information space owner.

Different types of boundaries and their relation to a certain information space are depicted in Figure 5.5.

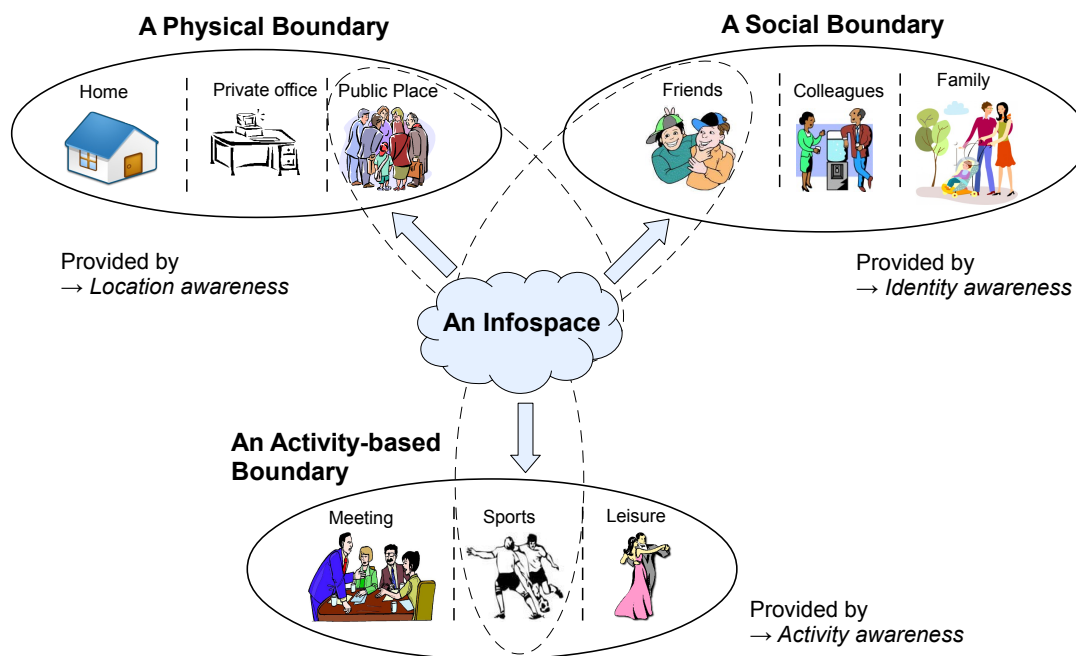


Figure 5.5: Different types of boundaries delimit an information space. Based on [JL02].

Figure 5.5 depicts how an information space can be defined through three different types of boundaries, for example, playing football (an *activity* boundary) with friends (a *social* boundary) on a public football field (a *physical* boundary).

An information space can be seen as a tuple consisting of five elements: a set of objects representing information or resources, O , a set of principles who own the space, P , a boundary predicate¹, B , a set of allowable operations on objects², Op , and finally a set of permissions, $Perm$. In a short form:

$$\text{infospace} : (O, P, B, Op, Perm).$$

In order to identify the boundaries, context-aware technologies are utilized (e.g. location determination in case of a physical boundary). This is depicted in Figure 5.5 as location, identity, and activity awareness respectively. Therefore, the authors of [JL02] claim that their model enables to "formally capture the [Marx's] borders" utilizing the abstraction of boundaries and consequently to identify when an undesirable border crossing occurs. "A trusted privacy runtime system" can then decide if certain data can be released upon a border crossing, control its granularity and conditions of such data exposure (e.g. to delete the data after the meeting).

The authors further extend their model of information spaces by introducing the concept of unified privacy tagging³, which uses metadata to identify an information space to which an object belongs and to assign the respective permissions. Every object in an information space is associated with a privacy tag, which is comprised of:

- *A space handle* – specifies the information spaces the object belongs to;
- *A privacy policy specifier* – represents permissions assigned by the information space owner for different types of operations;
- *A privacy property list* – describes an object's lifetime (e.g. the data should be deleted after the business meeting), representational accuracy (data granularity) and capturing confidence (the probability that a sensor's measurement reflects the actual object value).

Therefore, a privacy management solution presented in [JL02] utilizes a concept of infospaces (based on Marx's "personal borders crossings"), context-aware technologies for boundaries identification ("capturing the Marx's borders"), which enable to recognize when an undesirable border crossing occurs, and finally a "trusted runtime system" in conjunction with privacy tagging for privacy enforcement.

Concerns arise, however, in case the trustworthiness of the software component that processes the metadata (the information contained in the privacy tag) is put in question. Robust authentication mechanisms with utilization of tamper

¹Refers to the type of a boundary, i.e. a physical, social, or an activity-based one.

²A set of operations which are allowed in a certain space apply to all objects in this space.

³Privacy tagging is similar to the sticky policy paradigm discussed in [KSW03].

resistant modules can mitigate this problem, which at the same time inevitably increases the costs.

The privacy model based on information spaces was subsequently implemented within the Context Fabric (Confab) infrastructure for privacy-sensitive Ubiquitous Computing [HL04].

Modeling privacy utilizing abstractions similar to information spaces was performed by other research teams as well. The concepts of "virtual walls" [K⁺07a] and "bubbles" [BH07] outlining and delimiting the borders of a "digital territory" of an individual aim at extending the conventional physical measures of protecting privacy to the digital world of context-aware ubiquitous applications.

For privacy enforcement in the dynamic and context-aware UbiComp environment, fine-grained access control and authorization mechanisms are commonly used, which utilize the privacy-relevant contextual factors (such as location, communicating entities, etc.).

The next reviewed model utilizes a similar approach to privacy enforcement and was initially created for enterprise privacy management.

A Privacy Policy Model for Enterprises

The authors of [KS02] developed a privacy policy model which is oriented towards enterprises and aims at protecting personal data by enforcing enterprise-wide privacy policies through authorization management and context-dependent access control. In a privacy management system, which utilizes this privacy policy model, it was technically enforced that personal information is used only for authorized purposes defined by the privacy policy. In order to be able to clearly and unambiguously interpret the privacy policy, a privacy control language was developed, which additionally provides for decoupling from any particular implementation of the underlying privacy protecting system. The created privacy control language includes user consent, obligations, and distributed administration. Obligations are comprised of a set of activities that must be executed on each access request to personal data. The notions of user consent and obligations originate from law and can therefore be adopted from a legal privacy model, like the one described in Section 5.3.2.

In the privacy management system described in [KS02], users are organized in groups, which in turn build up a group hierarchy with different authorizations and access rights. The personal data circulating in the system are categorized according to the linkability to their owner ("the data subject"): personally identifiable information (PII), "depersonalized" information (can be linked if addi-

tional information about the individual is known, e.g. his/her pseudonym), and anonymized information, which is supposed to be unlinkable to the individual.

Purpose-binding – "a basic privacy principle" – is implemented in [KS02] by structuring the intended use of the collected data into categories called "purposes". Privacy statements may additionally require that certain conditions need to be satisfied before access to personal data is granted. Therefore, together with purpose binding, conditions check is performed on each access request.

The concept of obligations is used within the model in order to ensure that the necessary actions are performed after granting access to personal data. For example, properly maintaining the data retention period. Moreover, obligations can be used for modeling situations involving user's consent. For instance, when the obtained personal information is going to be shared with a third party, the respective obligation specifies that it may only be done if the explicit consent of an individual has been obtained. In case certain personal data, nevertheless, are to be disclosed to authorities even without the user's consent (e.g. for legal reasons), the system is obliged to notify the information owner (referred to as notification in the model).

There are two main types of users that can be distinguished with regard to access rights to personal data:

- *Owners*. The users who have provided their data to the system and are granted the rights to make any changes to them by default;
- *Users*. The persons who do not own the submitted information and process it for business purposes, if granted the respective rights (usually they are the employees of the enterprise).

Depending on the privacy policy, additional user types (or roles) can be introduced. For example, a *Guardian* type representing a person whose permission is needed in order to enable the processing of personal information of a minor (a *Minor* type respectively).

Authorizations are expressed using an authorization specification language (ASL), which specifies both direct authorizations (*cando*) and authorizations derived by the system using logical rules of inference (*dercando*). There exist several authorization modes: read, write, delete, disclose, activate. They represent which actions are allowed to be performed on personal data. An example of the direct authorization together with a condition and obligation rule can be the following: users can change all their personal information under no obligations (expressed as default in the obligations tuple), which is formally expressed

in the following way¹:

$\text{cando}(\text{personalinfo}(id), u, + \text{write}, [\text{obligation} = \text{default}]) \leftarrow \text{owner}(id, u).$

Literally expressing the authorization rule above: direct authorization (*cando*) for modification (*write*) of personal information (*personalinfo*) of the user (*id*) under no obligations (*obligation = default*) is granted if the user (*id*) is an owner of this information (*owner*).

Basic features of this privacy model are depicted in Figure 5.6.

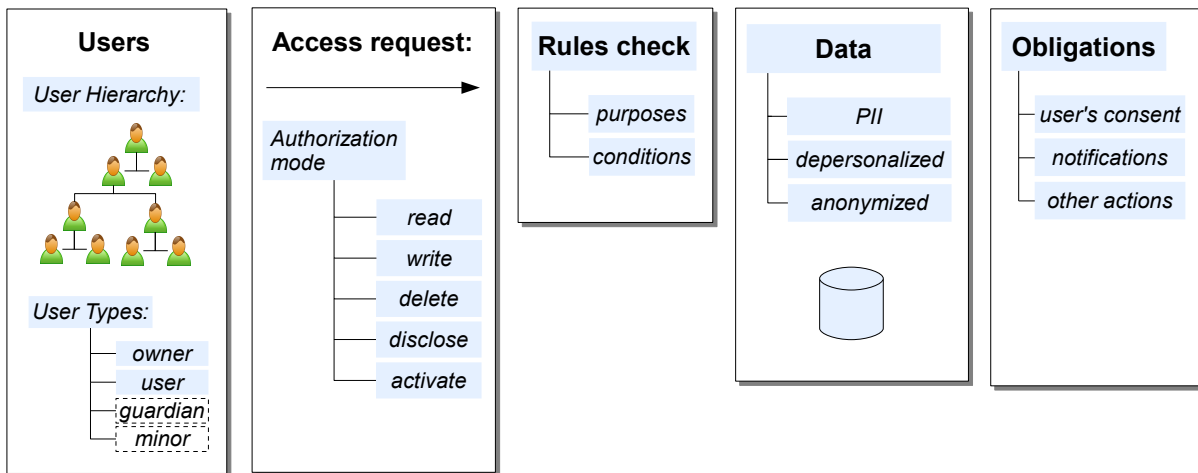


Figure 5.6: Basic components of the Privacy Model for Enterprises. Based on [KS02].

The authors of [KS02] claim that their privacy policy model is the first one that combines user consent, obligations, and distributed administration. It is a good example of how a privacy policy of an enterprise can be expressed using a privacy control language and enforced by the utilization of authorization modes, conditions, obligations and purpose binding. Moreover, the support of obligations and purpose binding enables to consider the legal perspective of privacy (see the legal privacy model in Section 5.3.2) therefore providing for a multi-disciplinary approach.

Whereas it is a well-defined and decent model, it does not take into account the peculiarities of privacy management in ubiquitous RFID systems discussed in Section 3.3.3. Numerous unobtrusive end devices in the RFID domain are very unlikely to constantly stay under control of a single enterprise. For example, RFID tags can be woven into garments during the production process. As soon as they leave the factory and are purchased, the enterprise is no longer controlling the operation of RFID tags and can not provide for an adequate protection of consumers' privacy. Therefore, a privacy model for such a system

¹The sign " \leftarrow " implies the "if ... then" construct like the one in propositional logic. The arrow points from the if predicate the consequent then.

should take into account and ensure, for instance, that the tags are *permanently* deactivated after the purchase even though it might impede the procedure of returns tracking.

Moreover, the issues of privacy perception by individuals need to be considered together with the implications of the underlying technical system, which determines how privacy requirements are ultimately interpreted and enforced. Referring to the above mentioned example: an expectation that an individual's location and identity stay private can be mapped to the requirement that a tag is either destroyed after the purchase or that it will answer only those queries containing a special "unlock key"¹. Furthermore, specific threats to privacy imposed by the underlying system (see Section 3.3.3) and its security peculiarities² (see Section 3.5) need to be considered as well while designing a privacy model for RFID systems.

Despite the aforementioned shortcomings, the privacy model presented in [KS02] can nevertheless provide the Privacy Engineer (PE) with the necessary basis for privacy modeling in the RFID domain, namely:

- The ways of treating privacy in a multi-disciplinary way (the support for user consent, obligations, and purpose binding);
- The utilization of a privacy control language for expressing privacy requirements;
- Privacy enforcement using flexible access control mechanisms together with distributed administration, authorization modes, conditions, obligations, and purpose binding.

Similarly to the privacy model described in [KS02], the authors of [FHO98] presented a formal task-based privacy model, which was developed to enable technical enforcement of legal privacy requirements. In this case, the privacy policy was specified and implemented utilizing the approach of the Generalized Framework for Access Control (GFAC)³. The authors focused on providing the support for legal privacy requirements in the technical system, therefore considering privacy issues of a system in an interdisciplinary manner, namely from the technical and legal perspectives. The sociological implications of privacy described in Section 5.3.1 were not considered, however. Since the perception of privacy by an individual is strongly influenced by societal norms, it is important to take the sociological perspective of privacy into account while designing a privacy model (as it was partially done in the Information Spaces model, see

¹The concept of "unlock keys" was described in [WSRE03].

²Security enables to technically enforce privacy, see Section 3.4.1.

³GFAC was described in [LP90]

Figure 5.5). Moreover, similarly to the Privacy Model for Enterprises described above, the task-based privacy model of [FHO98] does not take into account the specific threats to privacy and security inherent in the underlying ubiquitous RFID systems.

The authors of [Vau07], on the other hand, provided for a detailed privacy model for RFID systems considering specifics of their operation, namely limited memory and computational capabilities, the ability of physical interference (an RFID tag is not tamper proof and can be corrupted). Depending on the adversary capabilities, several attacker models were developed. The authors used their model to assess the ability of tags to resist the possibility of unsolicited identification, tracing and linking.

Despite the fact that this model was specifically targeted at RFID systems, it focused only on implications of the respective identification protocols. Providing formal definitions of privacy and security from this perspective and their detailed assessment, it did not take into account other important issues influencing the privacy of the users, such as physical implications of RFID tags with regard to privacy (see Section 3.3.3) and the possibility of implementation attacks (see Section 3.5.2 and Appendix A), to name a few. Furthermore, formally considering privacy in a rather narrow way, the authors did not provide for an interdisciplinary approach. Therefore, neither the implications of privacy perception by individuals (the sociological perspective) nor the issues of legal privacy regulation (the legal perspective) were taken into account.

The next section summarizes the reviewed privacy models and provides for the comparative analysis with regard to their applicability to the RFID domain.

5.3.4 Privacy models: a short summary

Table 5.1 provides for a concise comparative analysis of the reviewed privacy models.

Having conducted a review of existing models which consider privacy from different perspectives (sociological, legal, and technical), a conclusion can be made that neither of them fully reflects the problems of privacy management in RFID systems. However, combining the main concepts reflected in each of the reviewed models, provides the Privacy Engineer (PE) with the necessary basis for developing a privacy model targeted specifically at the RFID domain, namely:

1. Treating privacy as a multi-dimensional issue by considering the specifics of privacy perception in society (using the main concepts of Marx's sociological model, #1 in Table 5.1) and taking into account the implications

of legal regulation (can be adopted from the "Privacy-invading Activities" model, #2).

2. Bridging the aforementioned issues with the technical domain as it was done in technical privacy models (#3 and #4 in Table 5.1 respectively):
 - a) The utilization of the semantic construct of "Information Spaces" (#3) for capturing the "Personal Borders" described by Marx (#1) through the context-aware technologies (e.g. location determination, etc.).
 - b) Interpretation of the privacy policy can be performed using the privacy control language described in [KS02] (#4).
 - c) In order to identify the respective permissions for the Information Space, privacy tagging can be used in conjunction with a "trusted privacy runtime system"¹ as it was done in [JL02] (model #3).
 - d) Considering the legal issues by utilizing the notions of user consent, obligations, and purpose binding (specified through the privacy control language in [KS02], model #4).

Table 5.1: A comparative analysis of different privacy models.

#	Privacy model	Perspective	Relevance to RFID	Interdisciplinary approach	Main features
1.	Crossing "Personal Borders" [Mar01]	sociological	low	technical and legal issues are partially considered	Privacy perception by individuals; classification of privacy-violating scenarios using the concept of crossing "personal borders".
2.	Privacy-invading Activities [Sol06]	legal	low	technical issues are considered (partially comprising technical testimony) as well the social implications of privacy	Describes the activities that invade privacy of individuals, considers privacy violation from a legal perspective.
3.	Information Spaces [JL02]	technical	medium	implications of the sociological model of privacy (crossing "personal borders") are considered	Uses a concept of Information Spaces, which relates to the "personal borders" of the sociological model (#1); is claimed to provide for context-aware privacy management; utilizes "unified privacy tagging".
4.	A Privacy Policy Model for Enterprises [KS02]	technical	low	legal requirements were considered (through the concepts of user consent, obligations, and purpose binding)	Enforcement of the privacy policy of an enterprise through authorization management and context-dependent access control; development of a privacy definition language (considers user consent, obligations, and distributed administration).
5.	A Formal Privacy model for RFID [Vau07]	technical	high	not considered	Formally treats privacy implications of tag identification protocols in RFID; takes the peculiarities of RFID interface into account; is, however, fairly narrow.

¹This can be implemented in the RFID back-end.

Possessing the necessary basis for considering privacy in a multi-disciplinary fashion, the PE can add specific requirements pertaining to the RFID domain, which originate from the peculiarities of privacy management (discussed in Section 3.3.3), privacy enforcement (see Section 3.4) as well security related issues (Section 3.5) of RFID systems. The recommendations for designing a privacy-respecting RFID system described in Chapter 4 are going to determine the specific privacy requirements as well.

In the end, a holistic privacy model should therefore represent:

1. The privacy requirements of individuals who are the users of the system (issues of privacy perception by individuals (the sociological perspective));
2. The privacy implications of an underlying technical system (specific threats to privacy and security¹ which have a profound influence on privacy management in an RFID system);
3. Legal privacy requirements imposed by privacy regulation (the legal perspective);
4. Privacy requirements of an enterprise, which uses the RFID system for its business together with the additional measures that might be required for its certification (that influence the privacy policy of an enterprise as well), such as privacy assessment via the PIA framework (see Section 3.4.1).

5.4 Chapter summary

Within this chapter, the privacy modeling approach for privacy requirements engineering was presented. The motivation for using privacy models together with the suggestion of their utilization in the underlying privacy management system was discussed. In order to provide for the state-of-the-art view on this issue, several privacy models originating from different scientific domains (namely, from sociology, law, and technology) were reviewed and the assessment of their applicability to RFID was performed. The chapter concludes with the recommendations for developing a holistic privacy model for the RFID domain.

Creation of a privacy model provides the Privacy Engineer (PE) with a high-level and holistic view on privacy management in the RFID system under development. In order to implement the requirements represented by the model, they have to be inferred from it and consequently transformed into the implementable format. This can be done within the framework discussed in the next chapter.

¹Security in this case can be seen as the enabler of technical privacy enforcement.

6 Inferring implementable systems requirements from privacy models

Having created a privacy model for the target RFID system (as it was described in the previous chapter), it is necessary to obtain the respective privacy requirements from it, which in turn can be implemented in the underlying privacy management system. In this chapter, an approach to enabling the requirements inference from privacy models is discussed. It consists of the Framework for Transforming Abstract Privacy Models into Implementable UbiComp System Requirements outlined in our paper [GBP11a] which is further extended within the master thesis.

An overview of the framework is provided in Section 6.1. Further elaboration on this issue with the respective discussion is performed in Section 6.2. The use case validation of the suggested solution is presented in Section 6.3. Section 6.4 summarizes the chapter.

6.1 A framework for privacy requirements transformation: an outline

In order to provide a solution to the task of privacy requirements inference (from the created privacy model) in a consistent and determined way, the framework described in [GBP11a] can be used. Its main idea is similar to the meta-modeling approach extensively used in programming, which implies the process of transforming abstract models (platform independent) into the models which can be implemented in the target system (platform specific)¹ [AZW06]. This framework is intended to be used by the Privacy Engineer entity (PE, see Figure 4.3 on page 64), who is responsible for creation of the respective privacy model with subsequent requirements inference. The approach encompasses three main steps, depicted in Figure 6.1:

1. Creation of the privacy model according to the principles discussed in the previous chapter, see Section 5.3.4. Within the framework, this model is referred to as the "abstract privacy model" since it is system- and platform-independent. The latter implies that the abstract privacy model created for

¹For example, a transformation process like: meta-metamodel → metamodel → model.

the specific domain (in this case, for the RFID one) is nevertheless decoupled from the concrete underlying privacy management system (system-independent) as well as from the specific implementation platform (therefore, platform-independent).

2. During the second step, a consistent transformation of the abstract privacy model (created during the previous step) into a set of system-specific requirements is performed together with the refinement procedure, which aims at tailoring the abstractly represented privacy requirements of the privacy model to the specific underlying system. It is important to determine which requirements can not be fully supported by the underlying privacy management system¹ since it introduces inconsistencies between the privacy requirements expressed in the model and the ones which are going to be technically supported. In this case, it is required that inconsistencies are registered for a further review and resolution by the PE, whose task is to determine alternative ways of expressing a certain set of requirements (e.g. choosing another encryption algorithm requiring a shorter key) or recognizing it as unimplementable by technical means. In the latter case, a legal privacy enforcement (see Section 3.4.1) can be used as a palliative measure to tackle the problem. If the current legal regulation renders it impossible as well, this should be clearly notified for providing the respective feedback to the users (making them aware of certain privacy gaps).
3. The last step considers the actual implementation of the obtained requirements (therefore, it is system- and platform-specific).

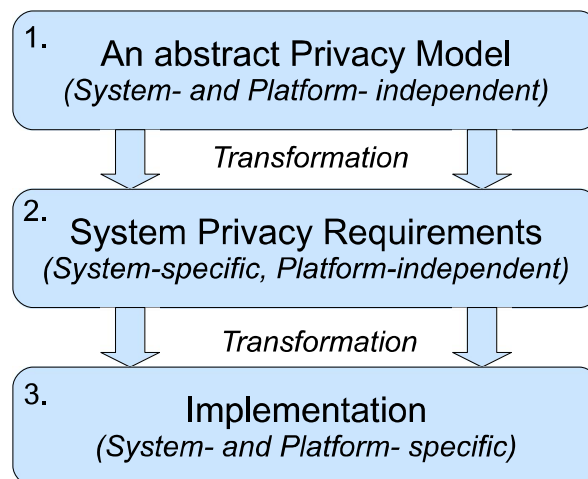


Figure 6.1: A Framework for Transforming Abstract Privacy Models into Implementable Requirements: a general structure. Published in [GBP11a].

¹For example, asymmetric encryption with a substantial key length (e.g. 2048-bit RSA keys) due to resource limitations on the tag side.

6.2 A framework for privacy requirements transformation: elaboration

6.2.1 Step 1: An abstract privacy model

The first step of the framework outlined in the previous section implies the creation of an abstract privacy model, which is decoupled from the underlying implementation of a privacy management system. This provides the Privacy Engineer (PE) entity with a high-level and *holistic* view on relevant privacy issues originating from various scientific domains therefore enabling a multi-disciplinary approach to privacy management. During the step 1, it is rather specified what *should* be considered in order to make the system under development privacy-respecting than which requirements *can* actually be supported by the underlying privacy management system (i.e. subsequently implemented providing technical privacy enforcement).

Therefore, it can be ensured that the whole set of privacy implications (\mathbb{R}_{gen}) relevant to the current domain (in this case, RFID) is considered. In order to perform this, the PE can use the information on privacy implications of RFID systems and peculiarities of privacy enforcement in this domain covered in sections 3.3.3 and 3.4 of the master thesis respectively.

6.2.2 Step 2: System-specific privacy requirements

The requirements developed during the first step (\mathbb{R}_{gen}) need to be further: (1) tailored to the specific underlying privacy management system (requirements refinement) and (2) properly formalized, in order to enable their subsequent implementation.

Sub-step 2.1: Requirements refinement

The outcome of this sub-step is a set of *implementable system requirements* (\mathbb{R}_{imp}) and, respectively, a set of requirements that can not be implemented in the underlying privacy management system (\mathbb{R}_{-imp}). Therefore, if \mathbb{R}_{gen} is the set of requirements created during the previous step 1, then the following holds true¹:

$$\mathbb{R}_{gen} \rightarrow \mathbb{R}_{imp} + \mathbb{R}_{-imp}.$$

For example, a requirement that the identity of a tag (e.g. tag id) is revealed only to legitimate parties (expressed in the abstract model, the 1st step of the framework), can be mapped to the requirement that the tag answers only to

¹The \rightarrow operator signifies the mapping operation, i.e. how a certain set of privacy requirements of the higher level (step 1) is transformed to the more specific one at the lower level (step 2).

those queries possessing a special key (e.g. adheres to the "unlock key" concept discussed in [WSRE03]). That imposes further constraints on the domain of end devices, namely the requirement that RFID tags must be capable of performing the respective cryptographic operations (key checks, etc.). In a formal way, it can be expressed as follows:

$$\mathbb{R}_{gen}^{reveal_id} \rightarrow \mathbb{R}_{imp}^{hash_lock} \wedge \mathbb{R}_{imp}^{crypto_ability}.$$

In order to mitigate the problem of pervasive availability of personally identifiable information (PII) discussed in Section 3.3.3, the abstract privacy model (step 1) may require to provide support for tags shielding. However, in certain cases it might not be possible, for instance, if RFID tags are woven into clothes and hence are partially distributed over the garment's surface. Therefore, the PE registers the requirement which can not be backed up by the underlying privacy management system for a future review: $\mathbb{R}_{-imp}^{shield}$. During the review process, this requirement can be either substituted by another implementable one with a similar effect (e.g. permanently destroying the tag after purchase¹) or, if it is not possible, be marked as eventually unimplementable (by technical means). In such a case, the PE needs to find a palliative solution using, for example, legal privacy enforcement (\mathbb{R}_{legal}) discussed in Section 3.4.1. If, however, this is rendered impossible as well by privacy regulation (i.e. the issue is uncovered by law), it should be carefully registered and explicitly mentioned in the system documentation in order to make the future end user aware of the relevant privacy gaps. This type of privacy requirements, which can be neither ensured by technical privacy enforcement nor mitigated using the legal one, is called *residual* (\mathbb{R}_{res}) within the framework and is subject to review² during the subsequent system upgrades.

The aforementioned types of privacy requirements used within the framework constitute the requirements tree depicted in Figure 6.2.

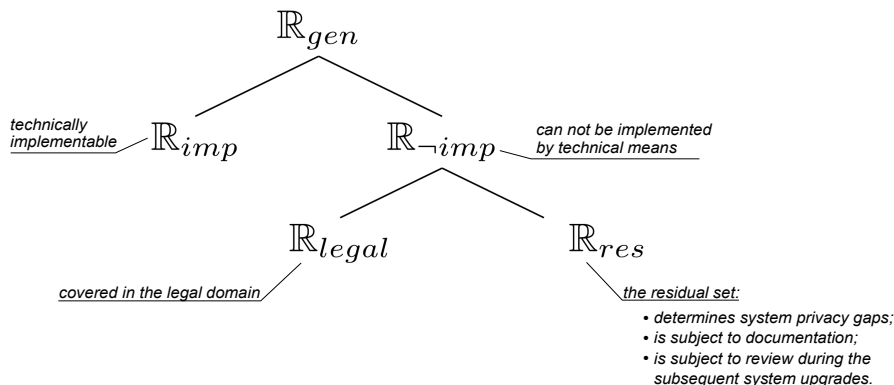


Figure 6.2: The requirements tree used in the framework.

¹This can be done by exposing it to a relatively strong electromagnetic field, for example.

²The review is necessary in order to determine if a certain set of residual requirements can be implemented (at least partially) thanks to system upgrades.

Sub-step 2.2: Requirements formalization

In order to enable the implementation of the refined privacy requirements, they have to be properly formalized, i.e. expressed in a way that allows their implementation. Since RFID systems have a specific structure, the formalization can be divided into two parts (see Figure 6.3):

- Requirements formalization for the RFID back-end;
- Requirements formalization for the RFID front-end.

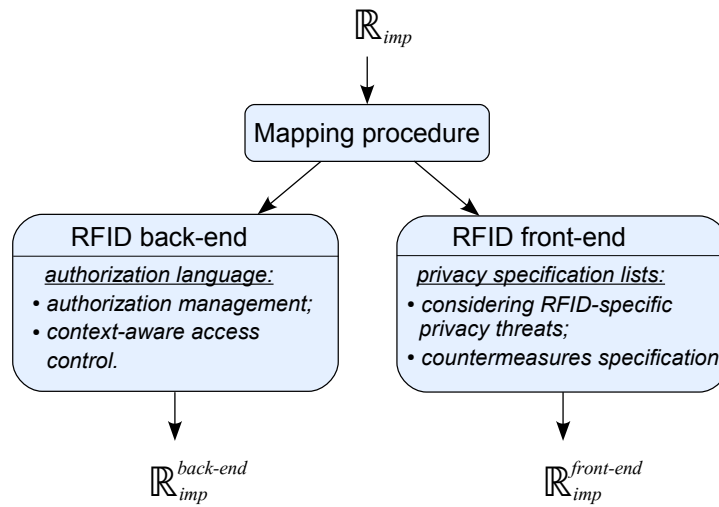


Figure 6.3: The requirements formalization process.

The process of requirements formalization not only enables the created requirements to be subsequently implemented but also fine-tunes and binds them to the specifics of the RFID system under consideration.

Requirements formalization for the back-end: the authorization language

Requirements formalization for the back-end can be performed through utilization of the authorization specification language (ASL) introduced in [KS02] (see Section 5.3.3), which is claimed to have the potential to express the "real world" privacy statements "possibly parameterized by the local country laws". It considers direct and indirect¹ *authorizations* (cando and dercando respectively) together with a set of *authorization modes* (or *actions*):

$$\mathbb{A} : \{\text{read, write, delete, disclose, activate}\}. \quad (6.1)$$

There exist several types of predicates used to express relationships between different elements of the RFID back-end data system:

¹Authorizations derived by the system using logical rules of inference.

1. Predicate $\text{owner}(o, u)$: associates a unique user u with an object o (can be a data item, etc.) therefore rendering him/her the owner of o . Aimed at implementation of the "data subject" concept in the legal domain¹.
2. Predicate $\text{consent}(o, p, u)$: signifies the consent of user u that the object o can be processed for purpose p .
3. Delegation predicate² $\text{isDelegate}(u', u)$: defines that a user u is authorized to act (see authorization modes defined by equation (6.1)) on behalf of the user u' (under certain conditions, e.g. for a specified amount of time, possibly with obligations).
4. Predicate $\text{opt-in}(o, p)$: denotes the opt-in choice, i.e. the data subject consents that the data he/she owns is processed for purpose p . It can be expressed through the predicates #1 and #2:

$$\text{opt-in}(o, p) \equiv \text{owner}(o, u) \wedge \text{consent}(o, p, u).$$

The predicate opt-out is dual to opt-in, therefore:

$$\text{opt-out}(o, p) \equiv \neg \text{opt-in}(o, p)$$

5. Predicate $\text{retentionTime}(o)$: considers the time elapsed (of type duration) since the object o has been stored. It can be used to ensure the compliance with the data retention laws³.
6. Predicate $\text{done}(o, u, a)$: represents events that happened in the past. It is `true` if a user u has executed action a on object o ; otherwise `false`.
7. Predicate $\text{certified}(t, p)$: *certifies* a task t for a certain purpose p . This predicate is used in case the distributed administration by the Privacy Engineer and the Security Engineer is performed (see Section 4.3 and Example 6.1 below).

Obligations are grouped into the *obligations set*, \mathbb{C} , and expressed in terms of *activities* (not to be confused with *actions* in equation (6.1)), such as `notify: u` (user notification) and `anonymize: o` (object anonymization). Therefore,

$$\mathbb{C} : \{\text{notify: } u, \text{ anonymize: } o\}.$$

Moreover, the authorization language considers the sets of *authorization subjects*, \mathbb{AS} , and *authorization objects*, \mathbb{AO} . The former consists of users (together with groups describing the user domains), processes, and purposes. The latter

¹"Data subject is the identified or identifiable natural person to whom the data relate" [Kos11]

²Delegation predicate is a generalization of the delegation concept, which was described in [KS02] solely with respect to young users (minor type) and their legal supervisors (e.g parents, the guardian type).

³In the EU, the Data Retention Directive [Eur06] provides legal guidance for data retention policies.

is comprised of objects, types, and purposes¹. In order to render certain actions (see equation (6.1)) as authorized (+) or denied (−), the *singed actions* set is used: $\mathbb{SA} = \{+a, -a \mid a \in \mathbb{A}\}$. Therefore, an *authorization* is a 5-tuple:

$$\langle o, s, \langle \text{sign} \rangle a, c, g \rangle, \quad (6.2)$$

where $o \in \mathbb{AO}$; $s, g \in \mathbb{AS}$; $c \in \mathbb{C}$; $a \in \mathbb{A}$. The $\langle \text{sign} \rangle$ signifies either "+" or "−". Therefore, a generalized example of a positive authorization is: $\langle o, s, +a, c, g \rangle$, i.e. a subject g authorizes the subject s to perform action a on object o provided that obligation c is followed (i.e. will become true). Figure 6.4 depicts the example.

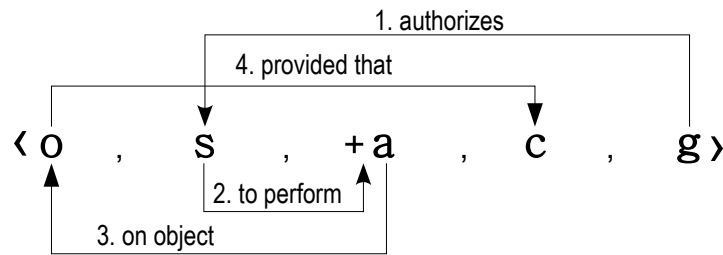


Figure 6.4: An example of a positive authorization.

The Authorization Specification Language (ASL) describes different *rules* which eventually express the access control policy. Rules are asserted according to the conditions which are called *literals* L_n in ASL. An authorization rule therefore is expressed as follows²:

$$\text{cando}(\underbrace{\langle o, s, \langle \text{sign} \rangle a, c, g \rangle}_{\text{an authorization}}) \leftarrow L_1 \wedge L_2 \dots \wedge L_n, \quad (6.3)$$

where $L_1 \wedge L_2 \dots \wedge L_n$ are literals, $n \in \mathbb{N}$, and *cando* signifies direct authorization. The other constituents comprise an authorization 5-tuple described by equation (6.2).

The following example demonstrates how different authorization rules can be expressed in ASL.

Example 6.1.

1. Providing the data subject with control over his/her personal information:

$$\text{cando}(\text{p_info}(id), u, + \text{write}, \underbrace{[\text{default}], \text{PE}}_{\text{obligation}}) \leftarrow \text{owner}(id, u).$$

The PE authorizes (+) the user u to change (write) his/her personal in-

¹Purposes reside in \mathbb{AO} set as well since they can be assigned to *subjects* (\mathbb{AS} set) as it is done in equation (6.4).

²The sign " \leftarrow " implies the "if ... then" construct like the one in propositional logic. The arrow points from the if predicate to the consequent then.

formation (p_info) under no obligations (expressed as $[default]$) provided that the user owns this information, i.e. is the data subject ($owner(id, u)$).

2. Rendering personal data inaccessible after a certain time, for example, for fulfilling the requirement of data retention period¹ (e.g. not more than 2 years according to the Data Retention Directive in the EU [Eur06]):

$$cando(o, s, -read, [default], PE) \leftarrow retentionTime(o) > 2Y.$$

The PE prohibits ($-$) any subject s from accessing (read) the object o if the time elapsed from the last successful access to it ($retentionTime(o)$) is more than 2 years.

3. Disclosure of personal information for statistical purposes is allowed only in anonymized form and provided that a user has explicitly consented to such kind of action (i.e. has opted-in):

$$cando(o, stat, +disclose, [anonymize : o], PE) \leftarrow opt-in(o, stat)$$

The PE authorizes ($+$) the statistics subject ($stat$) to gain access (the disclose action) to personal information (o) in anonymized form only (obligation $[anonymize : o]$) provided that the data subject has explicitly consented to this action ($opt-in(o, stat)$).

Furthermore, ASL allows to perform authorizations assignment in a distributed way, namely by the Privacy Engineer (PE) and the Security Engineer (SE) entities. In order to enable the process of distributed authorization, the separation of duties between the Privacy Engineer (PE) and the Security Engineer (SE) is performed in the following way. Data (o) can be accessed only for a clearly defined purpose (p), which is authorized by the PE to perform a certain action (action) on o , provided that a data subject has given explicit consent that the data is processed for this purpose ($opt-in(o, p)$). The PE then *certifies* a task t to act for the purpose p ($+certified(t, p)$). Lastly, the SE authorizes a user u to execute the task ($+x$). In this case, the *execute* action, x , is added to the actions set \mathbb{A} (equation (6.1)). Provided that $opt-in(o, p)$ evaluates to `true`, the procedure of distributed administration can be depicted as follows:

$$\begin{array}{ccccccc} \text{object} & & \text{purpose} & & \text{task} & & \text{user} \\ \{o\} & \xleftarrow[\text{(auth: PE)}]{\text{action}} & \{p\} & \xleftarrow[\text{(cert: PE)}]{+certified} & \{t\} & \xleftarrow[\text{(auth: SE)}]{+x} & \{u\} \end{array} \quad (6.4)$$

¹This can be achieved provided that the data rendered inaccessible will be eventually garbage-collected [KS02], i.e. deleted.

For example:

$$\text{cando}(\underbrace{o}_{\text{data}}, \underbrace{stat}_{\text{purpose}}, \underbrace{+read}_{\text{action}}, [\text{anonymize} : o], \text{PE}) \leftarrow \text{opt-in}(o, stat) \quad (a)$$

$$\text{cando}(\underbrace{stat}_{\text{purpose}}, \underbrace{t}_{\text{task}}, +\text{certified}, [\text{default}], \text{PE}) \quad (b)$$

$$\text{cando}(\underbrace{t}_{\text{task}}, \underbrace{u}_{\text{user}}, \underbrace{+x}_{\text{execute}}, [\text{default}], \text{SE}) \quad (c)$$

- (a) The purpose *stat* is authorized by the PE to access (+read) personal information (*o*) in anonymized form (the obligation *anonymize : o*) provided that consent of the data subject has been obtained (*opt-in(o, stat)*).
- (b) The task *t* is certified by the PE to act (+ certified) for the purpose *stat* (statistics;
- (c) The SE finally authorizes a user *u* to execute (+*x*) the task *t*.

It is assumed that on submitting personal data to the system, a data subject has previously consented to the system privacy policy which implies that the SE assigns the eventual authorizations to execute tasks to the users who need to gain access to personal data. This may be useful when a data subject having submitted certain pieces of personal data in order to e.g. be accepted to the university (the *purpose*) is not aware which employees are going to process his/her personal information. Therefore, having explicitly consented that the data are processed for a *concrete purpose*, the data subject implicitly leaves the further control to the SE and the PE of the organization, who perform the authorization management according to the established privacy policy.

In case it is required that a data subject should explicitly control which users (or user groups) are allowed to perform actions on personal data, an additional condition (in form of a literal, see equation (6.3)) can be added to equation (c) above. It signifies that the data subject has explicitly agreed that a user *u* processes personal data (for the purpose approved by the data subject in step (a)):

$$\text{cando}(t, u, +x, [\text{default}], \text{SE}) \leftarrow \underbrace{\text{opt-in}(o, u)}_{\text{added condition}} \quad (c')$$

Summarizing, ASL allows to effectively formalize privacy requirements specified in the privacy model and to flexibly perform distributed authorization management therefore enabling the concept of considering privacy and security in a joint fashion (see Section 4.3). Moreover, dynamically managing authorizations described by equation (6.4) (object, purpose, task, user) in a

context-aware manner (performing context monitoring¹) enables context-aware access control, which is often required in inherently context-aware RFID environments.

Requirements formalization for the front-end: privacy specification lists

Requirements formalization for the RFID front-end can be performed through the creation of so-called *privacy specification lists* (PSL), which associate the requirements obtained during the previous step with the specific privacy threats inherent in the RFID domain and determine the possible countermeasures respectively, which results in $\mathbb{R}_{imp}^{front-end}$ set. These countermeasures together with the privacy requirements expressed via ASL in the back-end ($\mathbb{R}_{imp}^{back-end}$) enable to consider privacy issues *across* the system components, namely in the back-end and in the front-end² of an RFID system.

The concept of PSL is depicted in figure 6.5.

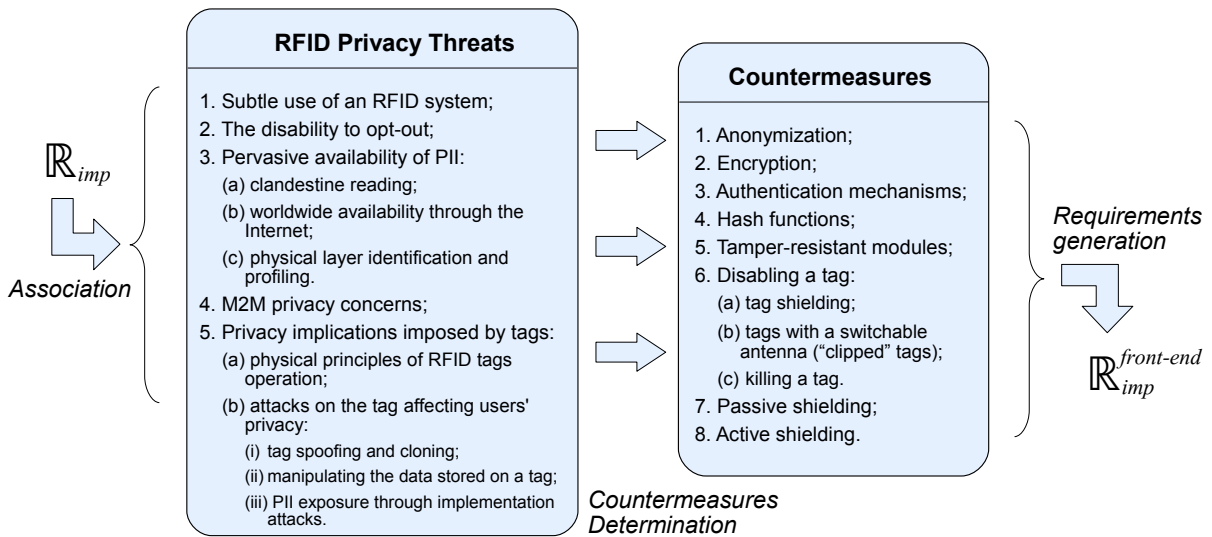


Figure 6.5: The concept of privacy specification lists (PSL).

The idea behind PSL is to relate the abstractly expressed requirements (\mathbb{R}_{imp}) to the inherent privacy threats in the RFID domain (the *association* procedure in Figure 6.5). The latter determine the respective countermeasures (*countermeasures detection*) which in turn enable to generate the formalized requirements ($\mathbb{R}_{imp}^{front-end}$) (*requirements generation*).

In order to effectively perform the procedure of requirements formalization in the front-end, Table 6.1 can be used by the PE. It considers the inherent privacy threats in the RFID domain and maps them to the respective countermeasures. The latter determine the privacy requirements formalized for the RFID front-end.

¹In order to perform this, a context-sensing subsystem (implemented as middleware) can be used. See Sections 3.3.3, 3.5.3.

²In this case, the bridging element (RFID readers, see Figure 3.1) is considered within the front-end category.

Table 6.1: Privacy specification lists: countermeasures determination.

Threats		Countermeasures									
		Anonymization	Encryption	Authentication	Hash functions	Tamper-res. mod.	Disabling a tag			Passive shielding	Active shielding
							shielding	switchable ant.	killing		
		1.	2.	3.	4.	5.	6.a	6.b	6.c	7.	8.
1. Subtle use		1.					✓	✓	✓		
2. Disability to opt-out		2.					✓	✓	✓		
3. Pervasive avail. of PII	3-a) clandestine reading	3.a	✓	✓	✓	✓	✓	✓	✓		
	3-b) availab. through the Internet	3.b	✓	✓	✓	✓	✓	✓	✓		
	3-c) physical layer identification	3.c					✓	✓	✓		
4. M2M privacy concerns		4.	✓	✓	✓	✓					
5. Privacy implications imposed by tags	5-a) phys. operating principles		5.a				✓	✓			
	5-b) specific attacks on tags (affecting privacy)	(i) tag spoofing	5.b.i		✓	✓	✓				
		(ii) on-tag data manipul.	5.b.ii		✓	✓	✓	✓	✓	✓	✓
		(iii) implem. at. (PII expos.)	5.b.iii				✓			✓	✓

Table 6.1 as well as Figure 6.5 are based on the implications of privacy and peculiarities of its enforcement in the RFID domain (Sections 3.3.3, 3.4.1 respectively) and specific attacks endangering privacy (Section 3.5.2). Therefore, a more detailed description of threats and respective countermeasures can be found earlier in the thesis. The main focus is now made on how this information can be utilized for the procedure of requirements formalization.

Several remarks, however, should be made with respect to Table 6.1. Firstly, "physical operating principles" (threat 5.a) denotes the vulnerabilities (with respect to privacy) of RFID tags physical operation, which for the most part is determined by the RF (radio frequency) interface. For example, the ability to modify data transmitted to the tag using the vulnerabilities of amplitude modulation (see Section 3.5.1 and [HB11]). Moreover, some tags operate using the principles of magnetism, which is different from RF and is based on the *reversible* process of magnetic hysteresis. The latter denotes that tags can be reactivated in future and therefore represents a privacy threat. As it can be seen from Table 6.1, the possible countermeasures against this threat reside in group 6, namely 6.a (tag shielding) and 6.b (using the tags with a switchable antenna¹) since the user needs to have a physical control over the tag's ability to communicate (in order to prevent the unwanted communication).

Secondly, the implementation attacks² leading to PII exposure (threat 5.b.iii) can reveal the secret keys (encryption and authentication ones) stored in the

¹A switchable antenna can be switched on and off according to the user's preferences (e.g. "clipped-tags" [KM05]), see Section 3.3.3.

²For more information on the implementation attacks see Appendix A.

tag's memory, which may expose the encrypted information (possibly PII) transmitted over the wireless channel and residing in the tag as well as pave the way to impersonation attacks due the authentication breach (caused by the exposure of authentication keys). The possible countermeasures are the utilization of tamper-resistant modules (countermeasure 5) as well as passive¹ and active² shielding (countermeasures 7 and 8 respectively). The latter should not be confused with countermeasure 6.a (shielding) which considers shielding for preventing the unwanted communication (Faraday cage), for example enclosing a tag into a conductive material (e.g. a foil).

Lastly, the countermeasure "hash functions" (#4) can be used for authentication purposes and integrity checks. For example, it implies the possibility of implementing the concept of "unlock key", which enables the tag to answer only those queries containing a special key [WSRE03].

Therefore, using the concept of PSL, the PE can obtain the formalized privacy requirements for the RFID front-end ($\mathbb{R}_{imp}^{front-end}$), which in conjunction with the ones of the back-end ($\mathbb{R}_{imp}^{back-end}$) comprise the eventual formalized requirements set:

$$\mathbb{R}_{imp}^{form} : \{ \mathbb{R}_{imp}^{back-end}, \mathbb{R}_{imp}^{front-end} \}.$$

It should be mentioned that requirements refinement and requirements formalization formally divided into sub-steps 2.1 and 2.2 in many cases can be performed together. The reason of their formal division is to more clearly identify the requirements transformation flow and to provide the necessary abstraction in the form of requirements tree (see Figure 6.2), which shows the main types of privacy requirements used within the system. This abstraction helps to identify which requirements need to be further mapped to the back-end and to the front-end of the RFID system, and which should be covered by the non-technical means.

6.2.3 Step 3: Implementation

The input of step 3 is comprised of the formalized implementable requirements (\mathbb{R}_{imp}^{form} set) and the requirements which can not be ensured by the means of technical privacy enforcement ($\mathbb{R}_{-impl} : \{ \mathbb{R}_{legal}, \mathbb{R}_{res} \}$). During the last step of the framework, the former is eventually implemented in the underlying system (both in the back-end and in the front-end).

The remained privacy requirements which can be backed up by legislation

¹An additional protective surface on top of the tag's circuitry, see Appendix A.

²Integration of sensors to detect the attempts of intrusion and act accordingly, e.g. reset the chip's configuration, delete sensitive data, etc. See Appendix A.

(\mathbb{R}_{legal}) are structured and finalized within the step 3. The respective references to the legal documents (e.g. directives) covering privacy issues are provided as well.

The requirements rendered by the PE as residual (\mathbb{R}_{res}) are subject to documentation since they determine the privacy gaps of the system. The latter need to be brought to users' attention and explained in a clear and understandable way (so that even laymen can be aware of system privacy gaps). Moreover, the ways of announcing and informing users of RFID activity, which might affect them, can be developed (e.g. a warning printed on a paycheck that the garment contains RFID tag woven into it, etc.).

6.2.4 A short summary

In this section, a framework for privacy requirements transformation was elaborated. It considers 3 steps during which the privacy requirements expressed in an abstract way (in form of a privacy model) are transformed into the format which can be subsequently implemented. The requirements transformation flow is depicted in Figure 6.6.

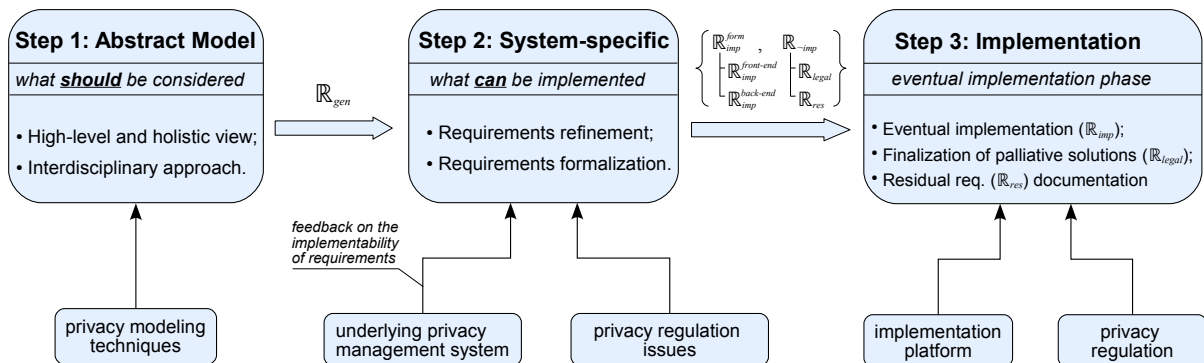


Figure 6.6: The requirements transformation flow.

6.3 Use case validation

In this section, it is demonstrated how the developed framework can be applied to several use cases. They represent different RFID scenarios which result in different sets of privacy requirements.

6.3.1 Use case 1: RFID tags woven into garments

The first scenario represents an RFID system deployed in the shop for garments management (e.g. ordering more items from the warehouse on demand),

shoplift prevention, and returns tracking. Suppose RFID tags are woven into clothes, which makes them unobtrusive and does not distract customers from shopping. In order to enhance the retail process, the customers are asked for their permission to leave the tags operational and in this way to enable the procedure of returns tracking. The ones consented to this kind of action are offered a 10% discount.

In order to protect the privacy of customers, the following issues need to be considered. It has to be ensured that after the item has been solved, the location privacy of the individuals, who have expressed their consent, stays intact. Moreover, it should be prohibited that another RFID infrastructure (e.g. deployed at his/her workplace) or various illegitimate readers in the vicinity can communicate with the tag woven into the garment. The customer wants to be sure as well that the tag is not linkable to the identity. The tags should be completely disabled for the customers whose consent has not been obtained.

From the enterprise perspective, the tags should contain the unique ID that can be linked to the specific garment model and the date of purchase. Additionally, only if the customer has explicitly consented, his/her identity can be linked to the tag ID as well (e.g. for a refund or garment exchange purposes on return).

The aforementioned scenario needs to be considered by the Privacy Engineer entity (PE) who performs privacy requirements engineering for the RFID system described above.

Step 1

Based on the system description presented above, the abstract privacy model needs to be created. It should encompass the relevant privacy facets (see Section 3.3.2) together with the social and legal issues. Therefore, among the 8 privacy facets, the location and the information ones are going to be relevant for the current use case. The communication privacy facet, for example, is not considered in this scenario since no communication as such is going to take place (apart from tag identification). The abstract privacy model, hence, encompasses the following issues:

1. Location of tag owners should not be exposed.
2. Tags should answer the queries coming only from the legitimate readers and only for the purpose of item identification on return.
3. The identity of the customer must be unlinkable to the tag unless the respective consent has been obtained.

4. The data which can be related to the customer via the corresponding tag is not allowed to be stored in the back-end database unless the customer has explicitly consented to this (as in the previous item of this list). If personal data are stored (provided that a customer's consent has been obtained), their exposure is allowed only for the concrete and clearly defined purpose.
5. If stored, personal data should not be retained for more than two years (according to the Data Retention Directive [Eur06]).
6. There should be no personal information stored on a tag (since it is not needed for the purpose the tags were woven into garments – returns tracking).

This simplified abstract privacy model encompasses the issues pertaining to location privacy (item 1) and information privacy (items 2-4). If violated, location and information privacy may additionally affect interpersonal privacy. For example, if the user location is combined with identity information, it may commit "a spatial border crossing" (see Section 5.3.1) and negatively affect the process of social interaction (e.g. affecting the public image of an individual).

The issues of user consent and purpose binding (primarily originating from the legal domain) are considered in items 2-4, 6. Furthermore, the legal perspective is taken into account in item 5 as well.

Having the abstract privacy model, the PE can proceed to the next step of the framework.

Step 2.

The input of this step is \mathbb{R}_{gen} expressed in an abstract way in the privacy model (step 1). According to Section 6.2.2, the abstract requirements need to be refined to the specific RFID system and formalized. In this example, this is going to be performed in a single step. Suppose the passive RFID tags woven into clothes possess moderate computational capabilities.

Requirements refinement and formalization for the RFID front-end

$$\text{cando}(o_{PII}, u, +store, [\text{default}], PE) \leftarrow \text{opt-in}(o_{PII}, p_{ret_track}) \quad (a)$$

$$\text{cando}(o_{PII}, p_{ret_track}, +read, [\text{default}], PE) \leftarrow \text{opt-in}(o_{PII}, p_{ret_track}) \quad (b)$$

$$\text{cando}(o_{PII}, u, -read, [\text{default}], PE) \leftarrow \text{retentionTime}(o_{PII}) > 2Y \quad (c)$$

- (a) The customer PII can only be stored if an explicit consent has been obtained. In this case an employee who performs the storage procedure (u) is

authorized to do it only a single time (expressed through the *store* action). This means that with this kind of authorization an employee has the one-time right to perform *write* the PII into the database. For all subsequent data access requests, a special authorization is needed.

- (b) The customer PII can be exposed for the explicit purpose returns tracking only if the customer has previously opted-in for this kind of action.
- (c) The PII data residing more than 2 years is rendered inaccessible¹.

Therefore, the aforementioned authorization rules formalize the abstract privacy requirements for the back-end.

Requirements refinement and formalization for the RFID front-end

The abstract requirements can be mapped to the following threats specified in PSL:

1. Pervasive availability of PII:
 - a) clandestine reading;
 - b) availability through the Internet;
 - c) physical layer identification.
2. Privacy implications imposed by tags:
 - a) physical principles of RFID tags operation.

The corresponding countermeasures render the following implementable requirements: \mathbb{R}_{imp}^{hash} , \mathbb{R}_{imp}^{kill} . Since there is no PII residing on the tag, it is enough to ensure that it answers only to a legitimate reader having a special "unlock" key (\mathbb{R}_{imp}^{hash}). Therefore, the costs of tag production can be kept down. Moreover, if the customer is not consented to keep the tag operational, it is to be possible to permanently destroy it, which renders the \mathbb{R}_{imp}^{kill} requirement.

In case the customer's consent has been obtained, the tag is not destroyed, which renders two unimplementable requirements: $\mathbb{R}_{-imp}^{shield}$ and $\mathbb{R}_{-imp}^{switch_ant}$. They are caused by physical layer identification (threat 3.c in Table 6.1) which can neither be mitigated by tag shielding nor by utilizing the switchable antenna (since the tag is woven into clothes and is therefore distributed over a certain part of it). Currently, legal privacy regulation does not address this specific problem. Therefore, the two aforementioned unimplementable requirements can not be backed up by the legal means either, which renders them as *residual*.

¹Such information should be subsequently deleted e.g. garbage collected. Deletion is however not expressed via ASL and is to be properly handled by the underlying DBMS.

Step 3.

Therefore, the PE now possesses the set of formalized implementable requirements, $\mathbb{R}_{imp}^{form} : \{\mathbb{R}_{imp}^{back-end}, \mathbb{R}_{imp}^{front-end}\}$, where:

1) $\mathbb{R}_{imp}^{back-end}$ is comprised of 3 requirements expressed via ASL:

$$\text{cando}(o_{PII}, u, +store, [\text{default}], PE) \leftarrow \text{opt-in}(o_{PII}, p_{ret_track}) \quad (a)$$

$$\text{cando}(o_{PII}, p_{ret_track}, +read, [\text{default}], PE) \leftarrow \text{opt-in}(o_{PII}, p_{ret_track}) \quad (b)$$

$$\text{cando}(o_{PII}, u, -read, [\text{default}], PE) \leftarrow \text{retentionTime}(o_{PII}) > 2Y \quad (c)$$

2) $\mathbb{R}_{imp}^{front-end}$ is comprised of $\{\mathbb{R}_{imp}^{hash}, \mathbb{R}_{imp}^{kill}\}$.

The legal requirements set is therefore empty. The residual requirements set is represented by $\mathbb{R}_{res}^{shield}, \mathbb{R}_{res}^{swith_ant}$ and is subject to documentation. It represents the privacy gaps of the system, which must be brought to the customer's attention so that he/she is able to make informed decisions pertaining to individual privacy in this RFID environment.

6.3.2 Use case 2: RFID-enabled keys in the enterprise

This use case considers active RFID tags used instead of conventional room keys within an enterprise. The system consists of a central server residing in the RFID back-end, which assigns access permissions to the keys enabling them to open the respective doors. Moreover, each key is associated with its owner – the employee of the enterprise. This information is stored in the back-end database as well.

In order to protect privacy of the employees, the following issues need to be considered. Firstly, the RFID key can reveal the otherwise private information about an individual. Each access request can be logged which enables the creation of employee behavior profiles. On each access (when the door is opened with the key), the key's ID (that can be directly associated with its owner), the time, and the location (door number) are registered in the database. Therefore, the employee possessing the RFID key is *traceable* throughout the enterprise. Moreover, there is a threat that he/she can be identified by the RFID key outside the enterprise, which raises even higher concerns over individual privacy.

Such a scenario affects location, information, interpersonal privacy and may even impose threat to bodily privacy if an individual is identifiable outside the enterprise (e.g. the attempts to seize the key from the legitimate owner to get access to the enterprise).

Therefore, inside the enterprise, strict access control policy to the sensitive data of door access history has to be applied. Only legitimate persons should have access to these data for a clearly defined purpose (preferably, in an anonymized form if the data are gathered e.g. for statistical purposes). PII retention period should be ensured accordingly as well.

Moreover, outside the enterprise, the back-end system is not able to control the information dissemination from an RFID-enabled key. Therefore, the privacy issues of *the front-end* are going to determine the degree to which the RFID system is privacy respective. In this context, it is important that an RFID key can be deactivated on leaving the enterprise (non-operational outside the enterprise) and reactivated again when the employee comes to work.

The aforementioned can be regarded as an abstract privacy model of the current RFID access control system. Within the second step, the PE of an enterprise generates the following privacy requirements:

Formalized privacy requirements for the back-end

- $$\begin{aligned} \text{cando}(o_{PII}, p_{statistics}, +read, [\text{anonymize: o}], PE) & \quad (a) \\ \text{cando}(o_{PII}, p_{legal}, +read, [\text{logging}], PE) & \quad (b) \\ \text{cando}(o_{PII}, u, -disclose, [\text{default}], PE) & \quad (c) \\ \text{cando}(o_{PII}, u, -read, [\text{default}], PE) \leftarrow \text{retentionTime}(o_{PII}) > 2Y & \quad (d) \end{aligned}$$

- (a) PII¹ can be read from the back-end database for statistical purposes only in anonymized form;
- (b) PII can be read for legal purposes under the obligation that such an action is logged (in order to enable the legitimacy check in future if required);
- (c) By default, PII can not be disclosed to any entity in the system.
- (d) PII is rendered inaccessible (and must be deleted) after their retention period exceeds 2 years.

Formalized privacy requirements for the front-end

The privacy requirements for the front-end determine how privacy of an employee is protected outside the enterprise, which imposes additional requirements of the tags. The following threats need to be covered:

1. Disability to opt-out (an employee should be able to opt-out from using the system, especially on leaving the enterprise);
2. Pervasive availability of PII:
 - a) clandestine reading;

¹In this example, PII is used with respect to the information obtained from door access requests.

- b) availability through the Internet;
 - c) physical layer identification.
3. M2M privacy concerns (since active RFID have a potential of establishing the communication);
 4. Privacy implications imposed by tags:
 - a) physical principles of RFID tags operation.

These threats determine the respective countermeasures, which in turn are used to generate the formalized requirements for the RFID front-end. The RFID tags are active and therefore possess relatively powerful computational resource and can be easily activated through the press of the button (whereas during the time the button is not pressed, the tag remains in the non-operational mode). Hence, the following requirements belong to the $\mathbb{R}_{imp}^{front-end}$ set:

$$\{\mathbb{R}_{imp}^{switch_ant}, \mathbb{R}_{imp}^{authent}, \mathbb{R}_{imp}^{encr}\}.$$

The implementability of the $\mathbb{R}_{imp}^{switch_ant}$ is decisive in this case since it ensures that the tag is operational only when its owner explicitly pushes the button on the key. Therefore, in this case there are no unimplementable requirements. Hence, the legal and residual sets are empty.

6.3.3 Use case 3: contactless payment cards

This scenario considers RFID-enabled contactless payment cards, which provide their owners with increased convenience¹ while performing payment procedures² in shops. Such a payment card is almost always carried with its owner during everyday activities. This has clear privacy implications since the purchasing habits of customers can be tracked, which leads to subsequent profiling and creation of behavioral patterns. Moreover, unlike the RFID-enabled keys discussed in Section 6.3.2, the contactless payment cards operate in the public environment where the customer can be easily misled e.g. while trying to pay using the faked reader (with a "certified" sign on it). The key difference to the previous use case is also the fact that the RFID-enabled key is in the *non-operational state* most of the time unless the user explicitly pushes the button to open the door. The contactless payment cards, to the contrary, should be operational during the shopping process.

The aforementioned outlines the privacy concerns with respect to RFID-enabled contactless payment cards. Therefore, the privacy model for this kind

¹For example, contactless payment speeds up paying procedures by requiring to simply "wave" the card in the vicinity (~10cm) of the respective reader. See for instance <http://usa.visa.com/personal/cards/paywave/index.html>.

²Such payment procedures are usually limited to around 20 €.

of RFID system should consider the following issues. Firstly, the merchants are to be prohibited by law to use PII obtained during the purchase for other purposes (e.g. marketing, etc) unless an explicit consent to do so has been obtained (purpose binding and user consent). Moreover, like in the previous use-case, privacy issues of the RFID front-end are going to determine how consumers' privacy is protected since contactless payment cards contain important PII, which can be exposed if the respective countermeasures have not been undertaken.

Therefore, the following privacy requirements are generated during the second step of the framework.

Formalized privacy requirements for the back-end

- cando(o_{PII} , u_{third_p} , $-disclose$, [default], PE) (a)
- cando(o_{PII} , $p_{marketing}$, $+read$, [default], PE) \leftarrow opt-in(o_{PII} , $p_{marketing}$) (b)
- cando(o_{PII} , p_{legal} , $+read$, [logging], PE) (c)
- cando(o_{PII} , u , $-read$, [default], PE) \leftarrow retentionTime(o_{PII}) $>$ 2Y (d)

- (a) Customer PII may not be disclosed to third parties.
- (b) Customer PII can be read for marketing purposes only if the respective consent has been obtained;
- (c) In cases when PII is to be accessed for legal reasons, this can be done under obligation that such an action is logged;
- (d) PII is rendered inaccessible (and must be deleted) after their retention period exceeds 2 years.

Formalized privacy requirements for the back-end

In case of contactless payment cards, the privacy-preserving mechanisms of the front-end to a large extent determine how privacy of customers is protected. Therefore, the following threats covered by privacy specification lists need to be considered:

1. Disability to opt-out;
2. Pervasive availability of PII:
 - a) clandestine reading;
 - b) availability through the Internet;
 - c) physical layer identification.
3. Privacy implications imposed by tags:
 - a) physical principles of RFID tags operation;
 - b) tag spoofing;

- c) on-tag data manipulation;
- d) PII exposure due to implementation attacks.

This renders the following requirements:

$$\mathbb{R}_{imp}^{front-end} : \{\mathbb{R}_{imp}^{encr}, \mathbb{R}_{imp}^{authent}, \mathbb{R}_{imp}^{tamper-res.}, \mathbb{R}_{imp}^{shielding}, \mathbb{R}_{imp}^{pas._shield}, \mathbb{R}_{imp}^{act._shield}\}.$$

The last two requirements (passive and active shielding) postulate the necessity to implement countermeasures against PII exposure through implementation attacks. Not to be confused with tag shielding ($\mathbb{R}_{imp}^{shielding}$) by e.g. enclosing it into a conductive material, which could be implemented by carrying a contactless paying card in a protected case (when not paying). Therefore, in this case like in RFID-enabled key system, there are no unimplementable requirements, which renders legal and residual sets empty.

6.3.4 A short summary

In this section, the framework presented in Section 6.2 was validated against several use cases. A simplified process of requirements transformation was demonstrated in each case. In the real world scenario, a lot of effort should be targeted at the creation of a holistic privacy model by the PE (in large systems, it can be a group of privacy experts) and at the subsequent procedure of privacy requirements inference.

Nevertheless, the validation process has demonstrated how the ideas behind the framework can be applied to practical scenarios.

6.4 Chapter summary

This chapter was devoted to the inference of privacy requirements from privacy models. As a solution, a framework for transforming abstract privacy models into implementable system requirements was suggested. It consists of three main steps. During the first step, a holistic privacy model is created. The second step is a core of the framework describing how abstract privacy requirements can be refined and formalized for the RFID domain. The main idea behind this is to consider the privacy requirements tree consisting of the requirements that can be implemented in the system (\mathbb{R}_{imp}) and the ones which can not be implemented by technical means (\mathbb{R}_{-imp}). The latter is further divided into two types: the privacy requirements which are covered in the legal domain (\mathbb{R}_{legal}) and the ones which are residual (\mathbb{R}_{res}). The residual requirements determine the privacy gaps of the system and are subject to documentation and future review

during the system upgrades (the new features introduced by upgrades may help to cover certain requirements from \mathbb{R}_{res}). Moreover, the privacy gaps should be brought to the attention of users so that they could make informed decisions and manage their privacy accordingly.

The implementable requirements are further formalized for the back-end and for the front-end of an RFID system under consideration. This enables to consider privacy *across* system components in a holistic way. In order to formalize the requirements for the RFID back-end, a modified version of an Authorization Specification Language (ASL) initially described in [KS02] was used. For the front end, the concept of Privacy Specification Lists (PSL) was developed, which considers the association of the non-refined requirements with specific RFID privacy threats. The latter are subsequently mapped to the respective countermeasures, which in turn determine the formalized requirements.

To the best of my knowledge, such an approach has not yet been considered and is firstly presented within this master thesis.

7 Conclusion

This master thesis is devoted to the development of approaches for designing privacy-respecting ubiquitous RFID systems. In order to perform this, the privacy peculiarities inherent in every UbiComp system were explored at first and their implications in the RFID domain were highlighted in Chapter 2.

Chapter 3 focused on privacy issues specific to RFID systems, which need to be considered while designing solutions for privacy management in this domain. Since privacy is itself a vague notion, the ways of its classification and definition were discussed in Section 3.3. The specific structure of RFID systems and their different classes to a large extent determine the peculiarities of privacy in this domain. Therefore, these issues were covered in Section 3.1.

Privacy enforcement mechanisms are the necessary basis for any privacy-management solution. Therefore, Section 3.4 considered this issue with respect to RFID systems. Since security is an inalienable part of privacy enforcement, it was discussed in Section 3.5.

Chapter 4 developed general suggestions for designing a privacy-respecting RFID system. The main focus was made on privacy requirements engineering which can be performed by applying the privacy modeling approach discussed in Chapter 5. In order to be able to efficiently infer privacy requirements from the respective models, a special framework was developed and validated against several use cases in Chapter 6.

Therefore, within this master thesis, it was shown how the problem of privacy management in ubiquitous RFID environments can be addressed in a holistic way. The specific privacy threats and the ways of its enforcement were structured and used for privacy requirements engineering in the RFID domain, which can be performed according to the developed framework.

Parts of the work presented within this master thesis were published in scientific literature. The respective references can be found in the references section.

The future work encompasses further elaboration of the developed framework for privacy requirements engineering and directly implementing the obtained requirements in the underlying privacy management system. Moreover, the integration of the user agent concept into the privacy management process should be performed since with the constantly increasing amount of RFID de-

vices, the user is not going to be able to manually manage his/her privacy preferences. Therefore, in the dynamic RFID environments of the future, the concept of the user agent performing management of the user defined privacy policies seems to be very perspective.

Bibliography

- [AIM10] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A survey. *Comput. Netw.*, 54:2787–2805, October 2010. <Cited on pages 33 and 36.>
- [All88] Anita L. Allen. *Uneasy Access : Privacy for Women in a Free Society*. Rowman & Littlefield, Totowa, N.J. :, 1988. <Cited on page 27.>
- [AP10] Sanjay Ahuja and Pavan Potti. An introduction to RFID technology. *Communications and Network*, 02(03):183–186, 2010. <Cited on page 18.>
- [APS02] Paul Ashley, Calvin Powers, and Matthias Schunter. From Privacy Promises to Privacy Management: A New Approach for Enforcing Privacy Throughout an Enterprise. In *Proceedings of the 2002 workshop on New security paradigms*, NSPW '02, pages 43–50, New York, NY, USA, 2002. ACM. <Cited on pages 40, 41, and 43.>
- [AZW06] Uwe Assmann, Steffen Zschaler, and Gerd Wagner. Ontologies, Meta-models, and the Model-Driven Paradigm. *Ontologies for Software Engineering and Software Technology*, pages 249–273, 2006. <Cited on page 85.>
- [BBP11] Manuela Berg and Katrin Borcea-Pfitzmann. Implementability of the Identity Management Part in Pfitzmann/Hansen’s Terminology for a Complex Digital World. In Simone Fischer-Hübner, Marit Hansen, Penny Duquenoy, and Ronald Leenes, editors, *Proceedings of PrimeLife / IFIP Summer-school on Privacy and Identity Management for Life*, IFIP Advances in Information and Communication Technology. Springer, 2011. <Cited on page 25.>
- [Bea62] William M. Beaney. The Constitutional Right to Privacy in the Supreme Court. In *The Supreme Court Review*, vol. 1962, pages 212–251. The University of Chicago Press, 1962. <Cited on page 26.>
- [BH07] Laurent Beslay and Hannu Hakala. Digital territory: Bubbles. In Paul T. Kidd, editor, *European visions for the knowledge age: a quest for new horizons in the information society*, pages 69 – 78. Cheshire Henbury, 2007. <Cited on page 78.>
- [BPPB11] Katrin Borcea-Pfitzmann, Andreas Pfitzmann, and Manuela Berg. Privacy 3.0 : = Data Minimization + User Control + Contextual Integrity (Privatheit 3.0 : = Datenminimierung + Nutzerkontrolle + Kontextuelle Integrität). *it - Information Technology*, 53(1):34–40, 2011. <Cited on page 31.>
- [Cav09] Ann Cavoukian. *Privacy by Design. Take a challenge*. Electronic resource, 2009. <http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf>. <Cited on pages 40, 45, and 60.>
- [CDMF00] Keith Cheverst, Nigel Davies, Keith Mitchell, and Adrian Friday. Experiences of developing and deploying a context-aware tourist guide: the GUIDE project. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, MobiCom '00, pages 20–31, New York, NY, USA, 2000. ACM. <Cited on page 34.>
- [CKK07] Jacek Cichon, Marek Klonowski, and Mirosław Kutylowski. Privacy Protection in Dynamic Systems Based on RFID Tags. In *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, pages 235 –240, march 2007. <Cited on page 42.>
- [Cou09] Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime. Cryptology ePrint Archive, Report 2009/137, 2009. <http://eprint.iacr.org/>. <Cited on page 116.>
- [CSS+09] Inhyok Cha, Y. Shah, A.U. Schmidt, A. Leicher, and M.V. Meyerstein. Trust in M2M communication. *Vehicular Technology Magazine, IEEE*, 4(3):69 –75, sept. 2009. <Cited on page 57.>
- [CT01] S.C.Q. Chen and V. Thomas. Optimization of inductive RFID technology. In *Electronics and the Environment, 2001. Proceedings of the 2001 IEEE International Symposium on Electronics and the Environment.*, pages 82 –87, 2001. <Cited on page 20.>

- [DAK10] S. Dominikus, M. Aigner, and S. Kraxberger. Passive RFID Technology for the Internet of Things. In *Internet Technology and Secured Transactions (ICITST)*, pages 1–8, November 2010. <Cited on page 55.>
- [DBID87] Janet A. Simons Donald B. Irwin and Beverly A. Drinnien. *Psychology: The Search for Understanding*. West Publishing Company, June 1987. <Cited on page 32.>
- [DC05] Yitao Duan and John Canny. Protecting User Data in Ubiquitous Computing: Towards Trustworthy Environments. In David Martin and Andrei Serjantov, editors, *Privacy Enhancing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, chapter 11, pages 167–185. Springer Berlin / Heidelberg, Berlin, Heidelberg, 2005. <Cited on pages 10 and 11.>
- [DeC08] Judith DeCew. Privacy. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Fall 2008 edition, 2008. <Cited on page 26.>
- [DZ83] J.D. Day and H. Zimmermann. The OSI reference model. *Proceedings of the IEEE*, 71(12):1334 – 1340, dec. 1983. <Cited on pages 7 and 30.>
- [EK07] T. Eisenbarth and S. Kumar. A Survey of Lightweight-Cryptography Implementations. *Design Test of Computers, IEEE*, 24(6):522 –533, nov.-dec. 2007. <Cited on page 42.>
- [EPS10] Antti Evesti and Susanna Pansar-Syväniemi. Towards Micro Architecture for Security Adaptation. In *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume, ECSA '10*, pages 181–188, New York, NY, USA, 2010. ACM. <Cited on pages 36 and 56.>
- [Eur95] European Parliament and Council Directive. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, 1995. <Cited on pages 25, 43, and 44.>
- [Eur02] European Parliament and Council Directive. Directive 2002/58/EC of the European Parliament and of the Council: concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Communities, 2002. <Cited on pages 36 and 44.>
- [Eur06] European Parliament and Council Directive. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Official Journal of the European Communities, 2006. <Cited on pages 44, 90, 92, and 99.>
- [FHO98] S. Fischer-Hübner and A. Ott. From a Formal Privacy Model to its Implementation. In *The 21st National Information Systems Security Conference (NISSC '98)*, 1998. <Cited on pages 25, 68, 81, and 82.>
- [Fin10] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*. Third Edition. A John Wiley and Sons, Ltd., 2010. <Cited on pages 20, 21, 38, 50, and 51.>
- [FWR05] M. Feldhofer, J. Wolkerstorfer, and V. Rijmen. AES implementation on a grain of sand. *Information Security, IEE Proceedings*, 152(1):13–20, October 2005. <Cited on page 42.>
- [GBP11a] Ivan Gudymenko and Katrin Borcea-Pfitzmann. A Framework for Transforming Abstract Privacy Models into Implementable UbiComp System Requirements. In Thomas Schlegel and Stefan Pietschmann, editors, *1st International Workshop on Model-based Interactive Ubiquitous Systems, Modiquitous 2011*, Pisa, June 2011. <Cited on pages 24, 29, 44, 59, 60, 62, 68, 69, 85, and 86.>
- [GBP11b] Ivan Gudymenko and Katrin Borcea-Pfitzmann. Privacy in Ubiquitous Computing. In *Interconnecting Smart Objects with the Internet Workshop*, Prague, March 2011. <Cited on page 60.>
- [GBPT11] Ivan Gudymenko, Katrin Borcea-Pfitzmann, and Katja Tietze. Privacy Implications of IoT. In *Workshop on Privacy, Trust and Interaction in the Internet of Things*, Amsterdam, November 2011. <Cited on pages 19, 36, 43, and 46.>
- [GD09] J.D. Griffin and G.D. Durgin. Complete Link Budgets for Backscatter-Radio and RFID Systems. *Antennas and Propagation Magazine, IEEE*, 51(2):11 –25, april 2009. <Cited on page 20.>

- [GH07] Sushant Gupta and Ankit Hirdesh. Overview of M2M. [Online]. Available http://sites.google.com/site/hridayankit/M2M_overview_paper.pdf, 2007. Accessed on 10.08.2011. <Cited on page 54.>
- [GMO01] Karine Gandolfi, Christophe Mourtel, and Francis Olivier. Electromagnetic Analysis: Concrete Results. In *Proceedings of the Third International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '01, pages 251–261, London, UK, 2001. Springer-Verlag. <Cited on page 115.>
- [HB11] Ernst Haselsteiner and Klemens Breitfu. Security in Near Field Communication (NFC): Strengths and Weaknesses. In *Workshop on RFID Security 2006*, July 2011. <Cited on pages 49 and 95.>
- [Hen07] Martin Hensel. RFID-Tags finden Gegenstände per GPS-Satellit. <http://www.searchnetworking.de/themenbereiche/drahtlose-netzwerke/allgemein/articles/68744>, June 2007. An Internet Article. <Cited on page 18.>
- [Hen08] Dirk Henrici. *RFID Security and Privacy*. Springer, 2008. <Cited on pages 15, 17, 18, 19, 21, 23, 24, 29, 31, 42, and 72.>
- [HFW11] Michael Hutter, Martin Feldhofer, and Johannes Wolkerstorfer. A Cryptographic Processor for Low-Resource Devices: Canning ECDSA and AES Like Sardines. In *WISTP*, pages 144–159, 2011. <Cited on pages 42 and 48.>
- [HHW11] René Hummen, Tobias Heer, and Klaus Wehrle. A Security Protocol Adaptation Layer for the IP-based Internet of Things. In *Interconnecting Smart Objects with the Internet Workshop*, March 2011. <Cited on page 54.>
- [HJS11] Michael Hutter, Marc Joye, and Yannick Sierra. Memory-Constrained Implementations of Elliptic Curve Cryptography in Co-Z Coordinate Representation. In *AFRICACRYPT*, pages 170–187, 2011. <Cited on pages 42 and 48.>
- [HL04] Jason I. Hong and James A. Landay. An Architecture for Privacy-Sensitive Ubiquitous Computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, MobiSys '04, pages 177–189, New York, NY, USA, 2004. ACM. <Cited on page 78.>
- [Hua06] Xu Huang. An Improved ALOHA Algorithm for RFID Tag Identification. In Bogdan Gabrys, Robert Howlett, and Lakhmi Jain, editors, *Knowledge-Based Intelligent Information and Engineering Systems*, volume 4253 of *Lecture Notes in Computer Science*, pages 1157–1162. Springer Berlin / Heidelberg, 2006. <Cited on page 21.>
- [Hut11] Michael Hutter. RFID Security, 2011. IPICS-2011 summer school. <Cited on pages 12, 115, and 116.>
- [Ins67] Legal Information Institute. *Katz v. United States* (No. 35). http://www.law.cornell.edu/supct/html/historics/USSC_CR_0389_0347_ZS.html, 1967. Syllabus of the case was viewed at the webpage of Cornell University Law School on 07.09.201. <Cited on pages 26 and 74.>
- [JA03] A.R. Jacobs and G.D. Abowd. A framework for comparing perspectives on privacy and pervasive technologies. *Pervasive Computing, IEEE*, 2(4):78–84, December 2003. <Cited on pages 72, 73, and 74.>
- [Jae97] Jaeger. *Microelectronic Circuit Design*. McGraw-Hill, 1997. <Cited on page 48.>
- [JL02] Xiaodong Jiang and James A. Landay. Modeling Privacy Control in Context-Aware Systems. *IEEE Pervasive Computing*, 1:59–63, July 2002. <Cited on pages 11, 76, 77, and 83.>
- [K⁺07a] Apu Kapadia et al. Virtual Walls: Protecting Digital Privacy in Pervasive Environments. In *Proceedings of the 5th international conference on Pervasive computing*, PERVASIVE'07, pages 162–179, Berlin, Heidelberg, 2007. Springer-Verlag. <Cited on page 78.>
- [K⁺07b] P.B. Khannur et al. An 860 to 960MHz RFID Reader IC in CMOS. In *Radio Frequency Integrated Circuits (RFIC) Symposium, 2007 IEEE*, pages 269–272, June 2007. <Cited on page 30.>
- [KGHG08] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*, CARDIS '08, pages 267–282, Berlin, Heidelberg, 2008. Springer-Verlag. <Cited on page 116.>

- [KM05] Günter Karjoth and Paul A. Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society, WPES '05*, pages 27–30, New York, NY, USA, 2005. ACM. <Cited on pages 30, 42, and 95.>
- [Kob87] Neal Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):pp. 203–209, 1987. <Cited on pages 42 and 48.>
- [Kos11] Eleni Kosta. Introduction to the European legal framework on data protection, 2011. IPICS-2011 summer school. <Cited on pages 44, 45, and 90.>
- [KPJ⁺08] Julie A. Kientz, Shwetak N. Patel, Brian Jones, Ed Price, Elizabeth D. Mynatt, and Gregory D. Abowd. The Georgia Tech Aware Home. In *CHI '08: CHI '08 extended abstracts on Human factors in computing systems*, pages 3675–3680, New York, NY, USA, 2008. ACM. <Cited on page 33.>
- [Kru10] J. Krumm, editor. *Ubiquitous Computing Fundamentals*. CRC Press, Taylor & Francis Group, 2010. <Cited on pages 10 and 32.>
- [KS02] G. Karjoth and M. Schunter. A Privacy Policy Model for Enterprises. In *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*, pages 271–281, 2002. <Cited on pages 62, 78, 79, 80, 81, 83, 89, 90, 92, and 106.>
- [KSW03] Günter Karjoth, Matthias Schunter, and Michael Waidner. Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data. In Roger Dingledine and Paul Syverson, editors, *Privacy Enhancing Technologies*, volume 2482 of *Lecture Notes in Computer Science*, pages 194–198. Springer Berlin / Heidelberg, 2003. <Cited on pages 11, 62, and 77.>
- [LA77] Hannah A. Levin and Frank Askin. Privacy in the Courts: Law and Social Reality. *Journal of Social Issues*, 33(3):138–153, 1977. <Cited on page 26.>
- [Lan01] Marc Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In Gregory Abowd, Barry Brumitt, and Steven Shafer, editors, *UbiComp 2001: Ubiquitous Computing*, volume 2201 of *Lecture Notes in Computer Science*, pages 273–291. Springer Berlin / Heidelberg, 2001. <Cited on pages 9, 10, 12, and 26.>
- [Lan02] Marc Langheinrich. Privacy invasions in ubiquitous computing. In *Workshop on Socially-Informed Design of Privacy-Enhancing Solutions (UBICOMP 2002)*. Springer, 2002. <Cited on page 23.>
- [Lan05] Mark Langheinrich. Personal Privacy in Ubiquitous Computing: Tools and System Support. Ph.D. Thesis., 2005. ETH Zrich. <Cited on page 43.>
- [LM07] M. Langheinrich and R. Marti. Practical Minimalist Cryptography for RFID Privacy. *Systems Journal, IEEE*, 1(2):115–128, dec. 2007. <Cited on page 13.>
- [LP90] L.J. La Padula. Formal Modeling in a Generalized Framework for Access Control. In *Computer Security Foundations Workshop III, 1990. Proceedings*, pages 100–109, jun 1990. <Cited on page 81.>
- [Mar01] Gary T. Marx. Murky conceptual waters: The public and the private. *Ethics and Inf. Technol.*, 3:157–169, September 2001. <Cited on pages 70, 71, 72, and 83.>
- [MBPL09] Aikaterini Mitrokotsa, Michael Beye, and Pedro Peris-Lopez. Classification of RFID Threats based on Security Principles. <http://lasecwww.epfl.ch/~katerina/papers/RFIDthreats.pdf>, 2009. Accessed online on 08.09.2011. <Cited on page 49.>
- [MBSK95] Sandra J. Milberg, Sandra J. Burke, H. Jeff Smith, and Ernest A. Kallman. Values, Personal Information Privacy, and Regulatory Approaches. *Commun. ACM*, 38:65–74, December 1995. <Cited on page 26.>
- [MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks Revealing the Secrets of Smart Cards*. Springer, 2007. <Cited on page 115.>
- [NESP08] Karsten Nohl, David Evans, Starbug Starbug, and Henryk Plötz. Reverse-engineering a cryptographic RFID tag. In *Proceedings of the 17th conference on Security symposium*, pages 185–193, Berkeley, CA, USA, 2008. USENIX Association. <Cited on page 116.>
- [NIS01] NIST. Specification for the Advanced Encryption Standard (AES). FIPS 197., November 2001. <Cited on pages 42 and 48.>

- [OMG08] OMG. The official CORBA standard. <http://www.omg.org/spec/CORBA/3.1/>, 2008. Accessed on 09.08.2011. <Cited on page 55.>
- [OOP03] Siddika Berna Örs, Maria Elisabeth Oswald, and Bart Preneel. Power-Analysis Attacks on an FPGA—First Experimental Results. In Springer, editor, *Cryptographic Hardware and Embedded Systems – CHES 2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 35 – 50. Springer Verlag, 2003. <Cited on page 115.>
- [Pet06] Gabriel Peter. *Pervasive Computing : trends and impacts*. SecuMedia, 2006. <Cited on page 6.>
- [Pfi10] Andreas Pfitzmann. "Accompanying Ambient Intelligence (AAmI) – Why You Should Take Your Sensors with You ". A sketch, April 2010. <Cited on page 60.>
- [PJDD08] N. Pillin, N. Joehl, C. Dehollain, and M.J. Declercq. High Data Rate RFID Tag/Reader Architecture Using Wireless Voltage Regulation. In *RFID, 2008 IEEE International Conference on RFID*, pages 141 –149, april 2008. <Cited on page 19.>
- [Pos09] Poslad S. *Ubiquitous Computing: Smart Devices, Environments and Interactions*. Wiley Publishing, 2009. <Cited on page 6.>
- [Poz05] David Pozen. The Mosaic Theory, National Security, and the Freedom of Information Act. *Yale Law Journal*, 115:628–679, 2005. <Cited on page 33.>
- [Pre11] Bart Preneel. An introduction to cryptology, 2011. IPICS-2011 summer school. <Cited on pages 48 and 49.>
- [PT11] Tim Polk and Sean Turner. Security Challenges for the Internet of Things. In *Interconnecting Smart Objects with the Internet Workshop*, March 2011. <Cited on page 50.>
- [Rep11] Report. Privacy and Data Protection Impact Assessment Framework for RFID Applications, Jan 2011. Accessed on 25.05.2011. <Cited on page 45.>
- [RM09] Natalia A. Romero and Panos Markopoulos. Grounding Interpersonal Privacy in Mediated Settings. In *Proceedings of the ACM 2009 international conference on Supporting group work*, GROUP '09, pages 263–272, New York, NY, USA, 2009. ACM. <Cited on page 27.>
- [Sha09] Stuart S. Shapiro. Privacy by Design: Moving from Art to Practice. *Commun. ACM*, 53:27–29, June 2009. <Cited on pages 40 and 60.>
- [SHT10] Jani Suomalainen, Pasi Hyttinen, and Pentti Tarvainen. Secure Information Sharing between Heterogeneous Embedded Devices. In *Proceedings of the Fourth European Conference on Software Architecture: Companion Volume*, ECSA '10, pages 205–212, New York, NY, USA, 2010. ACM. <Cited on pages 55 and 56.>
- [Sol06] Daniel J. Solove. A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3):477 pp., January 2006. GWU Law School Public Law Research Paper No. 129. <Cited on pages 23, 24, 73, 74, 83, and 117.>
- [ST04] Adi Shamir and Eran Tromer. Acoustic cryptanalysis: on nosy people and noisy machines. <http://www.cs.tau.ac.il/~tromer/acoustic/>, 2004. Preliminary proof-of-concept presentation. <Cited on page 116.>
- [Sta02] Frank Stajano. *Security for Ubiquitous Computing*. John Wiley & Sons, LTD, 2002. <Cited on page 5.>
- [UE04] Úlfar Erlingsson. The Inlined Reference Monitor Approach to Security Policy Enforcement. <http://ecommons.library.cornell.edu/bitstream/1813/5628/1/TR2003-1916.pdf>, 2004. PhD thesis. <Cited on page 69.>
- [Vau07] Serge Vaudenay. On Privacy Models for RFID. In *Proceedings of the Advances in Cryptology 13th international conference on Theory and application of cryptology and information security, ASIACRYPT'07*, pages 68–87, Berlin, Heidelberg, 2007. Springer-Verlag. <Cited on pages 82 and 83.>
- [VD10] Jean-Philippe Vasseur and Adam Dunkels. *Interconnecting Smart Objects with IP*. Morgan Kaufmann, 2010. <Cited on page 55.>

- [WB90] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, December 1890. <Cited on pages 24 and 26.>
- [WBC⁺09] E Welbourne, L Battle, G Cole, K Gould, K Rector, S Raymer, M Balazinska, and G Borriello. Building the Internet of Things Using RFID: The RFID Ecosystem Experience. *IEEE Internet Computing*, 13(3):48–55, 2009. <Cited on page 34.>
- [Web10] Rolf H. Weber. Internet of things - new security and privacy challenges. *Computer Law & Security Review*, 26(1):23 – 30, 2010. <Cited on pages 28, 29, and 44.>
- [Wei91] Mark Weiser. The Computer for the 21st Century. *Scientific American*, February 1991. <Cited on page 5.>
- [Wei08] Stephen A. Weis. RFID (Radio Frequency Identification), ch. 198. In Hossein Bidgoli, editor, *Handbook of Computer Networks*, v3 (3). Wiley Publishing, 2008. <Cited on pages 17 and 18.>
- [WSRE03] S. Weis, S. Sarma, R. Rivest, and D. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *1st International Conference on Security in Pervasive Computing (SPC)*, March 2003. <Cited on pages 42, 81, 88, and 96.>
- [WTJ⁺11a] Geng Wu, S. Talwar, K. Johnsson, N. Himayat, and K.D. Johnson. M2M: From Mobile to Embedded Internet. *Communications Magazine, IEEE*, 49(4):36–43, April 2011. <Cited on page 36.>
- [WTJ⁺11b] Geng Wu, S. Talwar, K. Johnsson, N. Himayat, and K.D. Johnson. M2M: From mobile to embedded internet. *Communications Magazine, IEEE*, 49(4):36–43, april 2011. <Cited on page 57.>
- [ZK09] Yang Zhang and Paris Kitsos. *Security in RFID and Sensor Networks*. CRC Press, 2009. <Cited on pages 31 and 51.>
- [ZSC11] Davide Zanetti, Pascal Sachs, and Srdjan Capkun. On the Practicality of UHF RFID Fingerprinting: How Real is the RFID Tracking Problem? In Simone Fischer-Hbner and Nicholas Hopper, editors, *Privacy Enhancing Technologies*, volume 6794 of *Lecture Notes in Computer Science*, pages 97–116. Springer Berlin / Heidelberg, 2011. <Cited on pages 30 and 31.>

A Implementation attacks on RFID tags

Whereas it can be proven that cryptographic algorithms are mathematically secure, their implementations on RFID tags might contain vulnerabilities. That means that an attacker does not have to directly break the cipher. It is possible to bypass the cryptanalysis phase if there is access to so-called side channels or an opportunity to perform fault analysis. These types of attacks can be as well called implementation attacks since they are rather targeted at the implementation of the cryptographic algorithm than on the cryptographic algorithm itself.

Such attacks fall into several categories, namely side-channel attacks, fault analysis, and reverse engineering.

Side-channel attacks

In [Hut11], the following side channel attacks were mentioned:

1. *Timing analysis*. Timing behavior of cryptographic implementations can leak information about the secret key. That is: the decryption time can be correlated to the values of the input ciphertext and reveal the key¹ if no special countermeasures have been undertaken.
2. *Power analysis*:
 - Simple power analysis. Secret key extraction by visual inspection of a power consumption trace during the execution of cryptographic procedures. See [OOP03] for details.
 - Differential power analysis. Targeted at an intermediate value of the cryptographic algorithm that depends on the secret key using statistical analysis. More on this type of attacks can be found in [MOP07].
3. *Electromagnetic analysis*. This kind of side-channel attack exploits correlations between secret data and variations in power radiations of electromagnetic field emitted by cryptographic devices [GMO01]. According to [Hut11], it allows attacks from a distance (far-field measurements).

¹For example, square and multiply operation takes more time than the multiply one, which can be associated with 1 and 0 values of the utilized key respectively.

4. *Acoustic attacks* [ST04]. Similarly to power analysis, the secret key can be gained through analysis of acoustic oscillations made by hardware while performing cryptographic operations. For more details, see [ST04].

According to [Hut11], randomizing techniques or masking can be used to remove the dependences between the actual cryptographic operations and the revealing factor (power consumption, electromagnetic emissions, etc.).

Fault Analysis

Fault analysis is based on the principle of fault induction into implementations of cryptographic algorithms in order to reveal internal states of the latter and consequently deduce the key. According to [Hut11], there exist several types of fault analysis attacks:

1. *Non-invasive*. Package encapsulating the circuitry is left untouched and only working conditions are modified (e.g. high temperature, exposure of an RFID tag to a strong electromagnetic field, etc.)
2. *Semi-invasive*. Involves decapsulation of an RFID package, i.e. physically opening it and performing, for example, optical fault injection.
3. *Invasive*. This type of fault analysis implies establishing electrical contact to the chip with its modification.

The possible countermeasures are shielding (passive¹ or active²) and redundant computation with final parity check [Hut11].

Reverse Engineering

Sometimes proprietary solutions to a large extent rely on the secrecy of the utilized cryptographic algorithms (so-called "security by obscurity"). However, according to [NESP08], "any algorithm given to users in form of hardware can be disclosed even when no software implementation exists and black-box analysis is infeasible". Reverse engineering implies reconstructing the key by using a combination of circuitry image analysis and protocol analysis. An example of a successful attack can be breaking the proprietary CRYPTO-1 cipher used for transport ticketing (like the one in Amsterdam, London, Boston, Los Angeles, etc.) and access control [KGHG08, Hut11]. The key can be revealed within 0.1 seconds using the algebraic attack presented in [Cou09].

¹An additional protective surface on top of the circuitry.

²Integration of sensors to detect the attempts of intrusion and act accordingly, e.g. reset the chip's configuration, delete sensitive data, etc.

B Privacy modeling: a legal taxonomy of privacy-invading activities

The following group of privacy-invading activities is considered in the Solove's privacy model [Sol06]:

- Information collection:
 - Surveillance – "watching, listening to, or recording of an individual's activities;
 - Interrogation – "various forms of questioning or probing for information".
- Information Processing:
 - Aggregation – gathering different data about the individual;
 - Identification – "linking information to particular individuals";
 - Insecurity – the possibility of obtaining private information due to information leaks and improperly realized access procedures;
 - Secondary Use – using the collected information with another purpose without obtaining the individual's consent, violation of purpose-binding condition;
 - Exclusion – the unawareness of the data subject (the individual) that others possess and use his private information (already collected).
- Information Dissemination:
 - Breach of Confidentiality – violation of trusted communication, exposing individual's private information that was supposed to stay confidential;
 - Disclosure – publicly revealing individual's private information, "occurs when certain *true* information about a person is revealed to others". The difference to the previous item – Breach of Confidentiality – is that "[...] the harm in disclosure involves the damage to reputation caused by dissemination" and "Disclosure can harm even if information is revealed by a stranger" (in contrast to Breach of Confidentiality where the party that has violated confidentiality was assumed to be a trusted communicating entity);
 - Exposure – "revealing individual's nudity, grief, or bodily functions";

- Increased accessibility – facilitating the process of access to information;
 - Blackmail – “the threat to disclose personal information” unless a certain demand is met;
 - Appropriation – the individual’s identity is used in the interest of the third party, e.g. for advertising, etc.;
 - Distortion – spreading of false or misleading information about the data subject.
- Invasions:
 - Intrusion – disturbing the individual’s tranquility and/or solitude;
 - Decisional interference – “involves the government’s incursion into the data subject’s decisions regarding her *private* affairs”.

Acknowledgments

From all my heart I would like to thank my family for their everyday support and love. Without you I wouldn't have achieved the half of what I did.

Thanks a lot to my friends who kept reminding me that life is "a multi-faceted issue".

I would also like to thank my advisor, Katrin, who let me be creative, provided me with her professional and human support, and kindly guided through the process of writing this master thesis.

Last but not least, I would like to express my gratitude to Andreas Pfitzmann who passed away last year for being so kind and inspiring me on my way to scientific excellence. I really regret that we worked only a few months together.