13

Security and Privacy in RFID Applications

Paweł Rotter
Joint Research Centre of the European Commission,
Institute for Prospective Technological Studies
Seville, Spain
Currently at:
AGH-University of Science and Technology, Automatics Department
Kraków, Poland

1. Introduction

RFID technology raises a number of security and privacy concerns, which may substantially limit its deployment and reduce potential benefits. Public consultations led by the European Commission with citizens, RFID manufacturers, system integrators, academic institutions and public bodies confirm that privacy and security is a major concern (www.rfidconsultation.eu). Features which make RFID especially vulnerable among information systems are:

1. Wireless transmission between tag and reader:
   Most of the attacks on RFID systems described in the next part of this chapter exploit the air interface.
2. The limited resources of the tag:
   The low power supply and small memory of low-cost passive tags limit the extent to which security measures can be applied.
3. The small size of tags:
   RFID tags can be almost invisible,[1] which allows them to be attached to items carried by people without their consent or even their knowledge.

The most common threat is unauthorised access to the data stored on the tag or sent via the air interface. Attackers can achieve this either by reading the tag with an unauthorized reader *(rogue scanning)* or by *eavesdropping* on a legitimate communication. Access to the data on the tag is a threat in itself, but it can also be the first step to other types of attack. For example, in a *replay* attack, the attacker repeats the authentication sequence captured when it was emitted by an authorized tag, and in this way he may usurp the identity of another person. The attacker can also make a *duplicate of the tag*, with has the same functionality. Another threat is the malicious *modification of the memory content* of the RFID tag, with a view to changing attributes reported by the tag or using the tag as a carrier of malware. Denial of service can be avoided by *blocking* (putting the anti-collision protocol in a practically infinite loop) and frequency *jamming*. By *reverse engineering* and *side channel attack,* the attacker may discover algorithms and data on the tag (including the cryptographic key). Moreover,

[1] The smallest passive tags commercially available in 2006 are of size 0.15×0.15×0.0075 mm (Harrop et al. 2008).

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

protection measures for RFID-based cards are more difficult to apply than for contact cards. Finally, RFID systems may be the subject of attack to backend, like any other information system.

Depending on the application in which an RFID system is commercialized, security and privacy threats should be differently treated. Some applications demand high levels of security (like access control systems) and privacy (like e-documents), while for others, like livestock tracking or some manufacturing processes, these concerns are less important. Also, types of risk depend on the application. For presentation in this chapter, we have selected the set of application areas where the most relevant privacy and security issues arise. (However, where the same issues appear in different applications, we have not tried to discuss all of them.) We have looked especially at those applications which are large in economic terms and involve a large number of users. Detailed criteria are presented at the beginning of Section 3. The four selected application areas are: item-level tagging, electronic ID documents, contactless smart card and RFID implants.

Item-level tagging is foreseen to be the main RFID application in terms of market value and number of tags, and the most pervasive one. The main privacy concern here is unauthorized tag reading. When tagging at item level becomes common, if appropriate countermeasures are not applied, attackers will be able to find out what items a person has in a bag (e.g. what type of medicine), the price and brand of clothes, etc. A set of tags attached to items usually carried by a person may allow his identification and tracking. There are many countermeasures, which can reduce and even eliminate the risk, but just the possibility of massive invasions of privacy and a "big brother" scenario has an important impact on image of RFID and its social acceptance.

Electronic identity documents may use different technologies. Nevertheless, for electronic passports, RFID has been selected, as it is more appropriate for the booklet form of e-passports than, for example, contact smart cards. The combination of two privacy-sensitive technologies – i.e. RFID and biometrics – brings particular concerns about privacy. The main threats are: secret reading of personal data and biometrics, copying the passport, tracking the passport's owner, and theoretically even the construction of a bomb which could be triggered by a passport of a specific nation or individual. Though several security measures have been proposed in the ICAO specification (Basic Access Control, Active Authentication, and Extended Access Control) there is ongoing discussion as to whether the protection they offer is sufficient.

Contactless smart cards and single-use RFID-based tickets increase convenience and efficiency in public transport and allow additional services to be offered. They provide detailed information about traffic patterns which can be used in traffic management (schedule optimisation) and enable new payment plans, like fee per kilometre. Apart from security risks typical to each RFID application based on wearable tokens, privacy is a special issue for public transport applications, since travel patterns of individuals can be recorded and stored in a central database.

RFID implants for identification and authentication of people are probably the most controversial among RFID technologies. They provide a permanent and physical link between the person and the tag. The first implant was approved for commercial use by the FDA in 2004. Since then, about two thousand people were injected with tags, mostly in order to be included in a healthcare information system. This system provides online access to medical record of a patient based on ID number communicated by the implant. In the future RFID implants may have a wide range of applications. However, privacy and security issues, as well as possible health risks, may limit or even stop further deployment of this technology.

Our purpose was not to give a complete discussion of all applications where privacy and security is important, which would be rather repetitive. Instead, we provided four examples, which cover the most of issues. Threats and measures in, for example, access control systems or electronic payment will be similar to those which are discussed here.
In this chapter, we focus mostly on the technical aspects of security and privacy and the technical countermeasures, but there are also legal, social and economic challenges related to security issues. Moreover it is important to bear in mind that security and privacy protection need to be followed by the creation of user trust and awareness. Even a secure system will not be successful if the user's perception of security and privacy protection is low.
This chapter is structured as follows: in Section 2, we present in more detail the threats mentioned above and corresponding countermeasures. In Section 3, we discuss selected applications. We provide a summary and conclusions in Section 4.

2. Threats to RFID systems – state of the art

In this section, we present the threats to RFID and corresponding countermeasures – see Fig. 1. We focus on those risks which are not an issue in other information systems. We do not

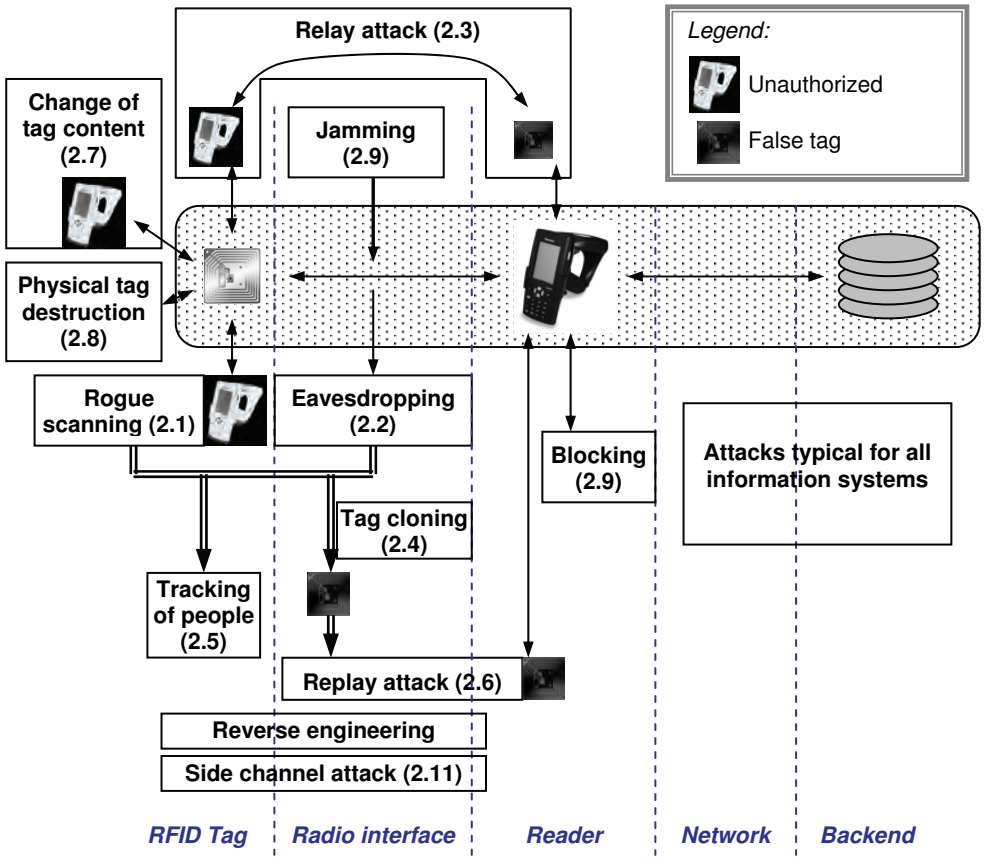

Fig. 1. Threats to RFID systems and number of subchapters where they are discussed

discuss *attacks on the backend* of the RFID system, which are similar to attacks on non-RFID information systems. Exhaustive information about risks and countermeasures in information systems can be found in, for example (Hansche et al., 2004).
It is interesting to observe that one type of attack may be a preparatory step for another one. For example, eavesdropping may enable cloning of the tag; this may then result in a replay attack and the final consequence may be unauthorized access to a restricted area. These kinds of relations imply that a single vulnerability of the system, even if it is not perceived as a problem in itself, may threaten security and privacy in areas which are not directly related to it.

2.1 Rogue scanning

A fake reader can be used for unauthorized reading of information from a tag. The range of a reader may be extended several times beyond the standard communication distance. For example for standard ISO 14443, used in proximity cards like MIFARE and in electronic passports, the standard communication range is 10 cm. Kirschenbaum & Wool (2006) built a "home-made" reader able to operate from 25 cm at a cost of $100. Further extension of the range up to about 35 cm is possible, probably at a similar cost. Fortunately, range increase is not only a matter of reader parameters. Simulations led by Kfir & Wool (2005) show that ISO 14443 cards can be read from maximum distance of 55 cm in the worst-case scenario, where there is only man-made noise and sophisticated signal processing by the attacker. For larger distances, it is not possible to separate the signal from the noise. However, even 25 cm is enough to read a card in someone's pocket.
Using *short-range tags* wherever possible makes rogue scanning more difficult. *Shielding* with an anti-skimming material (e.g. aluminium foil) when the tag is not in use, protects it from scanning. A specific and common countermeasure against unauthorized tag reading is the *authentication of the reader*. Risk can also be reduced by moving sensitive information to a *protected database* in the system's backend. In this case, in order to retrieve information based on an ID number read from the tag, the user must authenticate himself to access the backend part of the system, where authentication methods are not limited by the constraints of RFID technology. However, it should be noted that keeping personal data in a central database is generally perceived as more privacy invasive than when they are kept only on tokens owned by users. Moreover, although the back office can include stronger security than RFID tags, there is always some risk of compromising all the records in one attack. Other concerns related to central vs. local storage are discussed in Section 5.1 of the report (Snijder 2007).
Another countermeasure against rogue scanning is to let the tag send information only when it is *activated by the user* (e.g. by pressing a button), thus the possibility of unauthorized reading is limited to moments when a legitimate communication is demanded. This solution is appropriate for active tags, like car remotes, where the communication can be initiated by the tag. However, for most low-cost passive tags or smart cards, this solution is not practical. Also, in many applications, the full automation of the process is RFID's main asset.
Many privacy concerns can be avoided by *permanent deactivation* of tags which are not going to be used any more. This possibility has been foreseen in the EPC Global standard and will probably become common with the massive deployment of RFID in retail.

2.2 Eavesdropping

Eavesdropping on a legitimate communication is a secret monitoring of data sent via the air interface between an RFID tag and a reader. The attacker does not need to power the tag,

which is already powered by a legitimate reader. Because of this, the maximum range for eavesdropping may be significantly larger (for the same type of tag) than for rogue scanning. Eavesdropping is a passive action – the attacker does not emit any signal – and is therefore very difficult to detect.

The most common countermeasure is encryption of data transmitted between tag and reader, so the signal can still be eavesdropped but not understood. There are, however, several challenges. As we mentioned in the introduction, RFID tags have limited resources. In low-cost passive tags, the total number of gates is about 500-5,000 (Weis, et al., 2004) and not more than half of them can be dedicated to security.[2] Realization of advanced cryptographic algorithms requires from several thousand to about 25 thousand gates. Small amount of power that can be harvested by a tag antenna is also a limitation for processing data. Another issue is related to protection and administration of keys. If symmetric cryptography is applied, all tags and readers share the same secret, and there is a risk that it can be retrieved from any tag. Tags are generally not tamper-resistant and even if a cryptographic algorithm is well defined and does not allow an attacker to obtain the key from a communication, there is a risk that the key will be revealed by spying into the manufacturer's documentation, reverse engineering (of tag or reader) or by a side-channel attack. Advanced asymmetric cryptography algorithms are often too heavy for RFID, and neither are they free from problems with key management. Another possible countermeasure is shielding the tag and reader during information exchange. However, this is rarely applied, as it is not very practical. It is also important to use the standard with the smallest communication range sufficient for a given application.

2.3 Relay attack

Relay attack is a type of man-in-the-middle attack (Kfir & Wool 2005), where the attacker creates a connection between a legitimate reader and the victim's legitimate tag, as shown in Fig. 2. From the point of view of the RFID system, the communication looks as if the legitimate tag and the reader are close to each other when, in fact, they are communicating through the communication channel, usually wireless, established by the attacker. In this way, the attacker may authenticate himself in an access control system or a payment system. The maximum distance between a legitimate tag and an attacker's reader (called sometimes a "leech") is the same as in the case of rogue scanning, but the distance between a legitimate reader and an attacker's device which simulates a legitimate tag ("ghost") is much longer – up to 50 m. A successful relay attack against an RFID system complying with the ISO 14443A standard has been proven to be feasible (Hancke 2005).

Since the attacker only re-transmits information, without the need to understand it, the authentication protocol (e.g. challenge-response) does not protect against this kind of attack. This threat can be countered by using short range tags and by shielding tags (e.g. by keeping them in bags containing aluminium foil, when not in use). There is also a specific countermeasure against relay attack – distance bounding protocol – which estimates the distance between the reader and the tag, based either on response time (Hancke & Kuhn, 2005; Reid et al., 2006) or signal-to-noise rate (Fishkin & Roy, 2003).

[2] The number of gates in tag increases from year to year but still memory and power harvested by the antenna are strong limitations to the security on the tag side. In most applications the manufacturers focus rather on reduction of tag costs than increasing memory size.

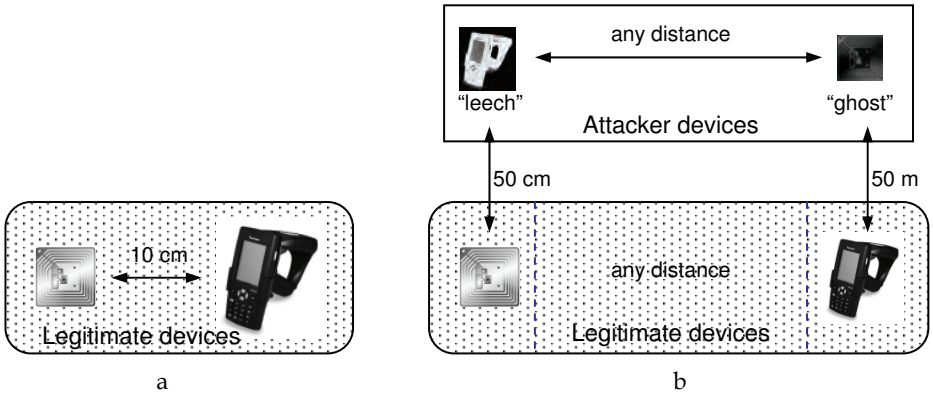

Fig. 2. A legitimate communication (a) and relay attack (b). Maximum ranges refer to ISO 14443 and are based on theoretical results received by Kfir & Wool (2005)

2.4 Cloning the tag

'Cloning' means making a duplicate of an RFID tag. A clone may be similar in form to the original or be a larger device with the same functionality. Duplicates can be used to access a restricted area, abuse private data or make an electronic transaction on behalf of a victim.

Cloning can be prevented by the use of cryptographic methods for authentication of the tag. If a challenge-response protocol is used, information which can be obtained by the attacker using the air interface (e.g. by eavesdropping) is not sufficient to duplicate the tag. Although reverse engineering, in theory, may allow duplication of any electronic circuit, these methods require special equipment and a very high level of knowledge. Moreover, there are countermeasures which can be applied at the circuit manufacturing stage.

Authentication of the tag should be based on well established cryptographic algorithms, which are constantly analysed by researchers. Although their security has not been mathematically proved, it can be assumed that their vulnerabilities are well known. The use of proprietary methods, where security is supposed to be based on secrecy of the algorithm, is generally not recommended. There are at least several examples where RFID authentication protocols, developed in laboratories of big companies, have been cracked. The best known cases are the cracking of Digital Signature Transponder (Texas Instruments) and of MiFare (Philips), described in Section 3.3. On the other side, looking at almost twenty years of contact smart card history, we cannot agree with popular opinion that security should be based only on the secrecy of the key. Especially when it comes to chip design, public chip schemes would make it much easier to retrieve the key directly from the circuit and therefore manufacturers make a considerable effort to hide the structure and mislead those who try to discover it (see section on reverse engineering).

Another frequent reason for security gaps (in the two cases mentioned and many others) is too short encryption keys. Short keys mean lower power consumption and lower cost, so manufacturers try to use the shortest keys which, at the moment, seem safe. However, the lifetime of a solution like this is often longer than foreseen and, due to progress in technology, the size of the key is no longer sufficient. Unfortunately, when the system is already deployed on a large scale (like DTA and MiFare), the cost of security updates is enormous.

2.5 Tracking of people

Tracking of people takes place when an attacker follows the movements of individuals through the RFID tags they carry with them. Tracking can be performed with rogue readers placed, for example, in doors, or by the deployment of eavesdropping devices in the proximity of legitimate readers.

Many countermeasures to reduce the risk of tracking have already been mentioned, like using short range tags, shielding them, authentication of readers and disabling tags when not used. However, we can foresee that, in the future, people will carry many RFID tags with them and therefore a personal device which controls access to them, possibly integrated in their mobile phones or PDAs, may be very useful – like the one proposed by Rieback et al. (2005). There are also countermeasures which can be implemented at tag-design stage, such as: pseudonyms (changing identifiers) or estimation of distance from the reader (Garfinkel et al. 2005).

2.6 Replay attack

In the case of replay attack, the attacker abuses another person's identity by repeating the same authentication sequence as the one provided by an authorized person. A replay attack may be led by a clone of the legitimate tag or by re-sending the eavesdropped signal from a PC equipped with an appropriate card and antenna.

In order to perform a replay attack, an attacker has to obtain some information which is sent by the tag during normal communication. The first line of defence is therefore to counter eavesdropping and unauthorized tag reading. A specific countermeasure against replay attack is authentication of the tag e.g. with a challenge-response protocol. If the protocol is well designed, the key necessary for calculation of response cannot be deduced from information exchanged through the air interface.

2.7 Malicious change of the tag content

As a result of malicious change of the tag content, the attributes of an item described by the tag may be distorted or an authorized person may be falsely rejected by the access control system. Furthermore, writable tags may become carriers of malware, e.g. data on RFID tag can be maliciously modified in such a way that they are interpreted by the system as a command. An example of a successful attack of this type is the SQL injection described by Rieback et al. (2006).

In some writable tags, memory content can be protected by temporarily or permanently disabling writing capability (*'lock'* and *'permalock'* functions in standard EPCglobal Class 2 Gen 2). Malware on RFID tags cannot affect the system if the implementation excludes the possibility of interpretation of the tag's data as a command. This is similar to switching off macros in MS Office which protects the system from running malicious code embedded in documents.

Using sophisticated equipment, like a focused ion beam, it is also possible to change the content of memory (EEPROM or ROM) in non-writable tags. This technique can be used to set a secret key to a known (zero) value, but it also requires that the location of the key in memory is known, expensive equipment, a high level of knowledge and considerable effort. In high security applications, measures like protective layers on chips and memory scrambling make this kind of attack impractical.

2.8 Physical tag destruction

Physical tag destruction, e.g. by heating in a microwave or hitting with a hammer, is the easiest and the cheapest way to disrupt RFID systems. This is a particular issue for applications where RFID tags are used not only for identification purposes, but also for the protection of items against theft, like in retail or in libraries. RFID tags in e-passports can be destroyed by owners who have concerns about possible abuse of their privacy – especially as an e-passport with a non-working RFID tag is still valid (Wortham 2007).

2.9 Blocking and jamming

Blocking is performed with a 'blocker' tag, which simulates the presence of an enormous number of tags and causes a denial of service (non-ending interrogation of physically non-existing tags by the reader). However, blocking may also be a useful mechanism and serve, as originally proposed, for the protection of consumer privacy, when a blocker tag protects from unwanted scanning (Juels et al. 2003). Another threat to the air interface is jamming, which paralyses the communication of an RFID system by generating a radio noise at the same frequency as that used by the system.

Blocker tags and jamming devices are easy to detect and localize immediately after starting operation and appropriate warning functionalities can be built into a system.

2.10 Reverse engineering

The term 'reverse engineering' is usually used for invasive methods of discovering circuit structure and even values of voltage at different points of the circuit during its operation. The goal is to retrieve the algorithm or the cryptographic key, often with the final purpose of copying the tag. This kind of attack requires a high level of knowledge and experience, as well as specialized and expensive equipment, like micromanipulators, focused ion beams, laser cutters, microscopes and chemical etching equipment.

The manufacturers of contact smart cards apply a wide variety of measures, which can also be used in contactless solutions, although with some limitations resulting from limited power supply. Typical measures are: dummy structures which do not have any function except to mislead attackers, scramble buses and memory cells, form protective shields on the top of chip (especially memory) and encrypt memory content. Active protection is also possible: sensors included in the circuit can detect symptoms of attack like change of voltage, clock frequency, temperature, etc. - for details, see Chapter 8.2.4 of a monograph (Rankl & Effing 2004). Due to resource limitations, RFID-based cards allow only limited protection and especially active methods are rather beyond this limit.

There are also methods of reverse engineering at the logical level, without any physical manipulation of the circuit. For example, details of the algorithm used in DST were discovered from a general outline which was published, together with observed challenge-response data for different values of the key, which could be arbitrarily set on blank tokens available from the manufacturer.

2.11 Side channel attacks

Channel side attacks are based on information gained from physical implementation of cryptosystem, like power consumption, time of computations or electromagnetic field (Bar-El 2003). *Power analysis attack* is based on the fact that different operations consume different power. Analysis of power changes can provide information which, combined with other

cryptanalysis methods, can help to recover the secret key. In *timing attack,* the attacker analyses time needed to perform operations. For example, in straightforward implementation, PIN comparison is done byte by byte and returns no-match result after the first difference. Based on time, it can be deduced which byte caused the rejection of a PIN number and a guess can be made, byte by byte. Analysis of the *electromagnetic field* around the chip during its operation is more difficult for RFID than it is for contact chips, because of the interference with a stronger field which comes from the communication with the reader. However, as shown in (Carluccio at al. 2005), after separation of the antenna from the chip, the electromagnetic field generated by operation of the chip can be analysed.
A basic countermeasure against side channel attacks is to design hardware and software to keep power consumption steady and ensure that the time taken by calculations does not depend on data or partial results of the operations. This can be achieved by avoiding conditional execution of any part of the code, even if the result of the calculation is not going to be used. In hardware design, manufacturers can add dummy registers and gates, which balance the consumption of energy but, again, resources for this kind of measure are very limited. An exhaustive list of references on side channel attacks can be found at http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html.

3. Discussion of selected applications

In this section, we will discuss the application areas which we found especially important and sensitive to privacy and security threats. Our selection is based on several criteria:

- The importance of the application in terms of economics (market value, number of tags) and social impact (number of users, social implications).
- Security and privacy-related criteria, proposed in (Rotter 2008):
  - Range of deployment of the system
    In systems operating locally within a restricted area, information between readers and the backend of the system is exchanged through a local network. Applications of this type, like some manufacturing processes or access controls, are generally less sensitive to security risks, as the physical security of the place is the first barrier to attacks. At the other extreme are global systems, where breaking security gives access to the data on millions of tags worldwide, or to a central database.
  - Type of link between an RFID tag and identity-related data
    Privacy risks only exist in systems where it is possible to establish a link between the RFID tag and the identity of a person. Systems where it is not possible to link a tag to the identity of a person, for example most industrial and livestock tracking systems, do not raise any privacy concerns. In item-level tagging for example, or in anonymous tickets in public transport, a tag can be temporarily linked to identity. In some other applications, this link is fixed and defined in the system – like e-Passports, payment systems, (e.g. Speedpass) and personal tokens for access control. Future applications of this type include credit card systems, location-based services and mobile phones equipped with Near Field Communication. Finally, systems based on RFID implants are the most privacy-sensitive as the link between a person and an RFID tag is physical and not very easy to remove.
  - Demand for security
    Demand for security depends mostly on two factors: a) the size of potential damage, in terms of loss of money, loss of customers or, for example, disclosure of

privacy-sensitive information, and b) the level of motivation of attackers, related to the potential prize they could win if they are successful. These two factors are often correlated but not always: for example, in medical information systems, wrong treatment may cause serious damage. In general, however, attacker motivation is much lower than it is, say, in payment systems or e-passports.

In the case of security (not privacy)–demanding applications, we pay more attention to the public sector, as we believe that the business sector will more easily find a proper balance between expenses for security measures and losses caused by insufficient security.

- Coverage of the most relevant issues related to security and privacy in the set of selected applications.

We do not offer a complete overview of all the application areas where privacy and security is relevant - for example, we do not discuss e-payment and access control. However, the privacy and security issues in these areas are similar (at least qualitatively) to those related to transport or other presented applications.

3.1 Item-level tagging

RFID is becoming very popular in logistics and the supply chain (Bose & Pal, 2005), where it is employed as a kind of barcode with new, very desirable features. For example, unlike printed barcodes, RFID tags do not have to be in line-of-sight to be read, and they enable multiple scanning (e.g. the whole truck or basket at once) allowing for further automation in many industrial processes. In contrast to a barcode, which replicates an identification number only, tags may contain other information e.g. product details or, if combined with sensors, the history of storing conditions, mechanical shocks, etc.

Threats to the privacy and security of users

Item-level tagging brings privacy threats, which may limit its deployment. RFID tags attached to objects people have bought can be interrogated by someone to reveal what items they have in their shopping bags (including, for example, medicines) or the prices they paid. Moreover, although the set of things a person carries changes, it does not usually change completely. Such a set, called the "RFID shadow" or "RFID constellation" of a person (Garfinkel et al., 2005), if regularly updated, may serve to effectively track that person. RFID tags used for retail cannot be read from more than several meters, even if the standard reading distance is extended by a more powerful reader. However, if attackers placed readers at the entrances of shops, metros, airports, etc., they would be able to track individuals. This possibility has raised concerns for some privacy organizations and individuals, like those presented in (Albrecht, McIntyre 2005).

Moreover, there is a potential risk of physical attack on a specific individual, based on his/her automatic identification. In the case of electronic passports some attention has been paid to the possibility of constructing a bomb triggered by information received from the RFID chip in the e-passport of a specific person or citizen from a specific nation ("American-sniffing bomb"), see e.g. (Juels et al., 2005). An RFID constellation could be used in a similar way and some features of tags used for item-level tagging make them even easier to exploit for potential attackers. First, they have a longer standard range, typically 30-70 centimetres, compared with 10 cm for the standard 14443A tag used in e-passports. In both cases, the standard range can be extended: for e-passports to about 30-40 cm, but for tags used in retail considerably further. Second, the e-passport has security protection mechanisms, which

make unauthorized identification of the owner more difficult, which are not included in tags used in retail. Another concern of some consumers and privacy organizations is 'function creep', i.e. using a large amount of data obtained by RFID systems for different purposes than original ones intended by the system. For example, the data collected by retailers could be used for unsolicited targeted advertising, customers could be discriminated against on the basis of their purchase history, and the police or intelligence agencies could request the data.

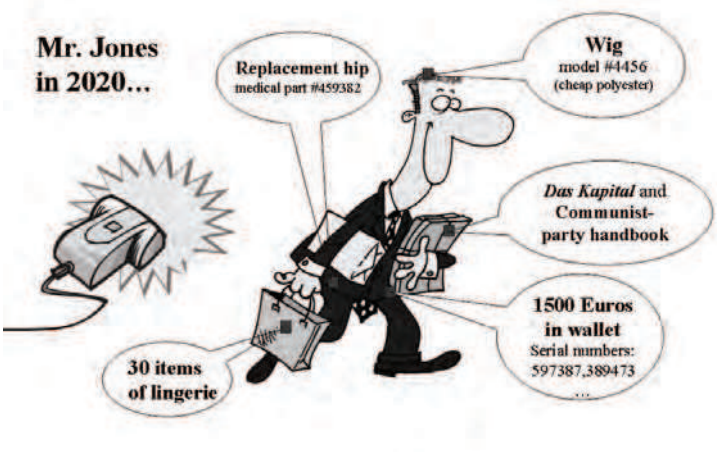

Fig. 3. The consumer privacy problem. Privacy concerns around RFID and the vision of society under surveillance may significantly influence future deployment of item-level tagging. Source: (Juels 2006)

Concerns about privacy and security are the main reason for low public acceptance of item-level tagging. Even the big retailers, which for economic reasons are definitely interested in quick deployment of RFID, must consider public opinion. Benetton's plans to attach RFID tags to items of clothing caused a boycott of the company's products, organized by CASPIAN[3] (http://www.boycottbenetton.com). Protest campaigns have been organized against some retailers - for example, WalMart. Undoubtedly, the concerns of consumers and their low acceptance of RFID in item-level tagging have slowed down its deployment. Another important implication of privacy and security issues for the RFID market is the need for the application of technical and legal measures, which make RFID (both single tags and whole systems) more complex, and therefore more expensive.

On the other hand, the demand for security can be seen as a market opportunity. Apart from the need for security to be built into RFID systems, we can foresee the demand for personal devices which help the user to keep control over the tags he owns. Such devices, for example the RFID guardian mentioned in the paragraph on countermeasures, can be integrated into mobile phones or PDAs.

Security threats – the retailers point of view

Item-level tagging is related to a number of privacy concerns, but there are only a few threats related to system security. An attacker who can change the memory content of an

[3] Consumers Against Supermarket Privacy Invasion and Numbering

RFID tag can modify information about the product. This action could falsify the price of the product and this could lead to small fraud or, if maliciously applied on a large scale to all products in a supermarket, could cause considerable losses. Writable tags, even those as simple as EPCGlobal tags, can be carriers of malware (e.g. SQL injection). Physically destroying the tag, or tearing it off the object, is the simplest and the cheapest way to disrupt RFID systems. This vulnerability may be exploited when an RFID system is used to protect items against theft. Blocking and jamming are threats to the air interface and may result in paralysing RFID system communication.

Generally, the demand for security in item-level systems is not very high and the risk is mostly related to material losses on the part of retailers, which are able to apply corresponding countermeasures and ensure an adequate level of security at reasonable cost.

Countermeasures

The basic security measure against unauthorized reading of RFID tags attached to items is deactivation of the tag at the supermarket check-out. A "Kill" command, foreseen in EPCGlobal standard (EPCglobal 2004), permanently and irreversibly disables the tag. Another method, which gives full control over deactivation to the user, is a design of tag which facilitates its easy mechanical destruction by the owner (Karjoth & Moskowitz 2005). Unfortunately, deactivation of the tag also disables post-sales services. For example, clothes tagged with RFID could automatically set the appropriate programme in a washing machine, a refrigerator could be "aware" of its content and report what kind of food should be bought (or even make an order on the Internet), and microwaves could prepare food according to instructions. If tags are deactivated when products are sold, none of this would be possible. A "killed" tag cannot be used if the item is returned to the shop or if the product is recalled, which can be essential for some products. For example, a tracking capability which facilitates recall in the case of safety defects is one of the main drivers for the introduction of RFID in tyres (Garfinkel et al., 2005). Disabling of tags after item purchase will also squander the chance to use RFID for automatic segregation of waste and recycling.

Researchers have therefore proposed several methods which give the user full control over the tags in his possession, so it is not necessary to deactivate them. RFID guardian, proposed by Rieback et al. (2005), is a device which the user carries with him, possibly embedded in mobile phone. It allows tag information to be read only if the user agrees and warns him about unauthorized reading attempts. However, this device has not been commercialised as yet.

In addition to technical aspects, legal privacy measures should also be applied. For example, retailers should be obliged to give customers at least the option to deactivate tags, and to mark places where RFID readers are operating with special signs.

3.2 Electronic identity documents

In order to make the identification of people more resistant to falsification, faster and more convenient, there is a need to store the data on identity documents in a form which allows automatic reading. Different technologies are used for this purpose, like cards with magnetic strips, contact smart cards or even optical memory, like in Italian ID cards. Although these technologies are not as convenient as RFID, privacy and security aspects and the low acceptance of RFID technology are sufficient arguments against its use. The situation is different in the case of electronic passports. The booklet form of the passport makes the use of contact solutions difficult. On the other hand, although the air interface of

RFID creates potential threats, this technology, due to data processing on chip, allows for much more sophisticated and robust security measures than, for example, magnetic or optical data storage. RFID-based e-passports have been recently introduced in many countries, including all the European Member States. Each e-passport contains personal data and a digital photo of the owner. The second generation (introduction in European Union is planned for 28 June 2009) will include also fingerprints. In the future, other biometrics, especially iris data, could be added.

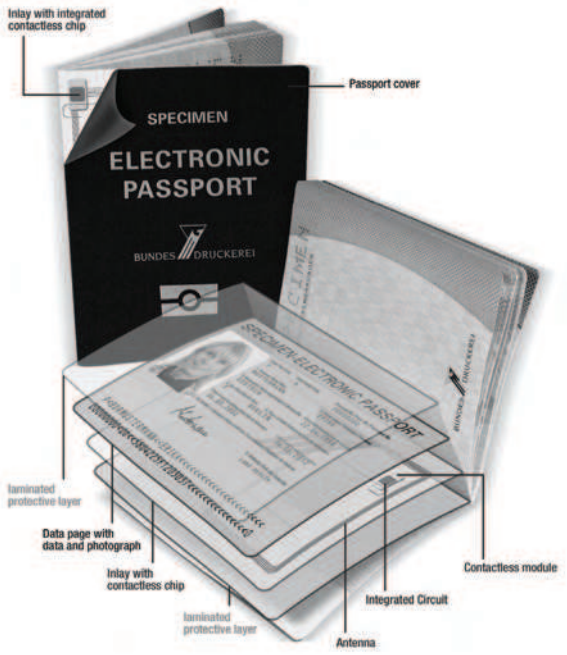

Fig. 4. The Physical form of an electronic passport is the same as a traditional one. Passports with RFID are marked with a sign " " on the cover. Source: Bundesdruckerei GmbH

Privacy and security of electronic passports

Personal and biometric data are particularly sensitive and the possibility of unauthorized access to these data by rogue scanning of passports in owner's pockets, or eavesdropping at border checkpoints, is a major privacy concern. The maximum range for rogue scanning is about 30 cm, while for eavesdropping it is at least several meters.[4] Another privacy threat is people tracking with extended-range readers built, for example, into door frames. Identification of the owner of a passport or of an issuing country might lead to the construction of a bomb triggered by the proximity of citizens with defined nationalities (Juels et al., 2005), see video at: http://pl.youtube.com/watch?v=-XXaqraF7pI.

[4] E-passports are based on standard ISO 14443, details on maximum range for scanning are discussed in section *Rogue scanning*. At the Black Hat 2005 Security Conference in Las Vegas, NV, a company called Felixis, demonstrated eavesdropping from over 20 m (Thornton et al. 2006).

Countermeasures

The standard security mechanisms offered by electronic passports is called Basic Access Control (BAC). The data printed on the last page of a passport (passport number, expiry date, name and date of birth of the owner) are scanned at the checkpoint and, on the basis of this data, the 128-bit key is calculated. The size of the key would be sufficient (the National Institute of Standards and Technology recommends 112 bit as safe till 2015) but the information which serves as a base for key calculation has limited entropy. Moreover, the data on the last page of a passport are interrelated, e.g. the passport number is related to issue date. As demonstrated in (Hoepman et al., 2006), the total entropy of the key can be decreased to merely 41 bits (an example which has been calculated for Dutch passports), which is definitely not sufficient.

Storing fingerprints in e-passports will require stronger security than BAC. As recommended by ICAO, fingerprints in European passports will be protected by Extended Access Control (EAC), which is based on asymmetric cryptography. EAC includes the authentication of both the passport and the reader and limits access to additional biometrics (other than face image) to countries which have an agreement with the issuing country, see (Gemalto, 2007) for details. Generally, EAC offers strong security but it has some weak points:

- Additional biometrics will be used only to authenticate citizens of "friendly" countries (authorized by the issuing country). Border controls, if any, between such countries are usually not very strong anyway. Identification of citizens of other countries will not be facilitated by additional biometrics.
- As an e-passport contains a passive chip, it does not have an internal clock and must rely on date information received from the reader. Therefore it cannot effectively verify if the reader's certificate is up-to-date. According to the standard, passports should keep the date sent by the reader in the most recent authentication, which mitigates the problem but does not solve it definitively.
- Revoking the authorization of a reader to read e-passports is technically impossible. This means that a stolen reader will keep its certificate until it expires. Even after this, it is possible to use the reader to read passports which had not updated the date after the expiry date of the certificate.[5]
- As noted by (Hoepman et al., 2006), shallow certificate hierarchy makes it difficult to use e-passports for many applications (problems with the management of certificates). On the other hand, reserving additional biometrics exclusively for border control facilitates user privacy.

As regards the tracking of people with rogue readers, the attacker would either need to break BAC security or use the tag identifiers which are part of the anti-collision protocol. The second possibility, discussed in (Hoepman et al., 2006), can be relatively easily eliminated by using a random number as an anti-collision identifier. Still, the information exchanged between the RFID tag and the reader *before* authentication allows, in many cases, the identification of the issuing country.

[5] Additional measures are possible: the certificate does not need to be kept physically on the reader but can be sent to the reader though a secure connection when it is needed. It must be also noted that a stolen reader would not be sufficient for secret scanning anyway, as BAC is additional barrier.

At the moment, Basic Access Control seems to be a weak point in e-passport security. The introduction of Extended Access Control will not solve this issue, as BAC will remain the main way of protecting access to personal data and digital photos. Simple ways of increasing the security of BAC, as proposed by Avoine et al. (2008), are: a) the introduction of progressive time delay[6] when several queries are received in a short period of time and b) increasing the entropy of BAC keys by random numbering of passports and by filling in the optional (usually not used) field on the last page of a passport with a random number. Apart from sophisticated cryptographic measures, shielding seems a simple, effective and inexpensive solution. It has already been introduced in the United States: one passport cover contains the chip and the other contains anti-skimming material, so the passport cannot be read when it is closed. Common introduction of shielding in e-passports would substantially increase the level of security. In general, as pointed out in (Snijder, 2007), there is a need for an integrated approach to privacy and security for e-passports, harmonized at international level.

Deployment of electronic passports is still in the early stages. They have demonstrated some vulnerabilities, which should be improved. On the other hand, it is also important to understand the security offered by electronic chips in the broader context (Kefauver, 2007). A single instance of the vulnerability of RFID in passports does not necessarily imply the vulnerability of the whole system. For example, though data from the chip can be copied relatively easily, they cannot be easily modified. The use of biometrics will therefore ensure that a clone will not be very useful for illegal border crossing. RFID and biometrics are additions to security measures used before and there is no doubt that the introduction of RFID substantially increases overall security.

3.3 Transport

The first widespread applications of RFID are related to cars. Remote control devices that open/close cars are nothing other than active RFID tags. Immobilizers, a fairly efficient way protecting against theft, are RFID passive tags embedded in a key, which communicates with the car reader to authenticate a key. Tags mounted in cars allow automatic collection of tolls. The Speedpass System facilitates fast payment at ExxonMobil petrol stations and McDonalds in the US (Garfinkel & Rosenberg 2005, chapter 10).

Contactless smart cards and single-use RFID-based tickets have been used for several years in mass transport, making it more efficient and effective. The throughput of passengers through metro gates has increased considerably in cities where RFID-based travel cards are used. Precise data about travel patterns help to optimize the schedule and number of vehicles to increase the system performance. Contactless cards make a big difference to convenience for passengers: it is much easier and faster to pass a metro gate or to cancel a ticket on a bus, if they do not even need to take the cards out of their wallets. At the end of 2007, in a trial programme, Oyster cards were built into mobile phones. Introduction of RFID creates opportunities for new services, like e-purse, rental of bicycles, and facilitates the use of special offers (e.g. holiday tickets). As such systems provide exact information about routes taken by each passenger, they enable new payment schemes, like for example payment per kilometre. Finally, RFID systems, if properly implemented, can provide high reliability and promise a more efficient fight against fraud.

[6] With upper bound, to prevent denial-of-service attack

Privacy concerns around RFID use in public transport

Privacy concerns about tracking of people through rogue scanning or eavesdropping in proximity of legitimate readers are similar to those which apply to electronic documents. Cards used in ticketing have similar range (10 cm with a standard reader) and work on the same frequency as e-passports, so we can expect that attackers would have the analogical maximum ranges of about 30 cm (theoretically up to 50 cm) for rogue scanning and several meters for eavesdropping.

There are some concerns about data which are legally collected by public transport companies. RFID systems provide precise data about each passenger's travel trajectories, which are kept in the system for some time, e.g. 8 weeks in the case of the London system. Although these data are considered confidential, the fact of their collection raises consumer worries about potential abuse. The Metropolitan Police regularly request journey information about Oyster card users. The information has been used as an investigative tool to track movements of criminals; however the rapid increase of the number of queries has attracted press attention (7 requests in the whole year 2004, 61 in January 2006 and 243 in March 2006). On the other hand, it seems that most users do not mind their travel data being collected since the convenience, lower prices and additional services compensate for this. In the Oyster system, users can choose between personalized and anonymous cards, which do not allow direct assignation of travel trajectories to a passenger name. In practice, many more people choose personalized cards, as these provide more services.

Security issues

As previously mentioned, the use of proprietary solutions may cause security gaps in the system. Nevertheless, due to the limited resources of RFID tags, many companies try to develop their own security algorithms, in order to provide security at lower computational or memory cost than well known and researched solutions. This was the case of the Digital Signature Transponder (DST), used in many immobilizers, for example in Ford and Toyota cars and in the Speedpass system. In 2004, researchers from the John Hopkins University and RSA Laboratories managed to break DST security. They used a general outline of the algorithm published on a website by a Texas Instruments researcher and found out the details by reverse engineering.[7] Having discovered the algorithm, they were able to break a 40-bit key in a brute force attack based on two input-output pairs (Juels 2005), see Bono et al. (2005) for details.[8] The story does not imply that systems which use DST with 40 bit keys are entirely unsafe. The challenge-response protocol of tag authentication is only one of several layers in car anti-theft protection and in Speedpass security. Moreover, cracking requires specialized equipment and knowledge, while most car thieves are opportunists. On the other hand, the level of protection is undoubtedly significantly lower than intended by the developers.

Another successful attack against proprietary encryption was reported at the beginning of 2008. Researchers were able to recover, in an algebraic attack, a 48-bit key used in the MiFare Crypto-1 algorithm. This algorithm has been implemented in about one billion RFID tags, mostly in public transport: London Oyster Card, Dutch public transport OV-

[7] They use so-called blank tags – tags where a secret key is programmable, and analysed authentication sequences with different key values. They did not use any invasive methods.

[8] Some photos and videos are available at: http://www.carthiefstoppers.com/About-RFIDs-and-the-Texas-Intruments-DST.html

Chipcard and Boston Charlie Card, and also some access control applications. According to preliminary results, published in (Courtois et al., 2008), the attack can take only several minutes and can be based on a single eavesdropped transaction. Although the researchers published only general information and the details needed for a repetition of the attack were not revealed, it is highly probable that they will be discovered and used in a malicious attack soon. Public transport systems, built at high cost with the promise of fraud reduction, may even increase it. Moreover, the fraud can be more troublesome, as free journeys with cloned cards would be charged to the accounts of particular passengers.
The security issues described in this section apply largely to other application domains, especially access control systems and electronic payment.

Countermeasures

Cases like DST and MiFare Classic show that security measures applied at the production stage may suddenly become insufficient. Unfortunately, if the system based on an insecure solution has already been developed, it may be extremely costly to upgrade it, especially if the security gaps exist at tag design level. Therefore, special attention should be paid at the manufacturing stage in order to avoid errors like:

- Security gaps in proprietary encryption algorithms.
- Insufficient key size – this can be long enough while the tag is being designed but, due to technological progress, become too short after several years.
- Insufficient key entropy – for example, a 32-bit nonces used in MiFare Classic has, in fact, only a 16-bit entropy, due to a weakness in the pseudo-random generator (Nohl & Plötz, 2007).

If security gaps are reported when the system has been already developed, there are still solutions which can help to make it more secure, and avoid the need to immediately replace the tags. De Koning Gans et al. (2008) propose the use of strong encryption in the backend and the storage of encrypted information only on the tags. In any case, systems should not rely only on the security of the tag and it is important to include fraud detection in the backend, as has been done in the DST-based Speedpass system.
In order to ensure privacy a number of privacy-enhancing technologies (PET) can be applied, like those proposed by Heydt-Benjamin et al. (2006). However, they make public transport systems even more complex and costly, and it seems that, in the near future, the main goal of developers will be to reduce costs and decrease organizational complexity by providing security at the minimum level necessary, rather than to deploy advanced PET methods.

3.4 RFID implants

RFID implants are passive tags implanted under the skin, to provide a means of personal identification. As they operate without a battery, they can be operational for many years once implanted. The use of RFID implants for the identification of people provides some advantages compared to established methods. The identification process is practically immediate and fully automatic – and therefore extremely convenient: the user is not required to take any action. Implants cannot be lost, stolen or forgotten. They are a reliable method of identification, especially when compared to biometrics, where due to the statistical nature of the matching process, there is always some error probability. Implants are more durable than tokens and many types of biometrics, which usually change during a person's life. RFID implants can be used by everyone without exception, including people

with cognitive impairment. The user can always be identified, even if he is unconscious or not carrying any identity documents.

Present commercial applications

In 2004, the first and, until now, the only RFID implant – the VeriChip – obtained approval from the U.S. Food and Drug Administration. The VeriChip implant (www.verichipcorp.com), which stores only an identification number, can be read from a distance of about 10 cm with a handheld reader and 50 cm with a door reader. The ID number is long enough to identify uniquely everybody in the world. Other data related to the owner are not stored in the implant, but in a centralized database.

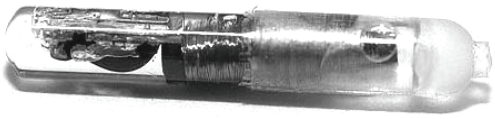

Fig. 5. VeriChip implant (original size 3×13 mm). Electronics is encapsulated in bioglass in order to make it biocompatible.

The first commercial application, called VeriMed, is designed to identify patients in healthcare. An authorized doctor can access a patient's medical files through a password-protected website, using the patient's ID number which he can get from an RFID reader (www.verimedinfo.com). Another commercial application based on the same type of implant is VeriGuard – a system for access control to physical spaces like, for example, offices. Implants are also used in entertainment: for example, members of the Baja Beach Club in Barcelona and a Rotterdam club, who have RFID chips implanted, benefit from a quicker VIP service. To date, about 2,000 people have been implanted with VeriChip tags. RFID implants can be potentially used in the future for identification and authentication in many application areas, either as the only ID technology or in combination with other methods – a detailed discussion can be found in (Rotter et al., 2008).

Security and privacy concerns

In spite of their high potential, RFID implants raise some serious concerns, largely related to security and privacy. The permanent and physical link between an RFID tag and a person makes RFID implants more susceptible to privacy risks than any other kind of contactless tokens. The user can be identified any time, without his consent or awareness. Here, the tracking of people, already a concern in item-level tagging and e-documents, is much easier, effective and more difficult to prevent. RFID implants used for authentication are particularly vulnerable to coercive attacks, where attackers force authorised users to provide their credentials. RFID implants carry the risk of physical harm, as attackers could cause injuries by extracting the implants from the victims' bodies. For this reason, the use of RFID implants for secure authentication is questionable, regardless of any technical security solutions. It is even argued that implants should not include high security in order to make their extraction by an attacker unnecessary (Halamka et al., 2006). However, lack of security reduces the reliability of the identification and therefore limits possible areas of application. In addition, RFID implants, especially in their current form, are susceptible to cloning and replay attacks – for a detailed description of VeriChip cloning, see: http://cq.cx/verichip.pl.

Security measures for present and future use of implants

Their lack of an internal power source and the small size of their antennae limit the processing power of RFID implants. It is therefore difficult to include advanced authentication methods in their design. Currently deployed RFID implants do not include

even basic security. The tag, when interrogated, sends back an identification number without any type of encryption. It is, however, possible to include some security measures like encryption of the identification number and authentication of the reader. There are examples of individuals who have been implanted with RFID tags, which were originally manufactured for industry or supply chain purposes, and are equipped with cryptosecurity features (Graafstra 2006).

Fig. 6. An X-ray of Amal Graafstra's hand. The chip in the right hand is a Philips HITAG S 2048 and is equipped with crypto-security. Source: http://www.amal.net/rfid.html

Implants, even if not equipped with strong security features (authentication protocol), can be used as an element of access control systems safely, increasing the security and the efficiency of the overall system. Combined in multimodal systems, they protect against spying for passwords or against stealing tokens. In systems with authentication based on passwords and tokens, implants as an additional modality counteract unauthorized delegation of privileges to colleagues. In secure environments, implants could be used for continuous detection of presence in the sense that access (e.g. to control boards, or computers) is blocked immediately when authorized people leave and then can be re-established through other, more secure authentication methods. In any case, when strong security is required, implants should be used only as an *additional* means of authentication.
It is worth noting that security and privacy issues are not the only concerns related to implants. Social acceptance of implants is, at the moment, very low. Unclear health implications, especially the possible relation between implants and cancer (Lewan, 2007; Wustenberg, 2007; Rotter et al., 2008), understandably limit the number of people who would like to use them and may even stop their further deployment.

4. Conclusions

Concerns about privacy and security may limit the deployment of RFID technology and its benefits, therefore it is important they are identified and adequately addressed. System developers and other market actors are aware of the threats and are developing a number of countermeasures. RFID systems can never be absolutely secure but effort needs to be made to ensure a proper balance between the risks and the costs of countermeasures.
The approach taken to privacy and security should depend on the application area and the context of a specific application. In this chapter, we selected and discussed four application areas, but there are many others where privacy and security issues are relevant. In Table 1, we list the main threats and the application areas in which they arise.

Threats	Application areas	Main countermeasures
Rogue scanning of confidential data from personal documents	E-documents, e-payment, mass transport, access control cards, healthcare	Using short-range tags, shielding, authentication of the reader, moving sensitive information to a protected database, activation of tag by the user
Rogue scanning of data of items carried by a person	Item-level tagging (retail)	Permanent deactivation ("kill" command), RFID privacy management devices like RFID guardian
Eavesdropping of confidential data from personal documents	E-documents, e-payment, mass transport, access control cards, healthcare	Data encryption, using short-range tags, shielding tags with reader during information exchange
Rogue scanning or eavesdropping of other non-public data	Logistics, administrative process, industry	Data encryption, using short-range tags, shielding, authentication of the reader, moving sensitive information to a protected database, restricted physical access
Relay attack	E-payment, e-documents, access control	Using short-range tags, shielding, distance bounding protocols
Tag cloning and replay attack	E-documents, e-payment, mass transport, access control cards	Tag authentication with challenge-response protocol, tag design which counters reverse engineering
People tracking	Item-level tagging, e-documents, public transport, RFID implants, e-payment, access control cards	Reader authentication, 'kill' command (in some applications, mostly retail), random identifiers in anti-collision protocol, changing pseudonyms, using short-range tags is possible, shielding (in some applications)
Change of tag content (e.g. registers value)	E-payment, transport (ticketing), some of applications for access control, e-documents and administrative process	Limited use of re-writable memory in tags, disabling writing feature ("lock" and "permlock" commands)
Physical tag destruction	Item-level tagging (anti-theft protection), e-documents (possibility of destruction by citizens concerned about their privacy)	Adequate physical location of tags on objects in retail
Blocking and jamming	Applications where attacker can benefit from denial of service (e.g. security-related)	Facilities for detection and localization of jamming devices.
Reverse engineering and side channel attacks	High security applications: e-payment, access control, e-documents	Protective layers, dummy structures, memory and bus scrambling, encryption of memory content; design of the tag which ensures data-independent time and power consumption

Table 1. Threats to privacy and security in RFID systems, application areas where they exist and the main countermeasures

Security and privacy must be considered in the early stages of RFID system development; a large part of technical security measures should be taken into account at the stage of tag design. Developers should consider not only present but also future levels of risk resulting from foreseen improvements in the technology used by attackers. Updating security later is very costly, much more so than it is in traditional information systems. Here, when a new vulnerability is discovered, it is rarely possible to solve the problem with a software upgrade like a security patch. Special attention should be paid to the concept of privacy by design (EDPS, 2007).

In object-level tagging, the low price of the tag is essential for massive deployment. To keep tag costs down, ways may be found by research and development to shift security and privacy behind the tag, either to another part of the RFID system (readers-backend) or to personal devices for tag management.

The future will bring further automation. The 'Internet of things' is a vision of a global network where not only computers but also billions of items tagged with RFID can communicate. This, together with sensor networks where RFID-type communication will also play an important role, will become part of a pervasive intelligent environment, called Ambient Intelligence (Daskala, Maghiros 2007). If security is not properly elaborated before it happens, huge amounts of data continuously collected in such an environment will be beyond control.

There is a need to complement technical security with legal measures and their enforcement, and to promote best practices by industry. Technical solutions alone will not be sufficient to protect against illegal retention and abuse of personal data or function creep. Moreover, the deployment of RFID and its benefits may be limited not only by real threats but also by the concerns of potential users, resulting from their lack of awareness. Awareness and trust should be created simultaneously with the development of appropriate measures to counter real threats.

5. Acknowledgments

This chapter is based on research done within the EU-funded project "Study on RFID Technologies: Emerging Issues, Challenges and Policy Options", led by JRC-IPTS.

The author would like to thank Ioannis Maghiros from the European Commission, DG Joint Research Centre – IPTS for many helpful comments and suggestions and Patricia Farrer from DG JRC – IPTS for help with preparation of the manuscript.

The views expressed in this article are those of the author, and in no way represent the European Commission's official position.

6. References

Albrecht K., McIntyre L. (2005). *Spychips. How major corporations and government plan to track your every move with RFID*. Nelson Current 2005.

Alien Technology (2005). *EPCglobal Class 1 Gen 2 RFID Specification*. Alien Technology. Whitepaper 2005

Atkinson, R. (2006). RFID - There's Nothing To Fear Except Fear Itself. *Opening Remarks at the 16th Annual Computers, Freedom and Privacy Conference, 4 May 2006, Washington DC.*

Avoine, G. (2004). Privacy Issues in RFID Banknote Protection Schemes. *International Conference on Smart Card Research and Advanced Applications - Cardis, August 2004*

Avoine, G., Kalach K. & Quisquater J.J. (2008). Passport: Securing International Contacts with Contactless Chips. Financial Cryptography, January 2008, LNCS, Springer-Verlag.

Bar-El, H. (2003). Introduction to Side Channel Attacks. Whitepaper, Discretix 2003. Available at: http://www.discretix.com/wp.shtml

Bono et al. (2005). Security Analysis of a Cryptographically-Enabled RFID Device. *14th USENIX Security Symposium, pages 1--16. USENIX, 2005*. Available at: http://www.usenix.org/events/sec05/tech/bono/bono.pdf

Bose, I. & Pal, R. (2005). Auto-ID: managing anything, anywhere, anytime in the supply chain *Communications of the ACM, vol. 48, no. 8, August 2005, pp. 100-106*

Carluccio, D.; Lemke K. & Paar C. (2005). Electromagnetic side channel analysis of a contactless smart card: first results. *Ecrypt Workshop, July 2005.* Available at: http://www.iaik.tu-graz.ac.at/research/krypto/events/RFID-SlidesandProceedings/Proceedings-WSonRFIDandLWCrypto.zip

Courtois, N.T; Nohl K. & O'Neil S. (2008). Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. *Cryptology ePrint Archive: Report 2008/166*, available at: http://eprint.iacr.org/2008/166.pdf

Damgard, I. & Ostergaard, M. (2006). RFID Security: Tradeoffs between Security and Efficiency *IACR eprint, July 2006*

Daskala, B., & Maghiros, I. (2007). Digital Territories. Towards the Protection of Public and Private Space in a Digital and Ambient Intelligence Environment. JRC-IPTS report EUR 22765 EN. Available at: http://ftp.jrc.es/EURdoc/eur22765en.pdf

De Koning Gans, G.; Hoepman, J.H. and Garcia, F.D. (2008). A Practical Attack on the MIFARE Classic. *Proceding of the 8th Smart Card Research and Advanced Applications, CARDIS 2008*

EDPS (2007). *Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'RFID in Europe: steps towards a policy framework'*. 20 December 2007.

EPCglobal (2004). *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID. Protocol for Communications at 860 MHz - 960 MHz. Version 1.0.9.* EPCglobal Inc, 2004.

Fishkin, K.P. and Roy, S. (2003). Enhancing RFID Privacy via Antenna Energy Analysis. Tech. memo IRS-TR-03-012, Intel Research Seattle, 2003.

Garfinkel, S.; Juels, A. & Pappu, R. (2005). RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy, May-June 2005*

Garfinkel, S. & Rosenberg, B. (2005). RFID: Applications, Security, and Privacy *Addison-Wesley Professional, July 2005*

Gemalto (2007). *Moving to the Second Generation of Electronic Passports.* Gemalto white paper, July 2007. Available at: http://www.gemalto.com/brochures/download/2nd_generation_passport.pdf

Graafstra, A. (2006). RFID Toys. *Wiley, 2006*

Halamka, J.; Juels, A.; Stubblefield, A. & Westhues, J. (2006) The Security Implications of VeriChip Cloning. *Journal of the American Medical Informatics Associacion, Vol. 13, Issue 6; Nov/Dec, 2006*

Hancke, G. (2005) A Practical Relay Attack on ISO 14443 Proximity Cards. *Manuscript, February 2005*

Hancke, G. (2006) Practical Attacks on Proximity Identification Systems (Short Paper). *IEEE Symposium on Security and Privacy, May 2006*

Hancke, G. & Kuhn, M. (2005). An RFID distance bounding protocol. *IEEE SecureComm 2005, 5-9 September 2005, Athens, Greece*

Hansche, S.; Berti, J. & Hare, C. (2004). Official (ISC)2 guide to the CISSP exam *Auerbach Publications*

Harrop, P.; Das, R. & Holland, G. *Item Level RFID 2008-2018.* IdTechEx Report, 2008.

Henrici, D. (2008). *RFID Security and Privacy. Concepts, protocols and architectures.* Springer-Verlag 2008.

Heydt-Benjamin, T.; Chae, H.J.; Defend B. & Fu K. (2006). Privacy for Public Transportation *Workshop on Privacy Enhancing Technologies - PET, June 2006*

Hoepman, J.H. et al. (2006) Crossing Borders: Security and Privacy Issues of the European e-Passport. *Advances in Information and Computer Security, volume 4266 of LNCS,* pp. 152-167. Springer Berlin / Heidelberg, 2006

Juels, A. (2004). Minimalist Cryptography for Low-Cost RFID Tags. *International Conference on Security in Communication Networks - SCN, September 2004*

Juels, A. (2005). Attack on a Cryptographic RFID Device. RFID Journal, 28 Feb. 2005. Available at: http://www.rfidjournal.com/article/articleview/1415/1/39/

Juels, A. (2006). RFID Security and Privacy: A research Survey. *IEEE Journal on Selected Areas in Communication.* No 24 Vol 2, pp. 381--394, February 2006.

Juels, A.; Molnar, D. & Wagner D. (2005). Security and Privacy Issues in E-passports. *SecureComm, September 2005*

Juels, A. ; Rivest, R. & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. *Conference on Computer and Communications Security - ACM CCS, October 2003*

Karjoth, G. & Moskowitz, P. (2005). Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. *Workshop on Privacy in the Electronic Society - WPES, November 2005*

Kefauver, B. (2007). ePassports: The Secure Solution. *ICAO MRTD Report, Vol. 2. No. 2, pp. 4-10. International Civil Aviation Organization, 2007*

Kfir, Z. & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems. *SecureComm, September 2005.*

Kirschenbaum, I. & Wool, A. (2006). How to Build a Low-Cost, Extended-Range RFID Skimmer. *IACR eprint, February 2006*

Lewan, T. (2007). Chip Implants Lined to Animal Tumors. Associated Press, 8 September 2007

Maghiros, I.; Rotter, P. & van Lieshout, M. (editors): RFID Technologies: Emerging Issues, Challenges and Policy Options. *EUR Technical Report, EC DG-JRC, IPTS, 2007.*

Marburger, A; Coon, J.; Fleck, K.; Kremer, T. (2005). Verichip. Implantable RFID for the Health Industry *Unpublished document*

Nohl, K.; Plötz, H. (2007). *Mifare - Little security despite obscurity.* Presentation on the 24th Congress of the Chaos Computer Club in Berlin, December 2007. Available at: http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html

Rankl, W. & Effing, W. (2004). *Smart Card Handbook.* John Wiley & Sons Ltd, 2004.

Reid, J., et al. (2006). Detecting Relay Attacks with Timing Based Protocols. *Proceedings of the 2nd ACM symposium on Information, computer and communications security, Singapore 2007, pp. 204-213*

Rieback, M.; Crispo, B. & Tanenbaum, A. (2005). RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. *Australasian Conference on Information Security and Privacy - ACISP, July 2005*

Rieback, M.; Crispo, B. & Tanenbaum, A. (2006). Is Your Cat Infected with a Computer Virus? *Pervasive Computing and Communications - PerCom 2006, March 2006.*

Rotter, P. (2008): A Methodological Framework for the Assessment of Security and Privacy Risk for RFID Systems. In: *IEEE Pervasive Computing, Vol. 7, No. 2, April/June 2008, pp. 70-77.*

Rotter, P.; Daskala, B. & Compañó, R. (2008). RFID implants: opportunities and challenges for identifying people. *IEEE Technology and Society Magazine*, Volume 27, Issue 2, Summer 2008, pp. 24 – 32

Snijder, M. (2007). Security & Privacy in Large Scale Biometric Systems. Report based on an experts meeting held in Brussels on 25 September 2006. EC, Joint Research Centre, IPTS. Available at: http://is.jrc.es/documents/SecurityPrivacyFinalReport.pdf

Thornton et al. (2006). *RFID Security.* Syngress Publishing, Inc., 2006.

Weis, S.; Sarma, S.; Rivest, R. & Engels, D. (2004). Security and privacy aspects of low-cost radio frequency identification systems. International Conference on Security in Pervasive Computing, March 2003, also published as LNCS Vol.2802, pp. 201-212, 2004.

Wortham, J. (2007). How To: Disable Your Passport's RFID Chip," Wired, vol. 15, no. 1, 2007. Available at: www.wired.com/wired/archive/15.01/start.html?pg=9.

Wustenberg, W. (2007). Effective Carcinogenicity Assessment of Permanent Implantable Medical Devices: Lessons from 60 years of Research Comparing Rodents with Other Species. 27 September 2007, available at: http://www.verichipcorp.com/files/RodentSarcomagenesis092807Wustenberg.pdf

Vaudenay, S. & Vuagnoux, M. (2007). About machine-readable travel documents. *Journal of Physics: Conference Series, Volume 77, Issue 1, 2007*

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Paweł Rotter (2009). Security and Privacy in RFID Applications, Development and Implementation of RFID Technology, Cristina Turcu (Ed.), ISBN: 978-3-902613-54-7, InTech, Available from: http://www.intechopen.com/books/development_and_implementation_of_rfid_technology/security_and_privacy_in_rfid_applications

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821