Inf Syst Front
DOI 10.1007/s10796-009-9210-z

Classifying RFID attacks and defenses

Aikaterini Mitrokotsa · Melanie R. Rieback ·
Andrew S. Tanenbaum

Abstract RFID (Radio Frequency Identification) systems are one of the most pervasive computing technologies with technical potential and profitable opportunities in a diverse area of applications. Among their advantages is included their low cost and their broad applicability. However, they also present a number of inherent vulnerabilities. This paper develops a structural methodology for risks that RFID networks face by developing a classification of RFID attacks, presenting their important features, and discussing possible countermeasures. The goal of the paper is to categorize the existing weaknesses of RFID communication so that a better understanding of RFID attacks can be achieved and subsequently more efficient and effective algorithms, techniques and procedures to combat these attacks may be developed.

Keywords RFID security · RFID attacks · Classification

A. Mitrokotsa (✉)
Information and Communication Theory Group, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Mekelweg 4, 2628 CD, Delft, The Netherlands
e-mail: A.Mitrokotsa@TUDelft.nl

M. R. Rieback · A. S. Tanenbaum
Department of Computer Science, Vrije Universiteit, De Boelelaan 1081A, 1081 HV Amsterdam, The Netherlands

M. R. Rieback
e-mail: melanie@few.vu.nl

A. S. Tanenbaum
e-mail: ast@cs.vu.nl

Published online: 29 July 2009

1 Introduction

RFID networks already exist in a broad range of environments and undoubtedly will permeate in even more areas of our lives. RFID systems consist of tiny integrated circuits (RFID tags) equipped with antennas, that communicate with their reading devices (RFID readers) using electromagnetic fields at one of several standard radio frequencies. Additionally, there is usually a back-end database that collects information related to the physically tagged objects.

RFID systems can be used to improve service quality, thwart product counterfeiting and theft, increase productivity and maintain quality standards in many areas. Common applications include highway toll collection, supply chain management, controlling building access, animal tracking, smart home appliances and keyless entry for automobiles. A potential future application is the inclusion of RFID tags in all Euro notes above €20. This initiative by the European Central Bank aims to prevent counterfeiting and track money laundering.

However, although the innovation and automation potential of RFID systems is large, these systems also have a number of inherent vulnerabilities. RFID systems are susceptible to a broad range of malicious attacks ranging from passive eavesdropping to active interference. For example, since simple RFID tags can be read without authorization, the contents of a handbag or a shopping cart can become visible to intruders without leaving a trace.

Unlike wired networks, where computing systems typically have both centralized and host-based defenses (e.g. firewalls), attacks against RFID networks can target the system's infrastructure in a decentralized manner, since both RFID readers and RFID tags operate on an inherently unstable and potentially noisy environment. Additionally, RFID technology is evolving quickly—the tags are multiplying and shrinking—and so the threats they are susceptible to, are similarly evolving. Thus, it becomes increasingly difficult to have a global view of the problem.

Threat models are necessary for managing risks efficiently. In this paper, we will structure the most common RFID attacks into layers (related but not identical to OSI protocol layering), both enumerating the threats as well as offering potential defenses for each layer.

The rest of this paper is structured as follows: Section 2 gives an overview of our layering and classification criteria. Section 3 discusses the physical layer, while Section 4 covers the network and transport layer. Section 5 concerns the application layer, and Section 6 focuses upon the co-called "strategic layer" (that we will define). Finally, Section 7 describes RFID-based attacks that cut across multiple layers, and Section 8 concludes the paper.

2 Classification overview

In this paper we classify attacks based on the layer where each attack is taking place, give the special characteristics, and discuss possible solutions that can be used in order to combat these attacks. We discriminate attacks that are deployed (Fig. 1) in the physical layer, the network-transport layer, the application layer, and the strategic layer as well as multilayer attacks which affect more than one layer.

Other classifications of possible threats and risks in RFID networks have also been proposed (Garfinkel et al. 2005; Ayoade 2007; Karygiannis et al. 2006; Avoine and Oechslin 2005). Garfinkel et al. (2005), Ayoade (2007) and Avoine and Oechslin (2005) have focused on privacy threats while Karygiannis et al. (2006) have proposed a detailed taxonomy of network, business process and business intelligence risks. Avoine and Oechslin (2005) have demonstrated that privacy issues cannot be solved without looking at each layer separately. We expand upon this by examining also other types of threats and give a better overview of the problem by discussing possible countermeasures in each case.

More specifically, in the physical layer we include attacks that affect the radio frequency (RF) signal, and the hardware of readers and tags as physical devices. In network-transport layer we describe attacks that exploit RFID protocols in standards such as ISO 15693/14443, the EPC 800 Gen-2 or other proprietary protocols. In the application layer we include attacks that exploit vulnerabilities of the commercial enterprise middleware and applications such as Oracle, SAP, the Object Name Service (ONS) or the EPCIS. Finally, in the strategic layer are included attacks related to logistical factors, real world constraints and costs versus utility tradeoffs. More precisely, in this layer we include attacks that take advantage of commercial secrets and critical information that is related with the production, the organization and the expansion policies that are adopted in competitive business environments as well as privacy and targeted security threats. Finally, we create a separate category of multilayer attacks that exploit vulnerabilities from multiple layers. The detailed classification is depicted in Fig. 2.

3 Physical layer

The physical layer in RFID communications is comprised of the physical interface, the radio signals used

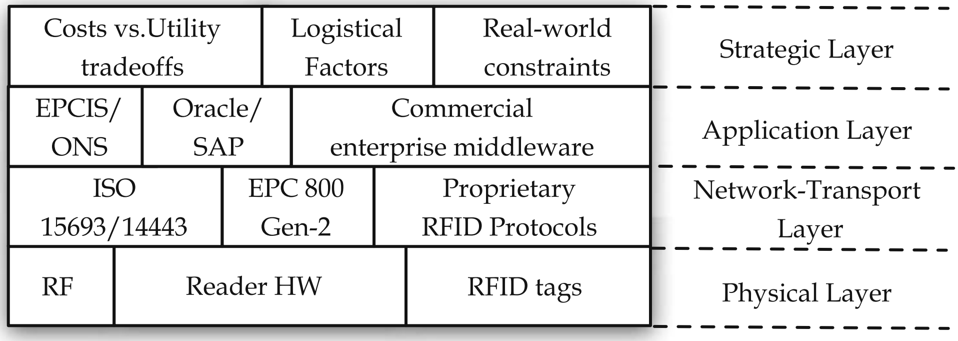

Fig. 1 Layers of RFID communication

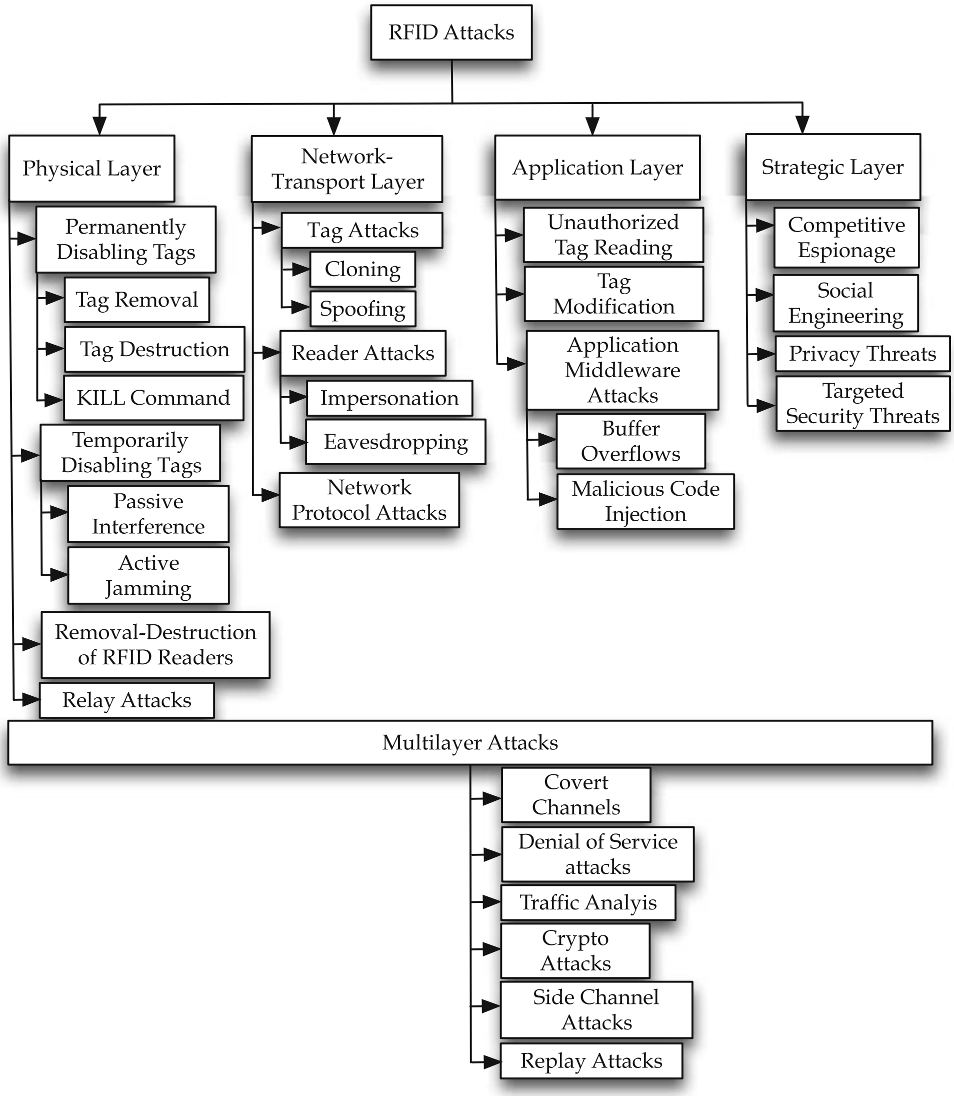

Fig. 2 Classification of RFID attacks

and the RFID devices. The adversary in this layer takes advantage of the wireless nature of RFID communication, its poor physical security and its lack of resilience against physical manipulation. This layer includes attacks that permanently or temporarily disable RFID tags as well as relay attacks. Furthermore, we discuss possible countermeasures.

3.1 Permanently disabling tags

Permanently disabling RFID tags include all the possible risks or threats that may have as a result the total destruction or substantially degraded operation of an RFID tag. Possible ways to render an RFID tag permanently inoperable are physical tag removal or destruction. In addition, privacy related countermeasures such as the the KILL command can be misused to achieve the same effect.

Tag Removal Since RFID tags present poor physical security, RFID tags that are not embedded in items can easily be removed from an item and may subsequently attached to another one (just like “switching” price tags). A trivial example of tag removal is the attempt of a thief in a supermarket to switch the RFID tag of an expensive product with that of a cheaper one and pay less at checkout. Thus, objects can easily become untraceable and the integrity of the data in the back-end system is compromised since the RFID system cannot correctly associate tag IDs with objects. This is not only a real threat, but it can also be easily performed, as it does not require special technical skills. It thus poses a fundamental security problem. Fortunately, such attacks cannot be carried out in a massive scale.

Tag Destruction Based on the same concept of poor physical security a tag may be physically destroyed even if there is no specific gain for the attacker. An RFID vandal who is just interested in annoying people or disrupting operation may easily destroy RFID tags with poor physical protection by applying pressure or tension loads, by chemical exposure or even by clipping any visible antennas off. A thief could destroy an RFID tag and then take the product bearing it through an automatic checkout portal without the store detecting that the product has been taken out.

But even if RFID tags escape from the malicious intentions of a vandal they are still susceptible of possible destruction caused by extreme environmental conditions such as too high or too low temperatures or even abrasion caused by rough handling. Moreover, active RFID tags can be rendered inoperable by removing or discharging their battery. Something that is not applicable to passive RFID tags since they receive operating power from RFID readers. Thus, a battery does not limit their lifetime.

Furthermore, RFID tags are extremely sensitive to static electricity. RFID tag's electronic circuits can be damaged in an instant by electrostatic discharge caused by conveyor belts or high energy waves. RFID tags can be rendered inoperable not only by accidental discharge, but also through the intentional misuse of special privacy-protecting devices such as the RFID Zapper (2007). This device can deactivate passive RFID-tags permanently. It operates by generating a strong electromagnetic field with a coil. Any RFID tag that is placed within the field receives a strong energy shock which renders it permanently inoperable.

KILL Command The Auto-ID center (2003) and EPC global created a command specification called KILL that is able to permanently silence an RFID tag. According to this scheme each RFID tag has a unique password which is defined by the manufacturer of the tag and its use can render an RFID tag permanently inoperable. Depending on the type of deactivation used, the KILL command may also partially or completely erase any data stored on the device. Although this feature can be used for privacy reasons it is obvious that it can be exploited by malicious adversaries in order to sabotage RFID communications.

3.2 Temporarily disabling tags

Even if an RFID tag escapes the threat of permanent disablement, it is still possible for it to be temporarily disabled. A prospective thief can use a Faraday cage such as an aluminum foil-lined bag in order to shield it from electromagnetic waves (such as those of the checkout reader) and steal any product undisturbed. RFID tags also run the risk of unintentional temporary disablement caused by environmental conditions (e.g. a tag covered with ice). Temporarily disabling tags can also be result of radio interference either passive or active.

Passive Interference Considering the fact that RFID networks often operate in an inherently unstable and noisy environment, their communication is rendered susceptible to possible interference and collisions from any source of radio interference such as noisy electronic generators and power switching supplies. Metal compounds, water or ferrite beads may also impair or even block the radio signal and lead to radio frequency detuning. This interference prevents accurate and efficient communication.

Active Jamming Although passive interference is usually unintentional, an attacker can take advantage of the fact that an RFID tag listens indiscriminately to all radio signals in its range. Thus, an adversary may cause electromagnetic jamming by creating a signal in the same range as the reader in order to prevent tags to communicate with readers.

3.3 Removal or destruction of RFID readers

Although the small size of RFID tags renders them more vulnerable to physical threats, RFID readers can also be subject to destruction or removal. RFID readers can be stolen especially if they are situated in unattended places. An RFID reader that includes critical information such as cryptographic credentials (i.e. keys) necessary to access specific tags can be the target of a malicious intruder. The impact of a stolen RFID reader is substantial since its potential manipulation could enable malicious attackers to gain access not only to RFID tags but also to the back-end system where possible modification would, of course, facilitate further data manipulation. This issue was a critical concern during the design of the European passport standard since only authorized readers should be able to have access to biometric passport's data. Moreover, vandalization could render RFID readers inoperable.

3.4 Relay attacks

In a relay attack, an adversary acts as a man-in-the-middle. An adversarial device is surreptitiously placed between a legitimate RFID tag and a reader. This device is able to intercept and modify the radio signal between the legitimate tag and reader. Subsequently, an ephemeral connection is relayed from the legitimate tag/reader through the adversarial device to the legitimate reader/tag. The legitimate tag and reader are fooled into thinking that they are communicating directly with each other. To make this type of attack even more sophisticated, separate devices could be used, one for the communication with the reader and one for the communication with the RFID tag.

Relay attacks can be discriminated in two main types referred to as *"mafia fraud"* and*"terrorist fraud"*. The *"mafia fraud"* was first introduced by Desmedt (2006) and involves the existence of an illegitimate party that relays information between the legitimate two parties. The *"terrorist fraud"* is an extension of the *"mafia fraud"* and involves the cooperation of the legitimate tag with the relaying illegitimate third party to convince the reader that the dishonest but legitimate tag is close. The dishonest and legitimate tag does not share any secrets with the relaying illegitimate party.

Of great concern is the fact that relay attacks may be successful even from considerable distances. For instance, a relay attack could be used to charge a payment to the victim's RFID card. Recently, a German MSc. student (Tanenbaum 2008) proved the vulnerability of the Dutch public transport by performing a relay attack on the Dutch transit ticket. The student just implemented the "ghost and leech" model as described by Kfir and Wool (2005) and created great concerns for the $2 billion Dutch public transport system.

3.5 Defenses against physical layer attacks

In order to safeguard RFID systems against low-tech attacks such as permanently or temporarily disabling tags, traditional countermeasures should be used, such as increased physical security with guards, fences, gates, locked doors and cameras (Karygiannis et al. 2007). Thus, intentional and unintentional physical destruction as well as use of aluminum foil lined bags could be mitigated.

Tag removal could be prevented by adopting these policies of physical surveillance or by using stronger ways to avoid easy removal of tags. More specifically, a strong mechanical bond or glue that would render the removal of the tag from the tagged object impossible without damaging the latter, would form an efficient countermeasure against tag removal. An alternative is to attach the tag in a product in such a way that renders it invisible or inaccessible (i.e. embedding it in the product). In the case of active RFID tags, an alarm function triggered when a tag is removed would serve as an additional method to combat tag removal. This procedure can be considerably facilitated using sensors that detect tag manipulation. The success rate of tag switching can be significantly reduced if additional checks are made in order to ensure that features of the tagged product and the associated tag ID stored in the back-end match.

Intentional or unintentional radio interference could also be limited by using walls opaque to relevant radio frequencies (Karygiannis et al. 2007). Furthermore, unauthorized use of KILL commands could be prevented with effective password management. For instance, the KILL command for Class-1 Gen-2 EPC standard (EPCGlobal Inc. 2005) tags requires a 32-bit password. Additionally, the use of a master password for a great number of tagged objects is a policy that should be avoided since the compromise of that single password would have a severe impact on the system.

For the protection against relay attacks possible approaches could be the encryption of the RFID communication or the addition of a second form of authentication such as a password, a PIN or biometric information. However, this requirement definitely eliminates the convenience and advantages of RFID communication.

An important metric that can be used to defend against relay attacks is the distance between the RFID tag and the reader. The shorter the distance is, the more difficult for the adversary is to launch a relay attack without being detected. A variety of techniques can be used in order to measure the tag-reader distance such as the round trip delay of the radio signal or the signal strength (Singlelee and Preneel 2005). One of the most promising solutions was the distance bounding protocol proposed by Hancke and Kuhn (2005) which is based on ultra wide band (UWB) pulse communication. However, not only do Hancke et al. not give any practical demonstration or evaluation results of the proposed approach, but their protocol has recently been shown to be vulnerable to *"terrorist fraud"* attacks (Reid et al. 2007).

Reid et al. (2007) have proposed another very efficient distance bounding protocol that is based on an XOR function used in a challenge response mechanism that leads to a large amount of side-channel leakage and thus allowing the reader to detect the actual presence of the tag. Reid et al. have also performed experimental analysis on the proposed protocol in a simulated environment for the detection of relay attacks in ISO 14443 contactless smart cards. However, the presented results are preliminary and do not provide exact figures of detection rates. A drawback of the proposed approach is the fact that it reduces the operating range of the employed smart card.

4 Network—transport layer

This layer includes all the attacks that are based on the way the RFID systems communicate and the way that data are transfered between the entities of an RFID network (tags, readers). In this section we describe attacks that affect the network transport layer and we discriminate them into attacks on the tags, reader attacks and network protocol attacks. We also provide possible ways to counter these attacks.

4.1 Attacks on the tags

- **Cloning:** Even the most important and characteristic feature of RFID systems—their unique identifier—is susceptible to attacks. Although in theory you cannot ask an RFID manufacturer to create a clone of an RFID tag (Laurie 2007), in practice replicating RFID tags does not require a lot of money or expertise considering the wide availability of writable and reprogrammable tags. An ominous example is the demonstration by a German researcher of the vulnerability of German passports (European Digital Rights (EDRI-gram) 2006) to cloning.

  In case that the RFID tag does not employ any security features then cloning involves just copying the tag's ID and any associated data to the clone-tag. However, if the tag has extra security features, then the attacker should perform a more sophisticated attack such that the rogue clone-tag may fool the reader to accept it as a legitimate one. The degree of effort required to achieve this attack depends on the security features of the RFID tags. Cloning results to the circulation of identical tags, the confusion concerning the associated tagged objects and the violation of the integrity of the system.
- **Spoofing:** Spoofing is a variant of cloning that does not physically replicate an RFID tag. In order to achieve spoofing the attackers employ special devices with increased functionality that are able to emulate RFID tags given some data content. In this type of attacks an adversary impersonates a valid RFID tag to gain its privileges. This impersonation requires full access to the same communication channels as the original tag. This includes knowledge of the protocols and secrets used in any authentication that is going to take place.

4.2 Reader attacks

- **Impersonation:** Considering the fact that in many cases, RFID communication is unauthenticated, adversaries may easily counterfeit the identity of a legitimate reader in order to elicit sensitive information or modify data on RFID tags. The feasibility of these attacks depends on the employed security measures for authenticating the RFID reader and varies from very easy to "practically impossible". For instance if credentials are stored on the reader then a stolen reader may reveal the necessary credentials for gaining access to RFID tags and back-end systems. However, if things are more complicated, the reader need to access the back-end to retrieve the necessary credentials.
- **Eavesdropping:** The wireless nature of RFID makes eavesdropping one of the most serious and widely deployed threats. In eavesdropping an unauthorized individual uses an antenna in order to record communications between legitimate RFID tags and readers. This type of attack can be performed in both directions tag-to reader and reader-to tag. Since readers transmit information at much higher power than tags, the former are susceptible to this type of attacks at much greater distances and consequently to a greater degree. The signal that will be eavesdropped is also subject to the location of the eavesdropper regarding the RFID tag and reader as well as the possible countermeasures employed for deteriorating the radio signal. More precisely, in inductively coupled systems (below 135 KHz) eavesdropping on the downlink (reader to tag) is possible up to several tens of meters while on the downlink (tag to reader) eavesdropping is possible in a much shorter range up to five times the RFID tag's nominal range (Federal Office for Information Security 2004). In backscatter systems eavesdropping is possible up to a distance of 100–200 m, while when a directional range is used the possible eavesdropping range reaches 500–1000 m. The recorded information can be used to perform more sophisticated attacks later. The feasibility of this attack depends on many factors, such as the distance of the attacker from the legitimate RFID devices.

4.3 Network protocol attacks

RFID systems are often connected to back-end databases and networking devices on the enterprise backbone. Nevertheless, these devices are susceptible to the same vulnerabilities of general purpose networking devices. Flaws in the used operating system and network protocols can be used by malicious attackers in order to launch attacks and compromise the back-end infrastructure.

Nevertheless, the security risks and challenges in the back-end databases and networking devices are not directly related to RFID communication and therefore are not the focus of this study. The connections between these devices are mostly wired. Thus, access to them is controlled via robust and well-tested security mechanisms. However, such networks may have a very wide reach, that is, if they are employed by a multinational company. This may render them vulnerable, since untrusted nodes can exist anywhere in the network.

4.4 Defenses against network-tranport layer attacks

Cloning attacks can be mitigated via challenge-response authentication protocols. These should also support robust anti-brute force mechanisms. Nevertheless, the inherent resource constraints that RFID tags present lead to weak authentication protocols that are inefficient against determined attackers. The 9798 ISO Standard (2009) provides challenge-response procedures for authentication in RFID systems and smart cards. In high cost RFID tags where resources are not very restricted, public key cryptography could also be used to combat cloning. Juels (2005) has demonstrated some techniques for strengthening the resistance of EPC tags against cloning attacks, using PIN-based access to achieve challenge response authentication. Public awareness of the security implications related to cloning attacks should be the key policy to defend against. However, this is not always the case. For instance, none of the countries that issue e-passports have anti-cloning mechanisms (Laurie 2007) as suggested by the ICAO 9303 standard (International Civil Aviation Organization 2002).

Another approach to combat cloning is the use of A Physical Unclonable Function (PUF) (Devadas et al. 2008; Tuyls and Batina 2006). PUFs can be very useful in challenge response authentication. It is embodied as a physical structure (in our case RFID tags) and maps challenges to responses. Its main properties is that it is easy to generate but hard to characterize. This is mainly because the PUF uses many random components that were introduced in the physical object during its manufacture.

More precisely, Devadas et al. (2008) have designed and implemented a PUF-enabled "unclonable" RFID tag in 0.18 μ technology. They have evaluated the proposed PUF-based RFID tag in terms of two metrics: the *intra-PUF variation* and the *inter-PUF variation*. Considering that the responses from PUF-circuits should be both *non-reproducable* and *unique*, the *intra-PUF variation* measures the former and the *inter-PUF* variation measures the latter. The results of the experiments demonstrate that performance is acceptable with respect to both metrics, although the *intra-PUF* variation is significantly affected by temperature.

Additionally, cloning can also be detected by simply correlating information in the back-end database. More precisely, in an RFID based access control system an employee carrying an RFID pass cannot be given access if according to the database he is already inside the building. Similarly someone may not pass passport control in Japan and 10 min later in Greece.

An interesting approach that is based on the audit log data in the back-end database for the detection of cloning and RFID tag theft was proposed by Mirowski and Hartnett (2007). More precisely, they have proposed an intrusion detection system for RFID systems called Deckard. The proposed scheme is based on a statistical classifier and focuses on the detection of cloning attacks. Although the proposed approach suggests that intrusion detection can be deployed in RFID networks, the evaluation of the proposed scheme indicates that further research is necessary in order to deploy robust and effective intrusion detection systems in RFID networks. More specifically, the detection rate ranges from 46.3% to 76.26%, while the false alarm rate from 2.52% to 8.4%.

Nevertheless, in certain cases and more precisely in authentication applications that involve implantable RFID tags (i.e VeriChip tags) there is an urgent reason for RFID tags to remain clonable. That is suggested by Halamka et al. (2006), who mention that otherwise the adversaries have more incentives to mount physical attacks against the bearers. The consequences of such attacks could be serious. For instance, in 2005 (Kent 2005) a man's finger was severed by thieves in order to steal his Mercedes car, that was protected by a fingerprint recognition system.

Passive eavesdropping attacks can be defended against through the encryption of the RFID communication channel. Of course, a simple remedy is to avoid storing data on the tag unnecessarily. The less information stored on the tag, the less is the potential for information leakage. All the data related to the tag should be retrieved from the back-end database. Thus, managing and securing the data is considerably facilitated since more efficient and trusted procedures can be employed in the back-end database without memory limitations. This way, the eavesdropping problem is converted to that of securely transmitting tags' IDs. Secure transmission of tags' IDs can be achieved using anti-collision protocols secure against eavesdropping such as those based on the tree-walking procedure (Quan et al. 2006).

Spoofing and impersonation could be combated by using authentication protocols or a second form of authentication such as one time passwords, PINs or biometrics. Nevertheless, password systems without encryption are considered to be only a weak form of authentication since they are susceptible to eavesdropping and can be cracked via trial and error. Thus, password authentication is more suitable for applications where the RFID tags are accessed a limited number of times—there, a one time pad is sufficient (European Commission 1995). Pseudonymization can also be used so that only authorized readers can have access to the "original" identity of an RFID tag. Many pseudonymization techniques have been proposed such as hash-lock (Weis 2003), randomized hash-lock (Weis et al. 2003) and chained hashes (Ohkubo et al. 2003).

Network protocol attacks could be countered by hardening all components that support RFID communication, apply secure operating systems, disable insecure and unused network protocols and configure the used protocols with least possible privileges.

5 Application layer

This layer includes all the attacks that target information related to applications and the binding between users and RFID tags. Such attacks employ unauthorized tag reading, modification of tag data and attacks in the application middleware. We describe these attacks as well as possible ways to combat them.

5.1 Unauthorized tag reading

In contrast to most electronic products, RFID tags are not equipped with an on/off switch. Moreover not all the RFID tags support protocols for authenticated read operations. Thus, adversaries may easily read the contents of RFID tags without leaving any trace.

The scope of such attacks remains small, however, since the attacker requires close proximity with the RFID tag. One meter is the upper limit for inductively coupled systems, while the construction of special readers with longer than normal radio ranges requires additional expense. Thus, the effectiveness of unauthorized tag reading is reduced in well monitored environments.

5.2 Tag modification

Considering the fact that most RFID tags that are in widespread use today, employ user writable memory, an adversary can exploit this to modify or delete valuable info. We have to note here that the ease with which such an attack can be performed is highly dependent on the RFID standard use and the READ/WRITE protection employed.

The amount of impact that this attack may have, will of course depend on the application in which the tags are used, as well as the degree to which tag data are modified. Thus, the inconsistency between data stored on the RFID tag and the corresponding tagged object/human may have serious implications (i.e. in health care applications, tags are used that may contain critical information about a patient's health or a medicine's recommended dosage). In more sophisticated and targeted attacks, data might be modified in such a way that the ID of the tag and any security related information (i.e. keys, credentials) remain unaltered. Hence, the reader can be fooled into thinking that it is communicating with an unmodified tag, while critical information might have been falsified.

5.3 Middleware attacks

- **Buffer Overflows:** Buffer overflows constitute one of the major threats and among the hardest security problems in software. Buffer overflow exploits store data or code beyond the bounds of a fixed-length buffer. Adversaries may use RFID tags to launch buffer overflows on the back-end RFID middleware. Although this might not be trivial, considering the memory storage of RFID tags, there are still commands that allow an RFID tag to send the same data block repetitively (Rieback et al. 2006) in order to overflow a buffer in the back-end RFID middleware. Other options include the use of other devices with more resources such as smart cards or devices that are able to emulate multiple RFID tags (e.g. RFID Guardian).
- **Malicious Code Injection:** RFID tags can be used in order to propagate hostile code that subsequently could infect other entities of the RFID network (readers and connecting networks) (Rieback et al. 2006). In this scenario, an adversary uses the memory space of RFID tags in order to store and spread in the back-end system the infecting viruses or other RFID malware. Although this type of attacks are not widespread, laboratory experiments (Rieback et al. 2006) have proved that they are feasible. Considering the fact that middleware applications use multiple scripting languages such as Javascript, PHP, XML etc. an adversary may exploit this and inject malicious code in order to compromise the middleware systems. More specifically,

RFID tags can be employed in order to perform code insertion in RFID applications that use web protocols and intercept scripting languages. In the same way, can also be performed SQL injection (Rieback et al. 2006), a special code insertion attack based on unexpectedly executing SQL statements that may lead unauthorized access to back-end databases and subsequently reveal or even modify data stored in the back-end RFID middleware.

5.4 Defenses against application layer

In order to defend against unauthorized tag reading and tag modification, controlling access to RFID tags should be our focus. Read-only tags trivially prevent unauthorized modification. Of course, this severely limits their application. A commonly proposed approach is the use of aluminum-lined wallets to protect RFID payment cards and e-passports against unauthorized reading. Many companies embraced this solution and sell this type of products (Emvelope 2005; MobileCloak 2009). However, since the sniffing of confidential data can nevertheless be performed at the time of actual use, the approach does not seem to be very effective. Blocker tags (Juels et al. 2003) are another method to prevent unauthorized tag reading. A blocker tag is a device with increased functionality that is able to simulate many RFID tags to a reader. Thus, the existence of any actual tag is masked through the mass of virtual tags generated by the blocker tag. Moreover, RFID Guardian (Rieback et al. 2005) is another approach that can be used to combat unauthorized tag reading. RFID Guardian is a flexible tool with wide functionality that can act as a personal RFID firewall that establishes a privacy zone around its user, where only authenticated readers have access.

Encryption techniques, authentication protocols or access control lists may provide an alternative solution. More specifically, approaches based on symmetric key encryption (Kinoshita et al. 2004), public key encryption (Fedhofer et al. 2004), hash functions (Weis et al. 2003), mutual authentication (Molnar and Wagner 2004; Dimitriou 2005) or even non-cryptographic solutions such as pseudonyms (Juels 2004), have been proposed. However, an important limitation on employing these schemes in RFID systems is that the latter have inherent vulnerabilities such as possible power interruptions or the disruption of wireless channels. Moreover, we have to keep in mind that employing all these encryption techniques even in non-critical applications such as RFID on underwear or chewing gums is definitely not worthwhile. The ultimate solution to avoid unauthorized reading would be the permanent deactivation (i.e. KILL command) of the RFID tags after the end of their use. However, this extreme solution would prevent advantages that can be derived from subsequent use of the RFID tags.

Buffer overflows and malicious code injection in the middleware can be combated with simple countermeasures. Performing regular code reviews and rigorous sanity checks to ensure the security of the system against vulnerabilities and bugs, by for instance ensuring that bounds checking takes place (c.f. Rieback et al. 2006). For databases, the use of bound parameters and applying least possible privileges among other things (Friedl 2007) will help protect the system. Finally, in general, turning off unnecessary middleware features such as back-end scripting, further promotes system integrity. Other simple measures include isolating the RFID middleware server so that in case it is compromised, access to the rest of the network will not be provided, checking the input data of the RFID middleware and eliminating special and suspicious characters.

6 Strategic layer

This layer includes attacks that target organization and business applications, taking advantage the careless design of infrastructures and applications. More specifically, in this layer are included competitive espionage, social engineering, privacy and targeted security threats. We describe these threats and we discuss possible ways that can be employed to counter them.

6.1 Competitive espionage

Adversaries may often have business or industrial competitors as a target. Exploiting the ability to track and detect tagged items, they may gather critical and confidential information in order to sabotage their competitors. Such information may include strategies and practices of the target relating to changing prices, production schedules (Karygiannis et al. 2007), marketing scenarios, availability of stock or contents of warehouses. Such attacks can be achieved via eavesdropping, or by gaining unauthorized access to back-end databases etc.

6.2 Social engineering

An adversary may even use social engineering skills to compromise an RFID system and gain unauthorized access to restricted places or information. Instead of going through the laborious process of hacking/cracking RFID communications, an attacker simply use a confidence trick to manipulate people into revealing confidential information. An attacker may simply take advantage of simple acts of human kindness, such as holding the door open (whereupon one may enter without an RFID badge in an otherwise restricted area) or lending an RFID tag (whereupon one may retrieve all its confidential information).

6.3 Privacy threats

RFID tags respond to any reader, authorized or unauthorized, without giving any indication about that to their owners. This special feature can be exploited by adversaries to track and profile individuals. The potential collection of personal information ranging from purchasing habits to medical information is one of the greatest risks in RFID systems and has led to mounting campaigns against the RFID usage. Privacy threats can have various dimensions depending on the behavior of the owner, the association of an individual with an item, the location of the owner, the preferences of the owner or a "constellation" of tags (Ayoade 2007). For instance, RFID tags produce traces that can subsequently be used to track the position of individuals. Although these data traces might be sanitized to avoid "location" privacy threats, they can still reveal information useful for the generation of movement profiles.

6.4 Targeted security threats

An adversary can use the information collected by an association or location threat in order to trigger malicious events and/or physical or electronic attacks. Typical examples of this attack is targeting and robbing people who collect valuable items (e.g. watches or jewelry), pick-pocketing purses with tagged bank notes, scanning trucks or ships that carry valuable or critical items or even the inventory of a house before burglars break into it. Moreover since passports are also tagged this could be exploited by terrorists to use an "RFID-bomb" that is activated only when people of specific nationalities are detected in range (European Commission 1995).

6.5 Defenses against strategic layer attacks

Attacks in this layer can be defended against using any of the countermeasures employed against attacks included in the other layers. More precisely, for privacy and targeted security threats a broad range of technical solutions have been proposed, including killing or temporarily silencing tags, blocking access to unauthorized readers (Juels et al. 2003; Rieback et al. 2005), relabeling (Inoue and Yasuura 2003) or clipping (Karjoth et al. 2005) tags, using pseudonyms (Juels 2004), distance measurements (Fishkin et al. 2004) and encryption techniques (Kinoshita et al. 2004; Fedhofer et al. 2004).

However, to effectively counter strategic threats we need to confront them as a problem that requires long-term effort. Companies and organizations that use RFID systems should establish and maintain a privacy and data protection policy and perform risk assessment to define threats and risks associated to the employed RFID infrastructure. It is important to receive guidance from a privacy officer and a legal counsel concerning the adopted strategic scenarios and privacy related issues. The security policy should be adequately communicated to all employees. The continuous training and education of the organization's personnel on RFID security and privacy policies is essential, as it promotes awareness and oversight on critical information. Karygiannis et al. (2007) provide a complete list of countermeasures that can be employed to eliminate the business and privacy risks related to RFID systems.

The privacy infringement in RFID communication should also receive attention from legislators and authorities, so that they may give guidelines for organizations and companies that use RFID systems. The Center for Democracy and Technology (2006) and the EPCGlobal (2005) have already developed a set of guidelines and principles that can be used by organizations to counter privacy challenges.

An encouraging initiative towards this direction is Florkemeier et al.'s (2004) proposed feature set that privacy aware RFID protocols should include in order to support the principles of "Fair Information Practices (FIP)" (the basis of the European Data Protection Directive 95/96/EC (European Commission 1995)). Florkemeier et al.'s proposal includes modifications of current RFID protocols that can be easily implemented with minor additional effort and can substantially improve RFID communication by providing transparency. For instance queries from readers should not remain anonymous but should reveal the ID of the reader.

7 Multilayer attacks

Many attacks that target RFID communication are not confined to just a single layer. In this category are included attacks that affect multiple layers including the physical, the network-transport, the application and the strategic layer. In particular in this layer are included covert channels, denial of service, traffic analysis, crypto and side channel attacks. We describe these attacks as well as possible ways to defend against them.

7.1 Covert channels

Attackers may exploit RFID tags in order to create unauthorized communication channels to transfer information covertly. Adversaries may take advantage of the unused memory storage of multiple RFID tags in order to securely transfer data in a manner that is difficult to detect (Karygiannis et al. 2006). For instance, a set of RFID tags implanted in human bodies, whose normal purpose would be to identify a person, could secretly report private information related to medical data or social activities.

7.2 Denial of service attacks

The normal operation of RFID tags may be interrupted by intentionally blocking access to them. Deliberate blocked access and subsequent denial of service for RFID tags may be caused by malicious uses of "blocker tags" (Juels et al. 2003) or the RFID Guardian (Rieback et al. 2005). Both approaches were proposed to safeguard RFID communications against privacy threats. Nevertheless, they could also be employed by adversaries to perform a deliberate denial of service. Another denial of service technique is the unauthorized use of LOCK commands. LOCK commands (Karygiannis et al. 2006) are included in several RFID standards in order to prevent unauthorized writing on RFID tags' memory. Depending on the applied standard the lock command is applied by a predefined password and can have permanent or temporary effects. Moreover, since RFID middleware includes networking devices, an adversary may take advantage of the system's limited resources and cause a denial of service in the RFID middleware. For instance, sending a stream of packets to the middleware so the network's bandwidth or processing capacity is swamped and subsequently denies access to regular clients.

7.3 Traffic analysis

RFID communication is also susceptible to traffic analysis attacks. An eavesdropper is able to intercept messages and extract information from a communication pattern. Even if the RFID communication is protected by encryption and authentication techniques, it is still vulnerable to traffic analysis attacks. The greater the number of messages intercepted, the more effective a traffic analysis attack will be.

7.4 Crypto attacks

When critical information is stored on RFID tags, encryption techniques are employed in order to safeguard the integrity and confidentiality of the protected data. However, determined attackers are employing crypto attacks to break the employed cryptographic algorithms and reveal or manipulate sensitive information. For instance, in Holland a security firm named Riscure (2006) has shown that the key used in a Dutch passport can be easily broken using a standard PC performing a brute-force attack for two hours. Moreover, in March 2008, researchers from the Raboud Universiteit of Nijmegen (2008) implemented an attack against the crypto-1 algorithm of the MIFARE card based on an exploit of the proprietary algorithm. The same type of card is used in the Dutch public transport protocol.

The researchers from the Raboud Universiteit of Nijmegen (Garcia et al. 2008) have also performed reverse engineering on the security mechanisms employed in the MIFARE classic contactless smart card; the authentication protocol, the symmetric cipher and the initialization mechanism. They describe the vulnerabilities of the employed security mechanisms and present two attacks. The first attack allows one to recover the secret key from a MIFARE reader. The experimental results demonstrate that this can be achieved in between 2 and 14 min. For the second and more serious attack, they demonstrate that the secret key can be recovered in 0.1 s, using ordinary hardware and without any pre-computation. Thus, by recovering the secret key in such a short time, the adversary could not only decrypt traces of communication but also clone cards and restore legitimate cards to previous states.

7.5 Side channel attacks

Side channel attacks take advantage of the physical implementation of a cryptographic algorithm rather than its theoretical vulnerabilities. In this type of attacks the information that is usually exploited includes timing information, power consumption or even electromagnetic fields. The efficient deployment of side channel attacks requires deep knowledge of the internal system on which cryptographic algorithms are implemented. Timing attacks are implemented by examining fluctuations in the rate of computation of the target while Simple Power Analysis (SPA) attacks extract information based on the variations of the power consumption.

Differential Power Analysis (DPA) is a special type of power analysis attacks which is based on the electromagnetic variations produced for instance during the communication between an RFID reader and tag. More precisely, the electromagnetic field variations when an RFID tag is performing a cryptographic operation can be used to reveal secret cryptographic keys.

7.6 Replay attacks

In a replay attack, an adversary copies valid replies of RFID communication and broadcasts them at a later time to one or more parties in order to perform impersonation. The copied messages are usually collected via eavesdropping or from sessions created by adversaries. Typical example of this attack is the unauthorized access to restricted areas by broadcasting an exact replay of the radio signal sent from a legitimate tag to the reader that grants access. Although replay and relay attacks are quite related their main discrimination is that in replay attacks there is usually an delay between the time of copying the legitimate answers and the time of replaying them.

7.7 Defenses against multilayer attacks

A covert channel attack is a challenging attack which is difficult to detect and defend against. The owners and users of RFID tags have no knowledge that their tags have been compromised and that they are used for a covert channel attack. Foiling these attacks is an open research issue. However, a possible mechanism to combat them should focus on reducing the availability of memory resources in an RFID tag (e.g. clearing the unused memory every few seconds or randomizing code and data locations).

Denial of Service attacks and traffic analysis are severe security threats in all types of networks (including wired ones). While theoretically these types of attacks can be countered, the scarce resources of RFID tags make their defense problematic and remain an open research issue. Crypto attacks can be eliminated through the employment of strong cryptographic algorithms following open cryptographic standards and using a key with sufficient length. Thus, incidents such as the revelation of MIFARE smart card's security flaws (Raboud University Nijmegen 2008) can be avoided.

Side channel attacks and more precisely DPA attacks, can be guarded against by limiting the electromagnetic emissions of the system. However, this usually implies limiting the operational range. Another approach of combatting side channel attacks and in general tampering attacks is to increase the complexity of the internal circuit of the RFID chip, thus making it more difficult for the attacker to understand the internal system and operations. However, increasing the complexity of RFID chips is restricted by the small physical dimensions of the tags as well as complexity and cost factors. Nevertheless, there are already some tamper-resistant RFID tags available such as the plusID tag (Swedberg 2006), developed by Bradcom, which according to the Federal Information Processing Standard (FIPS) (Information Technology Laboratory, National Institute of Standards and Technology 2001) belongs in security level 3 (tamper-resistant).

In order to defend against replay RFID attacks some simple countermeasures exist such as the use of timestamps, one-time passwords, and challenge response cryptography using incremental sequence numbers, nonces or clock synchronization. Nevertheless, these schemes are inconvenient and with doubtful efficiency considering the vulnerabilities to which challenge response protocols are susceptible to as well as the inherent limitations that RFID tags present. For instance, challenge response mechanisms based on clock synchronization cannot be used in passive tags since these tags have not on board battery and thus are unable to use clocks.

Another approach is the use of RF shielding on readers in order to limit the directionality of radio signals and subsequently the appearance of a ghost (Kfir and Wool 2005). Moreover a possible approach is based on the distance between the information requestor and the information owner. Fishkin et al. (2004) implied that the signal-to-noise ratio of the reader signal in an RFID system can reveal even roughly the distance between a reader and a tag. This information could definitely be used in order to make a discrimination between authorized and unauthorized readers or tags and subsequently mitigate replay attacks.

8 Conclusions

Due to the increasingly wider deployment of RFID systems, their security is more critical than ever. In this paper, we have tried to provide some structure within the universe of possible attacks that can affect such systems. By considering the point of attack, its systemic effects and countermeasures jointly, we can obtain a more coherent view of the threats and what must be done to counter them. Finally, we point out for which attacks further research is necessary in order for adequate defense against them to be available in RFID systems.

Acknowledgements We would like to thank Michael Beye for providing valuable comments and discussions and Christos Dimitrakakis for additional proofreading. This work was partially supported by the Netherlands Organization for Scientific Research (NWO) under the RUBICON "Intrusion Detection in

Ubiquitous Computing Technologies" grant awarded to Aikaterini Mitrokotsa. We would also like to thank Vrije Universiteit where part of this work has been undertaken.

References

22C3 (2007). RFID Zapper. https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html. Accessed July 2009.

Avoine, G., & Oechslin, P. (2005). RFID traceability: A multilayer problem. In A. S. Patrick & M. Yung (Eds.), *Financial cryptography and data security, 9th international C, FS 2005, Roseau, The Commonwealth of Dominica. Lecture notes in computer science, security and cryptology* (Vol. 3570, pp. 125–140). Berlin, Heidelberg: Springer-Verlag. doi:10.1007/b137875.

Ayoade, J. (2007). Privacy and RFID systems, roadmap for solving security and privacy concerns in RFID systems. *Computer Law & Security Report, 23*, 555–561.

Center for Democracy & Technology (2006). *CDT working group on RFID: Privacy best practices for deployement of RFID technology*. Interim Draft. http://www.cdt.org/privacy/20060501rfid-best-practices.php. Accessed July 2009.

Desmedt, Y. (2006). Major security problems with the "unforgeable" (Feige-)Fiat-Shamir proofs for identity and how to overcome them. In *Proceedings of the 6th worldwide congress on computer and communications security and protection (Securicomm'88), March 1988* (pp. 141–159). Paris, France.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., & Khandelwal, V. (2008). Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications. In *Proceedings of the 2008 IEEE international conference on RFID, 16–17 April 2008* (pp. 58–64). Las Vegas: IEEE Computer Society.

Dimitriou, T. (2005). A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proceedings of the 1st international conference on security and privacy for emerging areas in communication networks (SecureComm'05)* (pp. 59–66). Las Vegas: IEEE Computer Society.

Emvelope (2005). *Products*. http://www.emvelope.com/products. Accessed July 2009.

EPCGlobal (2005). *Guidelines on EPC for consumer products*. http://www.epcglobalinc.org/public/ppsc_guide/. Accessed July 2009.

EPCGlobal Inc. (2005). EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID protocol for communications at 860 MHz-960 MHz. Specification for RFID air interface. (Vol. 1.2.0). http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf. Accessed July 2009.

European Commission (1995). 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 European Communities,* (L.281), 31.

European Digital Rights (EDRI-gram) (2006). *Cloning an electronic passport. EDRI-gram, digital civil rights in Europe*. No. 4–16. http://www.edri.org/edrigram/number4.16/epassport/. Accessed July 2009.

Federal Office for Information Security (2004). *Security aspects and prospective applications of RFID systems*. RFID consultation website. http://www.rfidconsultation.eu/docs/ficheiros/RIKCHA_englisch_Layout.pdf. Accessed July 2009.

Fedhofer, M., Dominikus, S., & Wolkerstorfer, J. (2004). Strong authentication for RFID systems using the AES algorithm. In M. Joye & J.-J. Quisquater (Eds.), *Cryptographic hardware and embedded systems - CHES 2004. Proceedings of the 6th international workshop on cryptographic hardware and embedded systems (CHES'04). Lecture notes in computer science* (Vol. 3156, pp. 357–370). Berlin: Springer. doi:10.1007/b99451.

Fishkin, K., Roy, S., & Jiang, B. (2004). Some methods for privacy in RFID communication. In C. Castellucia, H. Hartenstein, C. Paar, & D. Westhoff (Eds.), *Security in Ad-hoc and sensor networks, proceedings of the 1st European workshop on security (ESAS '04). Lecture notes in computer science, computer communication networks and telecommunications* (Vol. 3313, pp. 42–53). Berlin: Springer. doi:10.1007/b105219.

Floerkemeier, C., Schneider, R., & Langheinrich, M. (2004). Scanning with a purpose—supporting the fair information principles in RFID protocols. In H. Murakami, H. Nakashima, H. Tokuda, & M. Yasumura (Eds.), *Ubiquitous computing systems, second international symposium (UCS '04), Tokyo, Japan. Lecture notes in computer science* (Vol.3598, pp. 214–231). Berlin: Springer. doi:10.1007/11526858.

Friedl, S. (2007). *SQL Injection attacks by example.* http://unixwiz.net/techtips/sql-injection.html. Accessed July 2009.

Garcia, F. D., de Koning Gans, G., Muijrers, R., van Rossum P., Verdult, R., Wichers Schreur, R., et al. (2008). Dismantling MIFARE classic. In *Proceedings of the 13th European symposium on research in computer security, Malaga, Spain. Lecture notes in computer science* (Vol. 5283, pp. 97–114). Berlin: Springer.

Garfinkel, S., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security & Privacy, 3*(3), 34–43.

Halamka, J., Juels, A., Stubblefield, A., & Westhues, J. (2006). The security implications of VeriChip cloning. *Journal of American Medical Informatics Association, 13*(6), 601–607.

Hancke, G., & Kuhn, M. (2005). An RFID distance bounding protocol. In *Proceedings of the 1st international conference on security and privacy for emerging areas in communication networks (SecureComm'05)* (pp. 67–73). Las Vegas: IEEE Computer Society.

Information Technology Laboratory, National Institute of Standards and Technology (2001). *Security requirements for cryptographic modules. Federal information processing standards publication*. FIPS PUB 140–2. 25 May 2001. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. Accessed July 2009.

Inoue, S., & Yasuura, H. (2003). RFID Privacy using user-controllable uniqueness. In *Proceedings of RFID privacy workshop*. MA, USA: MIT.

International Civil Aviation Organization (2002). *ICAO document 9303 - Part 1 machine readable passport* (Vol. 2). http://www2.icao.int/en/MRTD/Pages/Doc9393.aspx. Accessed July 2009.

International Organization for Standardization (2009). *ISO/IEC 9798: Information technology—security techniques—entity authentication, Part 1(1997), Part 2 (2008), Part 3 (1998), Part 4 (1999), Part 5 (2004)*. www.iso.org. Accessed July 2009.

Juels, A. (2004). Minimalist cryptography for low-cost RFID tags. In C. Blundo & S. Cimato (Eds.), *Security in communication networks, proceedings of the 4th international conference on security in communication networks (SCN'04), Amalfi, Italy,* *8–10 September 2004. Lecture notes in computer science, security and cryptology* (Vol. 3352, pp. 149–164). Berlin: Springer. doi:10.1007/b105083.

Juels, A. (2005). Stengthening EPC tags against cloning. In M. Jakobsson & R. Povendran (Eds.), *Proceedings of ACM workshop on wireless security (WiSec'05)* (pp. 67–76). New York: ACM.

Juels, A., Rivest, R., & Szydlo, M. (2003). The Blocker tag: Selective blocking of RFID tags for consumer privacy. In V. Alturi (Ed.), *Proceedings of the 8th ACM conference on computer and communication security, Washington, DC, USA* (pp. 103–111). New York: ACM.

Karjoth, G., & Moskowitz, P. A. (2005). Disabling RFID tags with visible confirmation: Clipped tags are silenced. In V. Atluri, S.D.C. di Vimercanti, & R. Dingledine (Eds.), *Proceedings of the 2005 ACM workshop on privacy in the electronic society (WPES '05)* (pp. 27–30). Alexandria: ACM.

Karygiannis, A., Phillips, T., & Tsibertzopoulos, A. (2006). RFID security: A taxonomy of risk. In *Proceedings of the 1st international conference on communications and networking in China (ChinaCom'06)* (pp. 1–7). Beijing: IEEE.

Karygiannis, T., Eydt, B., Barber, G., Bunn, L., & Phillips, T. (2007). Guidelines for securing radio frequency identification (RFID) systems: Recommendations of the national institute of standards and technology. *NIST Special publication 800–98, national institute of standards and technology, technology administration U.S. Department of Commerce.*

Kent, J. (2005). *Malaysia car thieves steal finger*. BBC News, 31 March 2005. http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm. Accessed July 2009.

Kfir, Z., & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smart card. *Proceedings of the 1st international conference on security and privacy for emerging areas in communication networks (SecureComm'05)* (pp. 47–48). Silver Spring: IEEE Computer Society Press.

Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., & Ohkubo, M. (2004). Low-cost RFID privacy protection scheme. *Transactions of information processing society of Japan, 45*(8), 2007–2021.

Laurie, A. (2007). Practical attacks against RFID. *Network Security, 9*, 4–7.

MobileCloak (2009) The off switch for "always on" mobile wireless devices, spychips, toll tags, RFID tags and technologies. http://www.mobilecloak.com. Accessed July 2009.

Mirowski, L., & Hartnett, J. (2007). Deckard: A system to detect change of RFID tag ownership. *International Journal of Computer Science and Network Security, 7*(7), 89–98.

MIT Auto-ID Center (2003) *Draft protocol specification for a 900 MHz class 0 radio frequency identification tag*. http: //epcglobalinc. org/ standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf. Accessed July 2009.

Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: Issues, practices and architectures. In *Proceedings of the 11th conference on computer and communications security (ACM CCS '04), Washington DC USA* (pp. 210–219). New York: ACM.

Ohkubo, M., Suzuki, K., & Kinoshita, S. (2003). Cryptographic approach to "privacy-friendly" tags. In *Proceedings of RFID Privacy Workshop.* Cambridge: MIT.

Quan, C. H., Hong, W. K., & Kim, H. C. (2006). Performance analysis of tag anti-collision algorithms for RFID systems. In *Emerging directions in embedded and ubiquitous computing, proceedings of EUC 2006 workshops: NCUS, SecUbiq, USN, TRUST, ESO, and MSA, Seoul, Korea, August 1–4 , 2006. Lecture notes in computer science, information systems and applications, incl. Internet/Web, and HCI* (Vol. 4097, pp. 382–391). Berlin: Springer. doi:10.1007/11807964.

Raboud University Nijmegen (2008). *Dismantling contactless smart cards*. 08-33A. Press Release. http://www2.ru.nl/media/pressrelease.pdf. Accessed July 2009.

Reid, J., Gonzalez Nieto, J. M., Tang, T., & Senadji, B. (2007). Detecting relay attacks with timing-based protocols. In *Proceedings of the 2nd ASIAN symposium on information, computer and communications security, Singapore* (pp. 204–213). New York: ACM.

Rieback, M., Crispo, B., & Tanenbaum, A. (2005). RFID Guardian: A battery-powered mobile device for RFID privacy management. In C. Boyd, N. González, & M. Juan (Eds.), *Information security and privacy, proceedings of the 10th Australasian conference on information security and privacy (ACISP '05), Brisbane, Australia, July 4–6, 2005. Lecture notes in computer science, security and cryptology* (Vol. 3574, pp. 184–194). Berlin: Springer. doi:10.1007/11506157.

Rieback, M., Crispo, B., & Tanenbaum, A. (2006). Is your cat infected with a computer virus? In *Proceedings of the 4th IEEE international conference on pervasive computing and communications (PerComm '06), Pisa, Italy* (pp. 169–179). Washington, DC: IEEE Computer Society.

Riscure (2006). *Privacy issue in electronic passport*. http://www.riscure.com/contact/privacy-issue-in-electronic-passport.html. Accessed July 2009.

Singlelee, D., & Preneel, B. (2005). Location verification using secure distance bounding protocols. In *Proceedings of the 2nd IEEE international conference on mobile, Ad Hoc and sensor systems (MASS'05)* (pp. 834–840). New York: IEEE Press.

Swedberg, C. (2006). *Broadcom introduces secure RFID chip*. RFID Journal. 29 June 2006. http://rfidjournal.com/article/view/2464/1/1. Accessed July 2009.

Tanenbaum, A. (2008). *Dutch public transit card broken: RFID replay attack allows free travel in The Netherlands*. http://www.cs.vu.nl/~ast/ov-chip-card/. Accessed July 2009.

Tuyls, P., & Batina, L. (2006). RFID tags for anti-counterfeiting. In D. Pointcheval (Ed.), *Topics in cryptology – CT-RSA 2006, proceedings of the cryptographer's track at the RSA conference 2006, San Jose, CA, USA, February 13–17, 2006. Lecture notes in computer science, security and cryptology* (Vol. 3860, pp. 115–131). Berlin: Springer. doi:10.1007/11605805.

Weis, S. A. (2003) *Security and privacy in radio-frequency identification devices*. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Weis, S., Sarma, S., Rivest, R., & Engels, D. (2003). Security and privacy aspects of low-cost radio frequency identification systems. In D. Hutter, G. Müller, W. Stephan, & M. Ullmann (Eds.), *Security in pervasive computing, proceedings of the 1st international conference in security in pervasive computing, boppard, Germany, March 12–14, 2003. Lecture notes in computer science* (Vol. 2802, pp. 201–212). Berlin: Springer. doi:10.1007/b95124.

Aikaterini Mitrokotsa is a postdoctoral researcher at the Faculty of Electrical Engineering, Mathematics and Computer Science of Delft University of Technology in the Netherlands. Formerly, she held a position as a visitor assistant professor in the Department

of Computer Science at the Free University (Vrije Universiteit) in Amsterdam. In 2007, she received a Ph.D in Computer Science from the University of Piraeus. Dr. Mitrokotsa's main research interests lie in the area of network security, intrusion detection systems, denial of service attacks and machine learning applications to RFID, fixed, wireless ad hoc and sensor networks security. She has been active both in European and National research projects while recently she has been awarded the Rubicon Research Grant by the Netherlands Organization for Scientific Research (NWO).

Melanie R. Rieback is an Assistant Professor of Computer Science at the Vrije Universiteit in Amsterdam, in the group of Prof. Andrew Tanenbaum. Melanie's research concerns the security and privacy of Radio Frequency Identification (RFID) technology, and she leads multidisciplinary research teams on RFID security (RFID Malware) and RFID privacy management (RFID Guardian) projects. Her research has attracted worldwide media attention, appearing in the New York Times, Washington Post, Reuters, UPI, Computerworld, CNN, BBC, MSNBC, and many other print, broadcast, and online news outlets. Melanie's research has received several awards (Best Paper: IEEE PerCom '06, Best Paper: USENIX Lisa '06, NWO I/O Prize, VU Mediakomeet, ISOC Award finalist), and Melanie has also served as an invited expert for RFID security discussions with both the American and Dutch governments. In a past life, Melanie also worked on the Human Genome Project at the Whitehead Institute / MIT Center for Genome Research.

Andrew S. Tanenbaum was born in New York City and raised in White Plains, NY. He has an S.B. from M.I.T. and a Ph.D. from the University of California at Berkeley. He is currently a Professor of Computer Science at the Vrije Universiteit in Amsterdam. Prof. Tanenbaum is the principal designer of three operating systems: TSS-11, Amoeba, and MINIX. TSS-11 was an early system for the PDP-11. Amoeba is a distributed operating systems for SUN, VAX, and similar workstation computers. MINIX is a small operating system designed for high reliability and embedded applications as well as for teaching. In addition, Tanenbaum is the author or coauthor of five books. These books have been translated into over 20 languages and are used all over the world. Tanenbaum has also published more than 140 refereed papers on a variety of subjects and has lectured in a dozen countries on many topics. Tanenbaum is a Fellow of the ACM, a Fellow of the IEEE, and a member of the Netherlands Royal Academy of Arts and Sciences.