Classification of RFID Threats based on Security Principles

Aikaterini Mitrokotsa and Michael Beye and Pedro Peris-Lopez

Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology (TU Delft), Mekelweg 4, 2628 CD, Delft, The Netherlands.

{A.Mitrokotsa, M.R.T.Beye, P.PerisLopez}@tudelft.nl

Abstract

RFID technology is an area currently undergoing active development. An issue, which has received a lot of attention, is the security risks that arise due to the inherent vulnerabilities of RFID technology. Most of this attention, however, has focused on related privacy issues. The goal of this chapter is to present a more global overview of RFID threats. This can not only help experts perform risk analyses of RFID systems but also increase awareness and understanding of RFID security issues for non-experts. We use clearly defined and widely accepted concepts from both the RFID area and classical risk analysis to structure this overview.

1. Introduction

RFID technology is a prominent area of research in ubiquitous computing. Its contactless nature and potential for data processing and storage gives it many advantages over existing machine-readable identification techniques (e.g. barcodes, optical recognition charters). Nevertheless, RFID systems have vulnerabilities making them susceptible to a broad range of attacks. In this chapter, we attempt to give a clear overview of existing threats against RFID technology. While privacy is an important issue and is extensively examined in the literature, security also needs considerable attention. A well-structured classification of RFID threats may

help us to facilitate a thorough understanding of RFID security and thus, choose and develop effective countermeasures.

Overviews of security issues related to RFID systems have been presented before. More precisely, initial works simply listed common attacks in RFID systems (Juels at al. 2006; Peris-Lopez et al. 2006). Other papers focused on privacy threats (Garfinkel et al. 2005; Avoine and Oeschlin 2005; Ayoade 2007), while yet others proposed a more detailed taxonomy (Karygiannis et al. 2006; Mirowski et al. 2009; Mitrokotsa et al. 2009). Karygiannis et al. (Karygiannis et al. 2006) proposed an RFID risk model focusing on network, business process and business intelligence risks. Mirowski et al. (Mirowski et al. 2009) focused on the RFID hardware layer and model attack sequences, while Mitrokotsa et al. (Mitrokotsa et al. 2009) discriminate RFID threats in four main layers: physical, network-transport, application and strategic layer. This chapter will build from the concept of layers but incorporate the cornerstones of information security and risk analysis (*confidentiality*, *integrity*, and *availability (CIA)*).

More precisely, we discriminate three main categories of RFID attacks, based on which part of the system they target: attacks that affect the *RFID Edge Hardware layer*, the *Communication layer*, and the *Back-end layer*. The *RFID Edge Hardware* consists of the RFID devices (tags and readers). The physical security of these devices is usually not very strong. Thus, they are vulnerable to tampering and other physical attacks; this is particularly true for tags, since their resources are often constrained due to cost and size limitations.

The *Communication layer* deals with the exchange of information. The main purpose of radio-based technology such as RFID is sending and receiving data. Thus, the radio link becomes a prominent point of attack - everyone can listen in, and signals are easily modified or jammed.

The last distinct part of the RFID system is the *Back-end layer* which is responsible for connecting RFID readers to databases and other supporting systems where RF transaction data are stored, analyzed and processed (Karygiannis et al. 2007). Since the *back-end layer* contains elements such as databases, webservers etc., many attacks on networking applications and systems can be launched. However, our analysis includes attacks that are specific to the RFID communication; many other sources (Kaufman et al. 2002) are available to give a better overview of attacks on networking systems.

In each of these layers, we subdivide three groups according to the security property that is being compromised. *Confidentiality* ensures that information or services cannot be accessed by unauthorised parties, *integrity* guarantees that information or services are not modified by unauthorised parties while *availability* ensures that information and/or services should be always available to all legitimate parties. Fig. 1 depicts the proposed classification.

This chapter is organized as follows. Section 2 describes the threats related to the *RFID-edge hardware layer,* Section 3 describes the threats related to the *Communication layer* and Section 4 presents the threats related to the *Back*-end layer. We should note here that while the presented classification of threats covers

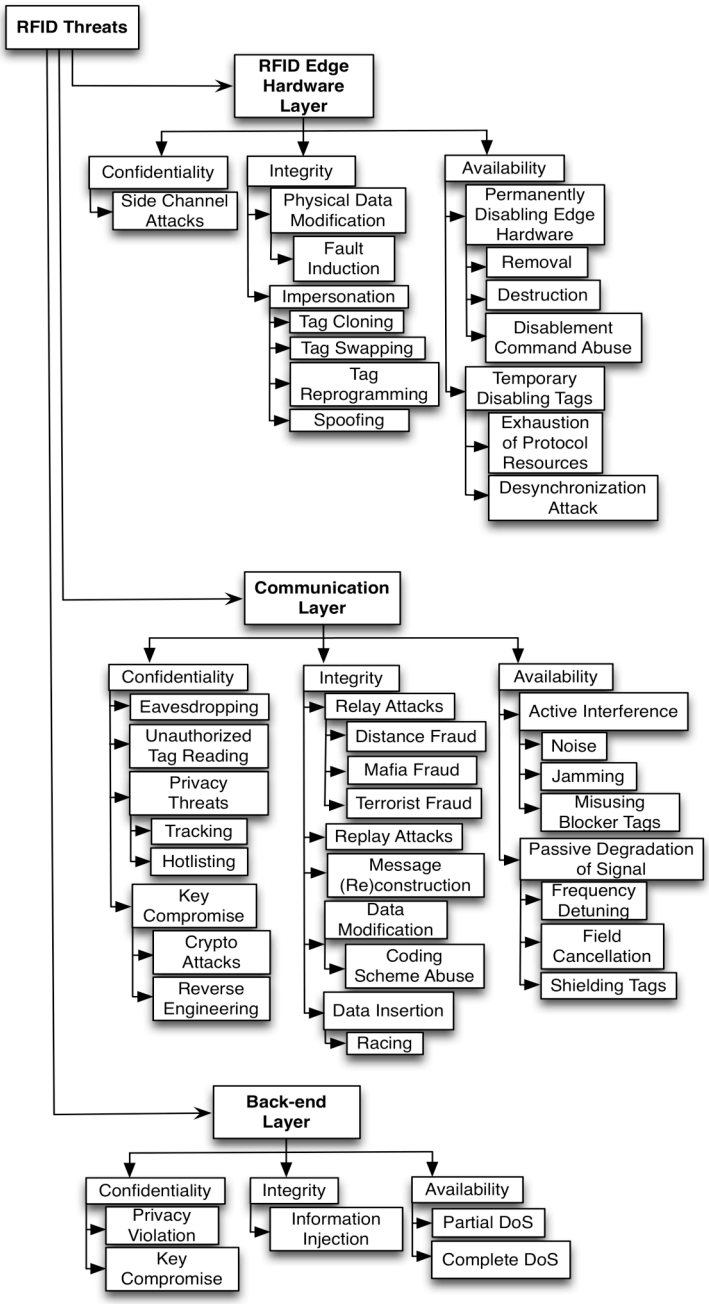

Fig. 1. Classification of RFID Threats.

all types of RFID systems, in some cases only a subset of RFID technologies is affected. This is indicated explicitly. More precisely, at the end of each of section we provide a table, which relates the threats of each layer to the associated damage caused by the threat, the cost to implement the attack/threat, the type of RFID tags most vulnerable to these threats as well as possible countermeasures and their associated costs. In each table we distinguish RFID tags into two main categories: *high* and *low* cost tags. *High-cost tags* include most *active* and *semi-active* tags, or more generally those tags, which are self-powered, have greater computational capabilities or radio range. On the other hand *low-cost tags* have more limited resources (gate equivalents and power consumption) and computational capabilities (small memory). Finally Section 5 concludes the chapter and presents some open issues.

2. RFID Edge Hardware Layer

In the *RFID Edge Hardware layer* we include attacks that may affect the RFID devices (tags and readers) by exploiting their poor physical security and their inadequate resistance against physical manipulation. This layer includes *side-channel attacks*, *physical data modification*, *and impersonation* as well as *temporary* or *permanent disablement of edge hardware*.

2.1 Confidentiality

To protect and preserve the *confidentiality* of information, it should be restricted only to authorised parties. The means of mounting an attack on the *confidentiality* of the system differ greatly, depending on which part of the system is targeted.

Side-Channel Attacks: When an adversary has physical access to the edge hardware, and sufficient time, she can attempt to extract information from it. This can be done by either deducing information from (side-channel) measurements, inducing errors in the operation of the hardware (fault attacks or "glitching"), thus influencing the output, or by directly reading out the memory (tampering). A brief overview is given by Berkes (Berkes 2006). Many of these attacks require specific equipment, and cannot be performed by a hobbyist, but rather by experts and well-equipped laboratories (Hancke and Kuhn 2008; Berkes 2006). The impact of a *side-channel attack* varies and depends on the application scenario. Thus, it may lead to retrieve the *kill* password of an RFID tag or even reveal the secret key used

for authenticating a tag to a reader. In the former case an adversary could silence RFID tags permanently and thus steal valuable products. In the latter case where the secret key may be revealed, the adversary may gain access to restricted places, critical information or even conduct financial fraud.

Let us briefly discuss the various ways of mounting such attacks:

- ***Side-Channel Analysis:*** is a non-invasive type of attack that may be conducted when the attacker measures fluctuations in timing delays, power consumption or emitted signals and radiation - information that may reveal critical data about the input and the internal states of the RFID devices. For instance, fluctuations in the backscatter signal may yield information regarding changes in the internal resistance. Several types of *side-channel attacks* can be distinguished, depending on which measurements are made to disclose information. More precisely, *Simple Power Analysis (SPA)* (Oren and Shamir 2007) or *Differential Power Analysis (DPA)* (Hutter et al. 2007; Hutter et al. 2009; Kocher et al. 1999; Plos 2008) attacks are based on the measured variations of the power consumption. *Timing* attacks exploit the fluctuation in the rate of computation of the target (possible delays), while in *Differential Electro-Magnetic Analysis (DEMA)* (Hutter et al. 2007; Agrawal et al. 2003) are measured the electromagnetic field variations caused while an RFID device performs cryptographic operations. In the latter case the adversary may reveal critical information such as secret cryptographic keys.
  Oren and Shamir (Oren and Shamir 2007) have performed the first *SPA* attack, which reveals the *kill* password of *ultra-high frequency* (UHF) tags. Their attack was based on observing the power trace reflected from the tag to the reader. Hutter et al. (Hutter et al. 2007) have performed the first *DPA* attack in RFID tags. More precisely, by performing power and electromagnetic analysis they were able to analyze hardware and software AES (Advanced Encryption Standard) implementations in *high frequency (HF)* tags. Even UHF tags have been proved to be vulnerable to DPA attacks by Plos (Plos 2008). Hutter et al. (Hutter et al. 2009) have also been able to perform a *DPA* attack in a public-key enabled RFID device.
- ***Fault Attacks:*** may be launched when the adversary tries to produce errors in the operation of the device targeting in illegally extracting information through regular output channels or side-channels. This is achieved by varying the input of the device, or by manipulating the environmental conditions (Hancke and Kuhn 2008) such as heat, cold, electromagnetic radiation (e.g. Ultraviolet (UV) light or X-rays), voltage levels, continuity of power supply or magnetism.
- ***Physical Tampering:*** When all else fails, one can try to physically take apart the device without destroying the data contained therein, in an attempt to (partially) recover it. Another type of physical tampering involves targeted manipulation or damage in specific hardware parts (Hancke and Kuhn 2008; Berkes 2006). An example would be changing individual cells in ROM (Read

Only Memory) to change the behaviour or seed of a cipher. Other invasive attacks rely on retention and direct reading of memory cells. Volatile memory loses its data when power is interruped. Some devices (like smartcards) have been protected with memory-erasing behaviour when attacks are detected. Some means of slowing this loss of memory can be to cool the hardware (Lowry 2004), to etch the state into the memory permanently (by means of radiation), or to tunnel into the hardware at great speeds, in order to cut off protective measures before they can react. Even without these exotic and often expensive methods, sometimes memory can be read after power-loss. If RAM (Random Access Memory) memory is powered at a constant state (0 or 1) for extended periods of time, an imprinting effect called "memory remanence" (Hancke and Kuhn 2008) will take place, which can allow (partial) recovery of data.

2.2 Integrity

Preserving the *integrity* of information can be defined as the assurance that all information and related methods that process it are accurate and complete (ISO 2005). *Integrity* can be easily subverted if *authentication* has been eschewed or once it is bypassed. Therefore, we will look at attacks that threaten proper authentication in the RFID systems, and their integrity. In the edge hardware this comes down to *physical data modification* and *impersonation* attempts.

Physical Data Modification: In RFID systems *physical data modification* can be achieved either by *fault induction* or by *memory writing*. *Fault induction* involves modifying data when it is being written or processed. *Memory writing* can be performed by using specialist equipment, such as laser cutting microscopes or small charged needle probes. This way, memory cells can be directly influenced and written to (the ROM attacks in (Hancke and Kuhn 2008) are a good example). Although difficult and time-consuming, this bypasses any software protections. The impact of *physical data modification* depends on the application scenario and the criticality of the information that was modified; for sure such attacks cause inconsistency between the data stored on the tags and the objects to which the tags are attached. Consequently, such an attack may lead to severe medical mistakes (i.e. modifying the data stored on a tag attached to a drug) or even counterfeiting original products.

Impersonation: Impersonation of RFID tags can be achieved by *tag cloning*, *tag swapping*, *tag reprogramming* or *spoofing*. In all cases the adversary targets and imitates the identity of tags or readers. Through this attack an adversary may gain access to restricted areas, sensitive information and credentials.

- **Tag Cloning:** Replicating RFID tags has proven to be very easy, since it does not cost a lot of money nor requires a lot of expertise, while all the necessary equipment such as software and blank tags are freely available. A representative example has been demonstrated by a German researcher, who has proven that German epassports are susceptible to cloning attacks (Reid 2006). If the RFID tag does not use any security mechanism then cloning simply includes copying the tag's identifier (ID) and any other associated data to the rogue RFID tag. Nevertheless, if the tag does employ security features then a more sophisticated attack should be launched so that the cloned tag becomes indistinguishable from the legitimate one. The amount of effort needed to launch a cloning attack depends on the security mechanisms used. But cloning does not just mean copying a tag ID and data but creating an RFID tag that follows the original one even to the form factor. The human eye should not be able to discriminate a legitimate from a cloned tag.

- **Tag Swapping:** Another quite popular impersonation attack is *tag swapping*; quite simple in its tactic but a real threat in retail product tracking and automated sales processing. *Tag swapping* involves removing an RFID tag from a tagged object and subsequently attaching it to another one (just like "switching" price tags). An illustrative example of *tag swapping* is a thief in a retail shop that picks out a high-priced item and a cheap one and switch their tags so that he "buys" the expensive one and pays less at checkout. Thus, the integrity of the back-end system is violated since it cannot correlate correctly the tag's ID with the object.

- **Tag Reprogramming:** Some tags are reprogrammable, either directly (through the Radio Frequency (RF) interface, usually when a password is supplied), or through some (wired) interface, which is supposed to only be used in the construction process. Other tags cannot be reprogrammed, because they use ROM. In impersonation attempts, the cheapest way of recreating the form-factor of tags can often be re-using existing tags, and simply reprogramming them if needed. One could steal and swap tags for this purpose, use discarded tags acquired through dumpster-diving, or buy tags of the same type if they are available on the open market (Juels 2005).

- **Spoofing:** Spoofing can be considered as a variation of tag cloning. However, their main difference is that spoofing does not involve the physical reproduction of an RFID tag. Furthermore, spoofing attacks are not limited to tags since the identity of RFID readers can also be spoofed. Successful deployment of this attack requires specialist equipment that allows the emulation of RFID tags or readers based on some data content. The adversary requires full access to legitimate communication channels as well as knowledge of the protocols and secrets used in the authentication process if there is any.

The goal of the adversary is to imitate legitimate tags or readers elicit sensitive information and gain unauthorised access to services.

2.3 Availability

An asset is considered to be available when it can always be accessed and used by all authorised parties (ISO 2005). The availability of the *RFID edge hardware* can be compromised when it is permanently or temporarily disabled (through removal, destruction or sabotage).

Permanently Disabling Edge Hardware: RFID tags and readers may be rendered permanently inoperable vial removal or destruction. RFID tags may also become irreversibly disabled if specific disablement commands are abused. *Permanently disabling RFID hardware* leads to permanent untraceability of tagged objects and thus to great loss in a supply-chain organization or a retail shop, depending on the scale to which this attack is performed.

- **Removal:** Considering the poor physical security that RFID tags present, they can be easily removed from the associated items if they are not strongly attached to or embedded in them. Tag removal is a serious threat that can be easily deployed without the need of exceptional technical skills. It is a threat that lead to untraceable objects and suggests a significant security problem. Luckily, this kind of attack cannot be launched on a massive scale. RFID readers may also be removed if they are situated in unattended places. However, their size renders this attack hard to deploy.

- **Destruction:** Poor physical security leads not only to possible tag removal but also to easy tag destruction. Unattended RFID tags run the risk of being vandalised by malicious attackers through chemical exposure, application of increased pressure or tension loads or even by simply clipping their antennas off. Nevertheless, even if RFID tags escape the violent intentions of vandals they might get destroyed by severe environmental conditions such as extreme temperatures or by abrasion produced by rough handling. Moreover, RFID tags may also be rendered deliberately inoperable by abusing privacy-enforcing devices such as the RFID Zapper (Collins 2006). This device's operation is based on the production of a strong electromagnetic field that burns out the tag's internal circuitry.

  While it is easier to physically manipulate RFID tags due to their small size, RFID readers may undergo similar threats. Considering the fact that RFID readers often store critical security credentials (i.e. encryption keys) they may become subject to vandalization and physical destruction, especially if they

are unsupervised. A compromised or stolen RFID reader may disrupt the RFID communication and violate the RFID system's availability.

- **Disablement Command Abuse:** Some tags have security features that permanently disable or lock them. The KILL command, a specification created by the Auto-ID center (Auto-ID center 2003) and EPC global is a command for permanently silencing a tag, thus rendering it unresponsive to requests. Several RFID standards use LOCK commands to prevent unauthorized writing to tags (Karygiannis et al. 2006). Usually a predefined password is used for authentication; the locking itself can be temporary or permanent (e.g. "permalock" in EPC tags). For practical reasons, multiple tags could share a password (i.e. all items in the same store). Otherwise, password management becomes problematic (large lists need to be shipped with the items). Although these features can be used for privacy-protection reasons, they can also be misused to render RFID tags permanently inoperable and sabotage RFID communications. In some cases, the password used is of low entropy (8 bits for 1 EPC Gen 1 tags, 32 bit for EPC Gen 2 tags), and could easily be brute-forced. Moreover, having one master-password may lead to successfully locking or killing a great number of tags and severely harming the system.

Temporarily Disabling Edge Hardware: *RFID edge hardware* may also be disabled temporarily by extreme environmental conditions (i.e. tags covered with water or ice), *exhaustion of protocol resources* or possible *desynchronization attacks*. Similarly to *permanently disabling edge hardware*, even if the disablement is temporary, such an attack may disturb the whole RFID system and in the simplest case scenario can provide free goods to a shop-lifter.

- **Exhaustion of Protocol Resources:** Some protocols allow a tag to only be read a certain number of times, or allow a limited number of unsuccessful reads before rendering it inactive (Ohkubo et al. 2004). Some protocols use counters or timestamps with a maximum value. When this value is reached, the tags become unreadable. Other protocols protect a tag from tracking, but only for a limited number of reads. An example is hash-chain protocols, which use hash-chains (pseudonyms) of fixed length stored on a tag. When these tags run out of pseudonyms, they once more become vulnerable to tracking attacks. The OSK (Ohkubo-Suzuki-Kinoshita) protocol (Ohkubo et al. 2003) is an example of a hash-chain protocol.

  Depleting the battery power of active tags and shortening their lifespan is another example of such attacks. Targeted attacks (but also repeated accidental reads by foreign systems on the same frequency) can cause tags to be "exhausted" and fail. In some cases this error is recoverable, in many it is not. In either case, it may have a financial impact due to interrupted operations and the costs associated with system recovery (Han et al. 2006).

- **Desynchronization Attack:** Some protocols rely on a form of synchronization between tags and reader/server. This can be in the form of counters (number of reads), timestamps, or updated pseudonyms and keys. When the update does not take place on both sides, desynchronization can occur through adversarial reads or update prevention (e.g. protocol interruption). Unless the protocol is designed to handle this or recover from it, the server will no longer be able to read or recognize the tag. Even in protocols which allow a limited amount of desynchronization, attacks or repeated errors (reads by other systems) can lead to desynchronization (Radomirovic and van Deursen 2008).

2.4 Evaluation of threats and possible countermeasures

Figure 2 relates the threats, associated with the *RFID-edge hardware layer*, to their potential *damage*, the *cost* of implementing each type of attack/threat and the class of tags that are more vulnerable against this type of attack. For each threat we also list possible countermeasures (*solutions*) that could be used to combat it as well as an estimation of the *cost* of deploying this countermeasure. We are actually presenting a qualitative estimate (*low*, *medium*, *high*) of the *cost* in both cases, that takes into account the effort, time and financial cost required to launch or combat an attack correspondingly.

The attacks that are more expensive to launch are mainly *side channel attacks* and some advanced types of *impersonation attacks*. From the countermeasures against attacks in the *RFID-edge hardware layer,* the most expensive are those that require either special tags (i.e. more robust or tamper resistant tags) or increased physical security (i.e. guards, cameras, gates). More precisely, side channel attacks constitute one of the most difficult attacks to combat. The most reasonable method to counter these threats involves limiting the electromagnetic emissions of the RFID system. Nevertheless, this measure leads to narrowing the operational range of the system. Another high cost countermeasure is to increase the complexity of the RFID tag's internal circuit, thereby confounding attempts of reverse engineering; a task quite challenging considering the small size required for RFID tags. Use of tamper resistant tags (Swedberg 2006; SAG Security Assembly Group 2010) could also make harder the success of such an attack. However, as such attacks are particularly costly, they may not be very prevalent.

	Attack	Potential Damage	Attack Cost*	Class of Tag	Solution - Cost*
Confidentiality	**Side Channel Attacks**	- Extract information (i.e. cryptographic keys).	**H**	Low Cost Tags	- Use of tamper resistant tags. **(H)** - Limit electromagnetic emissions. **(M)** - Increase complexity of the circuit. **(H)**
Integrity	**Physical Data Modification**	- Altering data stored on tag memory.	**H**	Low Cost Tags	- Memory protection. **(M)** - Secure cryptographic protocols. **(M)**
	Impersonation	- Supplant legitimate tags. - Elicit sensitive information. - Gain unauthorized access to services.	**M**	Low Cost Tags	- Use of tamper resistant tags (i.e. Physical Unclonable Function (PUF)). **(H)** -Memory protection mechanisms. - Physical protection (against tag swapping). **(H)** - Use of encryption techniques. **(M)**
Availability	**Permanently Disabling Edge Hardware**	- Avoid identification. -Untraceability of tagged objects.	**L**	High/Low Cost Tags	- Rugged, flexible tags. **(M)** - Increased physical security. **(H)** - Efficient key management (regarding command abuse). **(M)**
	Temporarily Disabling Edge Hardware	- Avoid identification. -Untraceability of tagged objects.	**M**	High/Low Cost Tags	- Have limited number of unsuccessful reads. **(L)** - Store both the old and the potential new key or pseudonym values. **(M)**

***Cost:** **H** high, **M** medium, **L** low.

Fig. 2. RFID threats and countermeasures related to the RFID edge hardware layer.

3. Communication Layer

This layer includes all the attacks that are based on the RFID communication and the transfer of data between the entities of the RFID network.

3.1 Confidentiality

Confidentiality in RFID communication is mainly violated by attacks such as *eavesdropping*, *unauthorised tag reading*, *privacy threats* as well as possible *key compromise*.

Eavesdropping: The open medium and the insecure nature of radio communication channel render eavesdropping one of the most critical encountered attacks against RFID systems. Eavesdropping in RFID communication is defined as surreptitiously listening and intercepting messages transferred between legitimate RFID entities. An adversary may eavesdrop on both channels reader-to tag (*for-*

ward channel) and tag-to reader (*backward channel*). Nevertheless, the *forward channel* is more susceptible to this threat since the readers' signal is much stronger. The success of the attack also depends on the location of the adversary, while the intercepted information may subsequently be used for the deployment of more sophisticated attacks. An eavesdropper may intercept messages and extract information that can be used for launching more sophisticated attacks. The same applies even if encryption and authentication techniques are used to protect the RFID communication (traffic analysis attacks).

Every type of RFID system has its own maximum range at which communication can take place. The *forward channel* (reader-to tag), especially in passive systems, has a longer range than the *backward channel* (tag-to reader). Also, since the passive tags use the *forward channel* to power themselves this creates an effective *third range*, that of the maximum distance the received power is sufficient for the tag's operation. The *nominal read range* for a system is determined by the minimum of the aforementioned three ranges. Note that an eavesdropper does not have to power a tag, and can use a larger antenna than a regular tag or reader and operate at an increased *rogue reading range*. Finally, *detection range* can play a role. This is the maximum range at which a tag or reader can be detected, but no sense can be made of actual information being transmitted.

Unauthorised Tag Reading: Unfortunately, RFID tags lack an on/off switch that would allow or prevent reading. Even worse, not all types of RFID tag are able to use secure authentication protocols that prevent unauthorised reading. Hence, in many cases RFID tags can be read without authorization and without any indication that they were read.

Both *eavesdropping* and *unauthorized tag reading* are widely-deployed attacks with considerable negative effects for the victim. These attacks, when performed for competitive espionage purposes may reveal secrets and sensitive information such as marketing strategies or availability of stocks.

Privacy Threats: There are several proposals that attempt to formalize privacy in RFID protocols. Initially, privacy is formalized by the ability to distinguish two known tags (Avoine 2005). However, the model rules out the availability of side-channel information (e.g. knowing the success/failure of a protocol instance on the reader). Juels and Weis extended this model using the side-channel information and allowing the two tags to be chosen by the adversary (Juels and Weis 2007). In (Vaudenay 2007), is presented a hierarchy of privacy models and is studied the restrictions of RFID systems regarding tag corruption and availability of side channels. Specifically, the proposed model captures the notion of a powerful adversary who can monitor all communications, trace tags within a limited period of time, corrupt tags, and get side-channel information on the reader output. Adversaries who do not have access to this side-channel information are called *narrow* adversaries. Depending on the amount of corruption, adversaries are called *strong*, *destructive*, *forward*, or *weak adversaries*.

We describe in detail two of the most significant privacy threats: *tracking* and *hotlisting*.

- **Tracking:** The response of RFID tags to authorized or unauthorised readers is performed silently without giving any sign of activity. This characteristic can be exploited in order to surreptitiously collect personal information that may be used to create profiles and track users. Collected information may vary from purchasing preferences, critical personal information such as medical data to location of individuals. For instance RFID tags produce traces that may subsequently be used to track the position of individuals. Even if these data are "anonymized" they can still give indication about the location of users and create movement profiles. Adversaries may even exploit the unused memory storage of multiple tags in order to create illegal communication channels and transfer information covertly (Karygiannis et al. 2006). It is hard to detect this unauthorized transfer of information. An example could be the use of RFID tags, whose normal use is the identification of people, to reveal personal information related to social activities.

- **Hotlisting:** Information related to the location of a user or the association of an individual with an object could be used by an adversary to enable other more direct attacks. More precisely, an adversary may target and rob people that collect valuable items (e.g. jewelry), scan the contents of house before breaking into it, pick pocket purses with tagged banknotes or scan cargos of valuable or sensitive items. Considering that passports are also tagged they might be used by terrorists to detect people of specific nationalities and trigger "RFID bombs" against them (European Commission 1995).

Key Compromise: An attractive target for adversaries is always information related to encryption techniques and key material. Knowledge hereof would allow them to easily impersonate tags and readers or to access other information through elevation of privilege. For instance, it may enable them to read sensitive information stored in e-passports and identify nationalities.

- **Crypto Attacks:** Sensitive data stored on RFID tags are usually protected by employing encryption techniques. However, a determined adversary could mount crypto-attacks in order to break the employed cryptographic algorithms and disclose or manipulate data. Targets of attack include password authentication schemes, ciphers, pseudo-random number generators, hash-functions. Examples of classic attacks are *brute force* (password/cipher), *chosen-ciphertext* or *known-plaintext* attacks (ciphers), *first pre-image* or *collision* attacks (hashes). A representative example of RFID crypto attacks was the demonstration that the Dutch passport can be broken via *brute force* attack (Riscure 2005). Furthermore, researchers from the Radboud University of Nijmegen (Garcia et al. 2008) have performed an attack against the crypto-1 al-

gorithm 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.

- **Reverse Engineering:** Reverse engineering is a term used to describe attacks that attempt to model the inner workings of a device or piece of software, usually in order to mimic its behaviour, or to be able to attack it more efficiently. Uncovering the detailed workings of a proprietary cipher, hash or protocol, can be a first step towards finding weaknesses. If "security through obscurity" has been relied upon, or the algorithm has not been rigorously tested, this can have a severe impact on security. The recent publications concerning the Mifare Classic tag and its proprietary Crypto-1 algorithm are a good example (de Koning Gans et al. 2008).

  Reverse engineering can also be an invaluable tool in *side-channel analysis*, probing or "glitching". A full understanding of the inner workings of the device is often required in order for such attacks to be successful. Even impersonation attempts can benefit from reverse engineering; knowing how the original device behaves is key in replicating it.

3.2 Integrity

The *integrity* of the RFID communication channel can be compromised through *relay, replay* attacks, *message reconstruction* or *modification/inserion of data*.

Relay Attacks: In a relay attack an adversary acts as a man-in-the-middle. An adversarial device is placed surreptitiously between a legitimate RFID tag and reader to intercept (and possibly modify) the communications between tag and reader. Tag and reader are fooled into thinking that they are communicating directly with each other. A large distance between a tag and a reader can be bridged by using two devices: one for the communication with the reader (the "ghost") and one for the communication with the RFID tag (the "leech"). Note that these devices may operate at larger ranges than the *nominal read* or power up ranges, especially the "ghost" as it does not actually rely on power from the reader.

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 (Kfir and Wool 2005) and created great concerns for the $2 billion Dutch public transport system. Another example of a high-impact attack would be to charge a payment to a victim's RFID-enabled credit card (Heydt-Benjami et al. 2008) without his knowledge.

Depending on which party is committing the fraud, different names are given to relay attacks.

- **Distance Fraud:** In this attack the adversary uses a rogue tag and try to convince a legitimate reader that she is nearer than she really is.
- **Mafia Fraud:** This attack involves three main parties: a legitimate tag *T*, a legitimate reader *R* and the attacker *A*. The attacker has at her disposal a fraudulent tag *T'* and reader *R'* and attempts to convince the legitimate reader *R* that she is communicating with the legitimate tag *T* while in reality the reader *R* communicates with the attacker *A*. Nevertheless, no disclosure of the private keys shared between the legitimate and reader is made.
- **Terrorist fraud:** "Terrorist fraud" involves a fully cooperating tag (owner), who does not share secret key material with the relaying party. This means that it will compute responses to challenges, but will not give the attackers the means to perform the computations on their own (Tu and Piramuthu 2007; Desmedt 1998).

Replay Attacks: Replay attacks are impersonation attacks that involve the re-sending of valid replies at a later time. These replies can be obtained through eavesdropping or adversarial sessions. They are related to relay attacks, but they take place "offline" in the sense that there is a clear delay between time of obtaining and time of re-sending the message. The simplest application scenario of a replay attack is the replay of an intercepted message transmitted from a legitimate tag to a legitimate reader in an RFID based access control system or in an RFID identification system (which does not use an advanced challenge-response authentication protocol). In these scenarios the adversary is able to gain access in a specific building or supplant the presence of a particular item just by replaying the intercepted message. Even, if the messages are encrypted a successful attack may be launched easily. The inclusion of a source of freshness (random number) in the messages is a necessary condition but by itself does not guarantee the protection against replay attacks.

Message (Re)construction: Protocols that include a random session variable (a nonce) are usually resistant to replay attacks. In some cases, this "freshness" can be eliminated though, by combining or analyzing several messages. This allows for the (re)construction of new valid messages which can be used in future impersonation attempts. Thus, this attack may enable an adversary to perform a more sophisticated impersonation attack (e.g. gain unauthorized access to a restricted place) in case that a simple replay attack is not sufficient.

Data Modification: Since RFID tags are usually equipped with writable memory, adversaries can exploit this to transform or erase data. The feasibility of this highly depends on the employed READ/WRITE protection as well as the used RFID standard. The impact of the attack depends on the application as well as the degree of modification. For instance, the modification of tags used in medical applications (e.g. carrying a medicine's recommended dosage or a patient's history) may have dreadful implications. Sophisticated adversaries may modify critical in-

formation without transforming the tag's ID or any security related info such as encryption keys or credentials. Thus, the reader is not able to indicate alterations. One of the main approaches used to modify data in RFID communication is by *abusing the coding scheme*.

- **Coding Scheme Abuse:** One way to modify data in transit is to replace or flip bits in transmissions. Some coding schemes are more vulnerable to this type of attack that others. For instance the NFC (Near Field Communication) tags (Haselsteiner et al. 2006) use "modified Miller coding" with 100% modulation ratio at 106 KBaud, while above 106 kBaud they switch to "Manchester" with a 10% modulation ratio. With 100% modulation ratio, meaning that a "0" and a "1" are encoded as "no signal" and "full signal" respectively. An adversary can change a "0" into a "1" bit by sending out a signal of his own, but she cannot change a "1" into a "0" because she has no effective way of reducing the signal strength from the legitimate reader. However, with a 10% modulation ratio a "0" is encoded as a weak signal (82%), while a "1" is a stronger signal (100%). Now an adversary can flip bits as she desires, by adding to both signals. Signals of 80% will seem like baseline noise, 100% will seem like a "0" and 125% will seem like a "1".

Data Insertion: Attacks that do not modify parts of a transmission, but add new data (or even whole messages), are termed data insertion rather than data modification attacks. This can take place at the edge hardware or in the back-end through various means, but the most easy and common place to execute such attacks is in the communication protocols themselves. Possible application scenarios of such an attack vary. For instance, this attack may enable an adversary to insert information and thus alter fields such as the prices of goods in a department store or a warehouse. One of the most challenging ways to perform data insertion is the approach called "*racing*".

- **Racing:** A specific way of inserting data is for an adversary to quickly send a response before the legitimate reader. This need for split-second timing gave rise to the term "racing". By doing so, one can let the reader perform part of the protocol (i.e. unlocking a tag) and hijack the session (for instance write different information to the tag, or close the session without updating pseudonyms).

3.3 Availability

Denial of Service (DoS) attacks are one of the most challenging threats against RFID communication layer, since they can be easily deployed while they are hard to defend against. This type of attacks can be discriminated to attacks that pas-

sively degrade the RF signal, and attacks that actively jam or disrupt communications.

Active Interference: Active interference may be the result of a *noisy* environment, of intentional *jamming* or the abuse of privacy protection approaches such as the *blocker tags* (Juels et al. 2003) or the *RFID guardian* (Rieback et al. 2005).

- **Noise:** Since RFID systems usually operate in an inherently noisy and unstable environment. Thus the RFID communication is vulnerable to possible interference and collisions caused by various sources of radio interference such as power switching supplies and electronic generators.

- **Jamming:** In RFID communication in some cases, where authentication mechanisms are not employed, RFID tags listen indiscriminately to every radio signal within their range. This can be exploited by adversaries to disrupt communication between legitimate tags and readers by deliberating causing electromagnetic interference via a radio signal in the same rage as the reader.

- **Malicious Blocker Tags:** The normal operation of RFID tags may be interrupted by deliberately blocking access to them. Intentionally blocked access and subsequent denial of service for RFID tags may be caused by abusing *blocker tags* (Juels et al. 2003) or the *RFID guardian* (Rieback et al. 2005). Both approaches were proposed to protect RFID communications against privacy threats. However, both of them could also be employed by adversaries to perform a deliberate denial of service.

Passive Degradation of Signal: The presence of metal compounds, water and other materials can also negatively impact radio communications. The *passive degradation of signal* can be caused by *basic degradation* or *more complex propagation effects* or even by *shielding tags*.

- **Basic Degradation Effects:** The presence of water, metal but also the human body and some types of plastics can interfere with radio transmissions. The negative effects vary from absorption (water and conductive liquids) and reflection/refraction (metal objects and surfaces) to dielectric effects/frequency detuning (dielectric materials like plastics or living tissue) (Sweeney 2005). Generally speaking, the higher the frequency, the greater the impact of metals and liquids on performance.

- **Complex Propagation Effects:** These effects take place when high frequency (UHF / Microwave) radio waves bounce off surfaces and collide in certain places, canceling each other out if their phases happen to be opposite at that particular point in space. This creates standing waves and multipathing/field cancellation. These dead zones have very bad reception, but

by slightly moving the source of transmission or the receiving antenna, these problems van be solved (the dead zones will shift or change). Such effects are very unpredictable and thus a naturally occurring problem rather than an attack since the effect is hard to produce in any controlled manner (Oertel et al. 2009).

- **Shielding Tags:** Faraday cages such as aluminum foil-lined bags can shield tags from electromagnetic waves, thus disrupting the communication between tags and readers. This can be exploited by a prospective thief to avoid the checkout reader and steal any product undisturbed.

Both passive and active interference could lead to interruption of RFID communications or even to a complete crash of the identification systems deployed in companies, organizations and merchant stores. The goal of the adversary would be either to sabotage the victim or to perform malicious actions (e.g. steal goods etc.) undisturbed and undetected.

3.4 Evaluation of threats and possible countermeasures

Similarly with Figure 2, Figure 3 summarizes the possible threats related to the RFID *communication layer* and refers to their main impacts (*damages*) as well as the possible defense mechanisms (*solutions*) that could be used in each case. Both *low* and *high cost* RFID tags are vulnerable to almost all threats included in this layer. The cost for implementing an attack varies from *low* (i.e. *eavesdropping* or *passive/active interference*) to *high* for more sophisticated threats (i.e. relay attacks). From the countermeasures against attacks in the *Communication layer*, in most cases the use of efficient encryption and authentication protocols can significantly safeguard an RFID system with a moderate (medium) additional cost. However, in other cases such as relay attacks more sophisticated defense mechanisms are required. A good way to guard against relay attacks is to use the distance between tag and reader as a measure of security. If the tag is very close to the reader, one can assume that no adversary is able to get between them and relay the messages without being detected. Several techniques can be employed to measure this distance: measuring signals strength, the time-delay or round-trip-time, or the orientation of the tag to the reader (triangulation, angle-of-arrival). Ideally, one should make protocols as tight as possible on their timing requirements, and tags should respond as fast as possible, to allow very little room for cheating. Distance bounding protocols (Hancke and Kuhn 2008 (Clulow et al. 2007; Singlee and Preneel 2005; Hancke 2005; Kim et al. 2008) are based on this principle and were introduced to combat relay attacks.

	Attack	Potential Damage	Attack Cost*	Class of Tags	Solution - Cost*
Confidentiality	**Eavesdropping**	- Case A: Intercept messages. - Case B: Extract information.	Case A:**L** Case B:**H**	High/Low Cost Tags	- Store critical data on the back-end. **(M)** - Shielding. **(M)** - Use of encryption techniques. **(M)**
	Unauthorized Tag Reading	- Extract information.	**L**	Low Cost Tags	- Use of authentication protocols.**(M)**
	Privacy Threats	- Traceability. - Collection of personal information.	**M**	High/Low Cost Tags	- Killing tags. **(L)** - Blocking access. **(M)** - Relabeling, use of pseudonyms. **(M)** -Use of encryption techniques. **(M)**
	Key Compromise	- Impersonate. - Access to sensitive information. - Break the whole system.	**H**	High/Low Cost Tags	- Strong & published, well-known cryptographic algorithms. **(M)** - Long keys. **(L to H)**
Integrity	**Relay Attacks**	- Manipulate communications. -Deception regarding its location (distance).	**M**	High/Low Cost Tags	- Distance bounding protocols (use of round-trip-time). **(M)** - Measure signal strength and triangulation. **(H)**
	Replay Attacks	- Impersonation. - Desynchronization.	**L**	High/Low Cost Tags	- Use of key updating schemes.**(M)** - Use of timestamps. **(L)** - Use of challenge-response protocols (with nonces, clock synchronization, counters). **(M)**
	Message (Re)construtions	- Impersonation. - Desynchronization.	**M**	Low Cost Tags	- Use of strong cryptographic techniques. **(M)**
	Data Modification/ Insertion	- Alter data on the tag or the back-end data.	**M**	High/Low Cost Tags	- Use read-only tags. **(M)** - Data Modification: use of efficient and secure coding schemes. **(M)** - Data Insertion: dependence between the challenge and the response in the authentication process. **(M)**
Availability	**Active/Passive Interference**	- Interruption of Communication.	**L**	High/Low Cost Tags	Active: - Open problem. - Use of opaque walls. **(H)** - Establish regulations. **(L)** Passive: -Select appropriate frequencies and RFID reader's location. **(L)**

***Cost:** **H** high, **M** medium, **L** low.

Fig. 3. RFID threats and countermeasures related to the communication layer.

4. Back-end Layer

The *Back-end layer* is also vulnerable to a broad range of attacks but consists of many different (non specific to the RFID communication) components. The *Back-end layer* generally consists of three components: the “server”, the “middleware” and the “application software” (O’Brien 2008). The “server” is responsible for collecting RF transaction data from the readers, while the “middleware” sanitizes and converts the data as needed for further processing by the rest of the back-end, which is usually performed by the “application software” such as databases

or business specific software. Attacks against the *back-end layer* may have severe implications.

The most likely points of entry to launch an attack are the information flowing in from the edge hardware and any existing networked connections (EPC Object Name Service or internet access, linking or sharing of databases with other parties etc). We will address only the threats that originate from the side of the edge hardware.

4.1 Confidentiality

Most of the information in a typical RFID system is kept at the *back-end* (e.g. key information, read history, additional information related to tags, items or owners). This renders the *back-end* an attractive target for disclosure attacks.

Privacy Violation: transaction histories or person-related information could be (mis)used by the owner of the system or attackers for tracking, “hotlisting", preferential or blackmail attacks.

Key Compromise: Key material is often stored on the server a good design choice in terms of security. However, even here secret keys are not entirely safe; if an adversary could gain control over the server or access its storage, a leak can occur. Aside from more generic attacks such as network attacks, social engineering, insider attacks etc, the RFID tags and readers themselves can be a potential point of entry to mount an attack. Obtaining key information directly from the *back-end* could enable an attacker to track, access or impersonate tags and readers at will. Forward security is essential to allow systems to recover from such high-impact attacks (Avoine et al. 2009). The impact of the key comprise through an attack to the back-end layer is similar to that when the key compromise is performed through the communication layer. This attack enables an adversary to gain access in critical information that can be used for his own benefit (e.g. perform financial fraud).

4.2 Integrity

The integrity of the information kept by the *back-end* is most directly threatened by *information injection* attacks. Again, these could occur through networked attacks or through the information flowing in from the readers and tags.

Information Injection: Code insertion attacks on the middleware can originate from the tag/reader side. One way of mounting such an attack is through exploits.

Considering the fact that middleware applications often use multiple scripting languages such as Javascript, PHP, XML, SQL etc. there is plenty of opportunity for security holes to exist. An example SQL injection attack is described in (Rieback et al. 2006).

Another avenue for information injection are *buffer overflow attacks*. These are a major threat and are among the hardest security problems in software to guard against. Buffer overflow exploits store data or code beyond the bounds of a fixed-length buffer. When the system attempts to normally process this content, data will flow beyond the buffer and onto the stack, causing it to be executed. Considering the limited memory storage of RFID tags, this may not be trivial, but there are still commands that allow an RFID tag to send the same data block repetitively in order to overflow a buffer in the back-end. 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). More sophisticated attacks involve using RFID tags to propagate hostile code that subsequently could infect other entities of the RFID network (readers and connecting networks). In these cases we speak of worms (replicating code requiring external data) and viruses (self-sustained replicating code). Again, an adversary could use either sophisticated tags or additional hardware in order to store and spread a virus or other RFID malware. The impact of such attacks can be extremely serious. For instance, an injected virus or malware could crash the whole backend system in a hospital identification system or alter the private information of patients.

Although these types of attacks are not wide-spread, and rather unlikely to be performed in real-life scenarios through simple passive RFID tags, laboratory experiments (Rieback et al. 2006) have proved that they are feasible. We should not forget after all that instead of using simple passive RFID tags to perform code injection other more powerful devices (instead of passive RFID tags) or access to the back-end database though other means could be used to successfully inject a virus or another type of malware.

4.3 Availability

Successful Denial of Service (DoS) attacks against the back-end of an RFID system can have a system-wide impact (unless adequate backup measures are in place). A primary point of attack is again the information flow from the edge-hardware.

Partial DoS: Flooding and spamming attacks can cause temporary failure in the back-end of an RFID system, or provide such a workload that processing of legitimate requests is slowed or delayed. One could think of using *blocker tags* (Juels et al. 2003) to spam readers with answers upon attempted read (these requests are all passed on to the server, unless care was taken to detect and prevent

this sort of attack by the reader). Also, open systems which allow untrusted readers to interface with the server could be spammed with (many) malicious readers, generating a large amount of traffic at one specific time (Burmester et al. 2006).

Complete DoS: If the chain of programs running in the *back-end* is hit by a successful DoS attack (the database is taken down, the server is crashed by bad input, etc.), the whole system will suffer from DoS, unless backups are in place and working. As said, we do not go into the plethora of attacks that could lead to DoS in databases, Operating Systems or networks, but again, the RFID edge hardware can be an extra point of entry that should be properly secured (Rieback et al. 2006).

The effects of a *partial/complete DoS* attack in a real application scenario vary from temporary interruption of services to the complete disruption of an RFID system. For instance, such an attack may enable an adversary to crash the RFID system of a rival company and thus resulting loss of revenue.

	Attack	Potential Damage	Attack Cost*	Solution - Cost*
Confidentiality	**Privacy Violation/Key Compromise**	- Tracking, "hotlisting". - Access to private information.	**M**	- Access Control Mechanisms. **(L to M)** - Firewalls, Intrusion Detection Systems. **(L to H)**
Integrity	**Information Injection**	- Manipulation/ erase of data.	**M**	- Data and code checking. **(H)**
Availability	**Denial of Service Attacks**	- Interruption of Services. - Crash of the whole RFID system.	**M**	- Access Control Mechanisms. **(L to M)** - Firewalls, Intrusion Detection Systems. **(L to H)** - Efficient search protocols. **(M)**

***Cost:** **H** high, **M** medium, **L** low.

Fig. 4. RFID threats and countermeasures related to the Back-end layer.

4.4 Evaluation of threats and possible countermeasures

Figure 4 depicts the association between the threats related to the *Back-end layer*, their potential impact (*damage*), the *cost* required to perform these attacks as well as possible defense methods (*solutions*) and their associated *cost*. In all cases the cost required to perform an attack is medium, as these are common attacks in network systems in general, while their impact can be very large in an RFID applica-

tion scenario. The countermeasures against such threats mainly include standard security mechanisms such as access control systems, intrusion detection systems and firewalls. The most expensive attack to combat is *information injection*, which requires detailed data and code checking; a very hard and time consuming task.

5. Open Issues and Discussion

In this chapter we presented a detailed overview of the most prominent RFID threats by dividing them in three main layers and then considering which of the three security principles (*confidentiality*, *integrity* and *availability (CIA)*) is being compromised in each case. This is the first time, to the best of our knowledge, that the concept of the main security principles has been used as a criterion to classify RFID threats. We believe that this point of view provides a structured description and global perspective of the problem. Additionally, we relate the treats at each layer to their impact, their delivery cost, the type of RFID tags most vulnerable to these threat, as well as possible countermeasures and their associated cost.

Many defense mechanisms have already been proposed to safeguard RFID systems against possible attacks. Some of these attacks are easy to combat (i.e. *unauthorized tag reading* and *tracking*) by using efficiently designed protocols and cryptographic primitives as well as implementing appropriate software. Other threats are harder or more costly to defend against (i.e. hardware-related threats, like tampering attacks or signal degradation), while others are still open problems and subject to research (i.e. attacks that compromise the *availability*).

It is obvious that there is a need for effective defense mechanisms to guarantee the reliability and security of RFID systems. In this chapter we provide a list of the main solutions used to combat these threats.

Acknowledgments

We would like to thank 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 and the ICT talent grant supported by the Delft Institute for Research on ICT (DIRECT) under the grant "Intrusion Detection and Response in Wireless Communications" awarded to Aikaterini Mitrokotsa.

References

Agrawal D, Archambeault B, Rao JR et al. (2003) The EM Side-Channel(s). In: CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, pages 29-45, London, UK. Springer-Verlag.

Anderson R, Kuhn K (1998) Low cost attacks on tamper resistant devices. In: Security Protocols 5th International Workshop Paris, France, April 7-9, 1997, Proceedings, LNCS, Vol. 1361, pages 125–136, Springer-Verlag Berlin Heidelberg.

Auto-ID Center (2003) Draft protocol specification for a 900MHz Class 0 Radio Frequency (RF) Identification Tag. http://www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFID Tag_Specification.pdf. Accessed 15 February 2010.

Avoine G (2005) Cryprography in Radio Frequency Identification and fair exchange protocols. PhD thesis, No. 3407, Ecole Polytechnique Fédérale de Lausanne, Switzerland, December 2005.

Avoine G, Lauradoux C, Martin T (2009) When compromised readers meet RFID - extended version. In: Workshop on RFID Security - RFIDSec'09, Leuven, Belgium.

Avoine G. Oechslin P (2005) RFID traceability: A multilayer problem. In: Patrick A, Yung M (eds) Financial cryptography and data security, 9th International conf., FS 2005, LNCS 3570, pages 125-140. Springer-Verlag Berlin Heidelberg.

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

Berkes J, (2006) Hardware attacks on cryptographic devices. Technical Report ECE 628, University of Waterloo.

Burmester M, van Le T, de Madeiros B (2006) Provably secure ubiquitous systems: universally composable RFID authentication protocols. In: 2nd IEEE/CreateNet International Conference on Security & Privacy in Communication Networks (SECURECOMM 2006), pages 1–9, Baltimore, MD, USA, IEEE Computer Society.

Clulow J, Hancke GP, Kuhn MG et al (2006) So near and yet so far: distance-bounding attacks in wireless networks. In: Proceedings of the European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS'06), pages 83–97, Hamburg Germany.

Collins J (2006) RFID-Zapper shoots to kill. RFID Journal. http://www.rfidjournal.com/article/print/2098. Accessed 15 February 2010.

de Koning Gans G, Hoepman JH, Garcia FD (2008) A practical attack on the MIFARE classic. In: Grimaud G, Standaert FX (eds) Smart Card Research and Advanced Applications, 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008, Proceedings, Series LNCS, Subseries Security and Cryptology, Vol. 5189, Springer-Verlag Berlin Heidelberg.

Desmedt Y, (1988) Major Security Problems with the "unforgeable" (Feige-)Fiat- Shamir proofs for identity and how to overcome them. In 6th Worldwide Congress on Computer and Communications Security and Protection (Securicomm'88), pages 147–159.

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.

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

Garcia FD, de Koning Gans G, Muijers R et al (2008) Dismantling MIFARE Classic. In: Jajodia S, Lopez J (eds) ESORICS 2008, LNCS 5283, pages 97-114. Springer-Verlag Berlin Heidelberg.

Han DG, Tagaki T, Kim HW et al (2006) New security problem in RFID systems "Tag Killing". In: Computational Science and Its Application – ICCSA 2006, Workshop on Applied Cryptography and Information Security (ACIS 2006), LNCS 3982, pages 375–384. Springer-Verlag Berlin Heidelberg.

Hancke GP (2005) A practical relay attack on ISO 14443 proximity cards. Technical Report, University of Cambridge, Computer Laboratory.

Hancke GP, Kuhn MG (2008) Attacks on time-of-flight distance bounding attacks. In: 1st ACM Conference on Wireless Network Security, pages 375–384, ACM, New York, NY, USA.

Haselsteiner E, Breitfuß K (2006) Security in Near Field Communication (NFC) - strengths and weaknesses. In: Workshop on RFID Security, pages 1–9, Graz, Austria, 12-14 July 2006.

Heydt-Benjami TS, Bailey DV, Fu K et al. (2008) Vulnerabilities in first generation RFID-enabled credit cards. Financial Cryptography and Data Security, 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12-16, 2007, LNCS 4886, pages 2-14. Springer – Verlag Berlin Heidelberg.

Hutter M, Mangard S, Felhofer M (2007) Power and EM attacks on passive 13.56 MHz RFID devices. In: Paillier P, Verbauwhede (eds) CHES 2007, LNCS 4727, pages 320-333. Springer-Verlag Berlin Heidelberg.

Hutter M, Medwed M, Hein D et al (2009) Attacking ECDSA-enabled RFID devices. In: Abdalla M et al (eds): ACNS 2009, LNCS 5536, pages 519-534. Springer-Verlag Berlin Heidelberg.

ISO (International Organization for Standardization) (2005) ISO/IEC 27001: 2005 Information Technology – Security Techniques – Specification for an Information Security Management System. http://www.iso.org/iso/catalogue_detail?csnumber=42103. Accessed 15 February 2010.

Jechlitschek C (2006) A survey paper on Radio Frequency Identification (RFID) trends, http://www.cse.wustl.edu/~jain/cse574-06/rfid.htm. Accessed 15 February 2010.

Juels A (2005) Strengthening EPC Tags Against Cloning. In: Jacobson M, Poovendran R (eds) ACM Workshop on Wireless Security (WiSe'05), LNCS 3982, pages 67–76. Springer-Verlag Berlin Heidelberg.

Juels A (2006) RFID security and privacy: a research survey. In: IEEE Journal on Selected Areas in Communications, 24(2):381-394.

Juels A, Rivest R, Szydlo M (2003) The Blocker Tag: selective blocking of RFID tags for consumer privacy. In: Proceedings of the 10th ACM Conference on Computer and Communication Security, pages 103–111. ACM New York, NY, USA.

Juels A, Weis S (2007) Defining Strong Privacy for RFID. In: Proceedings of the fifth annual IEEE International Conference on Pervasive Computing and Communications Workshop (PercomW'07), pages 342-347.

Karygiannis T, Phillips T, Tsibertzopoulos A (2006) RFID Security: A taxonomy of risk. In: Proceedings of the 1st International Conference on Communications and Networking in China (China'Com 2006), October 2006, pages 1-8, IEEE Press.

Karygiannis T, Eydt B, Barber G et al (2007) Guidelines for securing Radio Frequency Identification (RFID) systems. Special Publication 800-98, National Institute of standards and Technology, Technology Administration U.S. Department of Commerce, csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf. Accessed 15 February 2010.

Kaufman C, Perlaman R, Speciner M (2002) Network Security: Private Communication in a Public World. 2nd Edition Prentice Hall.

Kfir Z, Wool A (2005) Picking virtual pockets using relay attacks on contactless smartcard. In: Proceedings of the 1st International Conference on Security and Privacy (SECURECOMM'05), pages 47–48. IEEE Computer Society Press, 2005.

Kim CH, Avoine G, Koeunem F et al. (2008) The Swiss-Knife RFID Distance Bounding Protocol. In: Lee PJ, Cheon JH (eds), International Conference on Information Security and Cryptology - ICISC, LNCS 5461, pages 98-115. Springer-Verlag Berlin Heidelberg.

Kocher PC, Jaffe J, Jun B (1999) Differential power analysis. In: Wiener M (ed), Advances in Cryptology - CRYPTO '99, Vol. 1666. pages 388–397. Springer-Verlag.

Lowry J (2004) Adversary modeling to develop forensic observables. In: 4th Annual Digital Forensics Research Workshop 2004, pages 204–213, Baltimore, Maryland.

Meadows C, Poovendran R, Pavlovic D et al (2007) Distance bounding protocols: authentication logic analysis and collusion attacks. In: Poovendran R, Wang C, Roy S (eds) Secure localization and time synchronization for wireless sensor and ad hoc networks, Vol. 30 of Wireless

Networks and Mobile Communication Series, pages 279–298. Springer Science Business Media (LLC) US.

Mirowski L, Hartnett J, Williams R (2009) An RFID attacker behavior taxonomy. In: IEEE Pervasive Computing, pages 1536-1268. IEEE Computer Society.

Mitrokotsa A, Rieback MR, Tanenbaum AS (2009) Classifying RFID attacks and defenses. Special Issue on Advances in RFID Technology, Information Systems Frontiers, Springer Science & Business Media, LLC 2009. doi: 10.1007/s10796-009-9210-z., July 2009.

O'Brien DF, (2008) RFID: an introduction to security issues and concerns. Syngress Press.

Oertel B, Wölk M, Hilty L et al (2004) Security Aspects and Prospective Applications of RFID Systems. Federal Office for Information Security. www.rfidconsultation.eu/docs/ficheiros/RIKCHA_englisch_Layout.pdf. Accessed 15 February 2010.

Ohkubo M, Suzuki K, Kinoshita K (2004) Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In: Proceedings of the Symposium on Cryptography and Information Security (SCIS 2004), Vol. 1, pages 719–724, Sendai, Japan, January 2004.

Ohkubo M, Suzuki K, Kinoshita S (2003) Cryptographic approach to "privacy-friendly" tags. In: RFID Privacy Workshop, MIT, MA, USA.

Oren Y, Shamir A (2007) Remote password extraction from RFID tags. In: IEEE Transactions on Computers. 56(9): 1292-1296. 10.1109/TC.2007.1050.

Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM et al. (2006) RFID systems: a survey on security threats and proposed solutions. In: Cuenca P, Orozco-Barbosa (eds),PWC 2006, LNCS 4217, pages 159-170. Springer Verlag Berlin Heidelberg.

Plos T (2008) Susceptibility of UHF RFID Tags to Electromagnetic Analysis. In: Malkin, T.G. (ed.) CT-RSA 2008. LNCS, vol. 4964, pages 288- 300. Springer-Verlag Berlin Heidelberg.

Radomirovic S, van Deursen T (2008) Vulnerabilities in RFID protocols due to algebraic properties. In: 3rd Benelux Workshop on Information and System Security, Eindhoven, The Netherlands.

Reid D (2006) ePassport 'at risk' from cloning. http://news.bbc.co.uk/2/hi/programmes/click_online/6182207.stm. Accessed 15 February 2010.

Reid JT, Tang T, Gonzalez Nieto JM (2007) Detecting relay attacks with timing-based protocols. In: 2nd ASIAN ACM Symposium on Information, Computer and Communications Security, pages 204–213, Singapore, 2007. ACM New York, NY, USA.

Rieback M, Crispo B, Tanenbaum A (2005) RFID Guardian: A battery-powered mobile device for RFID privacy management. In: Mu Y, Susilo W, Seberry J (eds), Information Security Privacy, 13th Australian Conference, (ACISP 2008), Wollonong, Australia, July 7-9, 2008, Proceedings, LNCS 5107, pages 184–194, Springer-Verlag Berlin Heidelberg.

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 2006), IEEE Computer Society, Washington, DC, USA.

Riscure (2006) Privacy issue in electronic passport. http://www.riscure.com/contact/privacy-issue-in-electronic-passport.html. Accessed 15 February 2010.

SAG Security Assembly Group (2010) SAG RFID Tamper Proof Label. http://www.sag.com.tw/index.php?_Page=product&mode=show&cid=7&pid=32&SetLang=en-us. Accessed 15 February 2010.

Singlee D, Preneel B (2005) Location verification using secure distance bounding protocols. In: Proceedings of the IEEE International Mobile Ad Hoc and Sensor Systems Conference, IEEE Computer Society.

Swedberg C (2006) Broadcom introduces secure RFID chip. In: RFID Journal, 29 June 2006. http://rfidjournal.com/article/view/2464/1/1. Accessed 15 February 2010.

Sweeney PJ (2005) RFID for Dummies. Wiley Publishing Inc, Indianapolis, Indiana.

Tanenbaum AS (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 20 November 2009.

Tu YJ, Piramuthu S (2007) RFID distance bounding protocols. In: 1st International EURASIP Workshop in RFID Technology.

Vaudenay S (2007) On privacy models for RFID. In: Proceedings of ASIACRYPT'07, Vol. 4833, LNCS, pp. 68-87, Springer-Verlag Berlin Heidelberg.