Classification of RFID Attacks

Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum

Department of Computer Science, Vrije Universiteit
De Boelelaan 1081A, 1081 HV Amsterdam, The Netherlands
{katerina, melanie}@few.vu.nl, ast@cs.vu.nl

Abstract. RFID (Radio Frequency Identification) systems are emerging as one of the most pervasive computing technologies in history due to their low cost and their broad applicability. Although RFID networks have many advantages, they also present a number of inherent vulnerabilities with serious potential security implications. 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 systems 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.

1 Introduction

RFID networks exist in a broad range of environments and their rapid proliferation has been underway for quite some time. RFID systems consist of tiny integrated circuits equipped with antennas (RFID tags), 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 are vulnerable to a broad range of malicious attacks ranging from passive eavesdropping to active interference. Unlike in wired networks, where computing systems typically have both centralized and host-based defenses (e.g. firewalls), attacks against RFID networks can target decentralized parts of the system infrastructure, since RFID readers and RFID tags operate in 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, ISO 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 layers. 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.

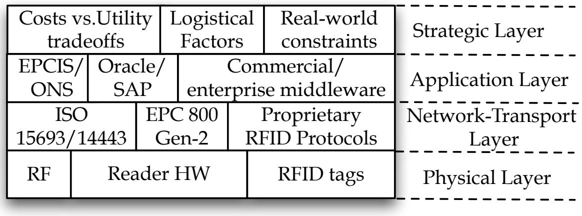

Fig. 1. Layers of RFID Communication.

2 Classification Overview

In this paper we classify attacks based on the layer that each attack is taking place giving the special characteristics and discuss possible available 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 ([1], [2], [14], [22]). Avoine et al. [1], Ayoade et al. [2] and Garfinkel et al. [14] have focused on privacy threats while Karygiannis et al. [22] have proposed a detailed taxonomy of network, business process and business intelligence risks. Avoine et al. [1] demonstrate 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 Frequencies (RF), the hardware of readers and the RFID tags as physical devices. In network-transport layer we describe attacks that take advantage of the implemented RFID protocols such as the standards ISO 15693/14443/18000, the EPC 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 or the EPCIS/ONS servers. Finally in the strategic layer is related with logistical factors, real world constraints and costs vs utility tradeoffs. In this layer we include attacks that take advantage of critical information that is related to 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 Figure 2.

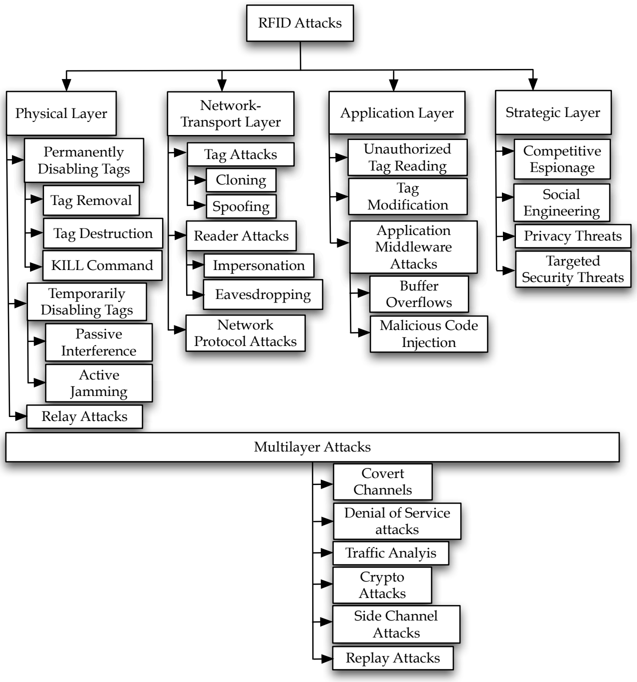

Fig. 2. Classification of RFID attacks.

3 Physical Layer

The physical layer in RFID communications is comprised of the physical interface and the RFID devices. The adversary in this layer takes advantage of the wireless nature of RFID communications, their poor physical security and their insufficient 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 of rendering an RFID tag permanently inoperable are tag removal, tag destruction or using the KILL command.

Tag Removal. Since RFID tags present poor physical, security, RFID tags that are not embedded on 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 could be the malicious 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. This kind of threat is a reality that can be easily performed without the requirement of special technical skills and poses a fundamental security problem. However, this type of attack does not have the potential to be carried out in a massive scale.

Tag Destruction. Based on the same concept of poor physical security, a tag may be physically destroyed intentionally 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. 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 batteries. Furthermore, RFID tags are extremely sensitive to static electricity. RFID tags' electronic circuits can be damaged in an instant by electrostatic discharge caused by conveyor belts or high energy waves.

KILL Command. The Auto-ID center [3] 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. Although this feature can be used for privacy reasons it is obvious that 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 an aluminium foil-lined bag (a simple Faraday Cage (FC)) 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 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. 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 from communicating with readers.

3.3 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. 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. 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 [33] 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 [24] and created great concerns for the $2 billion Dutch public transport system.

3.4 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 [23]. 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 (e.g. stronger glue, embedding tag in products). Intentional of unintentional radio interference could also be limited by using walls opaque to relevant radio frequencies [23]. 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 [10] tags requires a 32-bit password. 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. Another possible way to counter relay attacks is the distance bounding protocol based on ultra-wideband pulse communication proposed by Hancke et al. [15]. Another interesting approach that can be used to safeguard RFID systems against attacks (including physical layer attacks) was proposed by Bolotnyy et al. [5]. More precisely, they have proposed a hardware-based approach that relies on physically unclonable functions (PUFs) to provide security and privacy. PUFs provide an exponential solution to the critical key distribution problem and can protect against cloning even if an adversary has physical access to RFID tags.

4 Network - Transport Layer

This layer includes all the attacks that are based on the way the RFID systems are communicating 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 [26], in practice it has proven that the task of replicating RFID tags does not requite 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 [4] to cloning.

Spoofing. Spoofing is effectively a variant of cloning that does not physically replicate an RFID tag. 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.

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 information recorded 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 with 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 operating system and network protocols used, can be used by malicious attackers in order to launch attacks and compromise the back-end infrastructure.

4.4 Defenses against Network-Tranport Layer Attacks

Through appropriate data collection, it is possible to detect cloned RFID tags. Alternatively, 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. Juels [19] 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 [26] as suggested by the ICAO 9303 standard [16]. In order to defend against passive eavesdropping attacks encryption mechanisms could be used to encrypt the RFID communication. Spoofing and impersonation could be combated by using authentication protocols or a second form of authentication such as one-time passwords, PINs or biometrics. Network protocol attacks could be countered by hardening all components that support RFID communication, using secure operating systems, disabling insecure and unused network protocols and configuring the protocols used with the least possible privileges.

5 Application Layer

This layer include 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

Since not all the RFID tags support protocols for authenticated read operations, adversaries may easily read the contents of RFID tags (even from large distances) without leaving any trace.

5.2 Tag Modification

Considering the fact that most RFID tags that are in widespread use today employ user writeable 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 used standard used and the READ/WRITE protection employed.

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 [31] 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), or using a tag with more memory than the one expected.

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) [31]. In this scneario, an adversary uses the memory space of RFID tags in order to store and propagate the infecting viruses. Although this type of attacks are not wide-spread, laboratory experiments [31] have proved that they are feasible. Considering the fact that middleware applications are using 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 [31], 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. One approach proposed was the use of aluminum-lined wallets to protect RFID payment cards and epassports against unauthorized reading. Many companies embraced this solution and sell this type of products ([27], [8]). 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. Encryption techniques, authentication protocols or access control lists may provide an alternative solution. More specifically, approaches based on symmetric key encryption [25], public key encryption [11], hash functions [34], mutual authentication ([28], [7]) or even non-cryptographic solutions such as pseudonyms [18], 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 gum is definitely not worthwhile.

Buffer overflows and malicious code injection in the middleware can be combated with simple countermeasures. Performing regular code reviews to ensure the security of the system against vulnerabilities and bugs, by for instance ensuring that bounds checking takes place (c.f. [31]). For databases, the use of bound parameters and applying least possible privileges among other things [13] 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 [23] or marketing scenarios. 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 [2].

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 example of this attack is targeting and robbing people who collect valuable items (e.g watches or jewelry) trucks or ships that carry valuable or critical items.

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 [20], [30], relabeling [17] or clipping [21] tags, using pseudonyms [18], distance measurements [12] and encryption techniques ([25], [11]).

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. [23] provide a complete list of countermeasures that can be employed to eliminate the business and privacy risks related to RFID systems.

The privacy issues related to RFID communication should also receive attention from legislators and authorities that may give guidelines that should be followed by organizations and companies that use RFID systems. The Center for Democracy and Technology [6] and the EPC global [9] have already developed a set of guidelines and principles that can be used by organizations to counter privacy challenges.

7 Multilayer Attacks

A lot of 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 [22]. 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" [20] or the RFID guardian [30]. 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 [22] 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 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 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 [32] has proven that the key used in a Dutch passport can be easily broken using a standard PC performing a brute-force attack for two hours.

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

A common defense approach to attacks such as the above, is the use of a challenge response protocol. RFID tags and readers usually share a secret and use a challenge response protocol to authenticate their identities. Nevertheless, very often this approach is subject to replay attacks. In a replay attack, an adversary broadcasts a tag's response recorded from a past transaction in order to impersonate the tag to a reader. 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.

7.7 Defenses against Multilayer Attacks

Covert channels attacks are 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. 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 smartcard's security flaws [29] 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.

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. Nevertheless, these schemes are inconvenient and with doubtful efficiency considering the vulnerabilities to which challenge response protocols are susceptible to. 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 [24]. Another approach is based on the distance between the information requestor and the information owner. Fishkin et. al. [12] 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 tried to discover 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.

In this paper, we classified attacks based on the layer that each is taking place and we discussed possible countermeasures that can be used to combat these attacks. We discriminated them to attacks deployed in the physical layer, the application layer, the strategic layer and multilayer attacks. Finally, we point out for which attacks further research is necessary in order to achieve adequate defense against them.

References

1. Avoine, G., Oechslin, P.: RFID Traceability: A Multilayer Problem. In: Patrick, A., Yung, M. (eds.). In: Proc. of the Ninth Int'l Conf. on Financial Cryptography and Data Security (FC'05), Lecture Notes in Computer Science, Vol. 3570. (2005) 125–140
2. Ayoade, J., Saxby, S.: Roadmap for Solving Security and Privacy Concerns in RFID Systems. In: *Computer Law and Security Report* (2007)
3. Center, A.I.: 900 MHz Class 0 Radio Frequency (RF) Identification Tag Specification. In: Draft, www.epcglobalinc.org/standards/specs/900_MHz_Class_0_RFIDTag_Specification.pdf, (2003)
4. DN-Systems: BBC Reports on Cloning of the new e-passport. In: http://www.dn-systems.de/press/document.2007-01-04.2112016470, (2007)
5. Bolotnyy, L., Robins, G.: Physically Unclonable Function-Based Security and Privacy in RFID Systems. In: Proc. of PerCom'07. New York, USA (2007) 211–220
6. CDT: CDT Working Group on RFID: Privacy Best Practices for Deployement of RFID Technology. In: Interim Draft, http://www.cdt.org/privacy/20060501rfid-best-practices.php, (2006)
7. Dimitriou, T.: A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks. In: Proc. of IEEE Conf. on Security and Privacy for Emerging Areas in Communication Networks, (2005)
8. Emvelope: Products. In: http://www.emvelope.com/products. (2008)
9. EPCGlobal: Guidelines on EPC for Consumer Products. In: http://www.epcglobalinc.org/public/ppsc_guide/, (2005)
10. EPCGlobal: Class-1 generation-2 UHF RFID Protocol for Communications at 860MHz-960 Mhz. In: *EPC Radio-Frequency Identity Protocols*, Vol. 1.1.0, (2005)
11. Fedhofer, M., Dominikus, S., Wolkerstorfer, J.: Strong Authentication for RFID Systems Using the AES Algorithm. In: Proc. of Cryptographic Hardware and Embedded Systems (CHES'04), Vol. 3156. *Lecture Notes in Computer Science*. (2004) 357–370
12. Fishkin, K., Roy, S., Jiang, B.: Some Methods for Privacy in RFID Communication. In: Proc. of the 1st European Workshop on Security (2004) 42–53
13. Friedl, S.: SQL Injection attacks by example. In: http://www.unixwiz.net/techtips/sql-injection.html, (2007)
14. Garfinkel, S., Juels, A., Pappu, R.: RFID Privacy: An Overview of Problems and Proposed Solutions. In: *IEEE Security & Privacy*, Vol. 3. (2005) 34–43
15. Hancke, G., Kuhn, M.: An RFID Distance Bounding Protocol. In: Proc. of the 1st Int'l Conf. on Security and Privacy for Emerging Areas in Communications Networks (SecureComm 2005) (2005) 67–73
16. ICAO. ICAO Document 9303. In: http://mrtd.icao.int/content/view/33/202, (2006)
17. Inoue, S., Yasuura, H.: RFID Privacy Using User-Controllable Uniqueness. In: Proc. of RFID Privacy Workshop. MIT, Massachusetts, USA (2003)
18. Juels, A.: Minimalist Cryptography for Low-cost RFID Tags. In: Proc. of the 4th Conf. on Security in Communication Networks (SCN'04), Vol. 3352.*Lecture Notes in Computer Science*. Springer-Verlag (2004) 149–164
19. Juels, A.: Stengthening EPC Tags Against Cloning. In: Proc. of ACM Workshop on Wireless Security (WiSe'05). ACM Press (2005) 67–76
20. Juels, A., Rivest, R.,Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: Proc. of the 10th ACM Conf. on Computer and Communication Security. (2003) 103–111
21. Karjoth, G., Moskowitz, P.A.: Disabling RFID Tags with Visible Confirmation: Clipped Tags are Silenced. In: Atluri, V., di Vimercanti, S.D.C., Dingledine, R. (eds). In: Proc. of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES 2005). (2005) 27–30

22. Karygiannis, A., Phillips, T., Tsibertzopoulos, A.: RFID Security: A Taxonomy of Risk. In: Proc. of China'Com '06. (2006) 1-8
23. Karygiannis, T., Eydt, B., Barber, G., Bunn, L., Phillips, T.: Guidelines for Securing Radio Frequency Identification (RFID) Systems. In: NIST Special Publication 800-98, National Institute of Standards and Tecnology (2007)
24. Kfir, Z., Wool, A.: Picking Virtual Pockets Using Relay attacks on Contactless Smartcard. In: Proc. of the 1st Int'l Conf. on Security and Privacy. (2005) 47–48
25. Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., Ohkubo, M.: Low-cost RFID Privacy Protection Scheme. In: *IPS Journal*, Vol. 45. (2003) 2007–2021
26. Laurie, A.: Practical Attacks Against RFID. In: *Network Security*, Vol. 2007, No. 9. (2007) 4–7
27. mCloak: mCloak for RFID tags. In: http://www.mobilecloak.com/rfidtag/rfid.tag.html (2005)
28. Molnar, D. and Wagner, D.: Privacy and Security in Library RFID: Issues, Practices and Architectures. In: Proc. of Conf. on Computer and Communications Security. (2004) 210–219
29. Nijmegen, R.U.: Dismantling Contactless Smartcards. Technical Report 08-33A, Radboud Universiteit Nijmegen. www2.ru.nl/media/pressrelease.pdf, (2008)
30. Rieback, M.R., Crispo, B., Tanenbaum, A.S.: RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In: Proc. of ACISP'05. (2005) 184–194
31. Rieback, M.R., Bruno, B., Tanenbaum, A.S. Is Your Cat Infected with a Computer Virus? In: Proc. of the 4th IEEE Int'l Conf. on Pervasive Computing and Communications. (2006) 169–179
32. Riscure.: Privacy Issues with New Digital Passport. In: http://www.riscure.com/2_news/passport.html, July (2005)
33. Tanenbaum, A.: Dutch Public Transit Card Broken. In: http://www.cs.vu.nl/ ast/ov-chip-card/, (2007)
34. Weis, S., Sarma, S., Rivest, R., Engels, D.: Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems. In: Proc. of 1st Int'l Conf. in Security in Pervasive Computing, Vol. 2802. (2003) 201–212