Preface

This paper is intended for use by students of computer science, information security, engineering, and electrical engineering. The reader is presumed to have a basic knowledge of RFID devices at the level provided by the first series of presentations for the course Seminar Information Security Technology (2IF03) at Eindhoven University of Technology. The students of computer science and information security will find material which should be included in the basic education of every computer science student. This paper should furthermore allow students to acquire an appreciation of the breadth and variety within the field of RFID devices and its future as a fascinating area of research.

For the students of engineering and electrical engineering, the concepts introduced in this paper will provide a theoretical framework for improvements in that field of study. With the help of these concepts, it is theoretically possible to reduce some of the security problems that hamper the daily use of RFID on a broad scale.

April 2012

Maurice Aarts
Student
2IF03 (2012)

Organization

2IF03 (2012) is organized by the department of Computer Science & Mathematics, Eindhoven University of Technology (TU/e)

Executive Committee

Lecturer:	Boris Škorić (TU/e, NL)
Co-lecturer:	Nicola Zannone (TU/e, NL)

Program Committee

Lecturer:	Boris Škorić (TU/e, NL)
Co-lecturer:	Nicola Zannone (TU/e, NL)

Referees

A. Cedillo	D. Broekhuis	M. Morbitzer
A. Garcia Ramirez	G. v Enckevort	N. Zannone
A. Piepoli	J. Habraken	Ö. Payzin
A. Ricci	J. Kremers	P. Teeuwen
B. Lutgens	K. Reintjes	R. Kleinpenning
B. Škorić	M. Balazia	R. v Galen
C. Thijssen	M. Gurbanov	S. Damen

Sponsoring Institutions

None

Table of Contents

RFID Security - Skimming and Cloning

RFID Security - Skimming and Cloning

Maurice Aarts

TU/e - Eindhoven University of Technology, Eindhoven, NL,
m.a.p.aarts@student.tue.nl,
WWW home page: http://maurice.aarts.info/

Abstract. The use of radio frequency identification (RFID) technology is being used more pervasively in all kinds of applications. In their current form, RFID systems are often vulnerable to a wide range of malevolent attacks, such as, but not limited to, skimming and cloning. In this paper we will analyze both skimming and cloning attacks, explain how they are done and describe the possible impact of such attacks. We will demonstrate an actual attack using the EPC Gen2 RFID tag and finally we will present a number of precautions that should help to protect against such attacks.

Keywords: RFID, tags, attacks, skimming, cloning, authentication, EPC Gen2

1 Introduction - RFID

Radio frequency identification (RFID) technology is a wireless communication technology that allows the automatic identification of objects through radio waves over a short distance. RFID tags are electronic labels that can be attached to an object which can then communicate with a RFID reader in order to identify itself to the reader. A RFID tag consists of an integrated circuit chip and an antenna. A RFID reader is an active RF front-end device that emits an electromagnetic field which is used to energize circuits on a RFID tag[1]. Figure 1 shows an example of such a RFID tag and a RFID reader.

RFID can be used for the purpose of automatically tracking, identifying, categorizing and locating of labels, as well as anti-counterfeiting, supply chain management, and tolling. Some of the biggest advantages of RFID include non-line-of-sight operation, rapid identification speed and high identification rates. This helps to make RFID ideal to be used in many application domains ranging from military to public and commercial applications[2].

1.1 Types of RFID tags

There are four basic types of RFID tags that come in many different shapes, sizes and capabilities. These are: *active tags*, *semi-active tags*, *semi-passive tags* and *passive tags*[3]. The most significant difference between the four types of tags is how they are powered. There are also additional differences, which are listed in Table 1.

(a) A RFID Tag (b) A RFID Reader

Fig. 1. Radio frequency identification, a tag and a reader

Table 1. A comparison of different types of RFID tags

Type of tag	Active	Semi-Active	Semi-Passive	Passive
Range	0 to 30m[a]			0 to 3m
Size	Large	Large	Small	Small or Tiny
Sensors/Storage	Yes	Yes	Yes	No[b]
Power source	External	External	External/Field	Field
Lifespan	Until power source depleted[c]			More than 20 years
Price (per tag)	>$20	$10-20	$1-10	<$0.10

[a] Ranges of over 100m may be reached with a more powerful power source.
[b] Ultra low voltage sensors may be used within the reader's magnetic field.
[c] A semi-passive tag could possibly last longer if it can function as a passive tag.

Active tags: Active RFID tags are self powered with a battery or other power source. The tag uses its own power for all calculations and it can broadcast a signal at any time regardless of input from a RFID reader.

Semi-active tags: Semi-active RFID tags are almost identical to active tags, except that they will only start actively broadcasting a signal when they have been interrogated by a RFID reader. They use their own power for calculations.

Semi-passive tags: Semi-passive RFID tags are similar to semi-active tags in that they also have a battery or other power source on board. The difference from semi-active tags is that they use the power source for any computations and responses, and additionally use the electromagnetic field provided by a RFID reader to increase broadcasting power. This enables the tag to transmit its data to longer ranges.

Passive tags: Passive RFID tags rely solely on the electromagnetic field provided by a RFID reader for all power. When a passive tag is not in the vicinity

of a RFID reader it is inert, only within the electromagnetic field can it do calculations and transmit data.

RFID systems are susceptible to a broad array of malicious attacks ranging from passive eavesdropping to active interference. RFID has the vulnerabilities of any wireless system, where passive and active attacks can be performed easily. The limitations on cost, size and power consumption for low cost passive tags often result in low security features, in some cases the whole security relies on the premise that RFID is harder to copy than a bar code[2].

2 RFID Attacks

The major problem with RFID tags is that they act as an "always on" device in an open system. They transmit data to any RFID reader without any restrictions (provided they use the correct protocol and frequencies.) This allows sensitive information to be released about a certain object that the tag is attached to[4]. A RFID system is usually composed of three components, as shown in Figure 2; a RFID tag, a RFID reader and a host system that usually contains a database. A reader sends a radio signal to tags, receives the data transmitted from a tag, and sends the data to the back-end server. The back-end server is usually regarded as a secure server. Note that the communication channels' strength is asymmetric. The forward communication distance is much longer than the backward communication distance, which means that it is much easier for an adversary to listen to signals emitted by a reader than to signals emitted by a tag[5]. We will assume that the communication between the reader and the back-end server is secure and any attacks on that channel are outside of the scope of this paper. The channel between the reader and the tags is wireless, and thus it is relatively simple to eavesdrop or inject arbitrary messages. In the next sections we will briefly explain a number of possible attack strategies that RFID is vulnerable to.

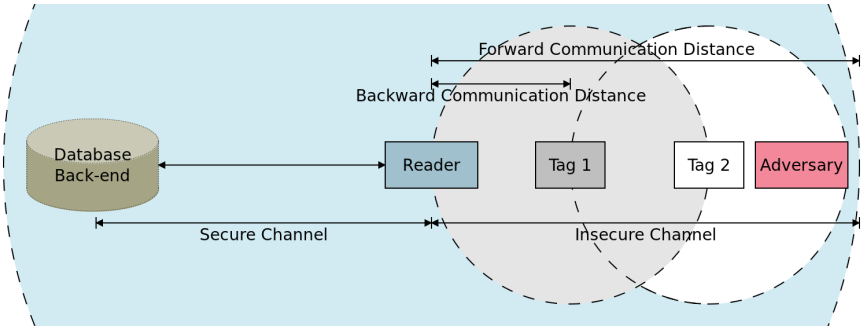


Fig. 2. A typical RFID system. The wireless transmission range of the reader and the tags are shown as the large (cropped) and small dashed circles respectively.

2.1 Eavesdropping and Replay attacks

Eavesdropping is when a third party listens to and records the frequencies being emitted by either the RFID reader or the RFID tag. When the eavesdropper records the data being transmitted by the reader it is called *Forward Eavesdropping* and when they record the data being transmitted by the tag it is called *Backward Eavesdropping*. If we assume that the adversary in Figure 2 is attempting to eavesdrop on the communication between the reader and tag 1 we can see that it can only do forward eavesdropping as it is out of the transmission range of the RFID tag and can thus only detect the data being sent by the reader. Due to these distance constraints it is significantly more difficult to do backwards eavesdropping than it is to do forwards eavesdropping. Eavesdropping is often used as part of a more complex attack called a *replay attack*, in which an attacker records part of the communications between a RFID tag and a legitimate reader. The attacked can then replay one side of the recorded communications to make either the reader think it is talking to a real RFID tag, or to make a RFID tag think it is talking to a legitimate reader. Eavesdropping also gives the attacker additional time to analyze the communication protocol used, possibly allowing him to break the encryption used or to find flaws in the implementation.

2.2 Skimming

Skimming is a type of attack in which an attacker places a RFID reader near a RFID tag without the RFID tag holder's knowledge and initiates communication with the RFID tag without authorization[6]. The reader creates an electromagnetic field which activates the RFID tag and causes the tag to transmit data back to the reader. This allows the attacker to read and record the data on the tag. A reader used for skimming may also transmit data to the tag in order to obtain additional information from it in a process called *active skimming*. If the reader only initializes the electromagnetic field and does not transmit any other messages it is referred to as *passive skimming*. Skimming also allows an attacker to make a (digital) copy of a RFID tag in a process called (digital) tag cloning.

2.3 Cloning

Cloning of a RFID tag is when an attacker makes a copy of an existing RFID tag and uses his copy for illegitimate purposes. Cloning of a RFID tag can be done both virtually or using physical hardware, and depending on the purpose of the cloned tag it may physically not even resemble the original tag. Using specially constructed RFID devices an attacker can program a 'reader' to act exactly like the RFID tag that was copied. The attacker can also choose to create an actual hardware implementation of the RFID tag which can then be used repeatedly without the need for additional hardware. A cloned tag will transmit exactly the same data as the original tag, and thus is capable of fooling the RFID reader into thinking that it is actually talking to the original tag. Passive RFID tags often only contain a unique identifier which it broadcasts when it is energized.

This means that if the attacker can construct a tag that replies using the same identifier as the original RFID tag, the reader can not discern between the two tags and will ultimately see them as the same tag. An attacker can also clone RFID tags by simply listing the identification numbers he needs and then asking a manufacturer to produce a set of such RFID tags; depending on the type of tags used and the integrity of the manufacturer, this may also prove fruitful.

2.4 Relay attacks

A relay attack is a type of attack that utilizes eavesdropping in a live environment. In this scenario the attacker has both a RFID reader referred to as a *leech* and a RFID device that can act as a RFID tag called a *ghost*. The attacker will then place the ghost near a legitimate reader and initiate a conversation with it. Instead of responding immediately it instead transmits the message it received to the leech-reader some distance away (within the range of the targeted legitimate RFID tag). The leech then enables an electromagnetic field and transmits the message it just received from the ghost. As the RFID tag thinks it is talking to the legitimate reader it will respond correctly and the leech then relays the response from the RFID tag to the ghost, which then transmits that response to the legitimate reader. Both the reader and the RFID tag think they are communicating with each other, and that the RFID tag is within range of the reader. However, this is not the case as the ghost and leech are actually relaying the messages over some distance. This allows an attacker to identify himself without the tag actually being in the vicinity of the reader[6]. Figure 3 shows a diagram of such a system.

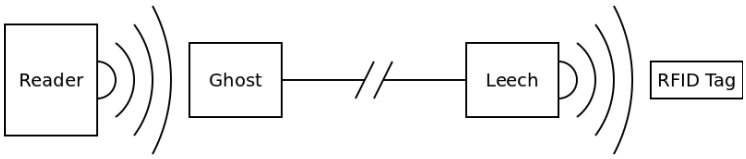


Fig. 3. A relay attack on a RFID system.

3 Impact

RFID devices were first used in World War II as friend-or-foe authenticators[7], but their use has grown incredibly since then. RFID tags are now used for a wide variety of different purposes, such as object tracking, localization, categorization, identification, authentication, verification, anti-counterfeiting, and supply chain management. This vast assortment of services that utilize RFID also means that an attack vector can cause a multitude of different problems depending on how

the RFID system is being used. Below we will cover a subset of possible problems with real-life RFID implementations. The actual implementation of the attack may not be as straightforward as we imply here, due to countermeasures implemented by the developers of the specific system. We will assume that the communication in the scenarios below is as basic as possible without any additional countermeasures that have to be worked around. Section 5 contains a subset of the possible countermeasures that could be used in the examples listed here.

3.1 Identity theft

If an attacker uses eavesdropping and skimming to clone a RFID tag in someone's passport, they can forge a duplicate of that passport for illegitimate purposes. The RFID tag on a passport contains all the information that is on the physical passport, including the photograph. If this information is not secure an attacker no longer needs to have physical access to the passport. They can simply walk by their victim with a RFID skimmer and copy the RFID tags' output. This allows them to copy the document without ever having had physical access to the original[8].

3.2 False authentication

Virtually all new car keys use RFID technology to remotely lock and unlock the vehicle, and many new cars even use RFID to allow the driver to start the car without actually using the key. For locking and unlocking, a car key uses active RFID techniques which allow it to transmit a certain (un-)lock sequence to the vehicle. If an attacker were to eavesdrop on this interchange between the key and the vehicle and clone the keys transmissions to his own device he would be able to lock and unlock the car at his desire. If the attacker also manages to get close enough to the key to skim it and clone the passive RFID component, he would also be able to start the vehicle without the original key. An almost identical (active) system is also used for garage door openers and other similar remote access systems.

3.3 Inventory fraud

In supermarkets and stores RFID devices are often used as price and/or theft indicators. When an item is scanned at the register, the RFID tag tells the register the price, which is then paid by the customer. Additionally its RFID tag is noted or destroyed, allowing that item to leave the premises without setting off the alarm at the entrance. RFID tag cloning is a big problem here, as an attacker can clone the tag of a cheaper item in the store and replace the tag on the item he is going to 'buy' with the tag of the cheaper item. The register will then recognize the item as the cheaper item and the attacker can walk out of the store with an expensive item for a much lower price.

Transport and shipping services often utilize RFID to track their packages within a warehouse or distribution system. An attacker can clone the tags on the original packages and create empty packages with the same tags as the original boxes. If the attacker then replaces the original boxes with empty boxes with cloned tags, the automatic distribution system will still think the packages are all there and accounted for, while the contents of the boxes have actually been stolen by the attacker.

3.4 Counterfeiting

Counterfeiting is a big problem with retail of medication, with different companies making reproductions of a certain medication and selling it under the same brand name as their competitors. In order to combat this, many pharmaceutical companies have adopted RFID tags as an additional verification that the medication being shipped is genuine. However, just as the contents of the medication are being cloned, so are the RFID tags. By cloning the RFID tag of a genuine product and affixing it to a counterfeit product it too will appear genuine on inspection[9].

4 EPC Gen2 Standard

There are many different types of RFID tags, of which one type is the EPC Gen2 tag[1]. EPC stands for *Electronic Product Code* and the EPC Gen2 standard is a complete specification for 96 bit EPC tags[7]. EPC Gen2 tags are designed to be a good balance of cost and functionality, but the security features on the Gen2 tags are minimal[1]. The tags protect the message integrity with a 16 bit Cyclic Redundancy Code (CRC) and are capable of generating 16 bit pseudo random strings. The tags have on chip memory, part of which is writable for the client. EPC Gen2 tags have support for *select*, *inventory*, and *access* queries. The *select* query is used to select a certain tag within the field of the reader. This allows the reader to communicate with only a single tag while the other tags ignore the messages being sent. The *inventory* query allows the reader to ask a RFID tag what it's EPC data is. Figure 4 shows the protocol used in the *inventory* query.

The *inventory* protocol is insecure as it allows all the types of attacks listed in Section 2. The reader sends a query (step 1) to the tag asking for an inventory. The tag then sends a 16 bit (pseudo) random number (step 2) back to the reader. The reader sends the identical random number string (step 3) back to the tag as an acknowledgement, after which the tag sends the EPC data (step 4) to the reader. An eavesdropper can listen to the entire communication and record all four messages. The attacker can then program messages 2 and 4 into another tag and thus simply clone this RFID tag. If the attacker replays messages 1 and 2 from the reader to a tag he can cause the tag to think that it is

[1] A large portion of this section was based on Alfaro et al's paper *Handling Security Threats to the RFID System of EPC Networks [1]*

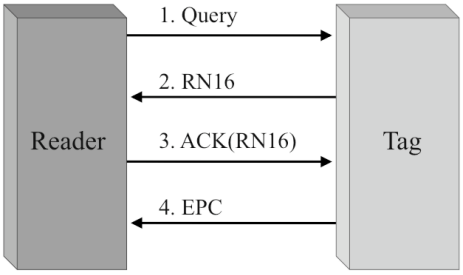


Fig. 4. Inventory Protocol of a EPC Gen2 RFID tag.

communicating with a legitimate listener. Identically, if he sends messages 2 and 4 to a reader he can let the reader think it is talking to the original tag. As there is no real authentication in the protocol it is trivial for a reader to simply send an inventory query and then to reply with the random number it receives, thus skimming is possible as well.

The EPC Gen2 tag is also required to be writable[1] which is protected using a 32 bit password. However the protocol used for writing, shown in Figure 5 is again insecure against many of the attacks from Section 2. Prior to a reader doing a write query it does a *select* query to select which tag it wants to write to, and an *inventory* query to obtain a 16 bit random number (step 3) from that tag. The reader then sends a request (step 5) to the tag containing the random number, upon which the tag responds with a random 16 bits "handle" (step 6) which the reader then uses to do another request to obtain a second 16 bit (pseudo) random number (steps 7,8). The reader will then send an access request (step 9) using the leftmost 16 bits of the 32 bits password XOR'ed with the second random number. If tag accepts the first part of the password, it will reply with a new 16 bits handle (step 10) which is required for the next query by the reader. The reader will then again request another random number (step 11) using that handle to which the tag will reply with a third string (step 12). The reader then sends another access request (step 13) with the other 16 bits of the password XOR'ed with the third random number. If the tag then responds with a new handle (step 14) again, the input was valid and the reader has permission to actually write data (step 15) after which the tag sends a header as acknowledgement.

This protocol can be attacked by simply eavesdropping on the messages sent in steps 8, 9, 12 and 13. The attacker can then XOR message 8 with message 9 and message 12 with message 13. By simply concatenating the two outputs they obtain the entire 32 bit password needed to write to the RFID tag, which gives the attacker full access. Once they have the 32 bit password the tag can be rewritten by the attacker by simply doing the same thing as the legitimate reader does to write data. The tag can also be cloned by recording the responses from

the original tag and programming them into the new tag. As the numbers are pseudo random, a reader can not know that they are hard coded instead of truly random. As there are not any messages that can not be relayed, this protocol is vulnerable to relay attacks as well, allowing an attacker to write data to a tag that is not in the vicinity of the reader. Assuming that the password has been found using eavesdropping, skimming also becomes possible as the skimmer can simply interact with the tag.

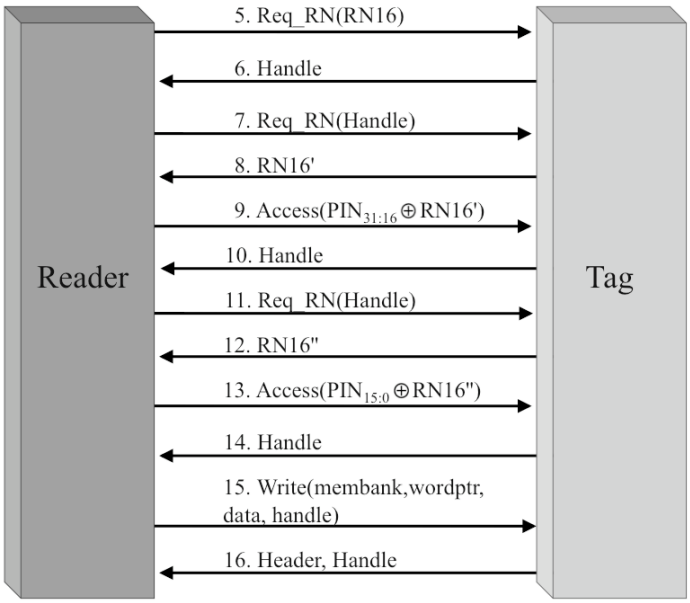


Fig. 5. Writing Protocol of a EPC Gen2 RFID tag.

5 Countermeasures and precautions

As it is long known that passive RFID systems have little to no security there have been a large number of developments in the area of countermeasures and schemes that help to secure the system. RFID systems can be secured on a number of different levels, and depending on where the specific system is vulnerable some techniques are more effective than others. In Sections 3.1-3.4 we gave a few examples of how cloning and skimming can be used to attack different kinds of RFID systems, in the next section we will name a few simple steps that can be taken to patch some of the security holes that exist in these systems. After that we will cover a number of countermeasures specifically for cloning, skimming and eavesdropping.

5.1 Identity theft

Identity theft can be avoided if the passport can not be skimmed, and the communication between the passport and a legitimate reader can not be eavesdropped on. In order to avoid skimming, new passports usually have a physical shield in the cover that folds around the RFID tag when the passport is closed. By effectively enclosing the RFID tag in a Faraday-cage, it is not affected by any electromagnetic fields around the passport, and thus the tag will not transmit the data stored on it. Eavesdropping can be avoided by simply building a Faraday-cage-like enclosure around all the legitimate readers. When the tag is within the enclosure it senses the electromagnetic field and replies to the reader which is also within the Faraday-cage. An eavesdropper is outside the enclosure, and as it is a Faraday-cage, the electromagnetic field doesn't reach the attackers reader. Another possibility to avoid eavesdropping is by lowering the transmission range of both the reader and the tag so that it becomes physically impossible to place an additional reader close enough to the system to actually be able to listen to the messages. Cloning of the passport can also be avoided by requiring the tag and reader to know certain secret information necessary to decode and encode messages, either as encryption or for mutual authentication[8].

5.2 False authentication

Almost all the wireless remote authentication systems used in car keys and garage door openers use a method called rolling codes for mutual authentication. In this system both the RFID tag and the reader have a certain pseudo random number generator (PRNG) which generates random numbers based on an initial seed number. When the RFID tag request to lock or unlock the device the reader is attached to, the tag sends not only the request, but also a random number generated by its PRNG. As the reader has the same PRNG, it calculates what the next random number should be and checks to see if that matches what the RFID tag is sending. If they match then the request is accepted, otherwise the reader will attempt to match the random string to the next 256 possible random numbers to check if they contain a match. If there is a match, the seed on both the RFID tag and the reader gets updated so that at the next attempt both will again generate the same pseudo random number[10]. Without knowing the next random number in the sequence it becomes almost impossible to authenticate to the reader. Using encryption or nonces and mutual authentication can also help to keep an attacker from being able to skim the output of the RFID tag and then later replay it to the reader.

5.3 Inventory fraud & counterfeiting

Both inventory fraud and counterfeiting can be avoided by preventing an attacker from cloning the tags, or modifying the data stored on them. Preventing the attacker from modifying the data is relatively trivial, simply ensure that the tag requires authentication before allowing a reader to write data to the tag, and an

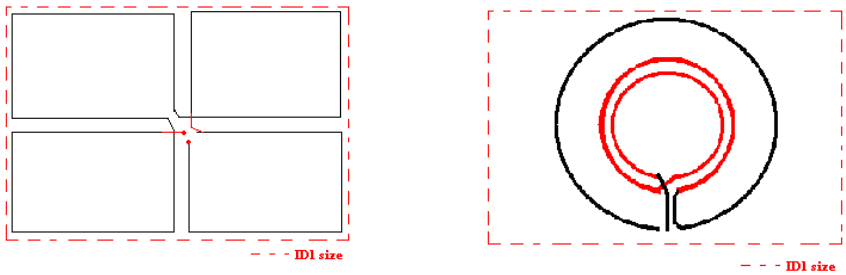
unauthenticated reader will not be able to write to it. This is largely dependent on the protocol used and so the protocol itself should be strengthened to avoid such attacks[11, 12].

5.4 Countermeasures - Cloning

Cloning of a RFID tag can be done using three basic techniques. The first technique is to use encryption for all communication between the tag and the reader. Using encryption and/or nonces makes it significantly more difficult to copy the tag, assuming the private keys are and remain private[13]. A second technique to make a virtually unclonable tag is by using mutual authentication[11, 13]. Both the RFID tag and the reader contain some secret information that allows both the tag and the reader to verify that they are communicating with a legitimate partner. This makes it almost impossible to skim the RFID tag and thus it is significantly harder to clone the tag. The third basic technique is by using physically unclonable functions (PUFs) or physically obfuscated keys (POKs) to store secrets on the RFID tag. These functions use the physical properties of elements of the tag itself to produce keys based on a certain challenge. These properties are unclonable as they are inherent to the physical materials used and a multitude of other factors, and thus it is impossible to make an identical clone the tag that contains such a PUF or POK[1, 14].

5.5 Countermeasures - Skimming and eavesdropping

Skimming an eavesdropping both rely on the RFID tag being physically accessible to the attacker. The most effective way to avoid eavesdropping and skimming is by not allowing an attacker to come close enough to the RFID tag to be able to communicate with it. As stated in Sections 5.1 and 5.2, two techniques to protect against skimming and eavesdropping are by electromagnetic shielding around either the tag against skimming or around the reader and tag together to avoid eavesdropping[8]. Another possible technique is by using a specially formed antenna[6], such as the ones shown in Figures 6(a) and 6(b). These antennas are formed in such a way that the RFID tag must be placed within a certain range of the reader, and in a certain position. By enforcing these restrictions, it makes it almost impossible for an attacker to place the skimming or eavesdropping device in such a way that it can listen in on the conversation without the authorization of the tag holder. The shaped antennas in a RFID also require a similarly shaped antenna in the reader and vice-versa, thus if an attacker wants to listen to the communication, it must also have a similarly shaped antenna. In the case of the square shaped antenna in Figure 6(a), the RFID tag must be placed on the reader in such a way that the antennas line up. This positioning does restrict the legitimate tag holder, but also ensures that an attacker must also place his device in a certain physical location. If it is then made physically impossible to place the device in such a location, the system is much safer to eavesdropping or skimming attacks.



(a) A four loop antenna design (b) A donut antenna design

Fig. 6. Multiple loop antennas for RFID devices

6 Conclusions and Future Work

The first part of this paper presented a brief overview of RFID technology and gave insight into the inherent weaknesses in the technology. We described attacks such as eavesdropping, cloning and skimming, as well as relay and replay attacks as they rely largely on eavesdropping. We have shown that current RFID tags are often still vulnerable to even the simplest of attacks. We highlighted some of the possible repercussions of allowing cloning and skimming in real-world applications and showed a number of relatively simple and efficient countermeasures to help secure RFID systems. This paper only touches on a few of the possibilities for further securing RFID systems.

RFID technology is still expanding and new implementations are being produced daily. Many of the countermeasures pointed out in this paper are still being actively developed and are excellent topics for further research; especially the physically unclonable functions and POKs seem liable candidates for cost-effective RFID devices and are definitely worth looking into.

References

1. J. Garcia-Alfaro, M. Barbeau, and E. Kranakis, "Handling security threats to the rfid system of epc networks," in *Security of Self-Organizing Networks, Auerbach Publications*, pp. 45 –64, sept. 2010.
2. J. Abawajy, "Enhancing rfid tag resistance against cloning attack," in *Network and System Security, 2009. NSS '09. Third International Conference on*, pp. 18 –23, oct. 2009.
3. D. Engels and S. Sarma, "Standardization requirements within the rfid class structure framework," in *Technical Report, Auto-ID Center*, jan. 2005.
4. M. El-Said and I. Woodring, "An empirical study for protecting passive rfid systems against cloning," in *Information Technology: New Generations, 2009. ITNG '09. Sixth International Conference on*, pp. 558 –563, april 2009.
5. P. Peng and Y. Zhao, "Anti-cloning and secure rfid mutual authentication protocols," in *Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on*, pp. 379 –384, oct. 2011.
6. R. Martins, S. Bacquet, and J. Reverdy, "Multiple loop antenna against skimming attack," in *Systems and Networks Communications (ICSNC), 2010 Fifth International Conference on*, pp. 142 –147, aug. 2010.
7. A. Noman, S. Rahman, and C. Adams, "Improving security and usability of low cost rfid tags," in *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*, pp. 134 –141, july 2011.
8. M. Saeed, A. Masood, and F. Kausar, "Securing epassport system: A proposed anti-cloning and anti-skimming protocol," in *Software, Telecommunications Computer Networks, 2009. SoftCOM 2009. 17th International Conference on*, pp. 90 –94, sept. 2009.
9. M. Lehtonen, F. Michahelles, and E. Fleisch, "How to detect cloned tags in a reliable way from incomplete rfid traces," in *RFID, 2009 IEEE International Conference on*, pp. 257 –264, april 2009.
10. J. Cashion and M. Bassiouni, "Robust and low-cost solution for preventing side-jacking attacks in wireless networks using a rolling code," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*, Q2SWinet '11, (New York, NY, USA), pp. 21–26, ACM, 2011.
11. B. Belcher, M. El-Said, and G. Nezlek, "Lightweight rfid authentication protocol: An experimental study," in *Information Technology Interfaces, 2008. ITI 2008. 30th International Conference on*, pp. 583 –588, june 2008.
12. H. Daou, A. Kayssi, and A. Chehab, "Rfid security protocols," in *Innovations in Information Technology, 2008. IIT 2008. International Conference on*, pp. 593 –597, dec. 2008.
13. T. Dimitriou, "A lightweight rfid protocol to protect against traceability and cloning attacks," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pp. 59 – 66, sept. 2005.
14. B. Škorić, "Lecture notes," in *Physical aspects of digital security*, (Eindhoven, NL), pp. 43 –64, TU/e, 2012.