An Overview of RFID Security and Privacy threats

Maxim Kharlamov

mkha130@ec.auckland.ac.nz

The University of Auckland

October 2007

Abstract

Radio Frequency Identification (RFID) technology is quickly deploying all over the world. Recently approved EPC Gen 2 international standard for RFID is going to become ubiquitous. It addresses many privacy and security issues of the previously used EPC Gen 1 standard. This paper will provide an overview and evaluation of how those problems are addressed in the recent standard.

1 Introduction

RFID technology has been used in a wide variety of applications for many years for now. Perhaps, its main application is Electronic Product Code (EPC): few years ago, when RFID tags became standardised and cheap enough, they have started to being widely used as a good alternative for traditional bar codes. It is very likely that in several years they will become ubiquitous. This process, however, raises different privacy and security risks.

1.1 Paper structure

Second section of this paper provides some essential background on RFID technology and EPC Gen 2 standard.

Third section gives a classification of the RFID security and privacy problems. This classification is built upon Garfinkel et al [3] and Ranasinghe and Cole [1] papers. Security issues taxonomy is mainly based on Ranasinghe and Cole [1] paper, since Garfinkel, Juels and Pappu in [3] did not give a clear security threats classification. The situation with privacy is vice-versa: it is better described in Garfinkel et al paper [3], therefore privacy threats list is based on [3].

Forth section provides an overview and discussion of how and to what degree aforementioned issues are addressed in EPC Gen 2 standard. This section is based upon Razaq el al [2], Xiao et al [4] and Juels [5] papers.

2 Background

There are many different and incompatible RFID standards. The main reason for it is that RFID technology has a wide variety of applications and different applications impose different requirements. However, the main principles of this technology remain the same.

2.1 RFID technology basics

RFID abbreviation stands for Radio Frequency Identification. It involves two main components: a reader (also called interrogator) and a tag (also known as transponder). A tag consists of an antenna and a chip. When a reader transmits a radio signal, electricity is induced in tag's antenna. This electricity powers a chip (in case of passive RFID tags, which is the most common) and the chip responds with its unique number (ID). Reading distance varies from several centimetres to several meters.

RFID technology is used in different applications such as: tracking animals, collecting road tolls, in security systems, passports, supply chains, stores, military, etc. Probably the main application is using RFID transponders in supply chains and in stores for tagging goods, so RFID tags are used as Electronic Product Code (EPC) and sometimes called EPC tags. Those tags are passive and they are cheap. This paper focuses on EPC tags used in stores.

2.2 EPC Gen 2 standard

The latest standard for EPC tags is EPC Class-1 Generation-2 UHF-RFID (short name EPC Gen 2) that has been recently approved by the International Organization for Standardization (ISO) as ISO-18600C. It offers many improvements over the earlier standard and addresses some security and privacy issues. In this paper EPC Gen 2 name is preferred over ISO-18600C because the former is well-known.

3 Security and privacy threats

3.1 Security model

According to [1], in terms of security, there are the following participants of the RFID communication:

1. Authorized/unauthorized reader. Authorized reader — a reader that is "allowed" to query a tag, for instance, an in-store reader that is registered in store's RFID system database.

2. Legitimate/fraudulent tag. Legitimate tag — similar to authorized reader, it is a tag that is registered in store's RFID system database and intended to be read by an authorized reader. Fraudulent tag is a tag that is non-legitimate.

3. Cloned tag — an identical copy of a legitimate tag.

This author thinks that this classification is incomplete and it is needed to add an object (an item without a tag or with a deactivated tag) and a tagged object (an object with an attached and functioning EPC transponder) to this list. The main reason for it is the presence of some attacks involving an object with an attached tag, not only a tag itself (see section 3.3, for example).

Communication channel in [1] is divided into three channels: powering channel (radio carrier that powers a tag), forward channel for transmitting reader's messages to a tag and backward channel for transmitting tag's responses back to a reader. The other mentioned in [1] channel is physical. This author thinks that this abstraction is unnecessary and could be omitted. The reason is that all mentioned entities (including channels) are actually physical and physical channel could be used to compromise not only security of a tag (as was stated in [1]), but also security of an authorized reader; even eavesdropping on communication channels is still are physical acts. So, there is no point in adding physical channel connected to every item in the following scheme (taken from [1] but modified, see Figure 1).

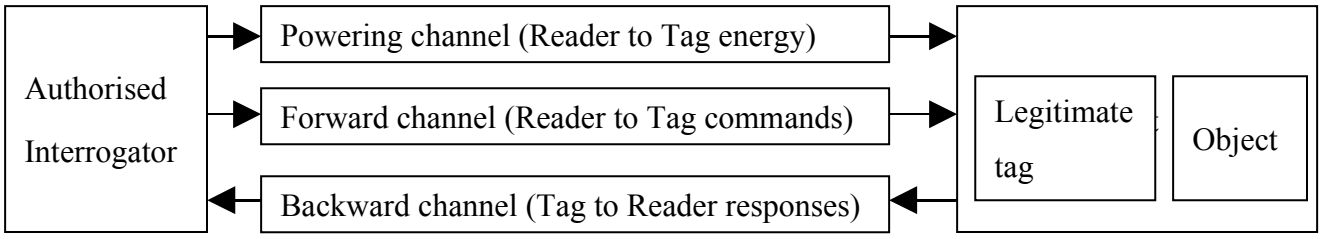

Fig. 1. Security model.

3.2 System model

The model of an in-store EPC system, which is considered in this paper, is shown on Figure 2.

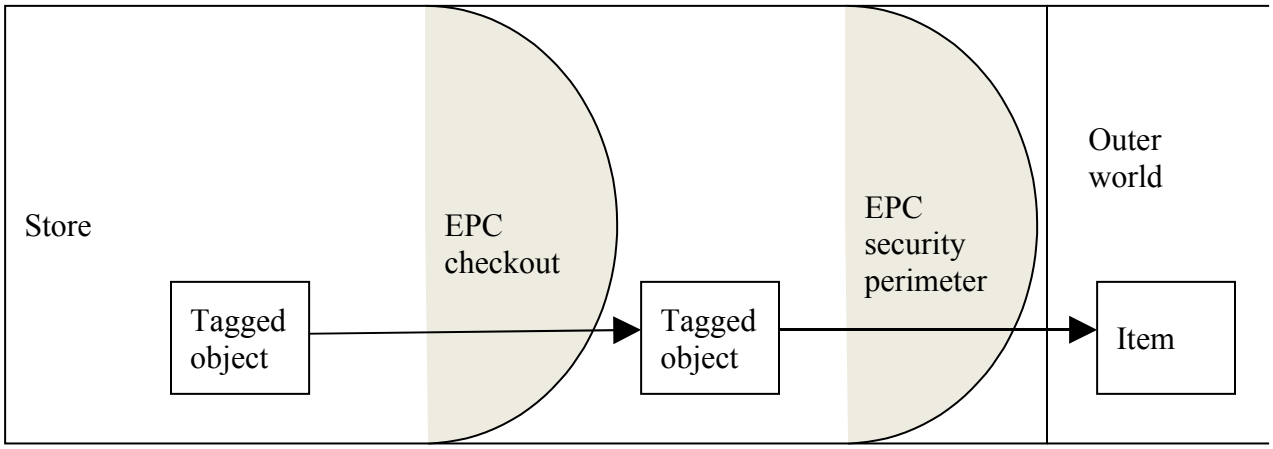

Fig. 2. In-store EPC system.

Goods in a store are tagged objects (objects with attached RFID tags). The presence of checkout and security perimeter is optional — neither of them could be present and it would mean that goods are tagged in order to simplify inventory, for instance. Checkout zone performs a function of automated or semi-automated calculation of the sum of purchase based on the information read from tags. Security zone provides security control that is especially useful if there is no EPC checkout, for example, checkout is based on barcodes. Even if both zones are present, security control could double check that all tagged objects passed through checkout are paid. Another possible function of security zone is deactivating passing tags. Physically those perimeters could be combined, but for purpose of clarity this author divided them. So, when passing checkout and security perimeters, EPC tags could be used for two purposes: identification (including price calculation) and/or security.

When a tagged object passes checkout it remains tagged. When it passes security zone, there are two options: it could remain tagged or the tag could be detached/deactivated. Thus, an item in the outer world could be either tagged or not.

3.3 Security threats

According to [1] there are the following security threats:

1. Passive/active eavesdropping;

2. Cloning;
3. Man-in-the-Middle;
4. Denial of Service (DoS);
5. Physical threat.

Passive eavesdropping is a threat of unauthorized reading of information from all three communication channels: power, forward and backward. In the case of in-store EPC the main threat is that competitors are able to collect information about goods which are processed through checkout or security zones and eventually figure out: customers' preferences, frequency of transactions, supply chain information, prices, earnings, etc. Ability to gather such information is also a threat for customers' privacy.

Active eavesdropping involves unauthorized reader sending signals in power and forward channel and collecting backward channel information from surrounding legitimate tags. It is a considerable threat. Active eavesdropping is a main source of all privacy issues. It also allows rivals not only to collect the same information as from passive eavesdropping, but also to perform covert inventory of stores and warehouses.

Passive and active eavesdropping often act as a preparation part for other attacks.

Cloning usually involves eavesdropping (either passively or actively) of a legitimate tag in order to obtain its ID and creating cloned tag using some tag-emulating device. Cloning threat is extremely dangerous in the case of security systems; fortunately, cloning it is not so useful for EPC tags. It is possible, though, to imagine the following scenario: somebody has a tagged knife, an adversary clones the tag and commits crime having this cloned tag within a scope of an RFID reader. As a result of it, an innocent person could be arrested.

Man-in-the-Middle threat is a little bit vague. Ranasinghe and Cole in [1] do not give an explanation of this threat; fortunately there is some explanation in [4]. It looks like passive and active eavesdropping are sub-threats of this threat. However, this author agrees with the decision to keep those threats separated and thinks that man-in-the-middle is a threat of various attacks which include not only eavesdropping but also intercepting into communication channels, changing information "on the fly". One example is power analysis attack, described in section 4.3.5.

Denial of Service is a considerable threat for businesses. DoS attacks could be devastating and very expensive for victims. There are various ways of implementing such attacks. “White noise” generators can paralyze a store’s functioning; blocker tags, well described in [3] can do the same. There are also some other attacks resulting in DoS, one of them is mentioned in [1]: screening a tag using metallic shield. Other possible attacks are in Xiao et al [4]: destroying a tag (hitting it, exposing to microwaves, etc.) and simply detaching a tag from an object and throwing it away. The latter attack is not always possible, though — some tags are not detachable, embodied in objects. DoS threat of EPC tags can be easily exploited by shoplifters in order to avoid detection when passing a security perimeter or even by usual customers to avoid paying for some of their goods during checkout (under certain circumstances, if checkout is automated enough).

Another interesting family of attacks was not mentioned in any paper. These attacks are caused by the fact that a legitimate tag could be not only detached from a tagged object but also attached to another object (and not necessarily to goods). It is possible to exchange RFID tags of two objects in order to decrease the payment sum. It is also possible to attach several tags to one object — as a bad joke, in the case of automated checkout some other client could pay more. It is possible to attach tags virtually everywhere, causing wrong payment sums calculation and/or false security alarms.

Physical threat — EPC tags are low-cost, therefore they are not tamper proof and vulnerable to various physical attacks. “The majority of physical attacks possible on devices in general are either non-invasive attacks (timing analysis, power analysis, analysis of certain glitches, radio finger printing, and exploitation of data remanence) or they may be invasive attacks (microprobing, Focus Ion Beam editing, or altering information stored in memory using a laser cutter microscopes)” [1]. The author of this paper thinks that non-invasive physical attacks should be classified as either eavesdropping or man-in-the-middle and physical threat should be narrowed down to invasive threat, but for completeness it should include invasive attacks also on authorized interrogators. As it was mentioned in section 3.1 all attacks could be classified as physical therefore physical threat creates clashes between categories: why, for example, power analysis is a physical threat? Why it is not man-in-the-middle attack? This paper will use invasion threat instead of physical threat.

Invasion attacks are highly unlikely to be seen in stores due to their relative complexity.

Ranasinghe and Cole in [1] also mentioned communication layer weaknesses threat that involves reading and writing arbitrary data into all three communication channels. It is not clear why did they

do that, because this threat is a part of eavesdropping/man-in-the-middle threat. Thus, this threat is redundant and will not be included in the list.

3.4 Privacy threats

In this paper the term “privacy” is used as a synonym of “personal privacy” (not a wider meaning, including privacy of in-store data, for instance). Personal privacy threats mainly arise from the fact that tagged objects could be brought to the outer world with functioning tags, if they were not deactivated or detached in security zone (see Figure 2). Those tagged objects could be then actively eavesdropped breaching privacy. It does not look like other security threats (cloning, man-in-the middle, DoS and invasion) can affect people’s privacy, even though cloning could be used to compromise someone’s reputation (like in example with a knife in section 3.3).

A very extensive classification of privacy threats can be found in [3]:

1. Action — monitoring clients’ behaviour inside stores;
2. Association — tag’s unique ID is associated with a consumer;
3. Location — the associated ID could be used to track a person;
4. Constellation — it is a set of tags around a person that could be used to spy on this person even without knowing person’s identity;
5. Preference — constellations allow revealing people’s preferences and it is also a value threat because sometimes even goods’ prices could be revealed to an adversary;
6. Transactions — tracking transactions between constellations;
7. Breadcrumb — tagged object is still associated with a particular person even after he/she gets rid of it.

Unfortunately, this classification seems to be too extensive. Action threat is just a combination of all other privacy threats applied to the clients in store. An example from [3] “Some manufacturers of “smart shelves”, for example, have suggested that the sudden disappearance of tags corresponding to several high-value objects might indicate that a person plans to shoplift” means shelf (constellation) suddenly loses goods (transaction) which are high-valued (preference/value). The only weak point here is that constellation is around a shelf, not a human, but that is quite acceptable for stores. Consequently, action threat is eliminated.

4 EPC Gen 2 security and privacy improvements

EPC Gen 2 tags offer two main security enhancements over the previous (EPC Gen 1) standard: better protected kill command and new access command. There are two types of EPC Gen 2 tags: basic and enhanced. Both types, as long as the commands will be discussed in the following two sections.

4.1 Basic tags and kill command

“Basic EPC tags have only one security feature … the privacy-enhancing kill command. When an EPC tag receives this command, it “self-destructs”, which is to say that it renders itself completely and permanently inoperable. To protect against accidental or malicious killing of tags, the kill command only takes effect when accompanied by a valid PIN. In the EPCglobal standard, the kill PIN is 32 bits in length.” [5] (EPC Gen 2 standard is called EPCglobal in [5]).

It is not very precise explanation, but from BasicTagAuth algorithm description presented in [5] it is possible to figure out the following steps in communication:

1. An interrogator sends a signal;
2. A tag responds with its ID;
3. The interrogator looks up its database for a 32-bit kill PIN corresponding to this ID;
4. The interrogator issues kill command with the PIN;
5. The tag checks whether it is correct PIN or not. If the PIN is correct, the tag stops functioning.

4.2 Enhanced tags and access command

In addition to kill command, enhanced EPC tags support access command, which is used to switch a tag to a secure mode. The tag generates 16-bit random number, uses it to scramble further communication and via this secure channel allows access to additional memory of the tag which could contain product description, price, etc.

From both [2] and [5] papers the following communication scheme was figured out:

1. An interrogator sends a signal;
2. A tag responds with its ID;
3. The interrogator looks up its database for a 32-bit access PIN corresponding to this ID;
4. The interrogator issues access command with the PIN;
5. The tag checks whether it is correct PIN or not. If the PIN is correct, the tag generates random 16 bit encryption key and sends it to the reader;
6. This key is used to encrypt further communication.

The most important part is the fifth step and here are two supporting citations for it:

"Tags will generate and use a 16-bit random or pseudo-random number generator (RNG) throughout the communication link session." [2].

"…tags transmit random pads (bit-strings) to readers. Readers use these pads effectively to encrypt sensitive data…" [5].

Let us see how those security features affect privacy and security.

4.3 Security

4.3.1 Passive eavesdropping

Basic EPC tags have no protection from this attack. Sensitive data in enhanced EPC tags seems to be more protected because of the access command, but it is easy to see that first steps of the communication are not encrypted. In particular, in step 5 the encryption key is sent in plaintext and can be sniffed by an eavesdropper. Used cryptography scheme is symmetric, in order to be secure it must have a secure channel to transmit the encryption key, but there is no such a channel, so the transponder on step 5 have no choice — it transmits the key openly. There are two problems for an attacker who wants to defeat access security: smarter sniffing devices should be used and they should be used from closer distance. The latter was explained in [5]: a tag has very little power to answer while a reader has plenty of it, so it is harder to eavesdrop on backward channel then on forward channel.

Juels in [5] agrees that encryption scheme is weak: "…an adversary capable of full eavesdropping on the communications between the reader and tag can easily harvest the correct PINs for a tag."

It is strange that Razaq et al in [2] said “Gen 2 provides a good mechanism for securing the data communication between the tag and reader.”

4.3.2 Active eavesdropping

EPC tags are still promiscuous — they show their IDs to any interrogator, since they have no mechanisms to authenticate/authorize interrogators without revealing their IDs. On the other hand, sensitive data in enhanced EPC tags cannot be obtained using active eavesdropping due to the fact that it is protected by 32 bit PIN (and it is too long to brute force 32 bit number over a slow radio connection).

4.3.3 Cloning

Both active and passive eavesdropping can be easily used to clone basic EPC tags. The security improvement of enhanced EPC tags is that if somebody wants to clone such a tag together with the protected information, passive eavesdropping should be used, because the sensitive data is protected by 32 bit access PIN.

4.3.4 Man-in-the-Middle

The situation is pretty the same as with passive eavesdropping. Man-in-the-middle attacks sometimes are harder to implement against enhanced EPC tags.

4.3.5 DoS and Invasion

There is no specific protection from DoS or invasion attacks in EPC Gen 2 standard — those tags are vulnerable to all such attacks. Kill command adds an additional attack: unauthorized killing of legitimate tags. That was in the earlier EPC standard where kill PIN was only 8 bit length vulnerable to brute force attacks. Now the PIN is 32 bits and it should not be vulnerable, but Xiao et al in [4] reported: “Power analysis is a form of side-channel attack, which intends to crack passwords through analyzing the changes of power consumption of a device. It has been proven that the power consumption patterns are different when the tag received correct and incorrect password bits. Professor Adi Shamir demonstrated the ability to use a password to kill a tag during the RSA Conference 2006.” So, in this attack power analysis (man-in-the middle) attack was used to crack kill PIN, thus it was simultaneously a DoS attack. Interestingly, if power analysis attack was able to break 32 bit kill PIN, then there is a good probability that it is able to break 32 bit access PIN also. That could open a possibility of combined attack: first reveal access PIN using power analysis and then ask for protected data using this PIN and active eavesdropping attack.

4.4 Privacy

As it was mentioned in section 3.4 the main cause of privacy threats is the presence of tagged objects outside stores. Those tagged objects could be actively eavesdropped (see section 4.3.2), but enhanced EPC tags offer some kind of protection: they will not (hopefully) release protected data. In terms of privacy protected data does not matter much, but it could make profiling/value attacks harder to perform. So, it could be considered as a small improvement.

Kill command is intended to solve the privacy problem. Truly, if tags are killed in security zone of a store their IDs cannot be read anymore, so there is no association and constellation threat and, consequently, no other threats. Kill command with short PIN exists in the previous standard and in terms of privacy longer kill PIN is meaningless.

There are some open questions about kill command. First, how a customer can be sure that tags were actually killed/detached? Usual customers do not have special equipment for it. Next, what if killing tags is unwanted (this problem was mentioned in [3]). The simple example is a discount card that clearly has to survive security/checkout perimeters.

If we consider privacy threats inside stores, then all threats are in place, but this is not as dangerous as outside threats. Moreover, it is impossible to fully overcome in-store threats if checkout/security perimeters are used: tags will be read at least once in one of checkout/security zones (otherwise there is no point in implementing EPC system inside a store). Gathered information is enough at least to raise preference/value threat, thus this threat is inevitable.

5 Conclusion

EPC Gen 2 enhanced tags offer some security improvements resulting in the fact that some security attacks are now harder to implement. Overall security is not improved much, unfortunately.

In terms of privacy the situation is even worse — there is only one minor improvement.

It looks like EPC standards should come a long way to reach acceptable security and privacy levels.

References

[1] D.C. Ranasinghe, P.H. Cole, “Confronting Security and Privacy Threats in Modern RFID Systems”, *Fortieth Asilomar Conference on Signals, Systems and Computers (ACSSC '06)*, pp. 2058-2064, October-November 2006.

[2] A. Razaq, W.T. Luk, L.M. Cheng, “Privacy and Security Problems in RFID”, *IEEE International Workshop on Anti-counterfeiting, Security, Identification*, pp. 402-405, 16-18 April 2007.

[3] S. Garfinkel, A. Juels, R. Pappu, “RFID Privacy: An Overview of Problems and Proposed Solutions”, *IEEE Security & Privacy* 3:3, 34-43, 2005.

[4] Q. Xiao, C. Boulet, T. Gibbons, “RFID Security Issues in Military Supply Chains”, *The Second International Conference on Availability, Reliability and Security (ARES)*, pp. 599-605, April 2007.

[5] A. Juels, “Strengthening EPC tags against cloning”, *Proceedings of the 4th ACM workshop on Wireless security*, pp. 67-76, 2005.