Seminar: Communication Infrastructure, RFID Security

Thomas Thrainer, 0356015, Thomas.Thrainer@students.jku.at

Johannes Kepler university Linz
FIM — Institut für Informationsverarbeitung und Mikroprozessortechnik

Abstract. RFID technology is becoming more and more widespread. Everybody presumably possesses already some form of RFID enabled devices. Such devices unlock cars, carry out contactless paying task in parking lots, open doors, protect clothing in retail shops or help keeping track of goods in supply chains. And that's only the tip of the iceberg, because more and more companies are discovering the advantages of RFID enabled processes.
But voices asking for customer privacy and data protection are getting louder. And there are also a number of possible attacks against companies using RFID in their supply chain, so the need for security in RFID solutions is evolving. But providing security on such constrained environments like RFID tags, which are only allowed to cost five $US-cents, is a very difficult task. This paper introduces some security issues concerning RFID technology and then takes a look at solutions which are able to provide basic security.

1 Introduction

Radio frequency identification tags, RFID tags, are generally small devices which can hold a limited amount of data. This data can be read by RFID readers at distances, depending on the type of tag, ranging from several centimetres up to several meters. As the name RFID implies, the data stored in those tags is usually used to identify entities like products, humans or keys.

RFID tags are very low cost, basic passive tags are aimed to cost as little as 5 US cents. This price combined with the opportunities offered by the ability to scan and track individual products rather than only product categories wirelessly makes the RFID technology very attractive to companies. The U.S. Department of Defence and Wal-Mart require, for example, that shipments of goods are identifiable by RFID. Likewise, in Europe the Metro Group has teamed with SAP, Intel and IBM to from the Future Store Initiative [1]. These efforts will make RFID tags pervasive in our lives. Consequently, security and privacy issues concerning RFID technology will get more important and will gain more public attraction.

But RFID tags are not only used in supply chain management. There are numerous other uses, and it is likely that almost everybody already uses RFID technology in his daily life. Automobile immobilizers, for example, work with a

RFID chip integrated in the car key. Also, payment systems or proximity cards which are used to unlock doors are base on RFID technology [2]. These use cases highlight clearly the need for security and authentication mechanisms built into RFID tags.

2 Threats and vulnerabilities

When regarding security in conjunction with RFID technology, it's always necessary to differentiate between the different areas where RFID tags are used. It's obvious that security is a major concern when looking at payment systems or automobile immobilizers. But there are much more threats, of which one would not think in the first place. Figure 1 provides an overview about various threats RFID is facing during the stages of supply chains [2], but other types of usage might have other specific security issues.

Those security concerns become more and more important as RFID becomes more widespread. Following this evolution, also RFID readers will get available more easily. This will enable potential attackers to get hold of attacking equipment easily, and thus creating a much higher attack potential than nowadays.

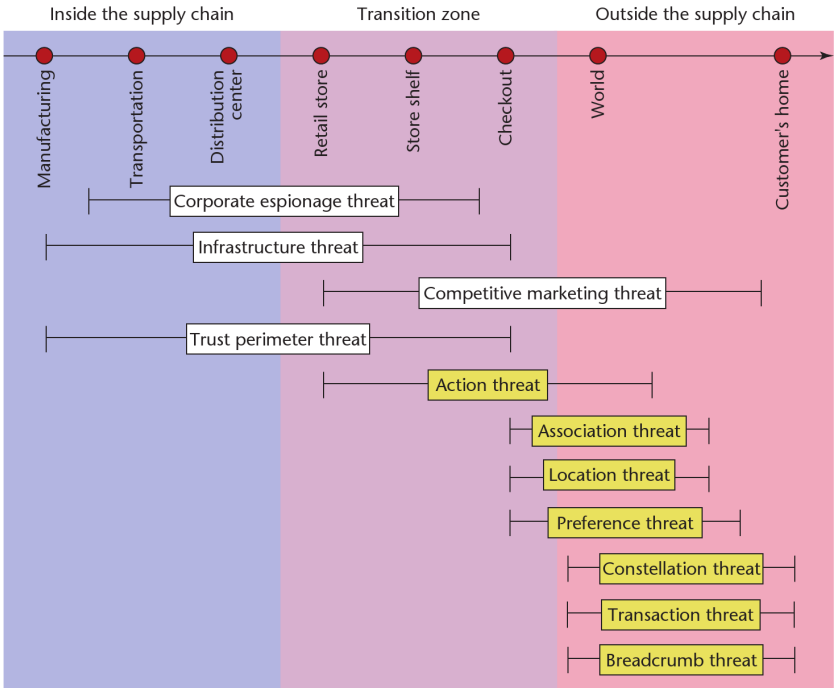

Fig. 1. Overview over threats in different stages of the supply chain [2]

2.1 Examples

Due to the high number of different threats and attack potentials, we only focus on some aspects of RFID security. Therefore we give examples of potential attacks and describe in which usage areas of RFID they apply. In section 3 on page 5 different countermeasures are discussed.

Espionage Espionage mainly affects suppliers but can be conducted in many stages of the supply chain. Attackers can scan RFID-tagged goods as they are transported, unloaded or even sold in shops in order to get in deep knowledge about the movements of merchandise. Performing regular scans of shelves in shops, for example, can give attackers knowledge about turn-over rates of products. They also could track the way products are shipped, or the delay it takes to bring good from the supplier to the retail shop. Due to the fact that each RFID-tagged product has its own unique ID and that they freely publish this information it is easy for attackers to build databases of product movement etc.

This type of knowledge can be very valueable for competitors and therefore it is very well thinkable that attackers are paid for gathering such information for them [2].

Privacy Numerous authors, e.g. [3,2,4,5], have pointed out that privacy will be an important factor for the acceptance of RFID technology on the large scale. And indeed, privacy concerns have already forced a big company, namely Benetton, to stop their RFID engagement because of customer boycots [4].

RFID tags without further security measures are readable by every RFID reader. The consumers privacy could therefore be compromised in various ways. An attacker could inventory a target as it moves by, and could find out which products he just bought, or if he carries any valuables which are worth stealing. This issue becomes even more frightened if one considers the (abandoned) plans of the European Central Bank to embed RFID tags in banknotes [4]. Another potential worst case scenario are customers, who just picked up their medicaments at pharmacies and want to keep their medical issues privately.

Such unauthorised reading of tag information could also enable companies to create profiles of their customers buying behaviour. Such profiles or the simple knowledge of products the customer currently possesses would allow customised marketing, and thus privacy limitations. Figure 2 on the following page illustrates this privacy problem.

According to the taxonomy given in figure 1 this problem is clearly situated outside of the supply chain in the world or even in the customers home.

Traceability Traceability is another aspect concerning privacy in conjunction with RFID technology. Basically, persons who carry RFID tags can be identified based on those tags. This enables attackers to trace a victims way and to create profiles of, for example, movements in a shopping mall.

Fig. 2. The consumer privacy problem [4]

Traceability is a special threat as it is difficult to mitigate. It was shown that even slight differences in the physical layer of RFID communications can be used to differentiate different RFID tags and thus to trace tags [5].

Cloning, Spoofing and Injection These three words all describe the same attack: Reading a RFID tag, storing its data and configuring another tag (or another device) to emit the exactly same data when interrogated. With this ability to copy or "clone" tags, a variety of attacks are possible. These attacks affect mainly the supply chain or the transit from the producer to the end user, but much less the security of the customer of RFID-enabled goods [2].

Being able to copy RFID tags, thieves could easily steal merchandise which is secured by RFID technology. They can quickly scan, for example, a box full of valuable goods to get the data of all tags included. Then, they can manufacture a copy of this box and include clones of the scanned tags. Finally, the two boxes can be swapped and the box containing valueables can be stolen by using some sort of physical blocking. Security infrastructure which relies on included RFID tags could not detect the theft.

Other attacks could have the supply chain infrastructure as target. If attackers manage to clone a RFID tag, the authorised reader is no longer able to tell which tag is the original one, and which one is the copy. Such cases could irritate the supply chain infrastructure and cause costs to resolve the problem manually.

But cloning respectively spoofing attacks are not limited to RFID tags used as pricing tags. Automobile immobiliser tags should not be cloneable, for example. Another threat is in conjunction with proximity cards for unlocking doors. Attackers should not be able to simply read the data transmitted during a suc-

cessfull unlock transaction and replay or spoof it again to get access. Similarly, contactless paying systems as used for e.g. parking lots should be protected against spoofing or replaying attacks.

3 Mitigations

There exist numerous different RFID tags for various applications, each with different feature sets, packaging sizes and costs. Obviously, very basic low cost tags don't have as elaborate security mechanisms built in as more expensive ones. Also, a big difference exists, security-wise, between active and passive RFID tags. The former ones get their power from built-in batteries whereas the latter ones rely on a reader to supply them with power. Active tags can have, for example, an own clock and therefore a notion of time, but passive tags only "live" when they are interrogated.

These big differences of available ressources result in numerous security approaches for RFID tags. In the following sections we describe some of those. The complexity and thus the ressources needed are roughly sorted in increasing order.

3.1 Physical approaches

The most simple approach to physically ensure security is to remove or destroy RFID tags completely when they are no longer needed. This is feasible for example if the tags are placed in adhesive pricing tags. They can simply be removed at the place of sale to ensure customer privacy. The downside of this approach is that no after sales benefits of RFID tags are possible, and that physically removing tags is cumbersome [4].

Another way of physically securing the customers privacy is to provide them with shopping bags, which disrupt RFID tags and readers. This could be done by embedding radio wave disrupting material in the bag, or by including a so called blocker tag. Blocker tags are described in the next section.

It is also possible to consider physical quantities for security applications. If we assume that attackers are generally far away from the target but authorised readers are much closer, then we could use the physical distance bedween reader and tag as measurement of trust. This assumption is generally correct because most attackers want to stay hidden and thus far away of the victim, but authorised readers as in points of sale or in customers fridges are much closer to the tags to read.

Kenneth P. Fishkin showed in [6,3] different methods to roughly measure the distance bedween reader and tag. The easiest measurement is the signal to noise ration which decreases as the distance increases. He also pointed out different applications for the estimated distance. Tags could assign different levels of trust to readers at different distances. They could only reveal very basic information, like the type of product, to far away readers. Readers at a smaller distance could also read the tags unique identification.

All these physical approaches aim to protect customer privacy and are targeted to secure tags used as pricing tags. They do not protect against attacks occurring within the supply chain. Event the use of physical quantities as measurement of trust can't provide security in supply chain, assuming that an attacker, who manages to get into the supply chain can also get as close to the products as he wants. The physical approaches don't provide security in other usage areas of RFID tags, like payment systems, automobile immobilizers or proximity cards.

3.2 Kill flags and blocker tags

Kill flags and blocker tags are both used to ensure customer privacy. Kill flags can only be used in scenarios, where customers don't need the RFID tag, while blocker tags provide a more elaborate control over purchased tags [7].

The idea of kill flags is, that RFID tags have the built-in opportunity to "kill" themselves. When they receive a special command, optionally in conjunction with a simple hard-wired password, they set a kill flag and will never again respond to any RFID reader. It would be possible to send this kill command during the checkout process in retail stores, effectively protecting the customer because he would never get any functional RFID tags.

There are a number of drawbacks of this approach however. On the one side, attackers could seriously interrupt workflows in the supply chain by simply "mass-killing" RFID tags of products. As tags on products should be very cheap, no special security features will be built into these tags. On the other side, killing tags destroys all the after-sales benefit for the user. Such benefits would include fridges knowing what they contain, micro-wave food which tells the micro-wave how to cook it or easier handling in case of reclamations.

Ari Juel et al. introduced the concept of selective blocker tags in [7]. This blocker tag effectively hinders RFID readers from reading tags with a certain bit prefix in their ID. As company codes usually are a prefix of the ID, blocker tags could for example just block interrogation of all tags on products from a certain company. Another usage could be in conjunction with a special private bit. Similarly to kill flags RFID tags could be told to switch the first bit of their ID to one during the checkout process, meaning that this tag is now in the private zone (given that public tags always have a zero as first bit of their ID). As long as the customer carries a blocker tag which blocks all reads in this private zone, no reader can access the tags after the checkout process. At home, however, the customer could disable the blocker tag and the full benefits would be accessible again.

On the technical side, blocker tags are very simple devices. They are basically normal RFID tags which do not comply completely with the standard interrogation protocol for RFID tags. The main idea is that they pretend to have all ID's starting with a given prefix. So whenever a reader tries to find all active tags with this prefix, the blocker tag responds. Therefore, the reader is no longer able to actually find the active tags.

There are, however, several issues with this approach. Attackers could abuse blocker tags to hinder legitimate readers to successfully scan shopping cards, for example. But there also exist problems with the usability of this approach, because customers would have to be aware of the tags they possess, and they would also have to have some means of configuring, enabling or disabling of their blocker tags.

3.3 Minimalistic cryptography

RFID tags aimed for e.g. product tags strive to be very low cost and have therefore little resources for cryptographic functionality. Those space and cost constraints prevent manufacturers to include standard cryptographic methods like asymmetric or even symmetric encryption. For this reason, different publications, e.g. [8,9,10], have founded the notion of *minimalistic cryptography* to deal with limited resources and to provide a reasonable amount of security. In order to accomplish this goal, a number of assumptions about the attacker are taken. The attacker cannot, for example, query the tag infinitely or perform an infinite amount of man-in-the-middle attacks [8].

One approach is the use of pseudonyms. Each tag has a set of identification numbers instead of only one identification. The tags emit each time they are interrogated the next pseudonym, starting over with the first when reaching the end of the set. Only readers which know all pseudonyms can make a connection bedween multiple interrogations. One problem is that attackers could simply read the tag several times in order to get all pseudonyms. To prevent this, tags can introduce a delay bedween successive reads. Another problem, closely related with the previous one, is that tags only have a limited storage capacity. So only very few pseudonyms can be stored on tags, making them quite insecure. Also, attackers could still read one pseudonym from a tag and perform a cloning attack with this information. To prevent this, Ari Juels proposed a protocol [8] which requires the reader to authenticate with the tag prior to reading any information. This also enables the reader to update, after the successfull communication, the pseudonyms of the tag.

Yong Ki Lee et al. propose a system where the actual identification numbers of tags are never transmitted [10]. Instead, only hash values of keys are sent. These hash values are guaranteed to be unique by the infrastructure, and can therefore be used to get the real key from a database. The reading infrastructure updates the key stored in the tag after each successfull interrogation, again without transmitting the key directly. Instead, the tag gets a value to XOR with the old key and enough information to validate this value. This system requires the tag to be able to store one key, compute a hash value from this key and to update the key with another value using the XOR operation.

A number of other approaches exist which are based on challenge response authentication. Simple challenge response protocols can ensure that either the reader or the tag has to authenticate with the communication partner, whereas more advanced ones require an authentication of both partners. These authentications can prevent cloning or spoofing attacks. As example the HB^+ algorithm

from Ari Juels et al. is given [9], which is based on the observation that RFID tags have computational limitations similar to those of human beings. He therefore re-uses well known protocols for human to computer authentication. It was shown however, that most of these simple challenge response protocols cannot protect against traceability [11].

Minimalistic cryptography can mitigate a whole range of security issues. But as these approaches make several assumptions about the attacker, one has to be carefull about the use case where to use minimalistic cryptography in. For proximity cards used as access control tokens, for example, it could be possible for an attacker to make as many man-in-the-middle attacks as he likes, if he manages to install a malicious reader next to the secured door. Also, the approaches described above only provide secure authentication but no secure communication. A malicious reader could thus still read all information transmitted as soon as an authorised reader establishes a connection.

4 Conclusion

RFID security is a very difficult task, due to the highly constrained environment. And there is no single answer to all problems of RFID security. Depending on the area where RFID tags are used, different problems are more or less important. This leads to solutions which are geared towards the specific problem and which try to find an optimal balance between the very specific needs.

On very low cost product tags, for example, the need for security is less important than the need for very cheap tags. Automobile immobilizers, on the other hand, will have a much bigger need for strong security. And even other use-cases, like animal tagging, virtually do not have any need for security at all. So there is no "one" solution for security problems in RFID technology, but there is always the need to investigate further and to find the best solution for every case. This paper only gave a very brief overview over a couple of approaches, but there exist much more for other applications.

References

1. Niederman, F., Mathieu, R.G., Morley, R., Kwon, I.W.: Examining rfid applications in supply chain management. In: Communications of the ACM. Volume 50., New York, NY, USA, ACM (2007) 92–101
2. Garfinkel, S.L., Juels, A., Pappu, R.: Rfid privacy: An overview of problems and proposed solutions. In: IEEE Security and Privacy. Volume 3., Piscataway, NJ, USA, IEEE Educational Activities Department (2005) 34–43
3. Fishkin, K.P., Roy, S., Jiang, B.: Some methods for privacy in rfid communication. In: Security in Ad-hoc and Sensor Networks. Volume 3313 of Lecture Notes in Computer Science., Berlin/Heidelberg, Germany, Springer (January 2005) 42–53
4. Juels, A.: Rfid security and privacy: A research survey. In: IEEE journal on selected areas in communications. Volume 24., IEEE Institute of Electrical and Electronics (February 2006) 381–394

5. Avoine, G., Oechslin, P.: Rfid traceability: A multilayer problem. In Patrick, A., Yung, M., eds.: Financial Cryptography – FC'05. Volume 3570 of Lecture Notes in Computer Science., Springer-Verlag (2005) 125–140
6. Fishkin, K.P., Roy, S.: Enhancing rfid privacy via antenna energy analysis. Technical Report IRS-TR-03-012, Intel Research, Seattle (2003)
7. Juels, A., Rivest, R.L., Szydlo, M.: The blocker tag: selective blocking of rfid tags for consumer privacy. In: CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, New York, NY, USA, ACM (2003) 103–111
8. Juels, A.: Minimalist cryptography for low-cost rfid tags. In: The Fourth International Conference on Security in Communication Networks – SCN 2004. Volume 3352 of Lecture Notes in Computer Science., Springer-Verlag (2004)
9. Juels, A., Weis, S.A.: Authenticating pervasive devices with human protocols. In: Advances in Cryptology – CRYPTO 2005. Volume 3621 of Lecture Notes in Computer Science., Berlin/Heidelberg, Germany, Springer (August 2005) 293–308
10. Lee, Y.K., Verbauwhede, I.: Secure and low-cost rfid authentication protocols. In: 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN). (November 2005)
11. Avoine, G.: Adversarial model for radio frequency identification. In: Cryptology ePrint Archive. Volume 049. (2005)