Defending in the RFID system against eavestdropping

Tibor Radványi
Institute of Mathematics and Informatics, Eszterhazy Karoly College, Eger, Hungary
radvanyi.tibor@ektf.hu

Abstract— In this article we are going to deal with today's most dynamically improving RFID technology connected to the topic of automatic identification. We are going to introduce the possible attacks, emphasizing the UHF and the HF/NFC frequency ranges. Different defend methods are also going to be mentioned. Analysing the possibilities of defeating eavesdropping will be highlighted as well. The suitable cryptographic algorithms are going to be listed besides the ones which are non-suitable according to the boundaries of the technology. The size of the implemented memory and the persistence or non-persistence of a chip which is able to solve the possible calculation operations in the RFID tag strongly influences this issue. Passive UHF and HF/NFC tags do not contain a controller with calculation capacity, only a memory chip to store data. In this case defense means a reasonably bigger problem than if we are working with active devices where hardware tools able to serve calculation purposes are available. On the other hand these transponders might be extremely cheaper than the active ones. In the next few years tens of billions of transponders are expected to be installed according to the European Union's "Internet of Things" plan, and most of these transponders are going to be passive tags. This project is going to generate a large demand for using and distributing data that should be protected, in spite of the fact that their protection is not solvable or very hard to solve.

Index Terms— RFID, data security, cryptography, data protection, UHF, HF/NFC

1 Introduction

NOWADAYS, different types of identification systems can be found in a wide range. This is a code- and communication system that identifies people, objects and events. The most up to date and dynamically improving identification method is the RFID. Combined with sensors and positioning systems it can be used efficiently in many ways. It is used in manufacturing, logistics, pharmaceutical and military industries and in lot of other fields. It allows us to keep track of vehicular-, aerial-, water transport, and check the quality. The technology is used in modern passports, digital identifiers and the most up to date payment methods due to its effectiveness in identifying and safety. [1][2]

A product is exposed to countless dangers as it gets to the consumer from the manufacturer. It goes to a temporary depot from the factory. It is transported from the factory to the wholesaler then to a retail company and finally to the department stores. It is a pretty long process in which the products can get lost, exchanged or stolen.

The possibility of paying by mobile phones is still being discussed in Hungary and it would be a huge milestone in development. The users are not aware of its dangers and most of them can not or do not even want to deal with these problems. The manufacturers have to care about safety in order to prevent damage or data theft in these systems. Due to the decreasing cost of production sooner or later the passive RFID system's data storing limit will disappear. The active RFID tags can replace the passive ones because they are safer and do not require special algorithms in order to work on simpler systems.

Finally they realized that the safety and uninterrupted information usage is more important than the efficiency. We also think that the safety of the information is the most important, especially where data encrypting is essential. For example: Banking services should be slow but safe rather than fast. [3][10]

2 Attack through RF interface

One of the most common attack type against RFID systems comes through the RF interface. The RFID systems communicate via radio systems and electromagnetic waves at close and distant ranges as well. Because of this the attackers have the opportunity to attack through the interface since they do not need to access the reader or transponder directly. This kind of attack has a lot of different cases. I am going to write about these in detail in the following paragraph. [11,12,13,14]

An RFID system is considered long range if the distance between two devices is more than 1 meter. Usually UHF (868 or 915 MHz) or microwave frequency (2,5 or 5,8 GHz). If the tag gets out of the reading range of the system, there are two possibilities for interrupting the signal. One of these is that the tag does not get enough power from the antenna for functioning. The other possibility is that the reflected signal is too weak for the reader to sense. To increase the distance the reader's transmission power should also be increased. If we want to keep the efficiency of the reflection at doubled reading range, the reader's performance must be increased to sixteen times as normal. In 2005 a successful attack had been performed with the Yagi-Uda antenna from 21 meters. [4][10]

3 EAVESDROPPING

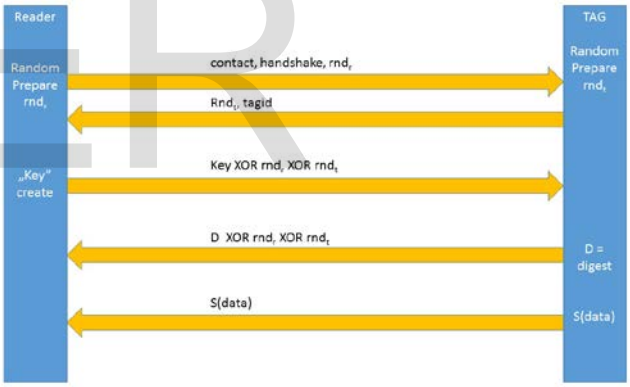
As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap. The eavesdropping of communication occurs between the reader and the transponder. The range of RFID systems varies from a few centimeters (eg.: 13.56 MHz) up to a few meters (eg.: 868 MHz). Finke and Kelter determined that 13.56 MHz inductive coupling systems can be eavesdropped from 3 meters. [4] The receiver can sense unmodulated signals from 100 meters even at a few kHz. Metal object such as fences, aluminum objects or even buildings may distort the signal. What does the success of eavesdropping our devices (reader and transponder) depend on? The number of influential factors is high. [7][8]

- Depends on the characteristics of the RF space. This defines the geometry, structure and output power of the antenna.
- Interfering object between the reader and transponder and the size and location of metal objects are also an important factor.
- It is influenced by the quality, structure and geometry of the attacker's device, and also depends on the power emitted by the reader.
- It is also an important factor that passive or active transponders are used in the RF communication. If the tag is passive, it uses the power generated by the reader, this way the reflected useful information participates in the communication with lower energy usage. In the case of UHF tags (868 MHz – 915 MHz) 1-3 meter. If the tag is active or semi-passive so it has its own power source this range can be increased up to 10-30 meters. In case of active tags the emitted information is easier to catch due to its energy and easier to hide in larger attack areas. The attack area is a space where the attacker sets his eavesdropping device until he can perform a successful attack.

The following attacks may occur during eavesdropping:

- Secret or personal data may get into unauthorized hands. In this case the attack does not effect the communication, and it is almost impossible to detect the attack. Using cryptographic protocols may help defending the data.
- The attacker modifies the eavesdropped data and the false information is transmitted to the reader. This act requires a specific device and it is really hard to perform.
- Another possibility is that the attacker does not modify the data but replaces it. This could happen when the transponder sends a lot of information to the reader, so the communication requires much more time. In these cases of eavesdropping the attacker may get detected and his data blocked. Using control data, cryptographic algorithms and combinations of protocols may help detecting the attacker.
- The "relay attack" is a much more complicated type of eavesdropping and it also requires serious technical preparation. In this case the attacker does not only gather data but also transmits it on another channel. eg.: WIFI – longer range. In the other place the data could get processed by another device eg.: during a purchase. This attack is really hard to block due to the properties of contactless payment methods. For the time being combined with other identifying methods it provides a good possibility. The simplest way is using a pin code but any personal or stationary biometric identification can be used. [15] [16]

It is clear that eavesdropping can be performed really easily sometimes. It holds a lot of possibilities for the attacker and it is really hard to detect and block. In order to protect data, if we can not secure the communication channel, we should make the information difficult to process in case of an attack. Cryptographic protocols provide data protection during information exchange.



1.figure. **reader and transponder communication**

4 SECURITY MEASURES

Encryption is the basic defense method against passive attacks, we use cryptographic protocols to block active attacks. This requires a predefined data exchange process. This way we detect active attacks, and block their harmful consequences.

The published protocols have much in common. [6]. Main steps:

1. The reader transmits a request to the tag.
2. The tag identifies itself to the reader.
3. The reader transmits the data to the background server.
4. The server processes the data based on its database.

- *Author name is currently pursuing masters degree program in electric power engineering in University, Country, PH-01123456789. E-mail: author_name@mail.com*
- *Co-Author name is currently pursuing masters degree program in electric power engineering in University, Country, PH-01123456789. E-mail: author_name@mail.com*
(*This information is optional; change it according to your need.*)

5. The server sends the authentication and the processed data.

The difference between the different levels are the use of cryptographic primitives. [5] The tag hashes the data before transmitting to the reader. The background server decodes the data and processes it using a shared key.

Against eavesdropping we should detail and confirm the processes mentioned in points 1 and 2. It is possible to include the background server in powerful security systems. Thus we have two possibilities. The first is when the cryptographic protocol affects all three layers the transponder the reader and the background server as well. The second one is when we try to force the defense to the communication between the tag and the reader, assuming that the inner data transmission between the reader and the background server is already safe.

Of course the following protocol highly depends on the use of active or passive tags in the communication. The existing requirements are already different and the available computing capacity also shows a huge difference. Take a look at the communication scheme on **figure 1.** As shown we use a XOR function in the encryption which can be easily implemented on hardware level, so there is no difficulty in using it in passive tags. The XOR protocol uses different keys in different directions.

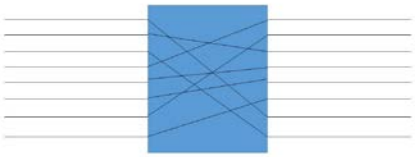
$$R \rightarrow T : x \oplus k1$$
$$T \rightarrow R : x \oplus k2$$

It is a safe solution to choose k1 and k2 randomly in case of every execution. One solution to implement this is generating XOR keys, in which R randomly chooses a new k(i) key depending on the i variable and it executes a XOR encrypting with k(i-1) keys. This way we get the following protocols:

$$R \rightarrow T : a(i) = x(i) \oplus k(i),\ k(i) \quad k(i-1)$$
$$T \rightarrow R : b(i) = x(i) \oplus k(0)$$

where i = 2,3,…a counter, that increases by one with every running. x(i) is the i'th random number and k(0) and k(1) predefined shared keys. k(1), k(2), … sequence does not vary randomly, but their value can not be followed by the attacker. Also an S function appears which requires a little detail. First, consider the so-called P and S boxes. These are the basis of cryptographic algorithms. Their advantage is that they are easy to implement electro-technically. This way they can be integrated to the passive tag's limited set of tools. In case of active tags this is not a problem, because the tag contains intelligence, a programmable processor so the whole AES algorithm is feasible at a relatively low energy input and short time.

In case of passive tags we use the combination of P and S boxes. The P box is a function that creates an 8 bit output from and 8 bit input. A fast and simple electro-technical device, and it's inverse function can be easily generated if we know the P box's assignment rule. It is responsible for mixing the 8 bit and a creating a bit permutation.



2. figure. **A possible P box**

The S box is a device that implements a nonlinear function which creates 4 bit output from 6 bit input. [19] The operation of the S box is described by a table of 4 rows and 16 columns. Each S box has a different table. These tables allow us to encode the S box. Out of the incoming 6 bits the 1'st and 6'th gives the row indexes, while the other 4's decimal equivalent gives the column indexes. This way we get the 4 output bits based on the table cells.

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

3.figure. **a possible S box**

Figure 1. shows the S function, which generates the memory content of the user S(data), and transmits it to the reader. This is a complex function that contains S and P boxes. As we know the used tables of S and P boxes

$$S^{-1}(S(data)) = data$$

Based on this we get back the data stored in the tags. The use of S and P boxes is defined by the reader's key. The reader is a specific computer which has the computing and storage capacity that is required for generating keys and decrypting S(data). The tags are the electronic realizations of S and P boxes. For data control we create a digest from the stored data. The well-known HASH functions are suitable for solving this problem. We implement one of the HASH functions in the tags, eg.: MD5 function. Using this method we are able to check the data after decrypting. This provides extra defense against data modifying, or data insertion attacks.

5 Conclusion

The use of RFID systems is constantly changing today. New technologies appear every day and manufacturers, multinational companies want these to get to the users. The fact that transponders are getting smaller and cheaper also helps them to spread. Thanks to the widespread of RFID systems they can be found in an increasing number of segments, and because of this we have to be more careful about their dangers and vulnerabilities. The above mentioned systems provide a basis for data carried by simpler and cheaper transponders. In addition to perform this we have to change the protocols used by

Class1Gen2 tags, and build in the sections that realize the communication and the S and P boxes.

6 Acknowledgements

This way I would like to thank the Nemzeti kiválóságok program for enabling the continuation of the research.

This research was supported by the European Union and the State of Hungary, co-financed by the European Social Fund in the framework of TÁMOP-4.2.4.A/ 2-11/1-2012-0001 'National Excellence Program'.

References

[1] Dr. Imre Sándor, Kis Zoltán, Molnár László, Pogátsa Attila, Schulcz Róbert, Tóth Gábor – RFID rendszerek vizsgálata felhasználás és technológia szempontjából - http://www.rfid.answare.hu:8080/site/kutatasi-erdmenyeink/radios-megoldasok/2006/rfid-rendszerek-vizsgalata-felhasznalas-es-technologia-szempontjabol.pdf/view.

[2] Klaus Finkezeller – RFID Handbook, Third Edition, 2010

[3] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez Tapiador and Arturo Ribagorda – LMAP: A Real lightweight Mutual Authentication Protocol for Low-cost RFID tags - http://events.iaik.tugraz.at/rfidsec06/program/papers/013%20-%20lightweight%20mutual%20authentication.pdf

[4] Hee-Jin Chae, Daniel J. Yeager, Joshua R. Smith, and Kevin Fu (University of Massachusetts) Maximalist Cryptography and Computation on the WISP UHF RFID Tag 2007

[5] Sindhu Karthikeyan and Mikhail Nesterenko_Kent State University, RFID Security without Extensive Cryptography 2005

[6] M. McLoone and M.J.B. Robshaw (Queen's University, Belfast, U.K.) Public Key Cryptography and RFID Tags 2008

[7] Ernst Haselsteiner, Klemens Breitfuß: Security in Near Field Communication (NFC) Philips SemiconductorsMikronweg 1, 8101 Gratkorn, Austria

[8] Radványi Tibor, Biro Csaba, Király Sándor: RFID tagek elleni támadás és a védekezés lehetőségei, Attack against the RFID tags and possibilities of the defense, Networkshop 2014 Pécs, , ISBN: 978-963-88335-5-6, elektronikus kiadás.

[9] Radványi Tibor, Bíró Csaba: Az adatvédelem helyzete az RFID-ban, . SzamOkt 2013. október 10-13, Nagyszeben (Sibiu, Románia), ISSN 1842-4546 283-289 oldal

[10] Jung-Sik Cho, Sang-Soo Yeo, Sung Kwon Kim: Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value, Computer Communications 34 (2011) 391–397

[11] A. Juels, RFID security and privacy: a research survey, Selected Areas in Communications 24 (2) (2006) 381–394. February.

[12] S.S. Yeo, S.K. Kim, Scalable and flexible privacy protection scheme for RFID systems, European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05 LNCS, 3813, Springer, 2005, pp. 153–163.

[13] S. Weis, S. Sarma, R. Rivest, D. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in: International Conference on Security in Pervasive Computing, March 2003, pp. 201–212

[14] S.A. Sarma, S.E. Weis, D.W. Engels, RFID systems and security and privacy implications, cryptographic hardware and embedded systems – CHES 2002, LNCS, vol. 2523, Springer, 2002. August, pp. 454–469.

[15] S. Yu, K. Ren, W. Lou, A privacy-preserving lightweight authentication protocol for low-cost RFID tags, in: IEEE MILCOM 2007, October 2007, pp. 1–7.

[16] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, T.-C. Chen, An improvement on RFID authentication protocol with privacy protection, in: Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, November 2008, pp. 569–573.

[17] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, Kwangjo Kim (KOMSCO, ICU, WPI Mutual Authentication Protocol for Low-cost RFID 2005

[18] NIST. Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.

[19] Lauren De Meyer, Beg Bilgin, and Bart : Extended Analysis of DES S-boxes, Proceedings of the 34rd Symposium on Information Theory in the Benelux, 30-31 May 2013, Leuven, Belgium (pp. pp. 140-146).