Providing Strong Security and High Privacy in Low-Cost RFID Networks

Mathieu David and Neeli R. Prasad

Center for TeleInFrastruktur (CTIF), Aalborg University,
Niels Jernes Vej 12, 9220 Aalborg Øst, Denmark
{md,np}@es.aau.dk

Abstract. Since the dissemination of Radio Frequency IDentification (RFID) tags is getting larger and larger, the requirement for strong security and privacy is also increasing. Low-cost and ultra-low-cost tags are being implemented on everyday products, and their limited resources constraints the security algorithms to be designed especially for those tags. In this paper, a complete solution providing strong security and high privacy during the whole product lifetime is presented. Combining bit-wise operations and secret keys, the algorithm proposed addresses and solves all the common security attacks.

Keywords: RFID tags, security, bit-wise, privacy.

1 Introduction

In wireless communications, the security aspect has always been a big issue. Maintaining the confidentiality and the integrity of the data is a main concern, as people expect to send information to a targeted authority only. Designing a system using wireless communications means considering a large number of security threats. Those threats will be listed further in this paper.

1.1 The RFID Technology

(RFID technology is not recent. It has been used for the first time during World War II with the “Identification Friend or Foe” (IFF) system to make the distinction between allied and enemies’ planes. It has been used afterwards for many years in very specific areas to perform particular tasks such as automatic car payment on the highway or cattle monitoring. Its relatively expensive price at that time made it difficult to be generalized. Thanks to efforts of miniaturization and improvement in the technology, it became possible to produce RFID Tags and readers for a relatively low price, leading to a renewed interest in this technology.

The RFID Technology consists of different devices that communicate over radio transmissions. A typical RFID network is composed of RFID Tags, a reader and a database (see Figure 1). The reader is able to communicate both with the database and the tags, while the other devices can only communicate with the reader. To retrieve information from the RFID Tag, the reader sends a request. The Tag (which is most often a passive device) uses the energy harvested from the request to send back an

A.U. Schmidt and S. Lian (Eds.): MobiSec 2009, LNICST 17, pp. 172 – 179, 2009.

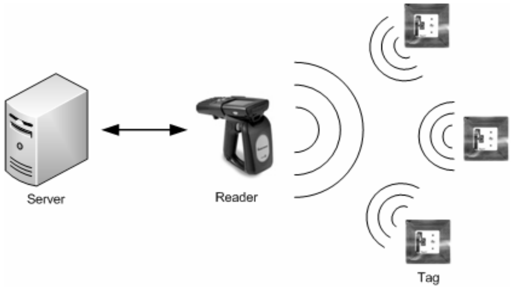

Fig. 1. RFID Architecture

answer. The aim of the RFID technology is to replace the barcode, introducing the Internet of things, where every single product has its own code.

1.2 A New Problematic

With the development of the RFID technology, a new kind of threat appears; the privacy threat. Privacy has become one of the most sensitive topics, since it has to deal with not only the privacy and integrity of the company, but also with the privacy of the consumer, who is the end-user in the production chain. These privacy threats become a reality as the deployment of RFID tags on everyday products is propagating, but even more because the RFID readers are small, relatively inexpensive, and have sufficient processing capabilities to read most of the tags. Solving those threats is one of the most challenging topics regarding this technology, both for the research aspect as for the social aspect it introduces.

1.3 Privacy Threats

So far, seven main privacy threats have been identified, compromising the privacy of the consumer:

The action threat concerns the behaviour or intent of a user that can be inferred from the evolution of the group of tags surrounding him.

The association threat focuses on the product itself. Not only the kind of products the person owns, but the precise product can be discovered (very limited edition, for example).

The location threat deals with tracking of people thanks to the tags they are wearing. Since most of the readers are fixed, it can be quite easy to monitor someone's location through the whole day, by checking all the places where some of the tags he is wearing, have been read.

The preference threat is related to the specific kind of product someone owns and buys, to define his consumer profile, and thus target him more specifically (target advertising, for example).

The constellation threat is highly related to the location threat except that it is not a targeted individual that is tracked but a random individual without knowing its identity.

The tracking of this person would be performed by tracking the constellation of RFID tags that he is wearing.

In **the transaction threat**, the tracking of goods does not stop at the consumer step, but goes further and keep on tracking the location and ownership of the tagged object through its entire product life (until the chip is destroyed). If some product goes from one person to another, you can conclude that they know each other and draw a link between them. Step by step, you can draw a complete social network, connecting all the links between people.

The breadcrumb threat is the issue that links someone to the objects he bought as long as the objects exist (i.e. the tag is working). When someone buys a product in a retail shop, the tag information is stored in the shop database (or even a larger database), and is not updated after the consumer's purchase. It can then create some trouble to the owner in case of a misuse by a third person.

We can infer from all those threats that the consumer privacy can be highly exposed if no action is done to avoid them. They are described in more details in [1]. Many researchers have been working on this topic and their contribution to this field is detailed in the next section.

2 Related Works

While facing an issue, two options are available. One consists in finding the solutions to solve the issue. In this particular case, the solution is to implement encryption and authentication in the process. Some research has been done to compare all the available encryption algorithms for ultra-low power devices [2]. However, this work is more focused on Wireless Sensor Networks, which embedded more computational resources than RFID Tags. A similar survey is presented in [3] and goes even more deeply in the energy consumption of each single computational operation. Many different ways have been explored to ensure security in RFID technology. Some works focus on the physical properties of the device to maintain security, using the physical imperfections of the hardware to guarantee authenticity [4]. Several security algorithms have been proposed as well, some relatively energy-consuming introducing "lightweight" elliptic curve cryptography primitives [5] or trapdoor-based mutual authentication [6]. Others are using considerable memory resources either through a key-table [7] or storing additional data to preserve untraceability [8]. Some propose a secured solution limited to a single reader scenario [7][9], which could be an unrealistic constraint in real case deployment. Finally, a few other protocols perform strong security and authenticity with simple bit-wise operations [10], [11]. These two last mentioned protocols seem to be the best alternative for low-cost RFID solutions, since they are not as energy-consuming and memory-demanding as the others, and do not present some major constraints or security gaps.

The other option consists in removing the issue itself. Authentication and encryption is a strong requirement in a wireless communication process to maintain privacy. However, this requirement becomes useless without communication. In fact, all the privacy threats are based on a simple assumption: tags and readers are able to communicate. As communications stop, the threats disappear (except the breadcrumb threat which is related to the physical product itself). So, the concept is to avoid communication between tags and reader. In this way, a possible solution was the use of a battery-powered mobile device called “RFID Guardian”, supposed to create interference around the guardian to preserve the privacy of the RFID Guardian holder [12]. The same principle has been studied by the RFID expert A. Juels et al. who propose a “blocker tag” that selectively allow communications with authenticated readers [13]. Those solutions present the disadvantage to constrain the user to hold an additional device permanently with him, and open the path to security gaps in case the device fails. The ultimate alternative is to temporarily deactivate the tag to make sure it is not able to communicate anymore, without purpose.

3 Proposed Solution

3.1 A Few Assumptions

In the production cycle, the privacy concerns appear at the very last link of the chain, when the consumer buys the product. The concept of the proposed solution is to ensure a strong security during the whole production process (see Fig. 2), and a strong privacy, once the consumer owns the product.

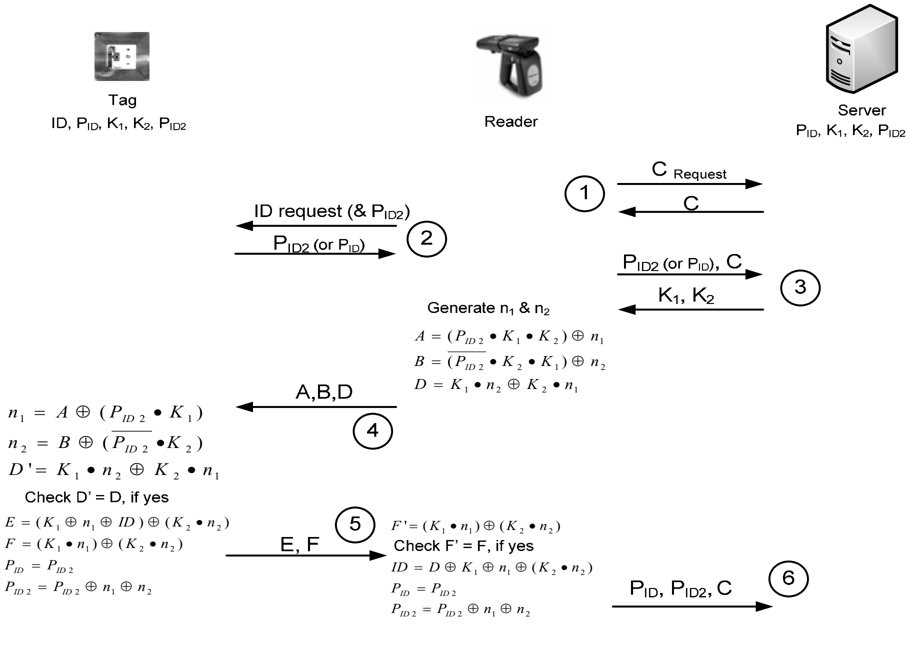
Tag
ID, P_{ID}, K_1, K_2, P_{ID2}
Reader
Server
P_{ID}, K_1, K_2, P_{ID2}
1
C Request
C
ID request (& P_{ID2})
P_{ID2} (or P_{ID})
2
P_{ID2} (or P_{ID}), C
K_1, K_2
3
Generate n_1 & n_2
$A = (P_{ID2} \bullet K_1 \bullet K_2) \oplus n_1$
$B = \overline{(P_{ID2}} \bullet K_2 \bullet K_1) \oplus n_2$
$D = K_1 \bullet n_2 \oplus K_2 \bullet n_1$
A,B,D
4
$n_1 = A \oplus (P_{ID2} \bullet K_1)$
$n_2 = B \oplus (\overline{P_{ID2}} \bullet K_2)$
$D' = K_1 \bullet n_2 \oplus K_2 \bullet n_1$
Check D’ = D, if yes
$E = (K_1 \oplus n_1 \oplus ID) \oplus (K_2 \bullet n_2)$
$F = (K_1 \bullet n_1) \oplus (K_2 \bullet n_2)$
$P_{ID} = P_{ID2}$
$P_{ID2} = P_{ID2} \oplus n_1 \oplus n_2$
5
E, F
$F' = (K_1 \bullet n_1) \oplus (K_2 \bullet n_2)$
Check F’ = F, if yes
$ID = D \oplus K_1 \oplus n_1 \oplus (K_2 \bullet n_2)$
$P_{ID} = P_{ID2}$
$P_{ID2} = P_{ID2} \oplus n_1 \oplus n_2$
P_{ID}, P_{ID2}, C
6

Fig. 2. Security Protocol

The security protocol is inspired by the works done in [10] and [11] combining a strong authenticity and reducing the computational load of the tag, without compromising the security. While the tag is created, four numbers are shared by the tag and the server; two Pseudo ID (P_{ID} & P_{ID2}, initially equals) and two keys, K_1 and K_2. All of them have a length equal to the tag ID. In this protocol, we assume that the link between the Reader and the Server, which are two powerful devices, is secured against all the traditional attacks related to networks. We also assume that the reader will always be able to communicate with the server, since readers are often equipped with the GSM technology, making the communication available everywhere, anytime.

3.2 The Protocol

- **1st step:** The reader requests a certificate of authenticity to the server. The server decides whether or not the reader is allowed to retrieve further information from the server, by sending back a certificate. This first step is done only once per reader, per day. If the reader wants to read multiple tags at the same time, it will just request a certificate once, and use it for all the tags. If the reader already has a valid certificate (the one of the day) the protocol starts in Step 2.
- **2nd step:** The reader sends a request to the tag, which replies with its P_{ID2}. If the reader cannot find a match in the database, it will send another request with the P_{ID2} to the tag, which will reply with its P_{ID}.
- **3rd step:** The reader sends the P_{ID} together with its certificate. If the certificate is authentic, the server replies with K_1 and K_2. The reader then generates 2 random numbers n_1 and n_2. It computes A, B and D with the keys shared by the tag and the random numbers.
- **4th step:** The tag computes the values of n_1, n_2 and D'. If K_1 and K_2 are genuine, D' and D will be equal. This step is necessary to authenticate the reader from the tag's point of view. Since K_1 and K_2 are not exchanged between tag and reader, a match in the D value means that the reader is legitimate.
- **5th step:** The tag computes E with its ID, F with the 4 secret values, and sends them to the reader. The reader will first check the value of F to check the authenticity of the tag. If the values match, it will be able to retrieve the ID from E using K_1, K_2, n_1 and n_2. Both reader and tag compute a new value of Pseudo ID (P_{ID2}) that will be used for the next communication.
- **6th step:** The reader sends an updated version of the Pseudo ID (P_{ID2}) as well as the previous version (P_{ID}) and its certificate, to maintain authenticity.

Thanks to n_1 and n_2 the values A, B, D, E and F are always different. Changing the value of P_{ID} is a necessity to avoid tracking of the tag. In fact, it's rather easy to track a tag that would always reply with the same message to a simple request. Storing the previous value of the P_{ID}, while the next value to be used is P_{ID2}, is to maintain the integrity of the network and avoid de-synchronization attacks.

4 Security Evaluation

4.1 Security Analysis

In this section, we will review a bit more in detail the security threat and the solutions proposed by the algorithm.

Eavesdropping happens when an attacker listens to the channel to retrieve information. Even if the attacker will receive the messages, it is not possible to determine the values of the secrets keys or the ID of the tag, since the messages are encrypted (A, B, D, E and F).

Relay attack occurs when a fake tag and a fake reader try to counterfeit a legitimate authentication. It cannot be done in the proposed solution because tag and reader don't exchange data to authenticate each others directly. The reader authenticates itself with the server, the tag authenticates the reader through D and the reader authenticates the tag through F. Any minor change in those values will be detected.

Unauthorized tag reading and **tag cloning** are solved through the use of authentication. If the reader is not allowed by the server it will never get any information related to the tag. Similarly, if the tag is not genuine, it will not be able to decrypt the values of A, B and D.

Tracking is done by simply listening to the data transmitted by the tag. Since the data sent by the tag is always different, P_{ID2} is changing in a random way since it involves n_1 and n_2, it is not possible to track the tags over time. Though, between two successful authentications, a malicious reader will always receive either P_{ID} or P_{ID2} from its requests and will therefore be able to track the tag. However, it assumes that the malicious reader is following the tag, which does not make sense in a realistic scenario (i.e. if the reader follow the tag, you do not need to read it in order to track it).

Replay attack occurs when a malicious tag tries to authenticate itself by repeating the authentication sequence (P_{ID}) of a genuine tag. While the reader will reply with A, B and D, the malicious tag won't be able to retrieve any information from those values.

De-synchronization attack is used by an attacker to update the values in only one part of the network, either the tag or the reader, in order to make it impossible for them to communicate further. In our scheme, before any update of data, there is a check (D and F) and if the values do not match, the intrusion is detected and the value of P_{ID2} is not updated in the server. If it is updated by mistake, the old value (P_{ID}) will be used to recover from the attack.

Forward Security is the possibility to maintain integrity of the communication over time. It means that even if the tag is physically compromised one day, and the attacker is able to recover the secret values of the tag, it will not be able to find the previous data, since every exchange of data includes two random numbers.

Disclosure attack is used to retrieve some secret information from one entity by sending a slightly modified message to see the impact on the answer. In our scheme, any change is detected and the attacker won't receive any answer.

As a conclusion of the security analysis, it appears that the proposed protocol is robust to any kind of attack. The Table 1 is a comparison of security threat in different ultra-lightweight protocols implemented for low-cost RFID tags. Our solution is slightly lighter than SASI and the authentication protocol is more advanced.

4.2 Privacy Analysis

We will review in this section the privacy issues presented in the section I and see how the protocol handle with them. The **action threat** as well as the **association threat** is solved since it is impossible to retrieve information from the tag without being authenticated by the server. The **preference threat**, the **transaction threat** and the **breadcrumb threat** are not directly in the scope of this paper since they deal with the association of a tag to its owner. This is mainly dependant on the application used

Table 1. Comparison of ultra-lightweight authentication protocols

	LMAP	M^2AP	EMAP	SASI	Ours
Resistance to de-synchronization attacks	No	No	No	Yes	Yes
Resistance to disclosure attacks	No	No	No	Yes	Yes
Privacy and anonymity	No	No	No	Yes	Yes
Forward Secrecy	No	No	No	Yes	Yes
Mutual Authentication	No	No	No	Partially*	Yes
Memory size on tag	6L**	6L	6L	7L	5L
Memory size on server	6L	6L	6L	4L	4L
Operation types on tag	$\oplus, \bullet, +, 2^m$	$\oplus, \bullet, +, 2^m$	$\oplus, \bullet, +, 2^m$	$\oplus, \bullet, +, 2^m, Rot$	$\oplus, \bullet$

* Authentication Reader/server is assumed, Tag/Reader is done only in one direction.
** L denotes the bit length of one pseudonym or one key.
2^m denotes the addition modulo 2.

and the usage of the tag. However, assuming the identity of someone would be revealed, it still remains impossible for an adversary to read the information stored in the tag, insuring the privacy of the person. Finally, the **location threat** and the **constellation threat** are probably the weakest link in this protocol. Both are related to tracking and we saw in the security analysis that between two legitimate readings, it is possible to track a tag. However, it assumes that it exist several malicious readers, placed in different strategic points, able to communicate with each others, and that no legitimate reading is done between the two malicious readings. The nature of the threat depends on the reader's ability to retrieve the identity of the tag's holder.

5 Conclusion

In this paper we presented a new solution to the security and privacy issue in RFID Technology. The solution we provided maintains a strong security despite its ultra-lightweight algorithm, and can overcome any kind of attack over the radio. The comparison with other similar protocols shows that it is more light, simple and at least as robust as the others. Thanks to its light weight and bit-wise operations, it can be easily implemented on ultra-low-cost RFID tags.

Acknowledgements. This work was supported in part by the European Commission, in the context of the project ASPIRE "Advanced Sensors and lightweight Programmable middleware for Innovative Rfid Enterprise applications", grant agreement FP7 ICT-2007-215417.

References

1. Garfinkel, S.L., Juels, A., Pappu, R.: RFID privacy: An overview of problems and proposed solutions. IEEE Security & Privacy 3(3), 34–43 (2005)
2. Kaps, J.-P., Sunar, B.: Cryptography on a Speck of Dust. Computer 40(2), 38–44 (2007)
3. Eisenbarth, T., Kumar, S.: A Survey of Lightweight-Cryptography Implementations. IEEE Design & Test of Computers 24(6), 522–533 (2007)
4. Bolotnyy, L., Robins, G.: Physically Unclonable Function-Based Security and Privacy in RFID Systems. In: The Fifth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2007, March 19-23, pp. 211–220 (2007)
5. SungJin, K., YoungSoo, K., SeokCheon, P.: RFID Security Protocol by Lightweight ECC Algorithm. In: The Sixth International Conference on Advanced Language Processing and Web Information Technology, ALPIT 2007, August 22-24, pp. 323–328 (2007)
6. Hwaseong, L., Eun Young, C., Su-Mi, L., Dong Hoon, L.: Trapdoor-based Mutual Authentication Scheme without Cryptographic Primitives in RFID Tags. In: The Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SECPerU 2007, July 19, pp. 73–78 (2007)
7. Huafei, Z., Bao, F.: Securing RFID Tags: Authentication Protocols with Completeness, Soundness, and Non-Traceability. In: The IEEE Wireless Communications and Networking Conference, WCNC 2007, March 11-15, pp. 2698–2702 (2007)
8. Shucheng, Y., Kui, R., Wenjing, L.: A Privacy-preserving Lightweight Authentication Protocol for Low-Cost RFID Tags. In: The IEEE Military Communications Conference, MILCOM 2007, October 29-31, pp. 1–7 (2007)
9. Yung-Chin, C., Wei-Lin, W., Min-Shiang, H.: RFID Authentication Protocol for Anti-Counterfeiting and Privacy Protection. In: The 9th International Conference on Advanced Communication Technology, Feburary 12-14, vol. 1, pp. 255–259 (2007)
10. Il Jung, K., Eun Young, C., Dong Hoon, L.: Secure Mobile RFID system against privacy and security problems. In: The Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SECPerU 2007, July 19, pp. 67–72 (2007)
11. Hung-Yu, C.: SASI: A New Ultra-lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. The IEEE Transactions on Dependable and Secure Computing 4(4), 337–340 (2007)
12. Rieback, M.R., Crispo, B., Tanenbaum, A.S.: RFID guardian: A battery-powered mobile device for RFID privacy management. In: Boyd, C., González Nieto, J.M. (eds.) ACISP 2005. LNCS, vol. 3574, pp. 184–194. Springer, Heidelberg (2005)
13. Juels, A., Rivest, R.L., Szydlo, M.: The blocker tag: selective blocking of RFID tags for consumer privacy. In: The 10th ACM conference on Computer and Communications Security, Washington D.C., USA, pp. 103–111 (2003)