Security, Privacy, Authentication in RFID and Applications of Smart E-Travel

Mouza Ahmad Bani Shemaili, Chan Yeob Yeun, Mohamed Jamal Zemerly

Computer Engineering Department, Khalifa University for Science, Technology and Research,
PO Box 573, Sharjah, UAE
mouza@kustar.ac.ae, cyeun@kustar.ac.ae, jamal@kustar.ac.ae

ABSTRACT

Radio Frequency Identification (RFID) technology is a new promising technology that will spread in the near future to enter all of our everyday activities. However, the security of this technology could be compromised, especially in the areas of privacy and authentication. Therefore, RFID tag data must be protected in ways that present sufficient computational challenges to adversaries. This paper reviews and analyzes the most common privacy and authentication proposed solutions. Moreover, the paper describes applications for the use of RFID in the airport environment keeping security aspects in mind, and the chance to use emerging technology such as RuBee.

Key Words: Smart e-Travel, Security, Authentication, Privacy, RFID, Rubee.

1. Introduction

Radio-frequency identification (RFID) is an automatic identification method, used to transmit the identity (serial number) of objects or subjects (people) wirelessly, through the radio waves. RFID technology is used anywhere that needs a unique identification system, so it can be used in products, animal, or to identify and track persons such as for building access purpose. In this paper we will focus on applying RFID technology in transportation, since RFID technology is able to collect greater data about the traveler than other technologies that are commonly being used.

Moreover, RFID technology can be faster, less expensive and more secure. Therefore, the RFID usage in transportation applications has been increased such as in transportation payments, and vehicle tracking and toll gates. An example of using RFID in Dubai in the United Arab Emirates is the use of Salik for toll payment by the Road Transport Authority (RTA).

In addition, RFID is used in Fleet management, e-Passports as in the UK, Norway, and Japan, RFID baggage sorting in the airport, such as in Hong Kong International Airport to prevent baggage loss, and many other applications throughout the world [1, 2].

An RFID system consists of three main components; a tag, a reader, and a server. A reader emits radio waves to activate the tag, and then the tag transmits its stored data to the reader which will relay the tag's data back to the server which controls the system's data.

Moreover, there are two types of tags: one is an active tag, that includes miniature batteries used to power the tag, and the other is a passive tag that does not have a battery, so it will need to be beamed by the reader to be activated. Passive tags are smaller, less expensive and used for a shorter range. Some smart tags have memories that can be written into and erased, while others have memories that can only be read, so the cost of the tag depends on the memory size that it contains [3].

RFID technology is predicted to be a substitute for the second generation of the bar code technology since there are four main advantages of RFID technology over bar code technology, such as:

1- RFID eliminates the need for direct line-of-sight reading that the code bar depends on.

2- RFID scanning can be done at greater distances than the bar code scanning.

3- RFID can scan multiple products simultaneously.

4- Since RFID can be used as a unique system identifier and can be used as a product pointer in the database, which can facilitate the tracking of all products' history. At a certain point RFID technology can be considered as the niche development technology.

However, they have limited power constraint (powerless for passive tags), limited communication range up to 5 m, and a small number of gates for logical operations. All of these limitations led to building RFID systems but without a security aspect. As a result RFID technology now faces some major security issues that may hinder its propagation if not handled properly.

The rest of this paper is organized as follows. Some of the security challenges and related work are summarized in Section 2. In Section 3, we analyze the privacy and authentication solutions. We describe applications of Smart E-Travel based on RFID in Section 4. We conclude this paper in Section 5.

2. Security Challenges

Although the use of RFID tags continues to increase according to a new report from In-Stat [4], which states that over 1 billion tags were produced last year, and by 2010, the number will rise to 33 billion**.** However, there have been issues which have been raised by privacy advocates over the use of RFID tags to track people or their tagged possessions.

Furthermore, a tag emits data to any reader without alerting its owner. This can be made worse if the tag contains some personal data such as name, birthday, etc. related to the tag owner so the attacker will not only be able to track the tag owner but also he/she could create a profile that relates to that person. On the other hand, RFID technology also faces major security issues concerned with authentication. Any attacker with suitable equipment is able to clone any legitimate tag and communicate with a legitimate reader as a genuine tag when in fact it is just a counterfeit.

Researchers are currently seeking solutions to solve the security issues in RFID, so that it can be proliferated without any problems in the future.

The following subsections deal with the privacy and authentication solutions for the RFID technology.

2.1 Privacy Solutions

In order to solve privacy issues, we must prevent a genuine tag from communicating with a malicious reader and refresh the tag identifier frequently. Therefore, tracking the tag by a malicious reader will be more difficult [5, 6]. Moreover, there are many solutions that are suggested by researchers to solve this problem, but we will explain the most important one here. In this subsection we survey some of the RFID privacy solutions [7 – 13].

A. Juels [7] proposed the idea of Minimalist cryptography which consists of storing a short list of random pseudonyms in the tag so each time a tag is queried it emits the next pseudonym in the list until the end of the list. Then it starts from the beginning until it ends. This scheme can be implemented in an RFID tag by just adding several hundred bits of memory to the tag enabling the read write feature. Using this mechanism helps to prevent the tracking of the tag by an illegitimate reader. However, the small storage in RFID tags leads to a short list of pseudonyms and hence limits the privacy protection.

K. Fishin *et al.* [8] addressed another solution for the privacy problem. This mechanism does not need any modification on the RFID communication protocol, or any change in the reader, but a little change in the tag. An algorithm calculates the distance between the RFID reader and tags using a variable based on energy analysis-through the signal-to-noise ratio of the reader signal. A closer reader is considered more trusted than a distant one. However, this mechanism has some limitations, such as the signal strength differing depending on the direction the tag is facing.

The European Central Bank proposed using RFID in banknotes but RFID had security issues relating to privacy. Therefore, **A. Juels, and R. Pappu** [9] proposed a

re-encryption scheme to solve the problem. Re-encryption is changing the appearance of the cipher text without changing the plaintext. The re-encryption scheme may be done by shops, banks, or by consumers that hold the banknotes. An RFID banknote has a memory that has a serial number, signature, cipher text, and a random number which are used in the El-Gamal algorithm [10], that is used to re-encrypt the cipher text, and saved it in the RFID tags. The drawback to this algorithm is that the re-encryption algorithm may not be done frequently enough.

P. Golle *et al.* [11] suggested universal re-encryption, which is a cryptographic technique that is similar to the El-Gamal cryptosystem except that it does not require a public key.

In the universal re-encryption, the input plain text must be encrypted by the recipient public key before it enters the mix servers that consist of the chain of involved servers. Then, each server involved in the scheme re-encrypts the input cipher text from previous server until it reaches the last sever so the recipient should have the whole output cipher text from the mixnet server then decrypts them all using his/her private key until it has the match cipher that is encrypted under his/her public key. This scheme can be used to enhance privacy in RFID tags so they can be re-encrypted under the agency that generates them.

Universal re-encryption may be an efficient scheme but it has some limitations such as the size of the cipher text is double the size of El Gamal's cipher text. Also, the recipient should decrypt all the output cipher text to have his/her plain text.

A. Juels, *et al.* [12, 13] invented a blocking mechanism. A blocker works by changing the tag bit, so 0 bit means that the tags can be publicly read and 1 bit means that tags are in a private zone (not allowed to be read publicly). Actually, the blocker mechanism depends on exploiting the singulation protocol in the reader. The singulation protocol enables a reader to identify the serial number of the tags individually. Therefore, a blocker tag simulates the tags in the air and always makes it seems like all possible tags are present, so a reader cannot figure out which tags are actually present, since the number of possible tags is huge *(at least a billion*), so a reader will stall. However, a blocker is polite as it tells the reader of its presence so the reader will not attempt to scan the tags in the privacy zone.

2.2 Authentication Solutions

Authentication is the process of ensuring that the users are the persons whom they claim to be. Therefore, the goal of authentication is only for authorized readers who can get the content of the valid tags. Moreover, private information would not be leaked in the presence of unauthorized entities [14]. In this section we survey some of the suggested RFID authentication protocols [15], [17], [18], [20], [21].

Li Lu, *et al.* [15] suggested the Key-Updating scheme to solve the problem of keys compromised in a tree approach scheme, [16] which states that a temporary key is used to store the old key for each non-leaf node in the key tree. For each non-leaf node, a number of state bits are used in order to record the key-updating status of nodes in the sub-trees such as 1 bit for having been updated, otherwise it will have 0 bit. Based on this design, each non-leaf node will automatically perform key-updating when all its children nodes have updated their keys.

Stephen *et al.* [17] invented a lightweight authentication algorithm that can be embedded in the low cost RFID tags which has a Randomized Access Control. This scheme provides mutual authentication between RFID reader and tag. A reader contains a list of the tags keys and each tag stores its own key. In the first step, a reader sends a "Who are you?" message to the tag. Then, the tag will generate a random number R and sends it along with the hash value of the tag stored key. When the reader receives the tag message it will start to compute the hash value for every key in the list and compare it with the tag message. Finally, after finding the corresponding key from the comparison then the reader will send a "You must be K" message, where 'K' is the tag identifier, to the tag so the tag will make sure that the reader is a valid one. This scheme is

efficient but, it is a heavy weight solution if the key list is long and it could be costly.

P. Peris-Lopez *et al.* [18] proposed a lightweight mutual authentication protocol based on the idea of Minimalist and index-pseudonyms (IDSs). Each tag stores a key divided into four parts of 96 bits (K= K1||K2||K3||K4) and these parts are updated after each successful authentication. This protocol consists of four steps. Tag Identification, Mutual Authentication, Pseudonym Index Updating, and Key Updating. However, this protocol is vulnerable to Desynchronization Attack [19].

B. Song and **C.J. Mitchell** [20] proposed a protocol which consists of three exchanges between the reader and the tag. Each tag stores a hash value of string μ [t= h (μ)] unique to each tag. Also, each server stores [(μ,t)new,(μ,t)old, D] where (μ,t)new is the new values of the string μ and corresponding h(μ)= t, and (μ,t)old is the previous stored data, and D is the data of the tag such as price. After a successful authentication both the server and tag will update their values. However, if the updated message does not reach the tag, then the tag will use its old identifier. This can be an advantage to hackers. If they are successfully able to prevent the tag update process then, tag anonymity will be lost and they can track the tag easily.

Y. K. Lee *et al.* [21] proposed a lightweight authentication protocol that can be used for low cost RFID called Advanced Semi-Randomized Acess Control (A-SRAC). First of all, a reader sends a query and a random number Rs to the tag. Then, the tag generates a random number Rt and sends it to the reader with the tag MetaID. After that, the reader relays this message back to the sever through a secure channel. The server looks up the key corresponding to the tag MetaID, then the server will check the uniqueness of the MetaID among other MetaIDs in the system. If that MetaID is not unique then the server will generate a random number R2 till it reaches the new unique MetaID. Then, the server will send R2 and h(key||R2||R1) to the tag through the reader. The tag will check the correctness of the message and if it is correct the tag will update the previous key with the new key.

3. Our Analysis and Discussion

In this paper we provide a review of some of the privacy and authentication solutions. Most of privacy solutions try to solve the tracking problem through changing the tag identifier frequently such as minimalist, re-encryption, and Universal re-encryption schemes. On the other hand, all of the authentication protocols described here are considered as mutual authentication protocols that required authentication for both the reader and the tag side. Hence, the protocols that authenticate just one side of the RFID parties, usually tag, are not that sufficient and vulnerable to communicate with other malicious parties either malicious readers or tags.

From Table 1 it can be seen that the best privacy solution is the Minimalist, while Table 2 shows that A-SRAC is the best authentication solution.

From all the privacy and the authentication solutions we can find out that there are some

Scheme	Complexity	Cost	Cloning Resistance	Replay attack Resistance	Anonymity	DOS Resistance	Forward secrecy
Minimalist [7]	√	X	√	X	√	X	√
Distance Measurement [8]	X	√	X	N/A	X	X	X
Re-encryption [9]	X	X	√	√	√	N/A	X
Universal Re-encryption [11]	X	X	√	√	√	N/A	X
Blocking [12,13]	√	√	X	N/A	√	X	X

Table 1. Summary analysis of privacy solutions

aspects that must be considered when we try to secure the transaction between a reader and a tag. Also, these are the aspects that we consider when we evaluate the privacy and authentication solutions in Table 1 and Table 2. These aspects are as follows:

1- Store critical data in the back end server (such as database) which must be in a secure environment, not in the RFID tag.
2- An attacker could store all the messages interchanged between the reader and the tag. Then, he/she can try to impersonate a reader, and resend the message causing a replay attack. Thus, to prevent a replay attack we must use challenge and response in the transaction between both the reader and the tag.
3- Attackers should not be able to use fake tags to impersonate a genuine tag. So, to prevent the cloning problem we must use a shared stored secret between the reader and the tag, and use this secret in the authentication process; note that, this shared secret must be computationally infeasible so that attackers cannot predict it.
4- Tags must have anonymity to prevent the tracking problem. So, the tag response must appear as a random number in order that the attacker will not be able to trace it, so must be refreshed frequently.
5- If the attackers were successfully able to prevent the tag updates value after a successful authentication, then the protocol will be vulnerable to a Denial of Service (DoS) attack. Therefore, the old and previous values must be stored in the back end server.
6- Compromising a tag key can lead to compromising the keys of other tags, if the tags share some keys with compromised tags. So, to provide forward secrecy, the tags must update keys after each successful authentication and the tags must not share the keys related to other tags.

Hence, RFID technology faces a lot of challenges and limitations. A new standard of emerging technology, that might supersede RFID called RuBee, has been recently approved by IEEE [22]. RuBee is an active long wavelength, inductive, packet protocol with a five- to ten-year battery life and a range of 1 to 50 feet and with optional sensors. RuBee takes advantage of low power magnetic near field physics and overcomes many of the technological problems seen with RFID near steel and water, so RuBee can work in harsh environments. RuBee is also unique in that it has Real-Time Range Management (RTRM), which makes it possible for a tag and a base station to dynamically change range from a few inches to tens of feet, and virtually eliminate the possibility of eavesdropping. Furthermore, RuBee may use Advanced Encryption Standard (AES) [23] for secure communications and also use authentication protocols that are similar to TLS. Therefore, we will try to apply RuBee in the future instead of RFID to gain more secure transactions.

In the next section we present an application of how to implement RFID in the airport considering the security aspects that were previously mentioned. Moreover, we think

Scheme	Complexity	Cost	Cloning Resistance	Replay attack Resistance	Anonymity	DOS Resistance	Forward secrecy
Dynamic Key-Updating [15]	X	√	√	√	√	√	√
Randomized Hash Locks [17]	√	X	√	√	√	X	√
Minimalist and index-pseudonyms [18]	√	X	√	X	√	X	√
Song and Mitchell protocol [20]	√	√	√	√	X	√	√
A-SRAC [21]	√	√	√	√	√	√	√

Table 2. Summary analysis of authentication solutions

that the real problem in most of this technology implementation is that it is applied without considering the security threats. Therefore, the real challenge can be how to apply the RFID technology in a safeguard way.

4. Smart e-Travel Applications

First of all, we aim to use an e-passport with a RFID chip in a secure manner. This paper focuses on the authentication issues. In the beginning, each e-passport holder must authenticate himself at the e-passport issuer authority, by providing his picture and fingerprint to adjust the data for each passport holder in a safe database. The e-passport tag will only contain the encrypted password of the matched tag holder data in the database. We can state the e-passport holder application in the airport as follows:

The passenger holds his e-passport which contains encrypted data that identifies the passenger and enters the airport. At the check-in point, there is a reader that reads the encrypted data in the passenger e-passport then it matches this data to the data in the back end database. If there is a match then the passenger is considered as an authorized person in the airport environment, and can enjoy the new facilities of the airport. First, after the authentication process the reader will ask for the mobile number of the passenger, the passenger mobile device must be able to read RFID tags [24]. Then, some applications will be downloaded to the passenger's mobile so now he can pass into the airport easily. The application can read the tags in the airport and show the passenger the airport layout such as airport bathrooms, or coffee shops. In addition, when the passenger's luggage, which contains an RFID tag to facilitate luggage tracking, reaches the flight, the passenger will be notified by an SMS message sent to his mobile telling him/her about the location of his luggage.

Of course, this scenario needs security features, so that nobody except the airport authority can read the passenger's personal data. Also, no unauthorized person can fool the airport reader and enter the airport illegitimately. Therefore, as a feasible security solution, we would like to suggest previously mentioned A-SRAC [21]. Since, A-SRAC is a light weight mutual authentication protocol that can solve most of the security shortcomings with low cost.

5. Conclusion

RFID technology is a real emerging technology but it is still in need of some enhancement in terms of security issues such as authentication and privacy. In this paper we made a review for some of the privacy and authentication solutions. From our analysis we think that Minimalist is the best privacy solution, and A- SRAC is the best authentication solution. We also discussed Rubee, an emerging technology that can be used for secure and smarter e-Travel in the near future.

References:

[1] Serge Vaudenay, "E-Passport Threats," IEEE Security and Privacy, vol. 5, no. 6, pp 61-64, Nov/Dec 2007, doi:10.1109/MSP.2007.164

[2] Softrail, "AEI technology", http://www.aeitag.com/aeirfidtec.html. Retrieved on 2008-10-12.

[3] Albert Puglia, Mike Puglia, V. Daniel Hunt, "*RFID A Guide to Radio Frequency Identification*", Wiley-Interscience, April 10, 2007

[4] In-Stat, "RFID Tag Market to Approach $3 billion in 2009", http://www.instat.com/newmk.asp?ID=1206.

[5] Sixto Ortiz Jr., "How secure is RFID?", Computer, Volume 39, No. 7, pp 17–19, 2006.

[6] Ari Juels, "RFID security and privacy: a research survey", IEEE Journal on Selected Areas in Communications 24(2): 381-394 (2006).

[7] Ari Juels, "Minimalist cryptography for low-cost RFID tags", Int. Conference on Security in Communication Networks – SCN 2004, LNCS volume

3352, pp 149–164, Amalfi, Italy, September 2004. Springer-Verlag.

[8] K. Fishin, S. Roy, B. Jiang, "Some Methods for Privacy in RFID Communication", Intel Research Seattle Tech Memo IRS-TR-04-010, June 2004.

[9] A. Juels, R. Pappu, "Squealing Euros: Privacy-protection in RFID-enabled banknotes". In Proc. Financial Cryptography, Gosier, Guadeloupe, FWI, LNCS 2742, Springer-Verlag, 2003, pp. 103-121.

[10] Taher El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms". Proceedings of CRYPTO 84 on Advances in cryptology: 10-18, Santa Barbara, California, United States, Springer-Verlag, 1985.

[11] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal encryption for Mixnets", In T. Okamoto (Ed.): CT-RSA 2004, LNCS 2964, pp. 163–178, 2004.

[12] Ari Juels, Ronald L. Rivest, and Michael Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy", In CCS '03: Proc. of the 10th ACM conference on Computer and communications security, pp 103–111, New York, USA, 2003. ACM Press.

[13] Ari Juels and John Brainard, "Soft blocking: flexible blocker tags on the cheap", Proceedings of the 2004 ACM workshop on Privacy in the electronic society, October 28-28, 2004, Washington DC, USA.

[14] M. Lehtonen, T. Staake, F. Michahelles, E. Fleisch, "From Identification to Authentication – A Review of RFID Product Authentication Techniques". Printed handout of Workshop on RFID Security – RFIDSec 06, July 2006.

[15] Li Lu, *et al.*, "Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems", In Proc. of PerCom'2007. pp 13-22.

[16] D. Molnar, A. Soppera, and D. Wagner, "A Scalable, Delegatable Pseudonym Protocol Enabling Owner-shipTransfer of RFID Tags", in Proceedings of SAC, 2005.

[17] A. Stephen *et al.*, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pp 201–212, 2004.

[18] Pedro Peris-Lopez, *et al.*, "EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags", OTM Workshops (1) 2006: 352-361.

[19] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", Proc. 22nd IFIP TC-11 Int'l Information Security Conf., May 2007.

[20] B. Song and C.J. Mitchell, "RFID authentication protocol for low-cost tags", in V. D. Gligor, J.-P. Hubaux and R. Poovendran (eds.), Proceedings of the First ACM Conference on Wireless Network Security, WiSec 2008, Alexandria, VA, USA, March 31 - April 02, 2008, ACM (2008), pp.140-147.

[21] K. Lee, Ingrid Verbauwhede, "Secure and Low-cost RFID Authentication Protocols", 2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN), November 2005.

[22] Mary Catherine O'Connor, "Visible Assets Promotes RuBee Tags for Tough-to-Track Goods", RF Journal, June 2008.

[23] Joan Daemen and Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", Springer-Verlag, 2002, ISBN 3-540-42580-2.

[24] "Prototype Nokia 3220 NFC RFID phone could reshape society", http://mobilementalism.com/2005/12/12/prototype-nokia-3220-nfc-rfid-phone-could-reshape-society/