Privacy Preserving on Radio Frequency Identification Systems

Hua Wang[1], Lili Sun[1], Jianming Yong[1], Yongbing Zhang[2]

[1]*University of Southern Queensland*
Toowoomba, Australia
(wang, sun, yongj)@usq.edu.au
[2] *Graduate School of Systems and Information Engineering*
University of Tsukuba, Japan
ybzhang@sk.tsukuba.ac.jp

Abstract

This paper focuses on the challenges on the privacy of Radio Frequency Identification (RFID) systems. RFID systems have already widely applied in industry and have been bringing lots of benefits to our daily life, it also creates new security and privacy problems to individuals and organizations. The security and privacy challenges are analysed after a brief introduction of various RFID systems and their associated operations. A proposal to protecting security and privacy of customers, as a solution of the challenge for low-cost RFID systems is designed. Finally, comparisons to related works of the proposal are described.

Keywords: RFID, Privacy, Security.

1. Introduction

Radio Frequency Identification (RFID) is an automatic identification method to identify objects and human beings without physical contact. The identification method relies on storing and remotely retrieving data using devices called RFID tags or transponders. A tag is a small microchip which is used for wireless data transmission between the tag and a reader. The microchip can be as small as 0.4mm2 [12]. RFID tags can be attached to or incorporated into a product, animal, or person for the purpose of identification using radio waves. RFID systems normally consist of tags, readers and database systems to process the data from tags as shown in Figure 1.

RFID has been widely applied in a lot of environments such as hospital [2], road toll, access control to facilities, and e-passport [6]. The major driver for the increasing application of RFID is the falling price of RFID tags which is going to be less than 5 cents [10]. According the low-cost tags and various application of RFID in our current life, we have started to concern the security and privacy surrounding RFID systems. Customers identity can be obtained and used by wicked readers since currently RFID systems do not provide protection on the identification, and unauthorized readers are able to collect customer identity and goods to generate customer profiles which will reveal private information [15]. For instance, customers carry retail items with tags of insecure RFID systems. An adversary may query the tags for contents since tags lack secure access. This might look as innocuous inspections, but nobody like people glancing their shopping items or peeking into their bags. Insure RFID system threats are not only limited to individual security and privacy violations, but also to companies and shops. A shop, for example, installs a smart system and stocks products with insure RFID tags. The RFID system can be attacked in various ways. A competitor of the shop may automatically query the shop's inventory, and derives sales information for making a business decision as a corporate spy. The competitor can also re-write the contents of cheap products to expensive items which will confuse the selling report of the shop.

The paper is organized as follows. In the next section, we describe the security and privacy issues in an RFID system, and followed by the mechanisms on security and privacy of low-cost RFID systems in section 3, including killing and sleeping tags approaches and hash-based access control on tags. A new protocol for low-cost RFID systems is designed in section 4. To achieve low computation and energy cost, *n* random numbers are used in the protocol. The protocol is securely designed for a large number of tags RFID system, and can prevent long-range eavesdropper attack.
Comparisons to other related work are analyzed in section 5 and the conclusions are in section 6.

2. Security and privacy

A reader needs to communicate with tags and an application system which processes the data from the reader. Generally we do not concern too much about the security between the reader and application system since we can use current secure techniques, rather than the

security challenges and technologies between the reader and tags. Privacy is also a serious concern for customers, and it may be an obstacle for RFID application when customers privacy is not able to guarantee. People may carry objects with communicating readers without even realizing the existence of tags. Passive tags usually send data out without security authentication when they receive a signal from readers. The data may also link to other secret information and location message that should be protected. Fundamental security objectives as confidentiality, integrity, authentication and anonymity are not achieved in RFID systems without the supports from special security mechanisms [16, 1]. For example, Confidentiality is defined as ensuring that information is accessible only to those authorized to have access. The communication between a reader and tags in RFID systems is not protected by secure mechanisms. Eavesdroppers may then obtain information during their communication. The data risk from a reader to tags means forward channel is higher than that from tags to the reader means backward channel since the different power ranges. The work power range in forward channel can be hundreds meters, but the range in backward channel usually is several mini meters. Tags memory can also read if there is no access limits [16].

Proposals for RFID security and privacy are categorised in two groups: one is for low-cost tags that cannot perform any computations, and the other is for higher capability tags (active tags) which are able to do some limited cryptographic operations [1]. We focus on the security and privacy of low-cost RFID systems in this paper.

The main challenge of low-cost RFID tags is that they are not able to process any kind of access control mechanisms on the data stored. This feature of the low-cost RFID tags provides a query response of any reader without authentication, and hence clandestine scanning of the tags is a possible threat. On the other hand, low-cost tags are normally deployed in a wide area. As a result of the deployment, private information may disclose through the tags they carry. For instance, tags on medicines may show what diseases a person has, and books include what are your interests. More ever, people never want to let others know the number and how much they have in their wallet, especially when walking alone in a street.

3. Security mechanisms

This section presents the existing mechanisms for security and privacy which include killing and sleeping tags in RFID systems and hash function engaged access methods.

Killing and sleeping

Customers security and privacy are protected if there is no response of tags carried by customers. The Kill idea of tags comes from this real truth [5]. For example, A RFID reader at a POS terminal can send a kill order to a RFID tag within the product customers bought, the kill order will change the tags state to be disable. To protect tags killed by unauthorized readers, such a command is authenticated by passwords.

Killing tags is an efficient solution to the security and privacy challenges: neither sensitive information nor private information tracking is possible. While killing approaches bring us a desirable solution, it also loses all the post-purchase benefits from RFID, for instance, returning a tag without any history. Furthermore, tags cannot be killed in some applications. A good example is the books in a library borrowed out which have to receive the information of tags again attached in the books during returning books. A solution to avoid losing the benefits is not killing tags but temporarily putting in disable state. Readers send a sleep command to tags rather than a Kill when tags are checked out. Tags cannot response during sleeping state including

stealthily read, but sleeping tags can come back if needed. Of course, all commands like kill, sleep, and wake up should be authenticated, for example using PIN. A question here is how to manage the authentication making an RFID system more efficient. It looks that customers can not remember too many PIN numbers which is an unrealistic requirement since we already have many accounts, and will have more tags in very soon future.

Hash-based access control

A simple secure scheme adopting one-way hash function is described in [16]. The tags in the scheme is hash-enabled with a portion of memory reserved for a temporary metaID and two locked or unlocked state. To lock a tag, a tag owner sends a hashed number to the tag as its metaID: metaID hash(key). This may occur either over the Radio Frequency channel or a physical contact channel. The owner stores both the key and metaID in a back-end database. The tags state is locked when a metaID is received, and its response to all queries is the metaID without other functionality. To unlock a tag, the owner has a searching of the appropriate key in the back-end database when he gets the metaID and delivers the key to the tag. The tag compares the value of hashed key to the stored metaID. It unlocks itself when the values match, and offers additional functionality to readers. This protocol is shown in Figure 2.

The proposed protocol is able to prevent unauthorised readers from receiving tag message due to the inverting difficulty of the hash function. Spoofing on the scheme is detected. An adversary can send a query for the metaID, and then spoof the tag to a authorised reader in a replay attack. The reader will send the key to the spoofed tag, but the reader may check the contents of the tag against the back-end application system to verify the responded contents and proper metaID. The adversary is detected since its response of the contents is failed.

This scheme requires implementing a hash function on the tag and managing keys on the application system. It may be economical in the near future since the computation and anergy cost is quite low. It is unknown if or not the hash function can be implemented with less resource than symmetric encryption algorithms. It may be not quite difference in the context of low-cost RFID tags. The minimal hardware complexity of a hash function remains a real open problem [8]. Unfortunately, tracking of individuals in the scheme is still existed since the metaID is a part of identifier, and the scheme is not suitable for large number of tags since the hash function operation in tags and the back-end system.

4. A randomized access protocol

In the hash-based access control scheme, a tag must not respond predictably to queries of unauthorized readers, but be identifiable by legitimate one. Additional operations are required to prevent the individual tracking. We present a new randomized access scheme to improve the hash-based scheme. The new scheme does not need a hash function to avoid the current RFID applications and individual tracing as well, furthermore, the new scheme can be applied for large number of tags. The basic ideas of the new scheme are to install a few random numbers to a tag when an RFID system is set up. Tags respond to reader queries by combining its ID and a random number r, and sending $ID \oplus r$ to a reader where r is randomly chosen from the stored random number. A legitimate reader identifies the tag by searching its ID database and the random numbers in the back-end application system until a match is found. The protocol is illustrated in Figure 3 and details are in protocol 1. The random number in the scheme makes the difficulty of inverting the real ID from $ID \oplus r$ even though it is revealed to an adversary. The tag's response is random and meaningless to anyone without the random number.

The protocol 1

Initinization:

The application system creates a unique identity for each tag and *n* random numbers r_1, r_2, ..., r_n. Each tag has its own identity and the *n* random numbers.

Procedures of identification:

1. Reader R sends queries to Tag;

2. Tag randomly selects a random number r_i ($i = 1, 2, ..., n$), and computes $ID \oplus r_i$;

3. Tag sends $ID \oplus r_i$ to R;

4. R does a searching in the back-end system for a match; and transmits $ID \oplus r_i$;

5. T unlocks itself if it receives $ID \oplus r_i$.

The proposed scheme does not have a hash function, but it still needs a lot of work on the searching of a large number tags in the back-end system. We present a classification of tags with proper prefix which will fast the searching. As we mentioned before, the forward channel from reader-to-tag is strong and easy attacked by unauthorized users who may derive the tag information. Assume all tags are classified with associate prefix, it means some tags share common ID prefix, such as a factory location or product code and class. The scheme does not broadcast insecure tag IDs on the forward channel, instead of, a reader broadcast a query including a certain prefix which means tags with the prefix only respond the query. The response is $ID \oplus r$ as we described before, and the prefix is excluded.

A long-range adversary can obtain the message through the forward channel but not the tag response in the backward channel which is only effect a short distance such as mm or even shorter. Tags in the RFID system are classified with prefix, legitimate readers can obtain the response of tags with the prefix. On the other hand, proper prefix may also be used to conceal the value of the portion of tags IDs. Assume two tags with ID values $b_1 b_2, b_1 \overline{b_2}$. A reader will receive b_1 from both tags without a collision, then detects on the next bit. The value b_1 is secret from long range eavesdroppers, the reader may send $b_1 \oplus b_2$ to simulate the desired tag without revealing any bit.

The extended scheme effectively protect against long range eavesdropper of the froward channel with little extra computation. Eavesdroppers within the range of the backward channel will obtain the response of $ID \oplus r$, but as we explain earlier, it is either useless since a random number is included inside.

5. Comparisons

The closed work to this paper are modest proposal for low-cost RFID systems for security and privacy [9] and YA-TRAP: a trivial RFID authentication protocol [14].

Ranasinghe et.al [9] proposed security mechanisms for low-cost RFID systems where re-encryption process based on public key encryption or private key encryption was used for a label authentication. The authors have also discussed both the framework of RFID systems and challenges in manufacturer and distributors, and the label was contributed to the security and privacy features. Their work is different from ours in several aspects. First, it focuses on challenges in manufacturer and distributors supporting the framework with labels of different tag classes. By contrast, our work has analysed the security and privacy issues in both passive and active tags RFID systems, and the computation and energy differences in these two tags systems. Second, the security mechanism proposed in their paper needs public key encryption or private key encryption in re-encryption process for label authentications. This is a high requirement for low-cost RFID systems since they have around 2000 gates computation for security. By contrast, we do not have this critical requirement in this paper. Instead of, a few random numbers r_1, r_2, ..., r_n are used in the new protocol for security and privacy which are more practical and significant for low-cost RFID systems. Third, they have not discussed if or not their proposal is suitable for a RFID system with large number tags, but the new protocol in this paper adopts the binary prefix supporting large number tags in RFID systems.

Tsudik [14] proposed a trivial RFID authentication protocol. The protocol involves minimal interaction between a tag and readers. Additionally, a single keyed hash function and pseudo-random function are performed in a tag. While Tsidik claimed that the hash function and pseudo-random function are simple techniques for inexpensive untraceable RFID tags, it is doubted whether these two functions work well for low-cost RFID systems. The major differences between their work and the work in this paper are in two aspects. First, each tag is equipped with a sufficiently strong, uniquely seeded pseudo-random number generator, and a keyed hash function. This assumption is reasonable for RFID systems with active tags with high costs or for future low-cost RFID system, but it may negatively effect the current low-cost RFID applications with the hash function engaged protocol since increasing 1000 gate counts in a tag will cost more 1 cent under current tag technology. By contrast, there is no hash function in our work nor a random generator function. Additionally, the designed protocol in this paper is able to apply for large number tags RFID systems, but the trivial RFID

authentication protocol did not analyse this scalable property for RFID systems.

6. Conclusions

We have discussed the security and privacy of RFID in this paper. RFID systems have been widely applied for a large number of applications associated to object identification. In the mean time, customers are beginning to worry about their security and privacy in the systems. This could be a big obstacle for a commercial application of RFID system, a number of security and privacy questions are still open due to the cost of tags. Although we still on the way to implement a 5-cent tag, a number of proposals exist even strict conditions, and most of them need hash functions which can only be used either future or a high cost. A protocol has been developed in this paper for low-cost RFID systems. The system is able to apply for a RFID system with a large number of tags and prevent long-range eavesdropper attacks, the individual tracking, and Tags in the system must not respond predictably to queries of unauthorized readers, but be identifiable by legitimate one. Binary operation only required in tags without hash function, the computation and energy cost of tags is very low and it is suitable for current applications such as privacy-enhancing identity management systems and commercial transactions without human intervention.

Acknowledgement

We would like to thank the reviewers' constructive comments on the paper.

References

[1] M. Felegyhazi and J.-P. Hubaux. Wireless Operators in a Shared Spectrum. In INFOCOM. http://infoscience.epfl.ch/search.py?recid=63742, 2006.

[2] K. Fishkin and J. Lundell. RFID in healthcare. RFID: Applications, Security, and privacy, pages 211–228, 2005.

[3] S. L. Garfinkel, A. Juels, and R. Pappu. RFID privacy: An overview of problems and proposed solutions. IEEE Security and Privacy, 03(3):34–43, 2005.

[4] A. Juels and J. Brainard. Soft blocking: Flexible blocker tags on the cheap. In WPES, 2004.

[5] A. Juels and R. Pappu. Squealing euros: Privacy protection in RFID-enabled ban-knotes. In R. N. Wright, editor, Financial Cryptography – FC'03, volume 2742 of Lecture Notes in Computer Science, pages 103–121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer-Verlag.

[6] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. In Consumer Privacy, citeseer.ist.psu.edu/juels03blocker.html, 2003.

[7] A. Juels, R. Rivest, and M. Szydlo. The blocker tag: Selective blocking of rfid tags for consumer privacy. In citeseer.ist.psu.edu/juels03blocker.html, 2003.

[8] M. Krause and S. Licks. On the minimal hardware complexity of pseudorandom function generators. In Theoretical aspects of computer science, volume 2010 of Lecture Notes in Computer Science, 2001.

[9] D. Ranasinghe, D. Engels, and P. Cole. Security and privacy: Modest proposals for low-cost rfid systems. In Theoretical aspects of computer science, volume 2010 of Lecture Notes in Computer Science, 2001.

[10] S. E. Sarma, S. A. Weis, and D. W. Engels. RFID Systems and Security and Privacy Implications. InWorkshop on Cryptographic Hardware and Embedded Systems, volume 2523 of Lecture Notes in Computer Science, pages 454–470, 2002.

[11] E. Schuster, S. Allen, and D. Brock. Global RFID: The Value of the EPCglobal Network for Supply Chain Management. Springer-Verlag, 2007.

[12] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh. An ultra small individual recognition security chip. IEEE Micro, 21(6):43–49, 2001.

[13] M. R. Travel. Preventing security and privacy attacks on. In citeseer.ist.psu.edu/742160.html, 2007.

[14] G. Tsudik. Ya-trap: Yet another trivial rfid authentication protocol. In Theoretical aspects of computer science, volume 2010 of Lecture Notes in Computer Science, 2001.

[15] S. Weis. Security and privacy in radio-frequency identification devices. Massachusetts Institute Technology, 2003.

[16] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Computing, volume 2802 of Lecture Notes in Computer Science, pages 201–212, 2004.

[17] S.-S. YEO and S. K. KIM. Scalable and flexible privacy protection scheme for rfid systems. 2nd European workshop on security in Ad-Hoc and sensor networks, 3813:153–163, 2005.