Privacy and Security Requirements for RFID Applications

Min-Shiang Hwang[1,*], Chia-Hui Wei[2], and Cheng-Yee Lee[1]

[1] Department of Management Information Systems

National Chung Hsing University

Taichung 407, Taiwan, R.O.C

mshwang@nchu.edu.tw

[2] Department of Computer Science

National Tsing Hua University

Hsinchu 300, Taiwan, R.O.C

chwei@cs.nthu.edu.tw

Received 5 April 2008; Revised 21 July 2009; Accepted 25 Aug. 2009

Abstract. This paper surveys recent technical researches on the problems of privacy and security for various applications in radio frequency identification (RFID). Most RFID system try to design a high level security, but not all of the RFID applications need it. The cost will increase if the privacy and security simultaneously improve, thus, how to balance the two issues are important. This paper provides an insight into the privacy and security requirements for RFID applications by the industrial processes. We will discuss and compare privacy and security in various cases. The results of our surveys are helpful for security engineers, who are responsible for the design and development in RFID.

Keywords: RFID, hash function, security, privacy

1 Introduction

The characteristic of RFID is small electronic component [13, 24], which can be embedded in any product. The RFID system has three different parts: the tag, the reader, and the backend database. The tag contains processing units, and limited memory, which can perform simple arithmetic operations. The tag transfers data through radio wave to the reader, and then the reader transfer data to the backend database. The backend database can authenticate whether the tag is legal or not.

The history of RFID began in approximately 1940s. At that time, RFID is used in World War Ⅱ, and it was acted as a "friend or foe transponder identification system" (IFF). After the 1970s, RFID was developed for commercial applications [9]. Recently, RFID is popular and widely used in various applications such as supply chain management, e-passports, door security control, luggage tracking, and automatic road tolls. As well known, the world's largest retailer Wal-Mart [9] announced that their products should be embedded RFID tags by 100 main suppliers at January 1, 2005. A global trade organization of air transport, the International Air Transport Association (IATA) [9], uses RFID to improve the baggage identification of the global airline industry. RFID is efficient and precise in identification for baggage or products. RFID has been applied to passports in UK [9] office in place of traditional paper passports, which can dramatically reduce the passport inspection time and offer passengers the ease in departure or entrance registration process. The identity and passport service of UK has now issued about eight million e-passports to UK citizens, which is a successful trial since 2007. In addition, RFID has been an implementation of Singapore's Electronic Road Toll Project [1] in 1998 and generated a 21-27 % reduction in traffic volume. Table 1 shows all information above.

With RFID progressing rapidly, many RFID related applications have been developed and used in our lives as describe in the last paragraph. The advantages of RFID are unique identification, small, and automation [18]. Beside, The cost down and time saving are mainly reasons for industry such as reduced employee costs, product transshipment reduction, inventory obsolescence reduction, and rich information exchange among participants in a supply chain [21]. The Above-mentioned are the advantages and the benefits of RFID, in a world where everyday objects are carrying RFID tags. Although RFID has many advantages and benefits, it still suffers sev-

* Correspondence author

eral challenges. The privacy and security are major issues [5]. Many researchers [2] have proposed various cryptographic operations in security mechanisms and attack models in order to protect the consumer and supplier. However, these proposed focus mainly on general cases but seldom consider about different industries. In this paper, we integrate and analyze security and attack conditions in RFID system in different cases.

The rest of this paper is organized as follows. In the following section, we describe current challenges in various cases of RFID system, and then discuss and compare privacy and security in RFID system in section 3. Concluding remarks are finally made in section 4.

Table 1. Various applications in RFID.

Company / Organization	Example	RFID application	Font size and style
Wal-Mart	Global retailer	RFID tags embedded to product	http://www.walmart.com/
The International Air Transport Association (IATA)	The trade organization of air transport	RFID tags embedded to luggage	http://www.iata.org/index.htm
UK home office	Government	RFID tags embedded to passport	http://www.homeoffice.gov.uk/
Singapore Government	Government	RFID tags embedded to card and automatic road toll	http://www.lta.gov.sg/motoring_matters/index_motoring_erp.htm
Intel	The semiconductor manufacturer	RFID tags embedded to semiconductor	http://www.intel.com/

2 RFID Applications in Various Cases

In this section, we review the literatures related to RFID in various applications. The various applications include: supply chain management, public transportation, and aviation or door security control with RFID system.

2.1 Supply Chain Management

Most products from the manufacturer to the end consumer require a complex and long procedure, which requires coordination, collaboration, and information exchanges among them to increase productivity and efficiency. Therefore Martinez-Sala et al. [11] proposed tracking of returnable packaging and transport units with active RFID in grocery supply chain. A simplified overview of this proposed procedure is shown in the following operations:

- *Manufacture:* The products are manufactured and packaged and then put on pallets and delivered on trucks when products are from the producer to the distribution warehouses.
- *Distribution warehouse:* The products are received from producer and then inventoried, stored and shipped when a retailer order is received. This stage is from distribution warehouses to retailer/supermarkets.
- *Retailer:* The products are inventoried again in batches and placed on display stands when the products are from retailers to consumers.

In traditional situation, intensive manual labor is required all over these steps for wrapping and removing, box inventorying and storing, arranging of display shelves as well as for recycling or collecting empty boxes. However, the traditional situation is not efficiency enough. This proposed focuses on the architecture and design on how to increase efficiency in transport units such as cases, boxes, pallets, and containers, which are managed worldwide with a limited or even with a lack of control and knowledge of their status on real time.

Another scenario is a more detailed procedure between the retailer and consumer, which includes four series of process by Liu et al. [10] as follows.

- *In-store stage:* The purpose of in-store stage is the ability to query products' locations and names in a retailer and then make an inventory regularly.
- *Checkout stage:* The checkout stage is used to query products' names and pay a bill when the consumer buys the products and then need the checkout.
- *Out-store stage:* After consumers buy the products and leave a retailer, the products still can be queried the products' names at home. If you have a smart machine for example, a smart refrigerator can soon know exactly what food contains through the tag, what you've already eaten today, and what food will run short. These smart refrigerators can query the tag by out-store protocol, which is skillful enough to know the state of the food in smart refrigerator.
- *Return stage:* The return stage will not be frequently used if after-care service seldom happens. Most stores have after-care service, which means they are willing to alter an exchange or refund unsatisfactory goods be-

cause they need to maintain the market by raising customers' satisfaction and, more important, their loyalty.

In most supply chain management, the RFID is attached in products such as those in Wal-Market; however, another special application is the global postal and courier service such as DHL Express [14][29], which needs supply chain management. Because the goods or letters come from all over the world, RFID system can improve the service and reduce the cost.

2.2 Transportation

There are multiple public transport offers that serve general users every day, which means people need many transport cards. Using an electronic ticket (e-ticket) [12] in multiple transport systems is easy and convenient. In Taiwan, passengers can purchase RFID card or purchase single journey tokens from the token vending machines in all stations, scan the RFID cards or tokens to enter a station, and exit at their destination station after the tokens were retrieved. Using e-tickets will make not worries for lost or stolen because they can be easily rebooked and available wherever the customer is located. Besides, RFID system can be used in the door security control in corporate and residential towers to identify guests and residents. Furthermore, prior to the 911 attack, passengers screening was solely a take of private enterprises; After the 911 attack, this responsibility of airport security was turned over to the government [19]. The aviation leadership, USA, and other countries recognize their need to take aviation security to a higher level. Therefore, aviation security management becomes an important issue. The aviation security includes:

- *Perimeter security:* They need cost-effective solution to control perimeter security and unique capability not only to detect an intrusion, but to deter, delay and defend the perimeter as well.
- *Passenger screening*: Millions of dollars of taxes have been spent on ensuring that passengers are screened properly in order to prevent unauthorized and dangerous items into the secure areas of the airport.
- *Carry-on baggage screening:* Baggage screening is an important measure to improve security when the issue of skyjacking is occurred. Make sure that mobile phones, keys, coins, and metallic decorative items are either placed in your carry-on baggage or in the small trays provided at the screening point. You should also remove your laptop computer from its case and place it in one of the trays provided.
- *Checked baggage screening:* To ensure checked items do not contain explosive materials or improvised explosive devices, your checked baggage may be screened in a number of ways, including:
  (1) X-ray examinations.
  (2) Testing for chemical residues using Explosive Trace Detection (ETD) equipments.
  (3) Physical searches.
- *Cargo screening:* There is a great risk of explosives or other types of incendiary devices making their way onto aircraft via the cargo holds. Most cargo screenings are done by private entities at warehouses and plants where goods are loaded into boxes. Transportation Security Administration (TSA) inspection teams will oversee the screening.

The aviation security has various security measures such as passenger's baggage tracking and screening, and an air line access controls etc. These technologies also include technician training and screener and supervisor training for: X-ray machines, carry-on baggage, checked baggage and cargos, primary and secondary walk-through metal detectors, explosive trace detectors (ETD), passenger passport/visa identification/verification systems, etc. The government tries to use security technologies biometric passports to enhance aviation security, but it is a controversial issue about privacy.

2.3 Other Cases

Family dogs and cats can even have RFID pet identification chips [17][27] implanted in them, so their owners don't worry about the pets' being lost. Besides, the primary goal of pervasive healthcare [7][22] is to be able to deliver necessary quality healthcare service anytime to anyone regardless of locations and other constraints. RFID tags are used in scenarios when an object needs to be identified, tracked, or when ambient condition surrounding an object is captured and stored among others.

3 Privacy and Security in RFID Applications

In this section, we review several threats to RFID applications and then discuss and compare privacy and security in RFID system.

3.1 Privacy and Security Threats

Many of us already use RFID tags routine, the RFID systems are convenient due to its fast speed in identifying an object, and therefore it become more and more popular in many industries. However, these functions result in many security and privacy problems. Previous studies [3] addressed several threats to RFID applications:

- *Cloning:* The attacker can read the tag and then clone the tag by writing all the obtained data into other tags because the tags are usually attached to the product within open environments such as supermarkets, hospitals, schools, and other public places.
- *Eavesdropping:* Eavesdropping on RFID readers is a major threat. The attacker surreptitiously listens to all the communications between the reader and the tag because they communicate via air such as radio frequency, which is easy to be sniffed or eavesdropped.
- *Replay attack:* The attacker repeats or delays the same message when valid data are transmitted. The adversary tries to intercepts the data and retransmits them, cheat or spoof the reader or the tag to obtain access data.
- *Denial of Service:* The attacker can send massive message to RFID system and attempt to crash the RFID system, which will result in the resource's unavailability to its intended users and the data's inconsistency to respond to other validity requirement.
- *Forward security:* The attacker can compromise a tag and obtain its current relation date such as resident data; they can trace back any of its previous conversation or shopping record.
- *Tag Tracing:* The tag always broadcasts a fixed serial number to somewhere nearby the reader; therefore, the adversary can identify a fixed serial number of the tag from different locations or transaction records.
- *Individual data privacy:* The attacker can know what items the consumer bought from the store or what books the consumer borrowed from the library by eavesdropping.
- *Data forging:* The attacker can modify the dates, items, and prices and then cause great loss if the tag can store extra data.

3.2 Comparison Privacy and Security in RFID Applications

As stated in Section 2, the various applications include: supply chain management, transportation, and other cases of RFID applications. In this section, we describe what requirements are concerned about privacy and security in other RFID applications.

According to Martinez-Sala et al. [11] and Liu et al.'s [10] proposed procedure; the supply chain management is separated to the supplier and the consumer. From the standpoint of a supplier, the tag tracing is the most important step in order to make inventory, but the RFID system still need to resist the tag cloning, replay attacks, data forging and denial of service. If the communication message is not encrypted, business spies or malicious employees can collect communication messages and then get the id and duplicate the tag. This situation lets the supplier believe that the product is still in list of inventory, however, the tag is a fake, and then the attacker can succeed in the tag cloning. Therefore, the tag cloning should be considered. Since the reader queries the tag in a new session, it is possible for any attacker to be authenticated as valid by replaying an old flow. This replay attack lets the reader believe that the tag is genuine. In addition, the attacker can simply drop or forge a last flow that is sent to the tag and result in desynchronizing the secret data which are shared between the tag and the server. This situation lets the database not find out the data due to the denial of service. From the standpoint of a consumer, individual data privacy and resistance of the tag tracing are major issues. However, only to resist tag tracing may not be enough to ensure privacy. The tracking of past events should be prevented namely forward security. Even if the attacker acquires the secret tag data stored in the tag, the attacker cannot trace back the data through past events in which the tag was involved.

As stated in Section 2.2, the e-ticket procedure is described. The e-tickets and e-passports should simultaneously satisfy some security and privacy as follows. The e-ticket needs to be proved by the reader that it is genuine; the reader also needs to be proved by the card that it is a genuine reader; this is called mutual authentication. E-ticket is desirable that all information exchanged between the card and the reader is protected against unauthorized eavesdropping and modification. Also, e-ticket needs to resist basic security such as the tag cloning, replay attacks, and denial of service. The door security application focuses on security the staff at many organizations has made the ability to program the RFID card at the door because it's critical to allow contract employees to enter a building, for example, they can only enter the building on the days they are authorized to be onside. The employee badges can be updated at the door without the employee being aware of the updated status or information which are now stored in the RFID card. The global postal and courier services and RFID pet chips have low privacy and security. A classification of privacy and security in RFID applications is shown in the Figure 1.

4. Conclusion

Although RFID applications have many advantages, it costs much to improve privacy and security at the same time. The cost sensitive has more concern rather than establish a high standard of security in development of RFID systems. At all above, we compare some various cases from different viewpoints in order to help security engineers, who are responsible for the design and development in RFID. These results are useful to improving RFID system.

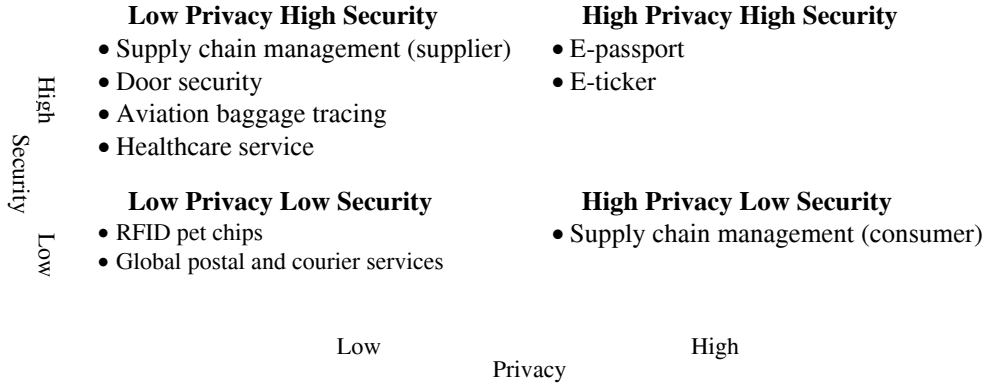

Fig. 1. A classification of privacy and security in RFID applications

References

[1] J. Ayoade, "Roadmap to Solving Security and Privacy Concerns in RFID Systems," *Computer Law & Security Report*, Vol. 23, No. 6, pp. 555-561, 2007.

[2] T. Cao and P. Shen," Cryptanalysis of Two RFID Authentication Protocols," *International Journal of Network Security*, Vol. 9, No. 1, pp. 95-100, 2009.

[3] Y. Chen, J.S. Chou, H.M. Sun, "A Novel Mutual Authentication Scheme based on Quadratic Residues for RFID Systems," *Computer Networks*, Vol. 52, No.12, pp. 2373-2380, 2008.

[4] J.H. Hoepman, E. Hubbers, B. Jacobs, M. Oostdijk, R.W. Schreur, "Crossing Borders: Security and Privacy Issues of the European e-Passport," *The First International Workshop on Security (IWSEC)*, *Lecture Notes in Computer Science* (LNCS), Vol. 4266, pp. 152-167, 2006.

[5] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Transactions on Selected Areas in Communications*, Vol. 24, No. 2, pp. 381-394, 2006.

[6] S.Y. Kang, D.G. Lee, I.Y. Lee, "A Study on Secure RFID Mutual Authentication Scheme in Pervasive Computing Environment," *Computer Communications*, Vol. 31, No. 18, pp. 4248-4254, 2008.

[7] J.E. Katz and R.E. Rice, "Public Views of Mobile Medical Devices and Services: A US National Survey of Consumer Sentiments towards RFID Healthcare Technology," *International Journal of Medical Informatics,* Vol. 78, No. 2, pp.104-114, 2009.

[8] V. Krotov and I. Junglas, "RFID as A Disruptive Innovation," *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 3, No. 2, pp. 44-59, 2008.

[9] J. Landt, "The History of RFID," *IEEE Communications Magazine,* Vol. 24, No. 4, pp. 8-11, 2005.

[10] A.X. Liu and L.A. Bailey, "PAP: A Privacy and Authentication Protocol for Passive RFID Tags," *Computer Communications*, Vol.32, No.7-10, pp.1194-1199, 2009.

[11] A.S. Martínez-Sala, E. Egea-López, F. García-Sánchez, J. García-Haro, "Tracking of Returnable Packaging and

Transport Units with Active RFID in the Grocery Supply Chain," *Computers in Industry*, Vol. 60, No. 3, pp. 161-171, 2009.

[12] K.E. Mayes, K. Markantonakis, G. Hancke, "Transport Ticketing Security and Fraud Controls," *Information Security Technical Report*, Vol.14, No. 2, pp. 87-95, July 2009.

[13] E.W.T. Ngai, T.C.E. Cheng, S. Au, K. Lai, "Mobile Commerce Integrated with RFID Technology in a Container Depot," *Decision Support Systems,* Vol. 43, pp. 62-76, 2007.

[14] Y. Park, J.K. Choi, A. Zhang, "Evaluating Competitiveness of Air Cargo Express Services," *Transportation Research Part E: Logistics and Transportation Review*, Vol. 45, No. 2, pp. 321-334, 2009.

[15] P.P. Lopez, T. Li, J.C.H. Castro, J.M.E. Tapiador, "Practical Attacks on A Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard," *Computer Communications*, Vol. 32, No. 7-10, pp.1185-1193, 2009.

[16] T.C. Poon, K.L. Choy, H.K.H. Chow, H.C.W. Lau, F.T.S. Chan, K.C. Ho, "A RFID Case-based Logistics Resource Management System for Managing Order-picking Operations in Warehouses," *Expert Systems with Applications*, Vol. 36, No. 4, pp. 8277-8301, 2009.

[17] M.R. Rieback, P.N.D. Simpson, B. Crispo, A.S. Tanenbaum, "RFID Malware: Design Principles and Examples," *Pervasive and Mobile Computing*, Vol. 2, No. 4, pp. 405-426, 2006.

[18] J.J. Roh, A. Kunnathur, M. Tarafdar, "Classification of RFID Adoption: An Expected Benefits Approach," *Information & Management*, Vol. 46, No. 6, pp. 357-363, July 2009.

[19] M. Stibbe, "Flight Paths to Security," *Infosecurity Today*, Vol. 2, No. 5, pp. 33-35, 2005.

[20] B. Sun, Y. Xiao, C.C. Li, H.H. Chen, T.A. Yang, "Security Co-existence of Wireless Sensor Networks and RFID for Pervasive Computing," *Computer Communications*, Vol. 31, No. 18, pp. 4294-4303, 2008.

[21] M. Tajima, "Strategic Value of RFID in Supply Chain Management," *Journal of Purchasing and Supply Management*, Vol. 13, No. 4, pp. 261-273, 2007.

[22] Y.J. Tu, W. Zhou, S. Piramuthu, "Identifying RFID-embedded Objects in Pervasive Healthcare Applications," *Decision Support Systems,* Vol. 46, No. 2, pp. 586-593, 2009.

[23] S.F. Tzeng, W.H. Chen, F.Y. Pai, "Evaluating the Business Value of RFID: Evidence from Five Case Studies," *International Journal of Production Economics*, Vol. 112, No. 2, pp. 601-613, 2008.

[24] L. Wang, Y. Lin, P.H. Lin, "Dynamic Mobile RFID-based Supply Chain Control and Management System in Construction," *Advanced Engineering Informatics,* Vol. 21, No. 4, pp. 377-390, 2007.

[25] S. Weis, "Security and Privacy in Radio frequency Identification Devices," *Master Thesis*, Massachusetts Inst. Of Technology (MIT), Massachusetts, USA, May 2003.

[26] S. Weis, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *The first International Conference Security in Pervasive Computing (SPC 2003)*, pp. 201-212, 2003.

[27] N.C. Wu, M.A. Nystrom, T.R. Lin, H.C. Yu, "Challenges to Global RFID Adoption," *Technovation*, Vol. 6, pp. 257-278, 2007.

[28] X. Zhang and B. King, "Security Requirements for RFID Computing Systems," *International Journal of Network Security*, Vol. 6, No. 2, pp. 214-226, 2008.

[29] X.d. Zhang, S.J. Yue, W.M. Wang, "The Review of RFID Applications in Global Postal and Courier Services," *The Journal of China Universities of Posts and Telecommunications*, Vol. 13, No. 4, pp. 106-110, 2006.

[30] Wal-Mart, [online] Available: http://www.walmart.com/

[31] The International Air Transport Association (IATA), [online] Available: http://www.iata.org/index.htm

[32] UK home office, [online] Available: http://www.homeoffice.gov.uk/

[33] Singapore Government, [online] Available: http://www.lta.gov.sg/motoring_matters/index_motoring_erp.htm