The Study on RFID Security Method for Entrance Guard System

Y.C. Hung[1] , C.W. Tsai[2] , C.H. Hong[3]
[1]Andrew@mail.ncyu.edu.tw [2]s0930316@mail.ncyu.edu.tw [3]chhong@csie.ncyu.edu.tw

Abstract: The RFID technology has been used by industries in recent years, for examples, replacing the traditional two-dimensional barcode, logistics management, military applications, identification. In fact, RFID technology has become one of the new killer technologies. The RFID uses radio frequency to convey information which involves, however, many security problems; Current RFID guidelines do not present solutions to these security problems. The methods put forward in published paper fail to offer complete solutions, either. This study identifies RFID security method for Entrance Guard system. The algorithms used include Hash, AES, random values, XOR four item technology, and use the three-way authentication structure to solve the safety problems of the certification of Entrance Guard system. The experiment showed the algorithms provided better protection on the current RFID systems against attack methods such as Eavesdropping, Traceability, Spoofing and Replay attacking.

Keywords: RFID , RFID Smart card , AES , HASH.

I. Introduction

Since World War II, RFID technology which was used for identifying enemy's or our flights has been over 60-year evolution. Now, in the big enterprises with over 5 billion US dollars annual sale worldwide, 70% of them has create RFID technology plan. This shows RFID technology has drawn the attention from general merchandise, retail business, government, storehouse industry, and so on, so RFID technology has just become the application in the top class of the new generation. Apart from being used on the logistics management, another application of RFID is to insert RFID tag into Smart IC card. This type of application is quite extensive, for example, Taipei MRT pass card, identification card of entrance security of multi-storey buildings, work ID from government and schools, student ID, and so forth. Through RFID wireless transmission and features of non-contact, the original issues of inconvenience and fabrication on the use of contact smart card. However, due to the RFID using wireless frequency to communicate and carry information as well, its new security issue has also gradually appeared. In additional, the issue of RFID system security has not yet been fully regulated in the book of national normal standard, so this issue is quite controversial.

In this study, RFID tag frequency is 13.56MHz, and according to ISO/IEC18000-3, it belongs to Passive Tag. There is no place for batteries in the tag, and the size is restricted, so the ability of calculation for the tag is limited with the small capacity of the memory. Therefore, the use of traditional encryption calculation and authentication mechanism cannot be applied. For this reason, it is hoped to use four technologies such as Hash, AES, Random values, and XOR with the combination of the 3-side authentication framework to bring up less calculation and high security identification mechanism to RFID smart card which is hardware restricted, for solving the security concern of the current use of RFID smart card identification and entrance guard system. Besides, with the difference of general security identification mechanism, this study has been added in active defence mechanism, for further enhancing the security of system, and reducing the opportunity of the data in RFID smart card to be eavesdropping,spoofing, traceability.

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 1 - 6.

II. Background Knowledge

II. 1 RFID

RFID stands for "Radio Frequency Identification" system, and it is similar to Smart card system. It is developed due to the defect of contact system by using radio frequency and carrying digital data, so the identification card and card reader do not need to contact each other but complete the exchange of data. Consequently, there is no requirement of direction under this way of carrying data, and the card could be immediately identified when it is put in the bag or purse. It's a chip of mini two-sided radio waves with card-pasted style, and only uses two connected point to connect one simple IC to another antenna, so the installation of receiving signal could be done. When the question of the electromagnetic remote wave was sent out, the card could right away to answer the required information by digital radio frequency signal, while RFID is composed of 4 parts, such as RFID tag, RFID reader, Backend database, frequency radio.[1][2]

(1) RFID tag

It is pasted or inserted to merchandise, goods, RF chips in smart card, and the main structure includes CLK circuit, AC to DC commutation wave filter, demod, codec, ip, memory.

RFID tag can be divided into two different types, active and passive:

◎ Active Tag

With one build-in small battery, the capacity of memory could reach 1MB, and there is longer radio communication distance (100 meters) by using communication, but there is limitation of deadline which is about 7 to 10 years, so the

cost is relatively high.

◎ Passive Tag

No build-in batteries, the coil inside the tag could send electric field out by readers to get energy. Due to the use of electromagnetic induction, the communication distance is short, and the cost is lower, small size, long duration with more competitive ability, so it highly possible to become the mainstream of market. There is a comparison between active and passive RFID tag in table 2-1 below.

Table 2-1 The comparison of tags

	Active	Passive
Power installation	Build-in	No Build-in
Valid period for use	Yes	No
Environment Condition	More Sensitive to high and low temperature	Can adapt to worse environment
Price	higher	Lower

(2) RFID reader

Reading, receiving past or inserting merchandize, goods, receiver of RF tag in the smart card. The main structure concludes: PLL, VCO, Demod, Codec, uP, Memory, time record generator. RFID reader can use antenna to read and write. Different RFID system has different type of antenna. For example, the reader in the entrance of supermarket: because the goods carried in different height, the antenna could be high as a person's height. The antenna do not need to activate tag anytime, but activate the transmission by cooperate the sensor in the food pad. Readers can be divided into two types: fixed and portable. The former can be place in the entrance of the supermarket, good shelves, warehouse entrance, wagons, container yard entrance, airport, and so on. The latter one is much lighter, with direction and shorter distance of interaction.

(3) Back-end database

The main function is to record details of the RF tag, when the reader received RF tag signal, it will link either by wireless or wire network to back-end database, to get the integration of details of RF tag for other application to use.

(4) Frequency radio

The frequency of RFID is to link the information transmission between tag and card readers. The frequency is sent from card readers out to tag, and the tag returns the information inside the tag. The option of frequency is mainly based on the distance between RF reader and RF tag. A lower frequency means a lower range of reading, and slower information transmission. But in the metal and humid environment, high frequency relatively has better reading ability. Besides, it depends on the frequency opened by each country. Every country uses different frequency. Generally speaking, the information transmission and communication frequency between FR readers with low frequency and RF tag are not controlled by government, but the ultra high frequency would be restricted. Take Japanese government as an example, the frequency of 950~960 MHz has been decided to open for RFID system to use. RFID system could be categorized by frequency into four: Low Frequency (LF,125KHz ~ 135 KHz), High Frequency (HF,13.56 MHz),Ultra High Frequency (UHF , 100MHz~960MHz), Microwave(over 1GHz).

II. 2 RFID Security Issue

RFID system carry information by wireless, so if RFID system does not provide complete security mechanism, then within the available range of information transmission, the attackers can randomly access, falsify, delete, and damage the information of RFID tag. This weakness has obviously threatened the organization, enterprises, personal information security and privacy. In the following text, the weakness of RFID used by attackers and may cause security problem attackers will be indicated.

A. Eavesdropping

Because RFID system uses wireless to transmit information and communication, the attackers could eavesdrop the information and message during the communication between reader and tag. So the way of this type of attack is called "Eavesdropping". In the transmission of RFID system, it can be roughly divided into reader-to-tag(forward channel) and tag- to-reader(backward channel). Forward channel came from reader, so the distance is long and the range is big (100meter), so it is easily to be eavesdropped without being noticed easily. Backward channel came from tag, so the distance is short, and the range is smaller, so it's more difficult to be eavesdropped without being noticed easily. As Figure 2-1 shown:

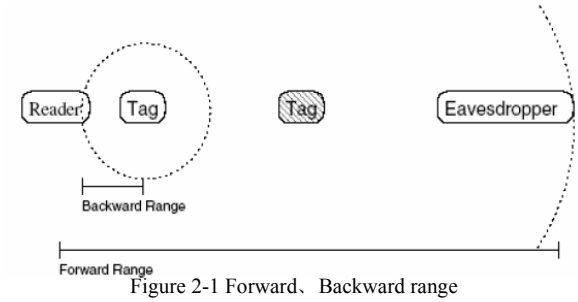

Figure 2-1 Forward、Backward range

The security issue of eavesdropping will cause two serious damages: the exposedness of personal information and business spy.

(1) The exposedness of personal information

In the aspect of the exposedness of personal information, this has been widely used in RFID smart card which save card holder's personal information. For example, health insurance card stores medical record, personal information,

and so on. For they are the information that card holder would not want to make known to the public, and necessary to be protected. However, because RFID system belongs to non-contact card, so the opportunity of being exposed is relatively higher.

(2) Business spy behavior

Nowadays, the industry of manufacture, logistics, retail, and military institute give every effort to popularize the use of RFID system, and RFID relatively brings quite a lot of benefit, convenience. However, under the tendency of RFID, the issue hidden behind would be monitored by attackers, the risk of being stole on information. RFID system could make the factory owners use the information stored in the tag memory to quickly get product name, model number, material, logistics procedure, and so on; on the contrary, the attackers could also get and monitor the product information in the same way. Therefore, the activity of business spy would become worse, and then lead to serious consequence if there is no further prevention of security mechanism.

B. Traceability

In RFID system, RFID reader could get the information and trace product through the returned message RF tag. It is also this feature that attackers could trace product and users through the returned message from FR tag, so it is called "Traceability". The main reason that attackers could trace tag is because normally the returned value from tag is fixed and unchanged. Some tag returns UID value directly, and this UID is also the unique identification value of RF tag. Therefore, attackers only have to set readers in many fixed point, then they could trace products and users. For example, sneaker factory owners want to carry out logistics and storehouse management, so they insert RF tag chip into shoes, and when customer A bought this shoes, then attackers could trace the customer A through the fixed RFID reader and make customer A's privacy public.

C. Spoofing

After the introduction of two security RFID issues of eavesdropping and trace, another issue is "Spoofing" which includes two major items: Theft and Counterfeiting.

(1) Theft

Through deceiving legal RF tag, attackers could deceive automatic book close system, entrance guard security system by RFID system features. For example, attackers could rewrite RF tag information or replace the RF tag information inside expensive goods with that inside the cheaper ones. Or attackers could falsify a host of RF tag to mess up the whole management of the supply chain.

(2) Counterfeiting

Counterfeiting is defined as can be read or intercepted to falsify the information of RF tag. Attackers could deceive RFID system through falsifying RF tag information. For example, they could forge IC card of entrance to invade company or military institute.

II. 3 RFID Existing Security Strategy

The solution of this RFID security issue could be divided into two categories: Non-Cryptographic Scheme and Cryptographic Scheme. There will be a brief description of several important solution: "Kill tag approach" in "non-Crypto-graphic scheme" and Hash based access control, Randomized access control, Hash chain in "cryptographic scheme". [3][4][5][6][7][8]

A. Kill tag approach

In order to prevent the occurrence of security issue when users get RF tag, the solution is to delete its memory information before they get it. The way is to put one 8-bit password in every RF tag, and then run "Kill" command. However, there are two problems existing in "Kill tag approach". One is the support from the manufacturing factory is required, and the other one is that to ensure the Kill command has been actually executed is difficult.

B. Rewriteable memory

Separating memory in RF tag into ROM and RAM, ROM can store public information, and RAM can store private information. Readers have to be authenticated before accessing RAM, with the implement of cryptographic scheme.

C. Hash based access control

Irreversibility of Hash is mainly to be used for authentication. Its structure is as Figure 2-2 shown:

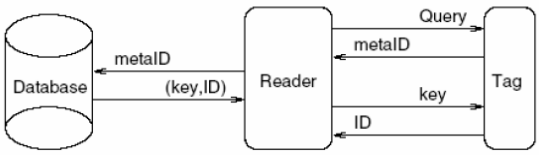

Figure 2-2 Hash based access control

In RF tag, metaID (metaID = has (key)) will be stored firstly. When readers query RF tag, RF tag would return metaID, and reader can search the back database to find the matched key value to complete authentication. This method could solve the problem of RF tag information being eavesdropped, but because the returned metaID value from RF tag is fixed, so it cannot prevent attacker's trace.

D. Randomized access control

This method is used to improve the issue of Hash based access control to be traced. Adding one random value R in the returned value, so the returned value that reader queried could be changed. Its returned value is $\{R, h(ID_k \| R)\}$ and the structure is as followed in Figure 2-3:

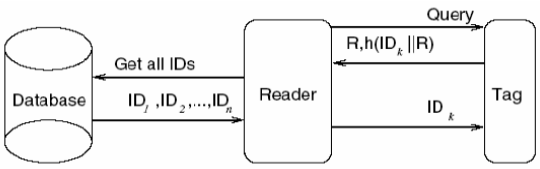

Figure2-3 Randomized access control

E. Hash chain

In RF tag, storing on initial value s(s1), and the way of communication with readers is similar. Only the returned value changed to $a_i = G(s_i)$, and after responding to readers, it would immediately changed to $s_i+1=H(s_i)$ where G、H are hash function. Its structure is as followed in Figure 2-4:

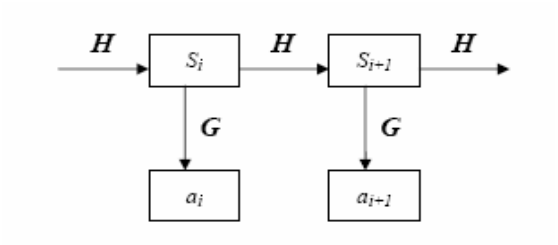

Figure 2-4 Hash chain

III. System Structure

III. 1 System Introduction

In current entrance guard systems, most of them use RFID smart card for user identification. This RFID technology gives the convenience and speed for identification check but this convenience also relatively generates the security issues. In this research, we provides a symmetrical encryption method (AES, HASH, Random value) and three-sides identification in the entrance guard security system structure of RFID smart IC card. This system structure not only protects the user information privacy, counterfeit prevention, and identity theft, but also protects the card holder to be traced. Besides, different from other security system structure with focus on the passive security shield, this system also provides active detection for smart IC Card security. After the card is attacked, the system will automatically turn on the reaction procedure to increase the security level on information and privacy protection. The system structure is depicted as Figure 3-1.

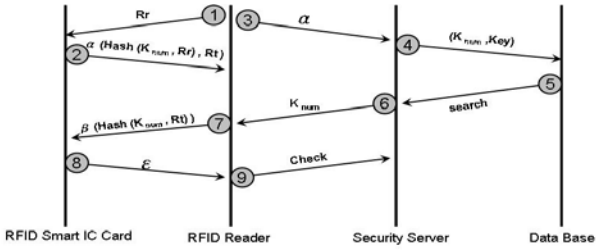

Figure 3-1 System Framework

The RFID smart IC card discussed in this research is the RF tag with frequency at 13.56Mhz. So the standard from ISO / IEC 18000 specifications should be followed. As a result, there will be some limitations for the hardware. In this research, we will embed a hash calculator, random generator and several logic gates in the RF tag, which will not violate the hardware limitation rules from the specifications. Before introducing the system structure flowchart, we can define the database structure saved inside the RF tag and security system database. {S_ count , Key $_{num}$, P_k (Data)} is the database structure in RF tag. S_ count records the scan counts for this RFID smart IC card by RFID reader. K_{num} is the identification serial number of the user data encryption key in this RFID smart IC card. P_k (Data) is the encryption code of card holder information encrypted by the K_{num} key. There are {K_{num} ,Key_i} and {ID , S_C_count} in the structure of security system database, in which Key_i is one of the key used in system encryption, K_{num} is the corresponding identification serial number for Key_i, ID is the user identification code and S_C_count is the identification number of times between the record system and card holder. The system data structure is depicted as Figure 3-2 in below.

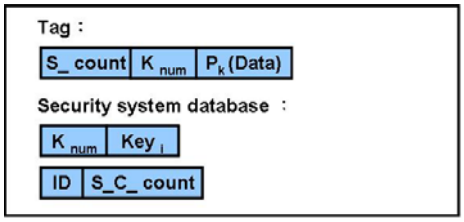

Figure.3-2 Data Structure

System flow

Here we will categorize in nine steps to explain the system flow structure from Fig3-1.

(1) When the card holder use RFID smart card to precede the identity confirmation, RFID reader will generate question message to the RFID smart card after the card holder puts the card within the save and read range of RFID reader. This question message includes Rr value, which is a 128bit random value generated by the reader.

(2) When RFID smart IC card is inside the reader sensor region, it will add the S_count value in the RF tag by the power from electromagnetic induction. Then it will generate α message as reply from the equation $\alpha=\{F_t(K_{num}, Rr)\| Rt\}$. Ft is a hash function embedded inside the tag and Rt is the random number generated by the random code generator. The transfer format of question message from RFID reader and α message replied by IC card will use the standard of communication structure defined in ISO/IEC 18000-3 specification book, as illustrated in Figure3-3 and Figure3-4.

SOF	Flags	Com code	IC Mfg	UID	Signed data Rr	CRC	EOF
	8 bit	8 bit	8 bit	64 bit	128 bit	16 bit	

Figure 3-3 Query message

SOF	Flags	UID	Signed data α	CRC	EOF
	8 bit	64 bit	128 bit	16 bit	

Figure 3-4αmessage

(3) RFID reader gets the α value and sends it back to the backend system for identification comparison.

(4) Security system searches the saved K_{num} in the backend database then it will compares $F_r(K_j, Rr)$ and α value.

(5)The system will send the Key_i and K_i, which are generated from the IC card of the card holder, back to the system. After full search in all K_{num}, the system will send back error message if it cannot find the matched K_i.

(6) RFID reader will send βmessage in order to get the card holder information from RFID smart IC card, in which $\beta=F_r(K_i, Rt)$.

(7) After RF tag confirms β message, it will try to compare to see if K_i and K_{num} are the same.

(8) Make sure β message is correct, feedback ε from $\varepsilon=(P_k(Data) \| S\_count) \oplus F_t(Rr)$.

(9) RFID reader will process the identification procedure though the Key_i、Rr、S_C_count value from the card holder. The identification process will get P_k (Data) || S_count from Fr(Rr) ⊕ε and then use the key to get the value of P_k (Data).

The 9 steps in above is the passive mode processing steps for security identification system. However, we also mentioned the active mode security identification system. The procedure will be addressed in below. According to the real needs, the system will define two security entrance guard values (T1 and T2). From the security identification step (9), the security system will get the S_count value from the εmessage. After the calculation of S_count and S_C_count difference value (n), it will compare the n value with the entrance guard value defined by the system. If n is larger than T1, the system will warn the card holder and inform that the card might be attacked. If n is larger than T2, the system will lock this RFID smart IC card and request the card holder to activate the card from the IT department. The security system administrator will use different key for encryption and change K_{num} value for card holder's personal information. By this method, the system will be able to perform the active security shield to enhance the security in the identification system.

III. 2 Security Analysis

In the second chapter, we have discussed the security problems in the RFID system. In this section, we will do the security analysis for the security identification process from the security problem in the RFID system in order to proof the security structure in this system. In this research, we assume that RFID reader, backend data transfer and communication are all inside a safe environment. Therefore, the research will not cover the discussion in security topics in RFID reader and backend data transfer connection line.

A. Eavesdrop

From the transfer structure inside this system, the data transfer (See Fig 3-1, step 8) in this identification process of RFID smart IC card and RFID reader (See Fig 3-1, step 1, 2 and 7) is protected from the hash function encryption. The hash function contains irreversibility which means that the attacker could not reproduce the original message even though thos message was eavesdropped by the attacker. Besides, two random numbers (Rr and Rt) are used in this identification process which offers different message for each identification process to increase the difficulty of force methods by the attacker. During the information transmission from the card holder, the system will send the information after the data process with $F_t(Rr)$ in xor calculation. The card holder's information was encrypted and saved in the RF tag memory. Though the attacker uses the stole Rr value to calculate $F_t(Rr)$ value and crack the xor calculation protection, the cost and time will be increased for attacker to crack and get the encrypted P_k (Data) based on several different encryption key used by the system. For example, it will cost 2^{128} to crack the information from 128bits key with AES encrypted calculation. If the key number is 2^5 , the cost will increase to 2^{640} for crack. Therefore, the attacker will not be able to steal the P_k (Data) value to solve the private information from the card holder.

B. Spoofing

In the entrance guard security system, the reproduction and theft of identification IC Card is a serious security topic. In this system, the attacker is able to get the P_k (Data|| S_count) *xor* $F_t(Rr)$ value by eavesdrop. If the attacker is able to analyze the interpreted P_k (Data) value to reproduce IC Card and deceive the security system, the identification procedure is required before the personal information check by the security system. At this time, the attacker must also hold this K_{num} value of the RFID smart IC card together to pass the identification procedure to the check process. However, the K_{num} value will be encrypted with hash function and random value in the transfer process. The attacker will not be able to get the K_{num} value by eavesdrop and to reach the goal of deceiving ssytem with P_k (Data) value.

C. Traceability

In traditional RFID system, the attacker could trace the

card holder from the fixed replied message from the attacker reader's quote only by couple fix location RFID reader via the RF tag chip embedded inside the card holder's RFID smart IC card. In the security system discussed in this research, the message value from each communication transfer between the whole RF tag and RFID reader is not a fixed value due to the extra embedded hash calculator and random value generator inside the RF tag (See Fig 3-1, Step 1, 2, 4, 7, and 8). Therefore, the attacker will not be able to trace RF tag from the fix reply message.

D. Man-in-the middle attack

If the attack is sent after reproduction of legally obtained RFID reader and RF tag message, the attacker could get (P_k (Data) || S_count) $\oplus$ F_t(Rr) value after performing Man-in-the middle attack. However, the attacker still encounters the same difficulty in the spoofing attack as discribed above. The attacker has to cract two encryption procedure to obtain the card holder private information. So this security system structure is able to prevent Man-in-the middle attack.

E. Replay attack

If the identification is not passed either in security system side or RF tag side, the system will stop the reply message immediately. Besides, the system uses two random numbers and active security shield mode so that resending attack is not able to attack the system.

F. Active reaction procedure

Different than other security system, we added two calculated value (S_ count、S_C_ count) and two security entrance guard values (T1、T2) in the RF tag memory. If the attacker's RFID reader attemps to save and get this RFID smart IC card, S_ count and S_C_ count will generate difference once the identification process is failed. If the identification process is finished from the legal RFID reader, the system will get the information inside the RF tag memory and compare the difference between S_ count and S_C_ count value. If the difference of S_ count and S_C_ count is larger than T1, the system will warn the card holder that the card might be attacked. If the differnece is larger than T2, the system will request the card holder to the security department to update the information inside the IC card. Different keys are used to re-encrypt the private information and modify the K_{num} value to ensure the system security and card holder's privacy. The reason to use this two stage entrance guard value is due to some unexpected issue in transfer and communication failure between RFID smart IC card and RFID reader, such as the high humidity in the rainy days or RFID smart IC card was placed inside the metallic box etc. Therefore, two entrance guard values are used to prevent these unexpectable reasons from the inconvenience of frequent changing card information.

IV. Conclusion

The development of RFID technology brings significant convenience to people but its security is also a big drawback. Without providing solutions, it will seriously affect the information security from personnel, company, military to government. This research provides an identification system for RFID smart card entrance guard system with Hash, AES, Random values and XOR technologies. Combined the identification from three sides, the goal is to resolve the security issues for RFID smart card, such as eavesdrop, traceability and counterfeit etc. In addition, the embedded RF tag hardware also meets ISO/IEO 18000-3 standard to proof the execution posibility. Besides, the active shield system was added in the structure to enhance the strength of the security systems to prevent the potential danger of system failuer from the attacker by resending attacks or Dos attacks to the system.

References

[1]. Flor, T.; Niess, W.; Vogler ,"RFID: the integration of contactless identification technology and mobile computing", *ConTEL 2003*, 2003, 2 , 11-13.

[2]. Juels and R. Pappu, , "Squealing euros: Privacy protection in RFID-enabled banknotes", *In proceedings of Financial Cryptography*, 2003, 103-121.

[3]. Juels, R. L. Rivest and M. Szydlo,, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", *In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security*, 2003, 103-111.

[4]. M. Ohkubo, K. Suzki and S. Kinoshita,"Cryptographic Approach to 'Privacy Friendly' Tags", *Nippon Telegraph and Telephone*, 2003.

[5]. Martin Feldhofer," An Authentication Protocol in a Security Layer for RFID Smart Tags",*IEEE Melecon*, 2004.

[6]. S. Weis, "Security and Privacy in Radio-Frequency Identification Devices", *Masters Thesis*, 2003.

[7]. S. A. Weis, S. E. Sarma, R. L. Riovest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Security in Pervasive Computing 2003*, 2003, 201–212.

[8]. Xingxin Gao, Zhe Xiang;,Hao Wang;,Jun Shen; Jian Huang, Song Song ,"An Approach to Security and Privacy of RFID System for Supply Chain", *IEEE International Conference* , 2004, 13-15.