The implementation of the passive RFID for door access control using cryptography method

Kuo-An Hwang
Professor, Department of Computer Science and Information Engineering & Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology
kahwang@cyut.edu.tw

Chen-Chun Hsu
Graduate student, Department of Computer Science and Information Engineering, Chaoyang University of Technology
s9527637@cyut.edu.tw

Chia-Hao Yang
Graduate Institute of Informatics, Doctoral program, Chaoyang University of Technology
s9433901@cyut.edu.tw

摘要

近年來台灣社會發展進步，犯罪總數與人數居高不下。尤其跟社會大眾最息息相關的居家安全便成為很熱門的研究議題，多數的門禁系統認證都以靜態的編碼系統為主，缺乏安全性，擁有容易遭到竊盜的風險。本研究利用被動式無線射頻辨識（Passive Radio Frequency Identification, RFID）技術應用在門禁控制上，提出在 RFID ISO 15963 被動式標籤使用動態性密碼防範風險，並且做到單張標籤能夠開啟多扇門的多重效益。當使用者利用標籤對門禁系統做出存取要求時，進一步驗證標籤的合法性，再加入一次性動態密碼保護標籤，避免竊取、側錄等情形發生，加強現有被動式 RFID 門禁系統保全。

關鍵詞：一次性動態密碼，無線射頻辨識，門禁控制。

Abstract

Recently, as social development in Taiwan progresses, the number of crimes and criminals has reached a relatively high level. Public-related home security has becomes a popular issue to be studied. Most of the access control systems mainly use a static encryption system which lacks the security and suffers from stealth by being cracked. In this paper, a passive radio frequency identification (RFID) technology is used on door access control. A RFID ISO 15963 passive tag with dynamic password avoids the risk by having the advantage of accessing multiple doors with only one single tag. When the user uses the tag to make acquisition to the access control system, an additional tag verification is performed to assure the authentication, and then a one-time dynamic password protects the tag from being stolen or tapped, thus the security of the existing passive RFID access system may be enhanced.

Keywords: One-time dynamic password, radio frequency identification, access control.

1. Introduction

In view of the number of crimes and criminals remians at a high level in Taiwan. In recent years statistics of the stealth crimes in figure 1. The total number of burglary crimes was 281,561 and number of criminals was 39,927 in Taiwan in 2006 [11]. Home security is closely related with the community and becomes a popular issue. According to the studies, there were many stealth crimes commited by non-violent burglary break-in (46%) and violent burglary (77%), thus a secure door access control identification system is an indispensible safeguard for the personal safety and property security[10].

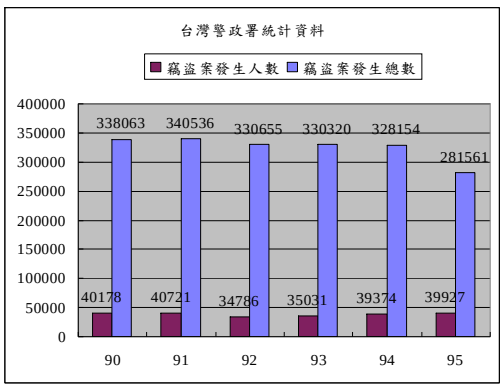

Fig. 1. Statistics of the stealth crimes

As a result, many research studies have focused on the issue of door access control.

Conventional door access security systems usually use more passive approaches, which are outdated for modern people pursuing innovative technologies. For frequently accessed doors (such as the doors of offices, hotel rooms, etc), the management of the keys is inconvenient. If a key is lost or the personnel are replaced, the locks and the keys must be replaced as well. In order to solve such a problem, new types of door locks, such as electronic locks with magnetic cards, password locks, etc. had invented. With the prevalence of the equipment, the door access management entered the electronic era. As the continuous development and application of these two electronic locks, their own disadvantages were gradually exposed. For example, private information was easily duplicated, the wear between the card and reader was high, and the malfunction rate was high, so the resulting security coefficient was low, etc.

Password access is the most prevalent identification method while the user login. However, for the systems with such an identification method, many non-secure factors are generated such that the systems are easily damaged and user information would be stolen by hacking [7]. If one wants to reduce the risk resulting from the password access system, it will be restricted often by many external complicating factors of the door access system. This phenomenon implies that the encryption technology of the existing door access system should be improved, such as the equipment exposure, convenience, etc. If it is required to reduce the risk resulted from the non-secure password system as much as possible, the most efficient way is to substitute the dynamic password for the conventional fixed password access.

In this research, the main objective is to propose a passive RFID technology [3] with an additional one-time dynamic password technology and then discuss the improvement of the passivity, non-flexibility, etc. of the conventional security equipment. By the using of RFID tag with a lower cost, i.e., the ISO 15693 cards, the burglar-proof security and the convenience for daily use of the door access system may be improved without changing protocol.

2. Related Background

2.1 Conventional door access technology and its related studies

Among conventional door access systems, the most popular systems may be divided into two categories [6], the contract type and the non-contact type door access systems. The contact type door access system need to use a card reader or enter a password along with the key to open the door. While the non-contact type system is the more popular door access system that uses the IrDA or RF remote control [5] along with a key to open the door. These systems do not support remote door opening and access monitoring functions. Thus, the above mentioned conventional door access systems lack a display for showing the user interface and may be restricted in terms of distance, angle, and penetration [2].

Graafstra [4], who needed to keep the keys for 100 different doors handy due to the requirement of working and proposed an RFID glass electronic tag. It is a passive electronic tag that does not require batteries, thus it is convenient for use to the door access control systems and transportation vehicles. However, a professional surgeon is required to implant the tag under the skin.

Masaki [9] proposed a new home security system that uses active RFID Tag and dynamic sensing technology to simulate the actions of an intruder, and the corresponding reaction alarm system was designed for these actions.

2.2 RFID encoding technology and related studies

Passive RFID systems are suitable to be incorporated in the door access system because they are compact and portable. However, the passive tag suffers from a weak verification problem, thus it is insufficient in terms of information protection. In addition, there are two very serious obstacles must be solved, one is security and the other is privacy. The conventional verification approach relies on the cryptography. The concept of the cryptography is based on the hiding of conflicts. His idea came from a group of randomly obtained and easily memorized numbers. As a result, many researchers started to study secure cryptography technology.

Sarma [12] proposed the public key encryption method. Each tag would have a dedicated public key for the vendor¡s unique reader, and a private key. The verification between the reader and the tag can be performed by the challenge¡ response technology. However, in the public key cryptography method, the RFID tag must have a powerful computation capability to perform the intensive and complicated operations. Thus, the existing RFID

tag for the door access system is not capable of performing in such a computation operation.

Wong [14] proposed a heuristic Jigsaw encoding method that converts a valid EPC code into a pseudo-EPC code. Such an encryption mechanism can protect the EPC information on the tag and identify the tags clone. Meanwhile, attacker may not be able to reverse it into a valid EPC code in a short period of time that appears to be useless in Hong Kong. Theoretically, the tags do not have directivity. However, the stability and the correctness for detecting the product should be re-evaluated and improved.

Weis [13] proposed to add an additional pseudo-random number into the randomized hash lock of the tag. When the reader sends out the inquiry, the tag will feed back a pair of numbers (r, hash (ID_K \\ r)), r is a random number that generated by the tag, while the other is a calculated hash value and based on the ID number of the tag ID_K in series of r. After the reader receives the pair of numbers, it will identify the tag k in it's tag ID list. The reader will figure out the ID_K of the tag for the unlocking of the door. The output value of the tag will be different for each access. Thus it can provide secure position privacy and avoid tapping or tracing.

2.3 One-time password algorithm related studies

Long [8] proposed a MOTP system architecture. The user provides a unique password to the MOTP module, the module will feed back a specific one-time password for verification through the web browser and web server.

Pseudo-random number is based on the priciple that used an artificially known series. It requires two vital statistical properties, uniformity and independence. Meanwhile it should conform to the following tagets; exactness, numerical stability, efficiency, robustness, and ease of implementation [1]. The above conditions are suitable as the encryption to be applied to the door access. One of them is called prime modulus multiplicative linear congruential method (PMMLCG), its equation is as follows:

$$y_{i+1} = [a \times y_i + c] \quad mod\ m \quad \text{----------(1)}$$

where m>0 (m is called the modulos), 0≦ c <m, (c is called the imcrement), 0≦ a <m (a is called the multiplier) and 0≦ y_i <m, (y is called the initial value or the seed). When m, a, c, and y_0 are integers, a pseudo random number within the range [0,m) can be generated by this equation. The pseudo random numbers $R_0, R_1, R_2, ...R_i$ can be normalized by y_i .

3. System architecture and design approach

3.1 System architecture

In this paper, passive RFID is used. There is non-directional requirement between non-contact RFID electronic tag and reader.

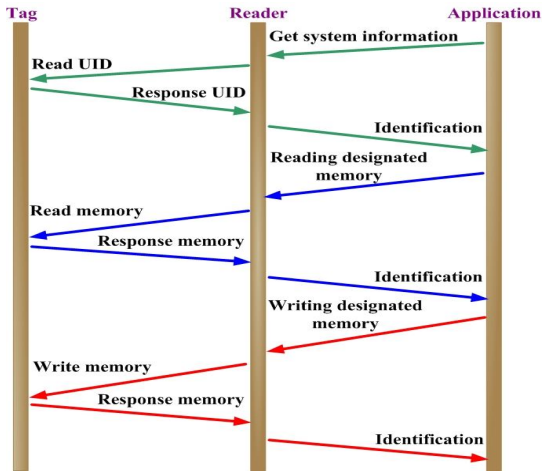

Fig. 2. System request & response command

So the system can be constructed with the three components: the RFID Reader, the RF electronic tag hold by the user and the application database computer systems. The messages of request or response were expressed in figure 2 .

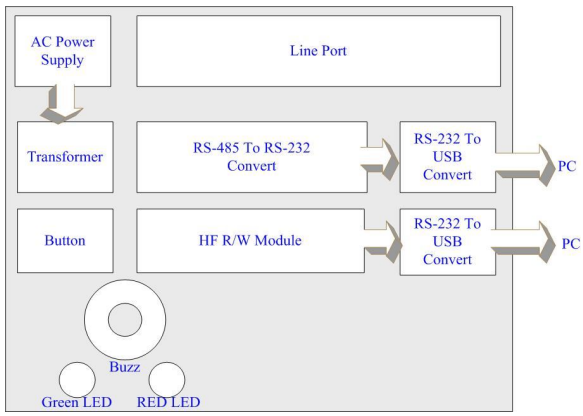

Fig. 3. RFID High-frequency reader equipment

The architecture of the door access security system is defined as the door access system and used in a typical resident house or a typical

company. It's main function is to monitor the door access of the company and the resident, such as visitors, attendance checking of employees, door open/close status, etc. It is mainly focused on the improvement of the disadvantages of the conventional door access system, such as the door access records, and passive security (for example, fixed access identification code). The entire hardware architecture consists of a section of cable module, RS-485 to RS-232 converter, a high frequency (HF) converter and an HF read/write module. The AC power is converted by the transformer and the button is used to trigger the reader to read the card. Two RS-232-to-USB converters are used for connecting the system to the computer. The triggered alarm is exerted with a buzzer and indicated with a red LED and a green LED. The block diagram of the system hardware is shown in Figure 3.

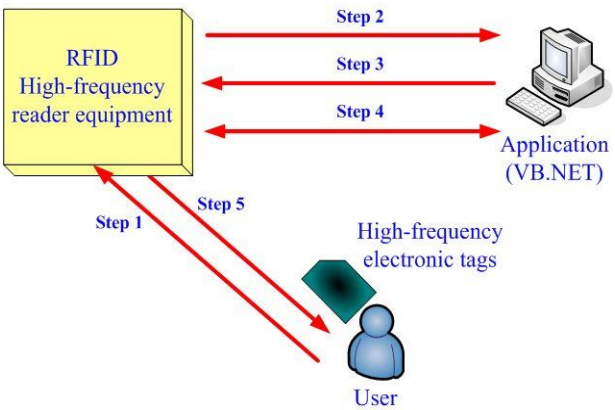

Fig. 4. Communication process of the hardware

The following five steps describe the communication process of the hardware that have shown in Figure 4:

Step 1: The user holds the HF electronic tag close the reading range of the reader/writer. The reader receives a signal and starts to identify.

Step 2: The signal is transmitted from RS-232 to the computer after being converted to the USB interface and then the verification of the identification is performed by the back-end application.

Step 3: After the application Completed the identification process and then feeds back rejection or acceptance command for the door access, meanwhile, the buzzer and LED indicators will show the alarm or welcome information.

Step 4: The back-end application will generate a one-time dynamic password by encryption and then send it back to the HF reader in the whole identification process.

Step 5: The HF reader stores the received one-time dynamic password into the specified tag memory. The door lock is unlocked after this process had completed.

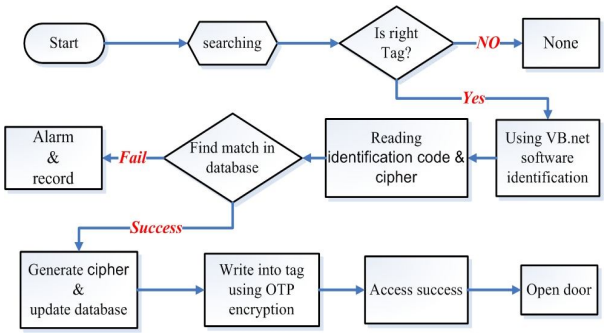

Fig. 5. Software identification procedure

The software detection procedure is in Figure 5. When the program starts to read card by pressing of start button, it will search whether there is any qualified tag nearby, and then start to identify it. First, reader will tell the UID (User Identification) of tag, if it successes, reader will find the memory address that match the tag from database and verify one-time dynamic password in it. If the results match, the system will generate one-time dynamic password to update the database. And then the password is written into the tag and the door is unlocked. If the procedure fails, it will exert the alarm sound.

In order to improve the security of the system, if a un-verified ID card and a one-time dynamic password is used to access the system reading/writing actions, and performed the password guessing actions, or the malfunction during the registration of door access by a verified user, etc., the system will record this information and send out an alarm sound, and perform the read/write operations for the forbidden door access on the tag. The forbidden time is 2^2 seconds for the first time and is extended to 2^3 seconds for the second time, and so on. During the forbidden time of the door access, the reader will not respond any command even if it receives a signal from the tag.

3.2 System design

During the design stage of the system, the security and convenience of the user are concerted with first priority conditions. Adopting the multiple factor verification system is a relatively safer way to protect the user¡s personal safety and property security. Thus, in this paper, the RFID technology is used for the identification of the door access system to determine whether the legal RFID electronic tag and the one-time dynamic password are correct or not. Meanwhile, the database will also be updated in real time in accordance with the system.

To make the system more secure and convenient for using, it uses the memory property of the ISO 15693 tag. It performs the encryption of the one-time dyanmic password for a single tag,and it is designed to allow the single tag card to access different door access systems at different times with differnt reading equipement. Currently ,to allow the tag to open the access systems of seven doors. The passwords are stored in seven different memory blocks for dynamic read/write operations. The final goal for this is to pass the verifications of two door access systems even when the two systems are not connected.

By the using of one-time dynamic password technology to encrypt the HF electronic tag, it will be helpful to prevent the electronic tag from being stolen and conterfeited. This system can be used as the supplement of the drawback of the existing conventional security system. Hence, by using such a one-time dynamic password communicatiom verification mechanism, the drawback of the conventional door access system can be eliminated for implemeting the door access system in this paper, and the system identification windows in figure 6.

Fig. 6. System Identification window

3.3 Applications of the one-time dynamic password algorithm

The main idea of this research is to adopt a one-time dynamic password as well as the passive tag that conforms to RFID ISO 15693 at the same time. In each electronic tag, there is an electrically-erasable programmable read-only memory (EEPROM) which has 64 memory blocks (0-63). Each block is 32 bits in length, i.e., the total memory size is 2048bits. The memory of the entire ISO 15693 tag is shown in Figure 7.

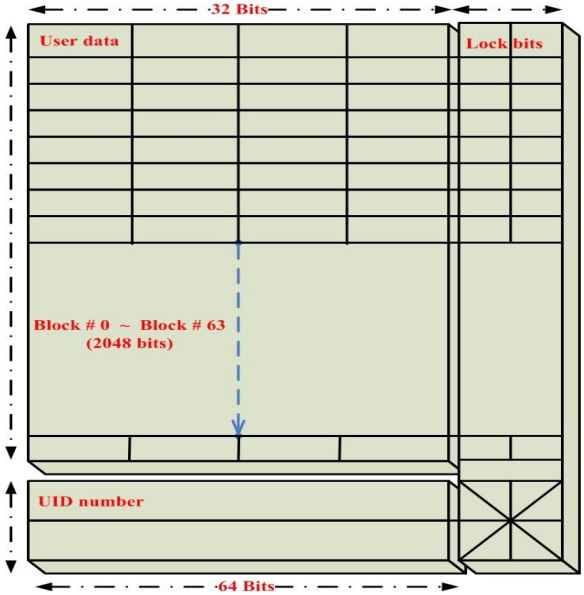

Fig. 7. Architecture of the memory in the tag

It uses a typical pseudo-random number generator ,and is based on the prime modulus multiplicative linear congruential method to generate the one-time dynamic password as described in Equation (1). we set $m = 2^{31} - 1 =$ 2147483647 and a = 16807. It can obtain $y_{i+1} = [16807 \times y_i] \ \ mod$ 2147483647, and the series of ordered pseudo-random numbers will be generated. Afterward, the predefined values of y_i can be used to verify whether the obtained numbers are correct or not.

It can further make an *XOR* operation to the pesudo-random numbers R_i and the public key between the reader and the tag ID_K, and then a series of 256-bit-long strings ($X_i = ID_K \oplus R_i$) can be obtained. Then, the obtained strings can be divided in four sections of 64-bit-long numbers. After the *XOR* operations on the four numbers ($X_{i1} = X_1 \oplus X_2$, $X_{i2} = X_3 \oplus X_4$),

and send the calculated numbers (X_{i1}, X_{i2}) to the tag for storing them in the tag memory. Only the tag verified by the user can have the information that can be acquired by the reader for the authentication by using y_i and ID_K.

Then, by applying the hash function on the key obtained from the data to convert it into a corresponding memeory address, thus such a hash table algorithm can efficiently distribute the random numbers that we just obtained uniformly into the memory. While applying such an algorithm to the tag, it is not necessary to perform a sorting of the files. The search speed is independent to the amount of data. It is uni-directional, and highly secure. It can also compress the data into a smaller range to utilize the space efficiently. Thus it is suitable to be applied on a passive tag whose memory size is limited. Figure 8 shows the configuration of the algorithms in the system and the applied working procedure.

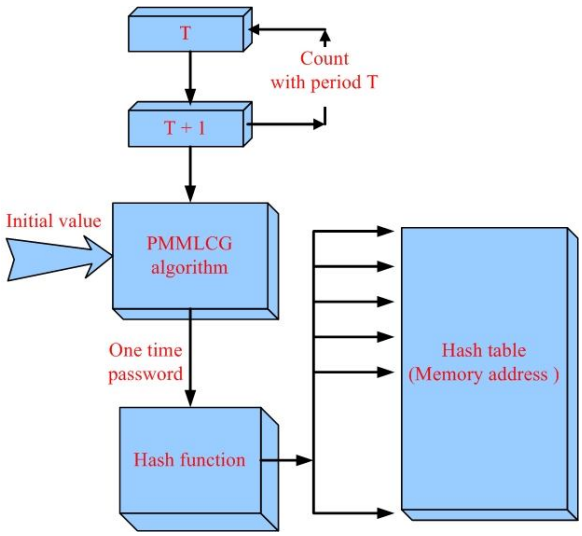

Fig. 8. Working procedure of the algorithms

In this system, it uses the Division method of the hash function. According to the definition, we can place the predefined parameters (X_{i1}, X_{i2}) in the function, thus we can obtain the following equation:

$$H_d(X_{i1}, X_{i2}) = X_{i1}, X_{i2} \quad mod\ m \quad \text{----------(2)}$$

However, because of the system is based on one-time dynamic password that is generated by the random number, the number will be much greater than the memory space on the hash table. Thus, there might be a situation that two different random numbers refer to the same memory address or the same bit patterns refer to the same location which causes the so-callsed collision or overflow. According to the empirical rules, to avoid a collision of the hash, it is better to choose a prime number of *m*. As a result, we set the value of *m* to be a prime number which is not greater than 63, i.e., $m = 61$. Thus, the consequent distribution of the data structure can be obtianed by calculating the equation $H_d(X_{i1}) = X_{i1}\ mod\ 61$; $H_d(X_{i2}) = X_{i2}\ mod\ 61$ to determine the memory address required for the distribution.

4. Conclusion

Most of the existing door access systems were based on the RFID ISO 15693 tags, they simply use a fixed password for the related verification which may generate misgivings of the door access security to some extent. The one-time dynamic password is proposed to solve the problems that are caused by the conventional equipment such as the fixed password, one key required for each door, etc. By the functional comparison, our system can achieve a secure, reliable and convenient goal and bring a better choice for the user in terms of a secure door access system.

In the future, the market of door access system will diverge into different categories according to the actual market demands. Obviously, one of the most important category is by incorporating the one-time dynamic password into the passive RFID communication technology. Currently, there are several specifications that have its own applicable niche market. It can be expected ,and there will be a wide variety of specifications for the door access applications that have its own niche market in the future.

References

[1] Banks, J., Carson, J., Nelson, B.L. and Nicol, D., ***Discrete-Event System Simulation***, 4th Prentice-Hall, Upper Saddle River, NJ, 2005.

[2] Chen, K.B., Lin, S.C., Wu, J.H., Huang W.K., Chang, Y.F., Chen, Y.C., ¡Door Access Identification System¡, ***ROC Patent No. 200606748,*** 2006.

[3] Finkenzeller, K., ***RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification***, John Wiley & Sons, Ltd., 2003.

[4] Graafstra, A., "Hands On," ***IEEE Spectrum***, Volume: 44, 18~23, 2007.

[5] Huang, K.A., ¡Door Access Identification

and Remote Controlled Security System¡, ***ROC Patent No. 118088***, 2000.

[6] Information and Communication Security Technology center of The Interior R.O.C (TAIWAN), retrieved form http://forum.icst.org.tw/phpBB2/, 2007.

[7] Lee, W.C., ¡A Study of Two-Factor Authentication System Using Open Source Software,¡ ***Int'l Conference on New Global Management Environment***, 2006.

[8] Long, M., Blumenthal, U., "Manageable One-Time Password for Consumer Applications," ***Digest of Technical Papers. International Conference on Consumer Electronics,*** 2007.

[9] Masaki, Fujikawa., Hiroshi, Doi., Shigeo, Tsujii., "Proposal for a New Home Security System in terms of User-friendliness and Prompt Intrusion Notification ," ***Proceedings of the 2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety***.

[10] National Police Agency, Ministry of the Interior, ¡Statistics of Crimes in Taiwan R.O.C.¡, Criminal Investigation Bureau, Taipei, 1973-2006.

[11] National Police Agency, Ministry of The Interior R.O.C (TAIWAN), ¡ Police Statistics in 2007,¡ retrieved form http://www.npa.gov.tw, 2007.

[12] Sarma, S.E., Weis, S.A. and Engels, D.W., ¡RFID Systems and Security and Privacy Implications,¡ ***CHES '02, Springer-Verlag***, LNCS Vol. 2523, pp. 454-469, 2002.

[13] Weis, S.A., Sanma, S.E., Rivest, R.L. and Engels, D.W., ¡Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems,¡ ***Security in Pervasive Computing***, LNCS Vol. 2802, pp. 201-212, 2004.

[14] Wong, H.M., Hui, C.L. and Chan, C.K., "Cryptography and authentication on RFID passive tags for apparel products," ***Computers in Industry***, Volume: 57, Issue: 4, May, pp. 342-349, 2006.