RFID Systems Integrated OTP Security Authentication Design

Chao-Hsi Huang [*] and Shih-Chih Huang [†]

[*] Institute of Computer Science and Information Engineering, National Ilan University, I-Lan, Taiwan, R.O.C. E-mail: chhuang@niu.edu.tw Tel: +886-3-935-7400

[†]Institute of Computer Science and Information Engineering, National Ilan University, I-Lan, Taiwan, R.O.C. E-mail: n0043016@ms.niu.edu.tw Tel:+886-3-935-7400

Abstract— **As radio frequency identification (RFID) technology matures, the application of RFID system also increased significantly and has been widely used in commodity storage, access management. We believe that it will become one of the major electronic money for the daily business consumption in the future. However, the stability and security of the data transaction will be more important for the demand of business applications. In the existed solution, we have not yet found an effective way that the Tag can be completely prevented forgery and attack.**

In this paper, we analyses the security problem of RFID authentication and propose security authentication for RFID tags based on a one-time password (OTP) authentication method. By the way of OTP authentication, we can improve the security of the RFID tag authentication. It can identify the authorized RFID Tag by additional OTP authentication. If an attacker uses eavesdropping to clone a RFID tag, the clone one can be identified by OTP authentication. We use RFC-6238 Time-Based One-Time password (TOTP) algorithm which is based on HMAC-SHA1 algorithm to enhance the authentication mechanism of RFID security. And we also use the computing power of NFC-enabled smart phone to generate TOTP by OTP generator which designed in this paper. The TOTP can be repeated and the security written to the tag. Thought using RADIUS authentication technology, manufacturers can easily apply this technology in the existing RFID system. It is easily provided to users to use roaming function between the different service providers, as long as they using the same frequency and standard of RFID technology.

I. INTRODUCTION

In recent years, radio frequency identification (RFID) technology has been widely used in identifing and tracking of merchandises, the access control of office and school, MRT Easy Card, ETC electronic toll, e-wallet of convenience stores… etc. It not only shows that RFID is mature technique , wide-range of applications and frequent used, but also shows that RFID technology which has a considerable degree of acceptance is used in addition to identification and the financial transactions. By over twenty-five million circulation of Taipei MRT Easy Card, we can almost believe that each one will have at least one or more RFID cards in Taiwan. With the smart phones, such as Apple iPhone and Android, are growing popularity, the smart phones combined with the NFC-enabled are also a growing trend.

RFID is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. It is quite convenient. However, the security threats about data transmission in a public wireless environment are more than the general wired transmission. It is more difficult to prevent the security threats in the wireless case.

According to analysis of currently known security mechanism in the RFID system, we find out the memory space of RFID tags is extremely limited due to the limitation of Tag hardware costs and RFID tags do not store and execute complex cryptography encryption and decryption operations due to there is no central processor in them. So currently they use some simple algorithms for encryption, or even some methods are just only simply logical operations. In fact, these simple encryption algorithms are difficult to implement and impractical on the commercial applications. This makes RFID not only in significant threat, but also hampered RFID financial transactions application. However, we can easily use the American National Standards level of security encryption algorithm through the way of OTP under the condition which we may not need to spend the cost of tag circuit design and modify. It can be applied to a variety of specification tag support more than 20bit rewritable memory space. It requires only a slight change in users' habits and expansion of the backend application authentication mechanism for the application.

To construct a safe and convenient RFID authentication system, we investigated the feasibility of use of RFID combined with one-time password authentication on the Tag and develop a system platform in this study. We hope to develop a suitable RFID tag authentication application platform to address current RFID system Tag identification safety problems. Based on the above considerations, we have the following purposes in the paper:

1. To explore the feasibility of enhance authentication security of RFID tags by OTP authentication.
2. Write one-time password to RFID Tag by Near Field Communication (NFC) in the case which RFID tag circuit without modifying, it reduces cost and complexity

to implement one-time password authentication in RFID system.

3. Integrated RADIUS AAA authentication mechanisms to provide a secure and flexible authentication mechanism that allows system vendor can easily integrate RFID OTP authentication mechanisms into existing systems.
4. Users are available to use the same Tag between differenct systems by roaming mechanisms.

Although the communication data between reader and tag transmission can be encrypted in the most of the current RFID systems, in view of the relevant researches have shown that these methods are now existing some security concerns and some method are not cheap if you want to apply in the real environment. In this paper, the method including RFID data transmission security issues research and develop a HMAC-SHA1 algorithm based on OTP authentication mechanism RFID tags authentication system[5] [10]. Users only need to have the NFC-enabled mobile phone and register information to the back-end system by installing the APP application software; they can easily to authenticate RFID tags using OTP authentication function. By testing RFID readers and tags security of the system in the identification process, whether we can match the expected results or not.

II. Literature Review

A. *The security threat of RFID Analysis*

In general, RFID communication process can be divided into two secure and non-secure channels [8]. Insecure channel is the communication channel between Tag and Reader, secure channel is the communication channel between Reader and backend system. Because the function of the device is more powerful in the secure channel, the existing computer communications security encryption protocol could be used to enhance the security "Fig. 1".

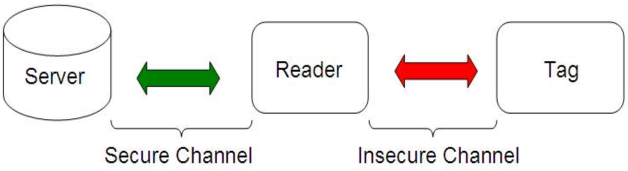


Fig. 1: Secure and Insecure Channel

The security threats of communication zone between Tag and reader can be classified as follows [2] [3]:

1. Eavesdropping attack:

Data transferred between tags and readers are transmitted by non-contact wireless signal. When a normal tag communicates with a normal reader, any other reader that fits specification for readers can get the transmission data in their interrogation zone. It would be exploited by attackers, if its content were not encrypted.

2. Traceability attack:

When a user's Tag pass through the reader that attacker pre-placed, the reader can read user's tag. And then an attacker can keep track of the user's current location and past trajectories.

3. Spoofing attack:

An attacker can sent messages to the reader or tag through forge a tag or a reader. Spoofing attack may detect Keys communicated between tags and readers, or forged transactions between the two. It makes the devices which are attracted by the attacker mistakenly thought that they communicated with the correct tag, or reader.

4. Replay attack:

An attacker will resend the communication content of an encrypted or unencrypted tag through steals the communication content between a tag and a reader. When the back-end security mechanisms do not protect against replay attacks, it also can be verified through encryption authentication because the resend data fitted the encryption algorithms of security mechanisms. It makes the reader may mistakenly believe that the attacker is a legitimate tag.

5. Cloning attack：

An attacker tries to read out the contents of the legal tag by using the reader and malware and to write the contents into a fake tag. Then using this fake tag deceives a legitimate reader.

6. Denial of service attack:

RFID reader and tag communicated through a wireless network, attackers send a large number of wireless communication signals, or use the non-legitimate tag communicated with a legitimate reader to occupy the reader communication resources, or cause a reader cannot communicate with the normal legitimate tag due to the asynchronous data between legitimate tag and back-end system.

B. *RFID Security Technology Analysis*

Currently, the known technologies of RFID security applications are as following [11]:

Password: It is a simple comparison reader password data sent over whether the same password in the tag. If the password data is the same, it is allowed to read and write tag information.

Hash Lock: It is mainly through the Hash function to lock or unlock tag. Both tag and reader have a common hash function. When we input a set of key, we can get a hash value through the hash function and by comparing the hash value to validate each other. This may be certified when the attacker repeatedly sent the same hash value, so it cannot defense against replay attacks.

Random Hash Lock: That it is different from hash lock is mainly through the random number generator. It makes the eavesdropper confuse to analyze the data by using each produced different value. Similarly, it cannot effectively defense against replay attacks.

One-time password list: Each tag will beforehand store password list in the back-end database and named multiple sets of tag pseudonyms αi, βi, γi used for authentication. Due to the communication process using pseudonyms, so there is no real ID of tag can be stolen. Used pseudonyms are no longer use in this way. So if stored pseudonyms were not enough, the tag is not able to be used when we run out of the passwords.

C. *One-Time Password Technology Introduction*

One-time password (OTP) refers to the password can only be used once and can be called a dynamic password.Its principle of operation is creating a set of passwords through three main token combined operations [6] [7]. The three main token respectively are algorithm identifier, sequence integer and seed. When a password is used, it must use the new password to pass the certification. The advantage of One-time password is that eeavesdropper cannot successfully passed certification even using this stolen password because the password has been automatically disabled. It is possible to prevent eavesdropping attacks and replay attacks. And every time the password is not the same, there is no way to get the correct password even in the face of the violence way to crack the code. Using the hash encryption method can prevent reverse engineering attacks because the password cannot be obtained from the originally keys by reversed calculation even if they know the encryption algorithm.

III. RESEARCH METHOD

A. *System Design*

We will design and develop a system that is divided into two main parts "Fig. 2". Front-end is responsible for using HMAC-SHA1 algorithm to generate 8 digital of the OTP password through truncate function and using pre-generated secret key K (shared secret) and counter C encrypted. And then write the OTP password to tag. When the user uses the tag which has finished writing the latest OTP passwords into, they can enter the back-end application system to use cards. Back-end database is recorded each tag with a corresponding secret key and counter. When a system certificates a card, it will be taken out the secret key from the database. Using the same way to generate the OTP password of current tag on the card is compared with the current back-end OTP generated password. It is checked whether both are the same passwords and the OTP has been used before. If the OTP password is the same and not used, a user can pass the authentication. Otherwise authentication fails.

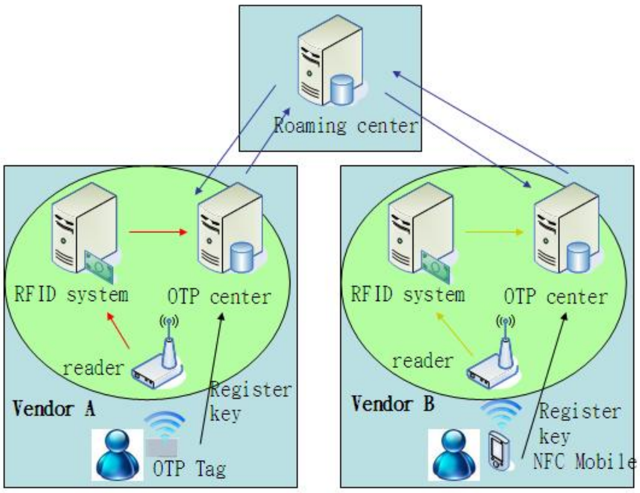


Fig. 2: RFID OTPAuthentication System Architecture

B. *Authentication Process*

The application process of the entire authentication system is divided into six phases: Tag OTP Key Allot Phase, Cards OTP Generation Phase, Tag Authentication Phase, Authentication Center OTP Validation Phase, Tag Authorization Phase and Tag Stop/Restart Phase. If the system needs roaming, it can increase Roaming Authentication Phase.

1. Tag OTP Key Allot Phase: Tag must register from the authentication center to join OTP authentication system at first. After completion of the registration, the system will be allotted OTP keys (or provided by the user) to the tag and record tag information, used keys and OTP type in the back-end database. In the future authentication, this key will be used as an authentication for OTP password.
   (1) Users login Certification Center and input tag's TID
   (2) Certification Center will search database to verify whether the key requested
   (3) Randomly generated the key by Certification Center
   (4) The key is allotted to users and recorded relevant information by Certification Center
   (5) Users will store the key into the OTP generator
2. Cards OTP Generation Phase：Before a user wants to use the tag to login, it will use the key to generate OTP and write OTP to the tag depending on the type of OTP generator.
   (1) Users use OTP generator to generate OTP according to the key
   (2) It is written OTP to the tag by OTP generator
3. Tag Authentication Phase：When users start to use the application service, it enters authentication phase in accordance with the card reader mechanism of the original application services.
   (1) Users use the tag to sense the reader
   (2) Tag's TID, OTP and other information are read out by the reader
   (3) Tag's TID, OTP and other information are sent to Certification Center by the reader
4. Tag Authorization Phase：When the tag completes OTP authentication, the system operators determine to reply whether the tag passed the certification and grant users the relevant permissions according to the authentication result.
   (1) Tag's TID, OTP and other information are received by Certification Center
   (2) According to other information, it determines self-certification or roaming authentication
   (3) When the system is self-certified, it will find the OTP key according to TID
   (4) It will get the authentication results through generating and comparing OTP according to the key
   (5) Certification results are replied to the application system by Certification Center

(6) Certification Center records related to successful and failure login information

5. Tag Stop/Restart Phase：The tag need to be unlocked because that the tag is locked by unmoral OTP authentication, or user's tag must be voided and terminated the use of. That enters this phase.
   (1) Application systems determine whether authentication is successful according to the authentication center replied results
   (2) Application systems grant users the relevant permissions
6. Tag Stop/Restart Phase：The tag need to be unlocked because that the tag is locked by unmoral OTP authentication, or user's tag must be voided and terminated the use of. That enters this phase.
   (1) When the number of consecutive failed authentication is more than five times, the tag is automatically locked and prohibited tag certification
   (2) When the label is locked, user applies to unlock

C. *OTP Generator*

The most important part of the whole system is how to produce OTP conformed to HOTP or TOTP specifications and the password is written to the tag according to keys allotted by the authentication center and HMAC-SHA1-based algorithm used. We developer OTP generator App on NFC-enabled phones which can read and write tags, and users can directly download OTP keys to the phone through App. When the user clicks App, OTP is automatically written to the tag using the NFC-enabled function.

D. *Certification center*

Certification center is divided into three parts, Certified Application, Registration Application and Database System：

1. Certified Application：

The main function is to compare whether the tag ID and password are correct send over by the application system. It uses client-server architecture and connects applications system and certification center over TCP / IP network protocols communicate. During the certification process, we use a RADIUS protocol based on RFC2318. It is open-source Free RADIUS software. Each time a user authentication is successful, the successfully login records in the contents of the counter. It retains records of the last five times as a check reference whether the password was repeated using. Each time a user attempts to login, it records login time of the last five times. When some people attempt to login over five times in 10 minutes, then the card will be locked. It is aim in order to prevent violent attacks as a reference.

2. Registration Application：

It mainly provides the services about user registration OTP authentication. It uses the Web server simply use a device with a browser, and data transmission encryption through SSL.

3. Database System：

It mainly provides that tags' data storage, OTP key information, the application disables records, login records and other relevant information.

E. *Roaming Center*

Through roaming mechanism, it can make their own users to operator themself OTP authentication in other systems as long as the center interfacing with roaming system. In other words, as long as a user registered with one system, he can use himself OTP authentication to the other business through the way of roaming. The users' keys are stored in the originally registered applicant organizations, so it will not be affected itself certified security by the other business. The system architecture of roaming center and certification center are similar, except that the roaming center only needs to store the information of certification center which joins the roaming system and not store any information about tag and OTP key.Equations

IV. Implement Results and Security Analysis

A. *OTP Generator Implement*

In this study we use MiFare Classic 1k card for a tested tag, the program operational processes show as the following table "Fig. 3", "Fig. 4":

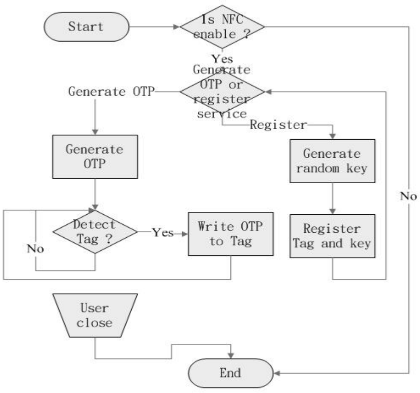
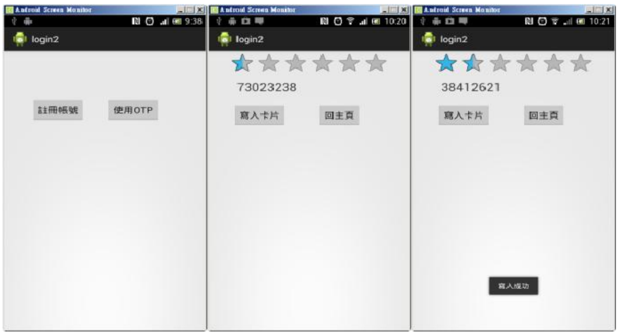


Fig. 3: Programming Operational Processes



73023238

38412621

寫入成功

Fig. 4: Program Execution, OTP Generator and Successfully Written

V. Certification Center Implement

Certification center mainly provides user registration and authentication OTP service. It is divided into Acknowledgment

1. Certified Application (RADIUS Server and OTP Server)
2. Registration Application (Web Server and register.php)
3. Database System (MySQL)

Its architecture can refer to the following diagram “Fig. 5”:

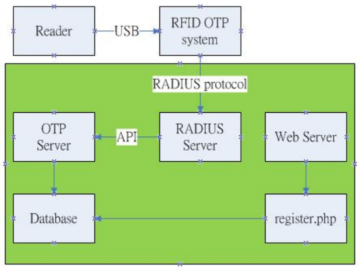


Fig. 5: Certification Center Architecture Diagram Successfully Written

When users registered through OTP generator, the user's card data and key information are recorded by the database. Users use the card which has been written by OTP generator read the card information by the reader, Tag ID, OTP and domain will be sent to the certification center through RADIUS to do certification. NFC-Reader certification client system program flowchart is as follows “Fig. 6”:

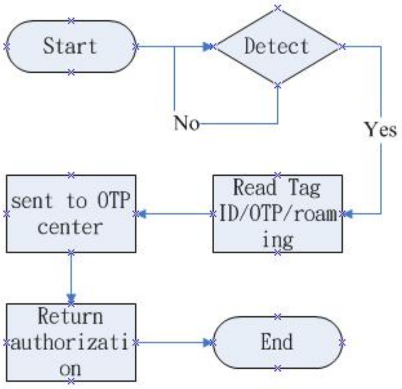


Fig. 6: NFC-Reader Authentication Client Program Processes

OTP Server program flowchart is as follows “Fig. 7”

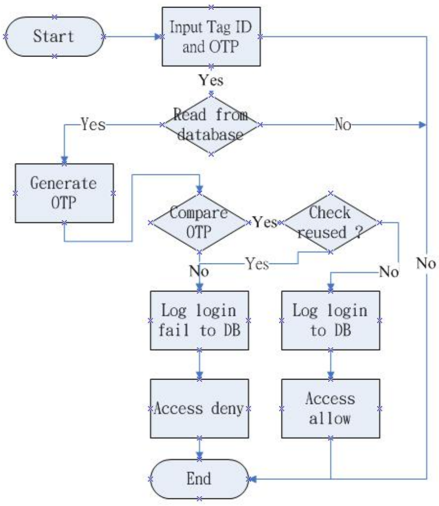


Fig. 7: NFC-Reader OTP Server Program Processes

VI. Roaming Center Implement

Roaming center using FreeRADIUS default installation, we modified the following profile in order to let it roam support our certification center.

1. Authentication Server configuration file: /etc/raddb/clients.conf

```
client 192.168.1.138 {
        secret = radiuskey
        shortname  = RFID1
        }
       client 192.168.1.139 {
        secret = radiuskey
        shortname  = RFID2
        }
```

2. Roaming file: /etc/raddb/proxy.conf

When the authentication of the domain which is niu.edu.tw gave 192.168.1.138 authentication server,

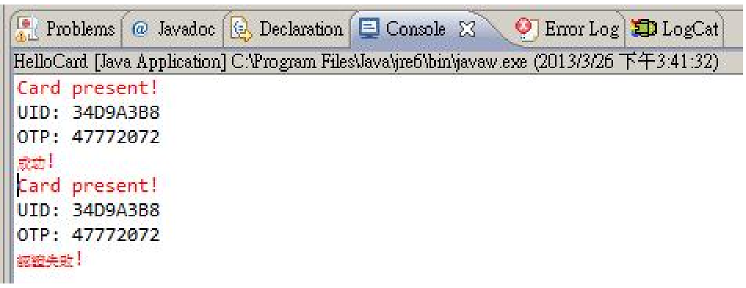
```
     realm niu.edu.tw
          {
       type         = radius
       authhost       = 192.168.1.138:1812
       accthost       = 192.168.1.138:1813
       secret        = otproaming
       nostrip
      }
```

When the authentication of the domain which is niu.edu.tw gave 192.168.1.139 authentication server,

```
realm ntu.edu.tw
      {
         type          = radius
         authhost       = 192.168.1.139:1812
         accthost       = 192.168.1.139:1813
         secret         = otproaming
         nostrip
      }
```

VII. Experimental Results and Security Analysis

From the experimental results, we learned that when a user can successfully log in due to use the correct OTP and when a user can not be authenticated due to have the used OTP. The relevant certification records are as follows "Fig. 8": In "Fig. 8", we can see that the first time to use OTP "47772072" can successfully log in, it shows as "成功!" and the second time to use the same OTP "47772072" cannot log in, it shows as "認證失敗!".



```
HelloCard [Java Application] C:\Program Files\Java\jre6\bin\javaw.exe (2013/3/26 下午3:41:32)
Card present!
UID: 34D9A3B8
OTP: 47772072
成功!
Card present!
UID: 34D9A3B8
OTP: 47772072
認證失敗!
```

Fig. 8: OTP Authentication Results

We are also to analyze whether this system can effectively prevent correlation attack about security threats mentioned before. The results show in(table 1).

TABLE I
SECURITY ANALYSIS AND COMPARISON TABLE

	RFID system	RFID OTP Center
Password length	static	dynamic
Encrypt algorithm	static	dynamic
Password	static	dynamic
cost to user	Low	Higher
Roaming	hard	Easy
Cost to developer	Low	Higher
Brute force attack	unable	able
Cloning attack	unable	able
Replay attack	unable	able
Eavesdropping attack	unable	able

VIII. Conclusion

We design a system for authentificating RFID tags, and TOTP mechanism is the focus of the major consideration in this paper. Compared to other RFID encryption, TOTP mechanism improves the security for certication of tags throught written by the dynamic password and backend system authentication methods. It can effectively prevent the security vulnerabilities such as dictionary attacks, replay attacks, data eavesdropping and tags forgery. Other researchs' design is to increase a special logic circuit in tags, so the applications can be used only on special tags. However, we can apply our system to any tag's format as long as these tags provide more than 20bits memory block which can be repeated to read and write. Therefore, this system can be applied to a wide range of tags and also reduce the related cost of application. The related encryption algorithm used in this paper is open, flexible and secure enough. We do not need to modify the tag in the case and just to amend the relevant algorithm complexity according our own needs. Through roaming mechanism allows users to simply use the same card, you can use the secure TOTP authentication in the various application systems.

We hope that we can promote RFID micro-payments and other value-added services through this authentication mechanism after the popularity of NFC smartphones in the future. It can also be provided to the RFID manufacturer as the reference of RFID tags designed about the security password mechanism. It also provides for application service providers, a feasible, safe, inexpensive RFID authentication system design.

References

[1]. Chen Hong-Yu, RFID System Getting Started Radio Frequency Identification System, Sung Gang Asset Management Corp.Limited

[2]. Nian Tian-Shou, Information and Network Security Technology, F8754 Flag Publishing Co.,Ltd.

[3]. Ma Jia-Lin，Liu Tian-Hua, Based on Multi-Reader RFID Security Analysis Research.

[4]. Tseng Yu-Chee, Lin Cheng-Kuan, Lin Zhi-Yu, Pan Meng-Hyun. Wireless Networks: Protocols, Sensor Networks, Radio Frequency Technology and Application Services. GOTOP INFORMATION INC. 2011

[5]. D.Eastlake, 3rd, RFC 3174:"US Secure Hash Algorithm 1 (SHA1)", September 2001

[6]. D.M'Raihi, RFC 4226:"HOTP: An HMAC-Based One-Time Password Algorithm",December 2005

[7]. D.M'Raihi, RFC 6238:"TOTP: Time-Based One-Time Password Algorithm",May 2011

[8]. Lijun Gao, Zhang Lu, Low-Cost RFID Security Protocols Survey, 2011 Cross Strait Quad-Regional Radio Science and Wireless Technology Conference.

[9]. N.Haller, Bellcore, C.Metz, RFC 2289: "A One-Time Password System", IETF, February 1998

[10]. R.Glenn, RFC 2104:"HMAC: Keyed-Hashing for Message Authentication", November 1998

[11]. Stephen August Weis, Security and Privacy in Radio-Frequency Identication Devices, Massachusetts institute of technology 2003.

[12]. Starbug Karsten Nohl, David Evans, Henryk Plötz,

Reverse-Engineering a Cryptographic RFID Tag,
USENIX Security Symposium. San Jose, CA. 31 July
2008.