

# Design of RFID System for User's Authentication Under Ubiquitous Surroundings

Dae-Yoo Kim and Jung-Tae Kim, *Member, KIMICS*

**Abstract**—In this paper we will discuss a general idea about an information system which provides information a user really needs in user's authentication. We will discuss how RFID could be applied for this kind of system especially from the standpoint of using RFID as a way to collect information of personal belongings. Also we will discuss security issues of using RFID as a component of the proposed system because while RFID could provide usefulness, it could also be very dangerous for revealing private information without user's awareness.

**Index Terms**—Authentication, RFID, Ubiquitous system

## I. INTRODUCTION

RFID is not really new. For several years, military and security applications have deployed fairly sophisticated implementations of active RFID, which uses battery-powered radio equipped tags to transmit pertinent information. However, the new wave of RFID, known as passive RFID, features cheap non-energized tags and is just poking into the marketplace. Radio frequency identification system is a command and useful tool in manufacturing, supply chain management and inventory control. Basically, the tag reader broadcasts a radio frequency signal to access information stored on the tags nearby. This information can range from static identification numbers to user written data or data computed by the tag. Recently, some universities introduced experimentally student identification cards attached a RFID tag which has functions such as the attendance management and the room access control in addition to electronic money. Actually, many student's administration functions can be carried out by using RFID tags and related technologies. However, when people are carrying RFID tags, the location privacy problem arises. The location privacy is about the location information of the RFID tag possessor.[1,3]

## II. CONCEPTS OF RFID SYSTEM

RFID tag has a property that an unjust reader can

access it easily. Moreover, since the RFID tag is based on radio communications, information transmitted between the RFID tag and a reader can be intercepted. When personal information is recorded in the RFID tag, it is infringement of privacy that the information is taken by the third party. On the other hand, when a unique ID is recorded in the RFID tag, the information doesn't have the value as personal information. However, since the RFID tag has the outstanding traceability, an owner's location of the RFID tag can be known and traced. This privacy about the RFID tag owner's location information is called location privacy.

### A. Characteristics of Technical of RFID

- RFID technical characteristics

It has an excellent characteristics compared to bar code and smart card. It makes easy to implement to application equipment. It will use 900MHz band width brand instead of 13.56MHz used in today.

### B. Principle of RFID tag technical

Antenna supply a power to tag and tag transmit the data by reply each other. There are two representative method. One is used by magnetic field, the other uses radio frequency. Received distance depends on characteristics of tag, we communicate by using 13.56MHz(5m). Figure 1 shows the overview of RFID system.

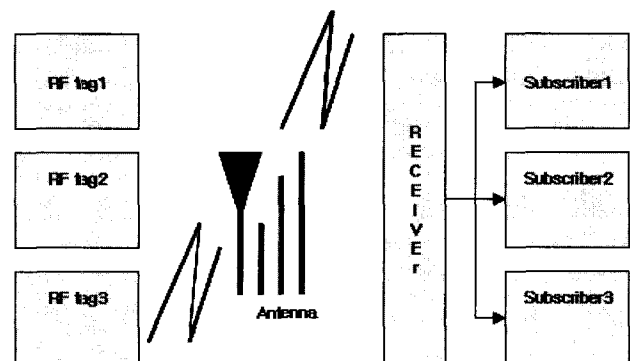


Fig. 1 Overview of RFID System

### C. Scenario of RFID SecureWarm

It is called RFID SecureWARM that we propose the authentication system.

A lot of users use a computer in school. But the computer system is opened by public over internet. It is vulnerable to security and not easy to manage. We propose the system that it can be operated by simple security method with secureWARM. Computer used in school is used by many unauthenticated students. Some student want to

Manuscript received May 21, 2007.

Jung-Tae Kim is with the Mokwon University, Department of Information Electronics & Imaging Engineering (phone: 82-42-829-7657, fax: 82-42-829-7653, e-mail: jtkim3050@mokwon.ac.kr)

keep his/her documents in computer storage. But, we can not recognize who, when and what file is stolen or not. This is key point we have to solve the problem, especially security affairs. We need to confirm and protect from unauthenticated person that access the information system.

### III. DESIGN RF SECUREWARM

We briefly review the operating process. The SecureWARM operation system execute after windows is booting. SecureWARM make secure mode to prohibit system usage. At this time, user put the card on the terminal to access system, secureWARM read information of card, send the information to server and judge whether the user is authenticated or not. If authenticated, secure mode is removed, we can access the system. If not authenticated, the system set the secure mode again. We can not access. Figure 2 shows operation of process, Table 1 represents operation flow according to user's behavior.

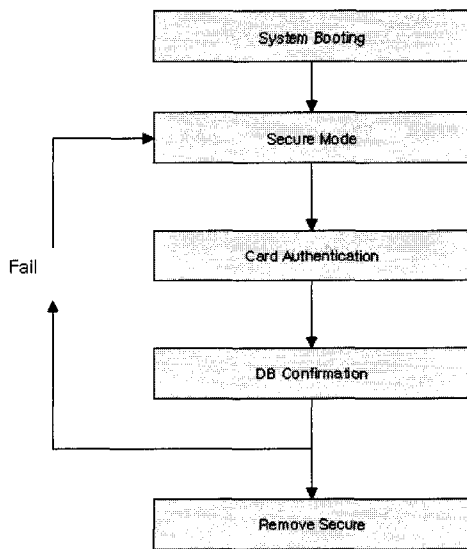


Fig. 2 Operation flow of SecureWARM

Table 1 Operation of flow for RF SecureWARM by user's behavior.

| Number | Display  | SecureWARM  | Remarks                       |
|--------|--|---|-------------------------------|
| 1      | Power on   | -   |                               |
| 2      | Start Windows  | Start Secure Mode   | Waiting User's Authentication |
| 3      | Put card on Receiver to use System                                     | Receive card information and request system DB server and store record in DB server                     | Confirmation User             |
| 4      | Permit only Authenticated User to access system because of secure mode | If user is authenticated, secure mode is removed. If not, user is protected by system using secure mode |                               |

#### A. RF SecureWarm Base Architecture & User Interface

Rf Secure is used to access only authenticated users. The major role is that it transfers operating system through input equipment such as keyboard and mouse to control system.

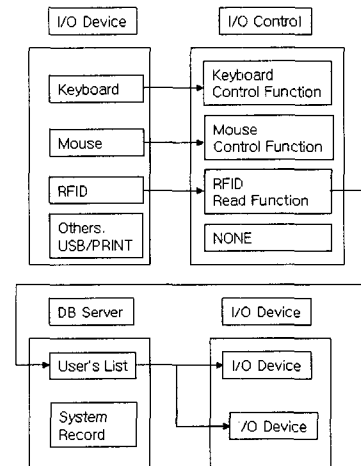


Fig. 3 RF SecureWARM base architecture

When authenticated and unauthenticated users are accessed, every information DB is stored in server and it makes a role on repudiation. The DB file can be added, modified and deleted for recording information of system. The process is shown in table 2.

Table 2 Flow chart of recording process

| Number | Event         | Processing  |
|--------|---------------|---|
| 1      | Start Program | Make system log table after system is on  |
|        |               | System time      Record current time  |
|        |               | IP address        Record current IP   |
|        |               | Current state     Start program   |
| 2      | User log-in   | Record data to system current state table<br>When card number of member information and card number of user is same |
|        |               | Card number        Record card number of user   |
|        |               | Current time       Record current system time   |
|        |               | IP address        IP address of current system  |
| 3      | User log-out  | Current state     Authentication of user' log-in  |
|        |               | Record user's log to system state table   |
|        |               | Card number        Record user's card number  |
|        |               | Current time       Record current system time   |
| 4      | System Finish | IP address        IP address of current system  |
|        |               | Current state     User log-out  |
|        |               | Record data to system log table   |
|        |               | System time       Record current system time  |
|        |               | IP address        Record IP address of current system   |
|        |               | Current state     Exit  |

#### B. Secure Mode

Secure mode supports the function of control that can not use the system when unauthenticated user access system. The screen shows that only authenticated user can access system after authenticate user's access. When we put RFID card on card reader, the card reader reads the data and requests authentication mechanism. Figure 4 shows the screen of secure mode.

### C. User Interface

Only administrator can control environmental setting, User interface of ordinary user is in unsecure mode at this time.

### D. RF SecureWARM

Administrator can set up the setting by putting card of administrator on receiver and can access the main menu.

### E. RF Secure Mode

This menu can manage to control user's request setting

- Skip card: can remove secure mode when we put card on receiver.
- Check card: can change the mode when the system is not used with a few minutes.

### F. Database Setting

This function records user's usage system in database.

- DBSelect : check version of data base.
- ServerIP : input IP address of DB server
- Password : input password account of DB server

## IV. EXPERIMENTAL RESULT

The experimental set up is shown in figure 5. The parameters are listed to implement system infra structure.

- Usage language
  - Delphi 7: usage in program of user interface form and communication module
  - Visual C++: control of keyboard and implementing DLL module for process control
  - MySQL: renew record of information and time of card used card
- Usage system
  - Windows 2k/NT/XP
- Hardware
  - RFID reader
  - RFID card(tag)
- Terminal usage
  - OS : windows 2K/NT/XP
  - Hardware : RFID reader, tag
  - program : RF security, MySQL

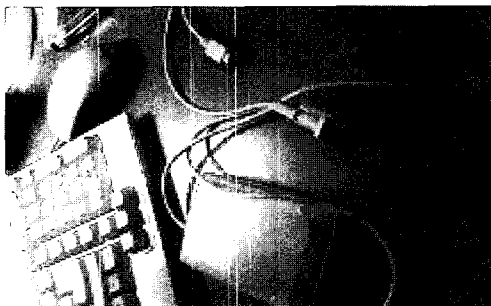


Fig. 4 Receiver of RFID Module used in Experimental Set-up

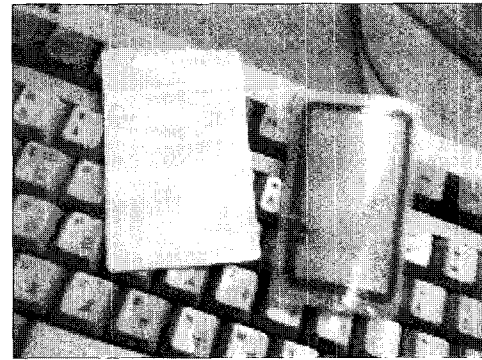


Fig. 5 Mifare Tag & Pico Tag

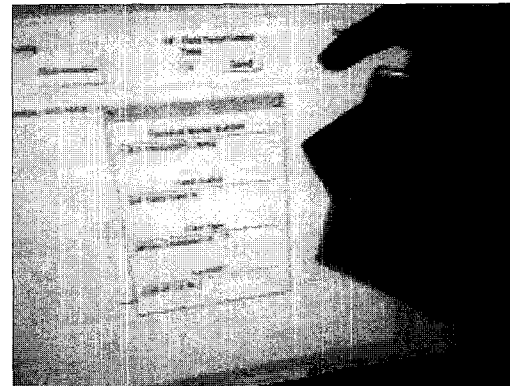


Fig. 6 Pico Tag Field and Screen of Testing

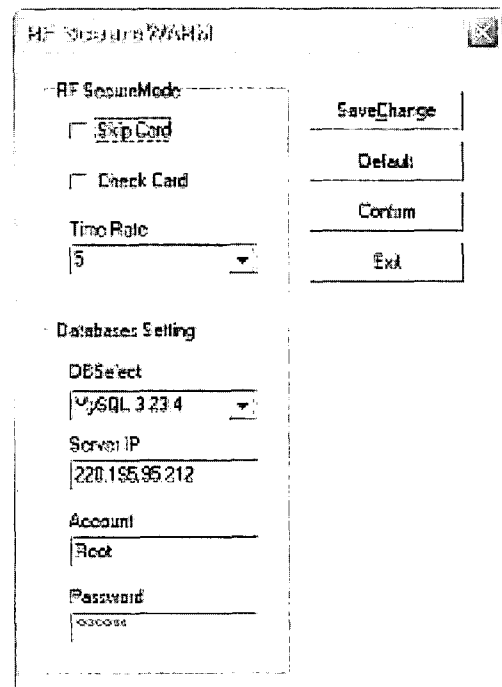


Fig. 7 Administrator Menu of RF SecureWARM

## V. CONCLUSIONS

New social infrastructure based on advanced information technology is a great challenge and it is also design of the future of our society. The RFID tag system

will be basic infrastructures to implement a stable, safe and efficient society. In this paper, we have proposed the authentication mechanism by using RFID system to realize user's authentication.

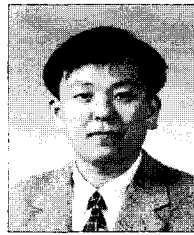
## REFERENCES

- [1] P. Ekdahl, and T. Johansson, "Another attack on A5/1", IEEE Transactions on Information Theory, V.49, N.1, pp.284-289, 2003.
- [2] S. A. Weis, etcs, "Security and privacy aspects of low cost radion frequency identification systems", security in pervasive computing, 2003.
- [3] H. Chan, etcs, "Security and Privacy in sensor networks," IEEE Computer, V.36, N.10, pp.103-105, Oct. 2003.



### Dae-Yoo Kim

He received his B.S. degree in Information Electronic Engineering from Mokwon University in 2006 and is currently working toward his M.S. degree. His research interest is in the area of Information security system technology that includes Network security system design, Data base security and Web security.



### Jung-Tae Kim

He received his B.S. degree in Electronic Engineering from Yeungnam University in 1989 and M.S. and Ph.D. degrees in Electrical and Electronic Engineering from the Yonsei University in 1991 and 1996, respectively. From 1991 to 1996, he joined at ETRI, where he worked as Senior Member of Technical Staff. In 2002, he joined the department of Electronic and Information security Engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of Information security system technology that includes Network security system design, Chaos Cryptosystem, Crypto-processor and Wireless Communication.