International Journal of Control and Automation
Vol. 8, No. 4 (2015), pp. 9-14
http://dx.doi.org/10.14257/ijca.2015.8.4.02

Vulnerability of Rechargeable RFID Tag Card based on NFC

WonHyung Park*, Dae Hyeob Kim* and Daesung Lee**

** Department of Cyber Security, Far East University*
Wangjang-ri, Gamgok-myeon, Eumseong-gun, Chungcheongbuk-do, Korea
E-mail: whpark@kdu.ac.kr, anoges@naver.com
*** Department of Computer Engineering, Catholic University of Pusan*
#57, Oryundae-ro, Geumjeong-gu, Busan, 609-757, Korea
Corresponding author E-mail: dslee@cup.ac.kr

Abstract

RFID (Radio-Frequency Identification) tags have been widely used because of convenience. These conveniences which RFID has made the RFID tag become a tool to certify him or herself. The RFID tags, which have the function to easily prove ownership, are mainly used to prove one's financial assets such as credit card or bus card passes. However, due to its ease of use to prove one's assets, RFID tag has lots of vulnerabilities. Nowadays the vulnerability of rechargeable RFID cards has become an issue. This paper researches about the vulnerabilities of existing RFID tags and suggests countermeasures.

Keywords: *NFC, Radio-Frequency Identification, IoT (Internet of Things), Rechargeable Bus*

1. Introduction

These days, electronic devices which exist in our society have become indispensably convenient in our daily lives. Electronic devices especially RFID tags are widely used in the part of the economy due to its convenience to prove him/herself.

Mobile major global companies Apple (IOS) and Google (Android) have announced the NFC-based application services as the next core business of smartphones. Google released the payment service 'Google Wallet' using NFC technology. It began trial in New York and San Francisco in the United States in the year 2011 on May 26th and is expanding its service area. Apple has filed a number of patents related to the NFC, and equipped the NFC function in the iPhone 5S (2013.10.25 Release). Apple also released a new wallet called the "Apple pay" which allows the customers to pay through the phone itself. The image below shows the market size of the world market RFID [1].

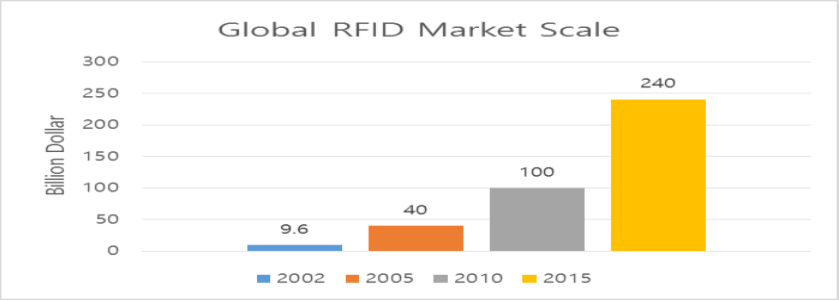

Figure 1. Global RFID Market Scale

ISSN: 2005-4297 IJCA

By these trends RFID tags, which have the simplicity and ease of payment, are being used in bus card, employee ID (identification), and payment system. The function to simply prove the individual's identity is convenient in our lives, but it also has security vulnerability.

2. Related Works

2.1. Difference of NFC and RFID

RFID and NFC technology are the same technology but can be divided by frequency and its power supply and P2P (Peer to Peer) connection [2]. NFC is included in the scope of the RFID. RFID includes three kind of frequency: Low Frequency (LF), High Frequency (HF) and the Ultra High Frequency (UHF). NFC (Near Field Communication) only supports a High Frequency (HF). But difference between the NFC and RFID is that NFC supports the P2P (Peer-to-Peer) technology. In addition, RFID and NFC are divided into Passive RFID and Active RFID. Passive RFID does not have its own power supply [3]. On the other hand Active RFID has the power supply in the internal tag. It is often mainly used to position a container box or location of things [4].

Table 1. RFID, NFC Chart

	RFID	NFC
Frequency	> Low Frequency (LF)125 -134 kHz > High Frequency (HF)13.56 MHz > Ultra High Frequency (UHF) 856 MHz to 960 MHz	> High Frequency (HF)13.56 MHz
Power	> Active Mode > Passive Mode	> Active Mode > Passive Mode
P2P	X	O

2.2. RFID Tag Security

There is security in RFID tag. Seeing the communication between the RFID tag and the external device can identify how security works. At the first step, RFID tag at HALT state waits for the signal from outside. Second step is when the external device sends a request to gain RFID tag unique serial number to identify the RFID tag. The external device requests and gains the serial number to communicate over a specific serial number in order to prevent collision. Third, external device authenticates to the sector by providing key to RFID to read and write the data. Two keys, which are implemented in RFID, are called writing Key and reading Key. The keys gained from external device set permissions to RFID, which allows external device to access reading and writing to the storage. If the external device has the right key, it can receive permission to read or write a value to the RFID tag [5, 6, 7].

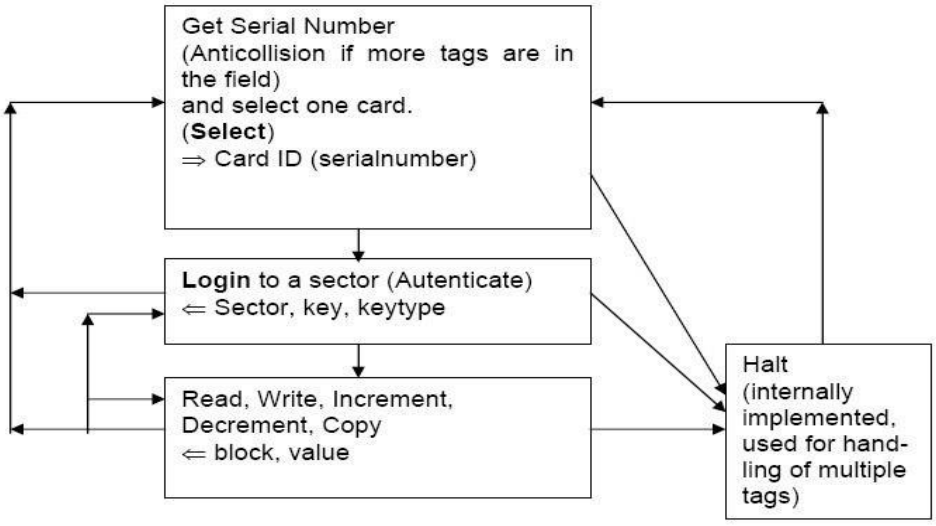

Figure 2. RFID Security

2.3. Read RFID Tags using an Android

Reading RFID from android device is simple. First you need a device which can support the RFID tag. After that, android will find the right RFID by searching the RFID which is in HALT state. Then Android will try to connect to the RFID tag by intent. There are two intents that Android uses to determine the RFID tag. First intent is NDEF (NFC Forum Data Exchange Format) Formatted Tag and second is Unmapped or Non NDEF Formatted Tag. By determining the intent, it tries to discover the right NDEF Tag technology by using NDEF Discovered, Tech Discovered and Tag Discovered. Successfully gaining the right intent, it passes a value to the activity to perform reading and writing functions. The figure below shows the process of reading the RFID tag on Android [8].

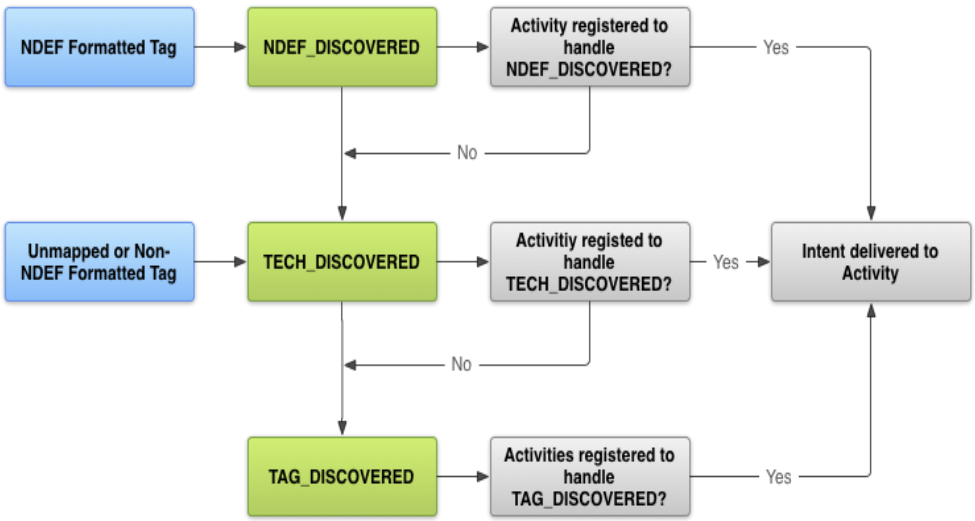

Figure 3. Android NFC

3. Rechargeable Vulnerability Bus Card with an NFC

A tool used for research is M25S Galaxy S2 (SHW-M250S), which supports Mifare and ISO/IEC 14443-3, ISO/IEC 14443-2. First, install the Mifare Classic Tool in Galaxy S2. Then, by using the app Mifare Classic Tool, Galaxy S2 the app can read RFID tag's Sector value. Most of the Key value of RFID is set to default key ('FFFFFFFFFFFF') to have computability to read from external devices. By the default key the total 1kB (kilobyte) information can be read from the RFID tag.

Total byte of Mifare Tag has 1kB of storage that we can write. The 1kB storage is divided to 16 sectors, which are 48bytes, and each sector has its own writing and reading Key. Each sector has three blocks; there are a total of 64 blocks in the RFID tag. Each block is 16 bytes. The first sector, which is sector 0, contains the RFID's unique serial number in the first block, block 0. However the default RFID prohibits writing to sector 0. From sector 0 to sector 15 it is possible to store data, when provided with the right Key.

The image below shows the whole information 18,000₩ (won) left RFID tag is read using the Galaxy S2.

```
+Sector: 1
010000000000000241D5046000058F4
010000000000000241D5046000058F4
010000000000000241D5046000058F4
------------FF040201FFFFFFFFFFFF
```

Figure 4. 18,000₩ Left

Fig. 4. Shows without security we could read the first sector, sector 0 from which we can able to determine the unique values of the bus card. Second, we could manipulate data at second sector (+Sector: 1), to recharge the bus card (RFID tag). We can see the value is only written in the second sector (+Sector: 1). In other words, the money value is recorded in the second sector (+Sector: 1). Figure below increased the readability by breaking the character by 2 bytes. In the figure, all the second sector (+Sector: 1) blocks values are identical.

The figure below shows the RFID tag when the value the money is 0₩ in the RFID tag. When you see the figure below you can see that some parts have changed. First, the offset range from 10 byte ~ 14 byte has initialized to 0. Second, offset range 15 byte ~ 16 byte, which was the value 58F4 can be seen that had turned into ADEF.

```
+Sector: 1
010000000000000241D00000000 ADEF
010000000000000241D00000000 ADEF
010000000000000241D00000000 ADEF
------------FF040201FFFFFFFFFFFF
```

Figure 5. 0₩ Left

For more detailed validation we charged 6,000₩ in bus card and read the RFID tag immediately. The Figure below shows charged 6,000₩.

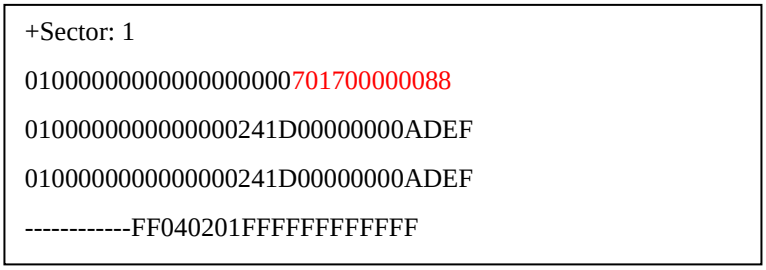

Figure 6. 6,000₩ Charged

As a result, the difference between the charged bus card and used bus card is in the second sector (+Sector: 1), first block (block 0). By these facts, we can see that using the block 0 of the second sector (+Sector: 1) contains the money value. And the offset range from 10 byte ~ 14 byte contains the value representing the amount of money. Fig. 7 shows that offset range from 10 byte ~ 14 byte which is "70 17 00 00" can be read as the Little Endian way. If we convert the "70 17 00 00" by Little Endian we could read "00 00 17 70" and by decimal the value is 6000. The figure below shows the results of the charging 12,000 won. It will look closely at the picture below, the values in the last 16 byte. Here, it can be seen that it has increased as much as 0x88 0x89 checking the money value.

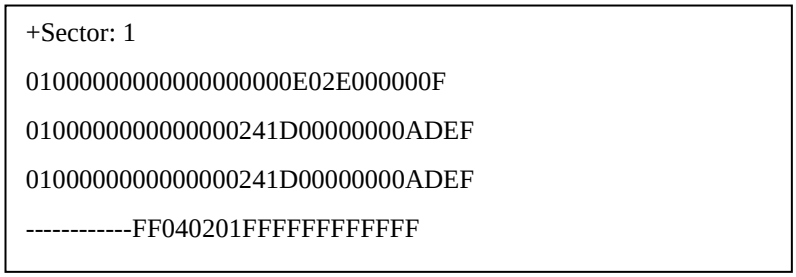

Figure 7. 12,000₩ Charged

4. Conclusion

It can be seen that the bus card has a vulnerability issue. This un-encrypted bus card is vulnerable to manipulating the value. There are two options to prevent the vulnerability of RFID tags. One is having a data to verify an existing value inside or outside of the RFID tag. Second is to encrypt the value so it cannot be read or manipulated.

RFID has been used in various fields. Among them, the RFID tags provide the convenience to identify him/herself in real life. It has the benefit of convenience, but it is vulnerable to security. In this paper, we researched that it is possible to recharge the bus card in an unusual way to prove the RFID tag's vulnerability.

References

[1] J. Hong, "Korea Database Agency", http://m.kodb.or.kr/info/info_06.php?field=&keyword=&type=trend&page=274&dbnum=129184 &mode=detail&type=trend, **(2004)**.
[2] R. Want, "An introduction to RFID technology", Intel Res., Pervasive Computing, IEEE, **(2006)**.
[3] H. Vogt, "Efficient Object Identification with Passive RFID Tags", Pervasive Computing, **(2002)**.
[4] L. M. Ni, Y. H. Liu, Y. C. Lau and A. P. Patil, "LANDMARC: Indoor Location Sensing Using Active RFID", Kluwer Academic Publishers, **(2010)**, pp. 1572-8196.
[5] A. Juels, "RSA Labs., Bedford, MA, USA, RFID security and privacy: a research survey", Selected Areas in Communications, IEEE Journal, **(2006)**.
[6] A. Juels, R. L. Rivest and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy", Proceedings of the 10th ACM conference on Computer and communications security, **(2003)**.
[7] S. E. Sarma, S. A. Weis and D. W. Engels, "RFID Systems and Security and Privacy Implications", **(2003)**.
[8] R. Wondratschek, "Reading NFC Tags with Android", http://code.tutsplus.com/tutorials/reading-nfc-tags-with-android--mobile-17278, **(2013)**.

Authors

WonHyung Park, he is a professor in Department of Cyber Security, Far East University, South Korea. He received Ph.D. degree in Department of Information Security from the Kyonggi University, South Korea, in 2009. he co-authored more than 40 technical papers in the area of information security. Also, he has been reviewer for International Journal(Computer-Journal) of Oxford Univ. press and IEEE International Conference(ICISA 2014, ICISA 2013 and ICISA 2010).

DaeHyeob Kim, he is a student in the Department of Cyber Security, Far East University, Korea. His research interests include network security, convergence and operating system.

Daesung Lee, he is a professor in the Department of Computer Engineering, Catholic University of Pusan, Korea. He received the B.S., M.S. and Ph.D. degrees from the Inha University, Korea, in 1999, 2001 and 2008, respectively, all in Electrical Engineering Computer Science & Engineering from Inha University. His research interests include security in IoT, convergence and operating system.

