A Method of Preventing Malicious Advertisements in NFC-adopted Applications

.

.

.

.

Abstract - Near Field Communication (NFC) is an enabling technology for interactive communication between devices at close distance of around 4cm or less. Due to undeniable intuitive advantages, NFC has been integrated into almost modern smartphones and used widely in various applications. As the number of smartphone users recently increased, there are variety of companies, organizations have adopted NFC technology in their business line. Some of popular applications are mobile payments, public transportation, building access control, coupon publishing, guided shopping and client-care services. Among them, the information in coupon distribution and client-care systems are relatively non-sensitive by dealing with common and public information. As a result of this, its protocol is still simple and does not guarantee for client from such phishing or malicious websites. In this paper, we propose a method for protecting users and clients from those malicious websites. As like anti-phishing program, we also set the authentication server and the server filters out the advertisement is certified or not. In order to ensure secure communications, we encrypted all message packets and then authentication server returns authentication code to client to verify the validity of advertisement link. The whole system is implemented and tested for evaluation purposes.

Keywords: NFC, security, malicious website, phishing website, NFC-coupon

1. Introduction

Due to rapid advance of mobile devices, several services are getting feasible in anytime and anywhere. These services are possible with modern smartphone supporting various network protocols including Bluetooth, Wi-Fi, and NFC. Particularly, NFC technology provides various useful services such as payment and access control systems. Since these services are dealing with sensitive personal and private information, the services should be kept in secret. The best solution for secure networking is encrypting the information with secure cryptography algorithm. In this paper, we would like to introduce a secure protocol for NFC marketing and promotion systems. When the consumer goes to the shop or supermarket, they touch their smartphone to displayed tag and get into link to see information and services. However, the tag or content in tag can be changed by some objective or subjective reasons and the link will be insecure. It is very dangerous if the clients access to some those malicious link, the attacker can steal private information or perform many malicious operations. If these bad situations happen, it can affect or emotionally wreck the relationship between sale companies and clients. Hence, we propose a secure NFC promotion protocol which is simple for only use lightweight encryption and hash function yet satisfy the essential security requirements for a NFC promotion system.

This paper is organized as follows. In Section 2, we introduce related technologies for our implementation. In Section 3, we define security attack types, describe our proposed protocol and present evaluation. In Section 4, we shows our program demonstration. Finally in Section 5, we conclude the paper.

2. Related Works

In this section, we explore the related ticket issue protocol and NFC technologies.

2.1 Kerberos

Kerberos is a network authentication protocol developed as part of project Athena at MIT. It is designed and used in distributed environment enabling clients and servers to establish authenticated communication by using secret-key cryptography. It uses a trusted third-party and optionally may use public-key cryptography during certain phases of authentication [1]. By providing strong authentication, Kerberos protocol messages are protected against eavesdropping and replay attacks. In order to be simple, we would like to adopt their basic architecture into our NFC advertisement protocol.

2.2 NFC

2.2.1 What is NFC?

Near Field Communication (NFC) is a set of short-range wireless, contactless technologies evolved from radio-frequency identification (RFID), typically requiring a distance of 4cm or less to initiate a connection. NFC allows to write small piece of data from NFC device to a tag which is unpowered chip or read data from tag. NFC also allows to exchange data between two NFC devices, like two NFC-enabled smartphones. Tags can range in complexity. The data stored in the tag can also be written in a variety of formats. However, many of the Android framework API are based on NFC Forum standard called NDEF (NFC Data Exchange Format).

Currently, NFC has become increasingly important enablers for ubiquitous computing. This technology simplifies and secures interaction with the automation ubiquitously. Many applications, we use daily, such as credit cards, car keys, tickets, health cards, and hotel room access cards will presumable cease to exist because NFC-enabled mobile phones will provide all these functionalities [2].

Compare to Bluetooth and RFID technology, the most widely used function of Bluetooth is data exchange among mobile phones or between a mobile phone and another Bluetooth-enabled device. However, secure data transfer cannot be performed completely with this technology because it is designed for wireless communication up to 10 meters, which allows malicious devices to alter the communication. RFID is also capable of accepting and transmitting beyond a few meters and has a wide range of uses. NFC technology can be identified as a combination of contactless identification and interconnection technologies. NFC communication occurs between an NFC mobile device on one side and an NFC tag (a passive RFID tag), an NFC reader, or an NFC mobile device on the other side. NFC is restricted for use within close proximity which is up to a few centimeters and also designed for secure data transfer. Besides, though the speed of data transfer of Bluetooth is greater, NFC is more simple and faster to connect. Currently, integration of NFC technology into mobile phones is considered a practical solution because almost everyone carries a mobile phone [2].

2.2.2 List of Near Field Communication Applications

Several hundred trials of near field communication have been conducted. The famous services are mobile payment and NFC access control. In South Korea, SK Telecom and Hana SK Cards provide mobile payment service and, SK Telecom launched guided shopping. Across the globe, there are lots of applications used and developed nowadays. Some popular ones are described from Figure 1 to 4.

Figure 1. NFC payment system

Figure 2. NFC access control or transport payment

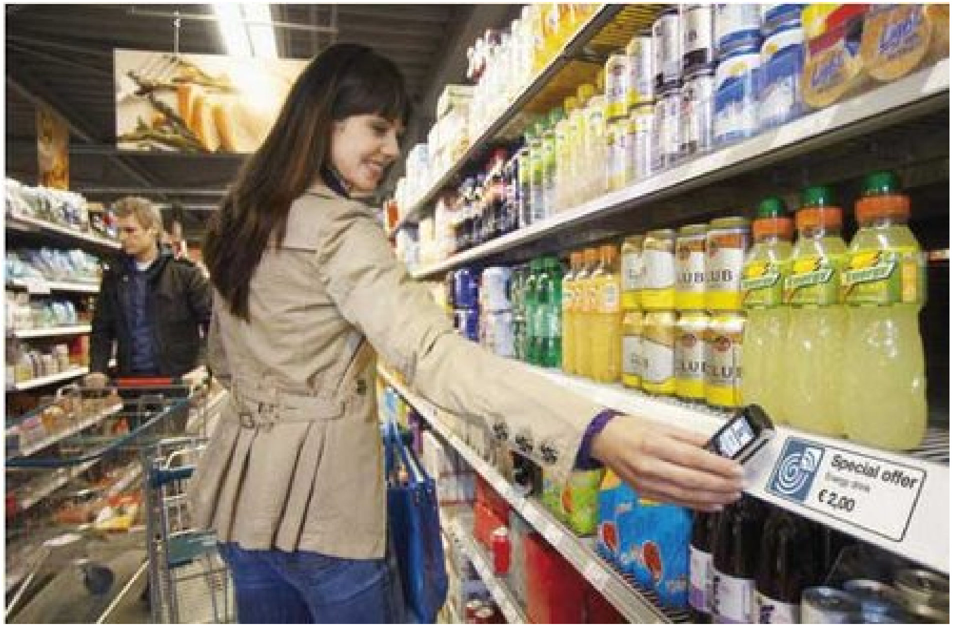


Figure 3. NFC special discount on display

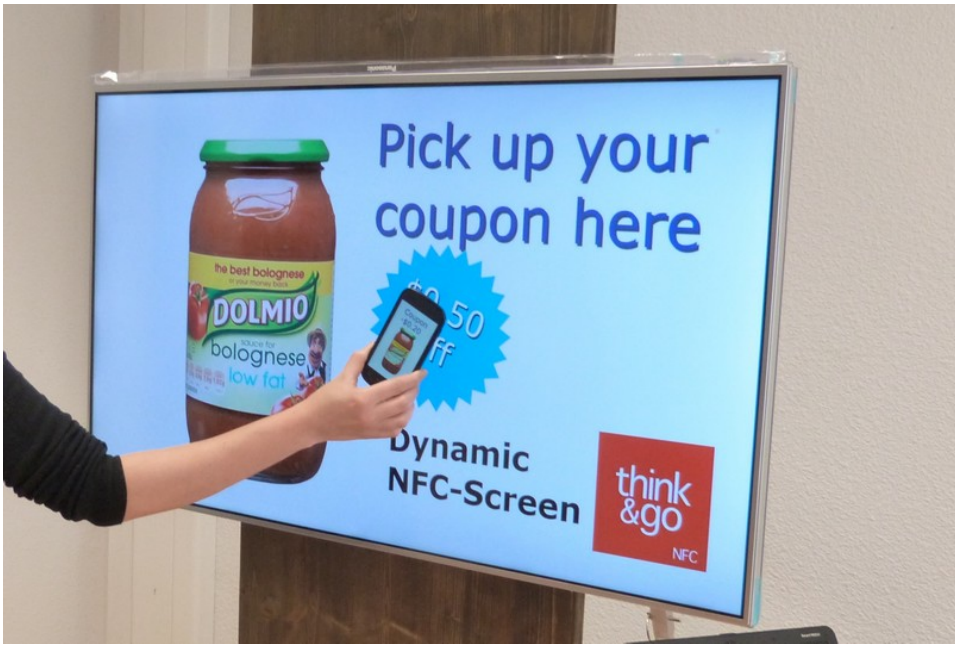


Figure 4. NFC coupon over screen

2.2.3 Networking Protocols

NFC has two different communication modes [2]. Firstly, it is communication in which both initiator and target are battery powered exchanges data through RF field. Secondly, the tag is passive which is radio-energy powered. The initiator active generates an RF field that power up passive tag. Initiator starts communication at selected transfer speed and targets answers using load modulation data at the same transfer speed.

2.2.4 Working Modes

The NFC ecosystem is generated from the synergy of several technologies, including wireless communications, mobile devices, and smart card technologies. Also, server-side programming, web, and cloud services, and XML technologies contribute to the improvement and spread of NFC technology and its applications. These technologies are combined and then provide three main working modes as described below [2].

Reader/writer mode: NFC device read and/or write passive NFC tag and stickers
P2P mode: NFC device exchanges data with other NFC peers, this operation mode is used by Android Beam
Card emulation mode: NFC device itself to act as an NFC smart card. The emulated NFC card can then be accessed by an external NFC reader, such as an NFC point-of-sale terminal.

3. Proposed method

In this section, we present our secure NFC advertising promotion process. The list of essential requirements for an NFC smart poster system then the proposed protocol, evaluation and comparison with previous works will be described respectively.

3.1 Attacking on NFC Smart Poster applications

Here are list of common attacks happen in NFC applications generally and NFC smart poster applications specifically. If the protocol can defeat against these secure stumbling blocks, the system will be run properly.

- Eavesdropping: In NFC smart poster application, the communication between reader and tag is unprotected in most case. Therefore, eavesdroppers can listen in. Moreover, if access control is not implemented then the tag’s memory can be read. We can use encryption method to get confidentiality.
- Data corruption: this is the way attacker crash, delete or modify the message, so the reader can not read the content of the card. An efficient access control and authentication protocol is necessary such as challenge-response to prevent it. Hash code is used to ensure data integrity property.
- Replay attack: The services server and authentication server can be died by communication traffic jam. This is replay attack. Nowadays, we often use timestamp technique to prevent this kind of attack.
- Tag content spoofing: This is the way in which attacker insert more space, tab or new line characters into the title record. With the possibility to lead a victim into loading a malicious website, many attacks can be carried out. Among of them is Man-in-the-Middle attack at which attackers can steal credentials or run malicious content. URI spoofing also include case of attacking the mobile telephony service. By this way, attacker modify the smart poster which displays a specific phone number. However, when it is activated, the phone dials another phone number. The case is same in short messages (SMS).
- Denial-of-Service attack: This kind of attack try to break the relationship between the customer and the service provider. For instance, when client touch their phone to the tag, the smartphone reboot every time. As a result, the clients likely stop using the service. Other case is when attacker can send many request to authentication server, the network bandwidth capacity is not enough to sustain, the clients will also feel waste time and not use this services anymore. The costly way to defend it is to buy more bandwidth.

Denial of service is about capacity. DoS (denial-of-service) and DDoS (distributed denial-of-service) are still a challenge for security specialists.

The above list is some type of attacks in NFC smart poster applications. Besides, there are some other important requirements for it such as the availability, performance of system, the ability of client can verify the authentication code is original from the server. And the trust, easy to use to promote client to use this services. The user can report problem whenever problem occurs as fast and easy as possible.

3.2 Proposed protocol

We use shopping scenario to explain our protocol. When the client go to the supermarket and want to see all promotion information of products, they close their NFC-enabled smartphone to the tag and they can check it. The problem is when some attackers remove the original tag and change into other tags with phishing or malicious website linking into them. The client does not notice that whether the page is phishing site or not. When they get to that link, they will be attacked. This vulnerable situation should be concerned seriously. This is a motivation of our works.

The Figure 5 shows diagram for protecting client from attacker. We need an authentication server to check whether the link is officially generated from manufacturer or not. It also discriminates client and checks who are allowed to get into that link and use the services. The clients require the authentication code, the server will return it with notice messages. After then, the client can open list of promotions or other information from seller for them.

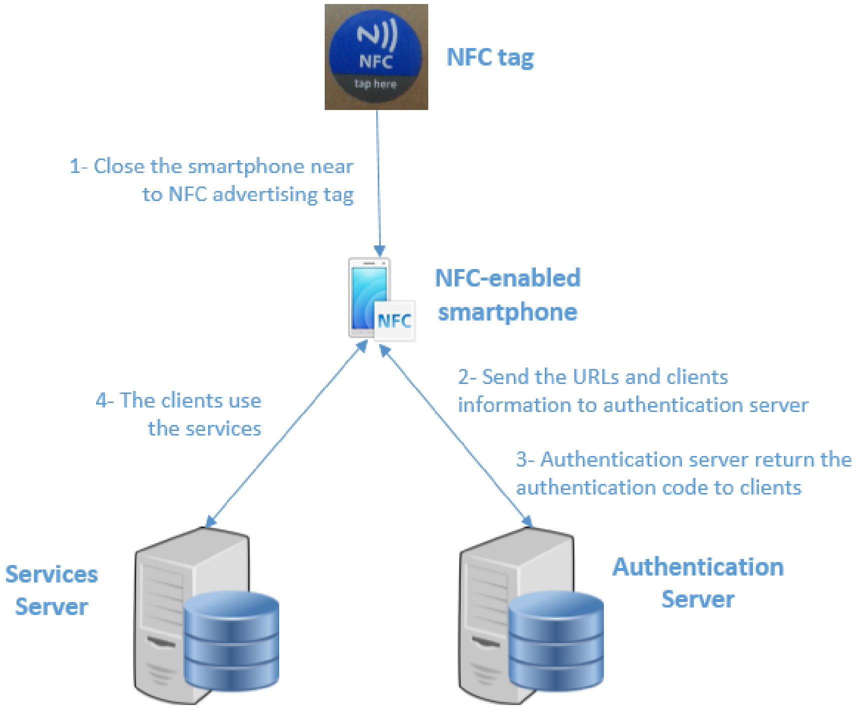

NFC tag
NFC
tap here
1- Close the smartphone near to NFC advertising tag
NFC-enabled smartphone
NFC
4- The clients use the services
2- Send the URLs and clients information to authentication server
3- Authentication server return the authentication code to clients
Services Server
Authentication Server

Figure 5. Secure website in NFC application

In this scheme, the Type Name Format (TNF) used is NFC Forum external type in which its value is 0x04 identified inside an NDEF message. TNF is 3-bit field in which its value represents the structure of the value of TYPE field. These values are defined by NFC Forum. We used external type instead of Absolute URI (0x03) for more secure. If Absolute URI was used, all NFC-enabled NFC smartphone can open it automatically after close the phone near the tag. And it will be dangerous in case the link is a malicious resource. If TNF external type was used, only smartphone with specific installed applications can read and user can choose options to perform activities or not. It is obviously more secure.

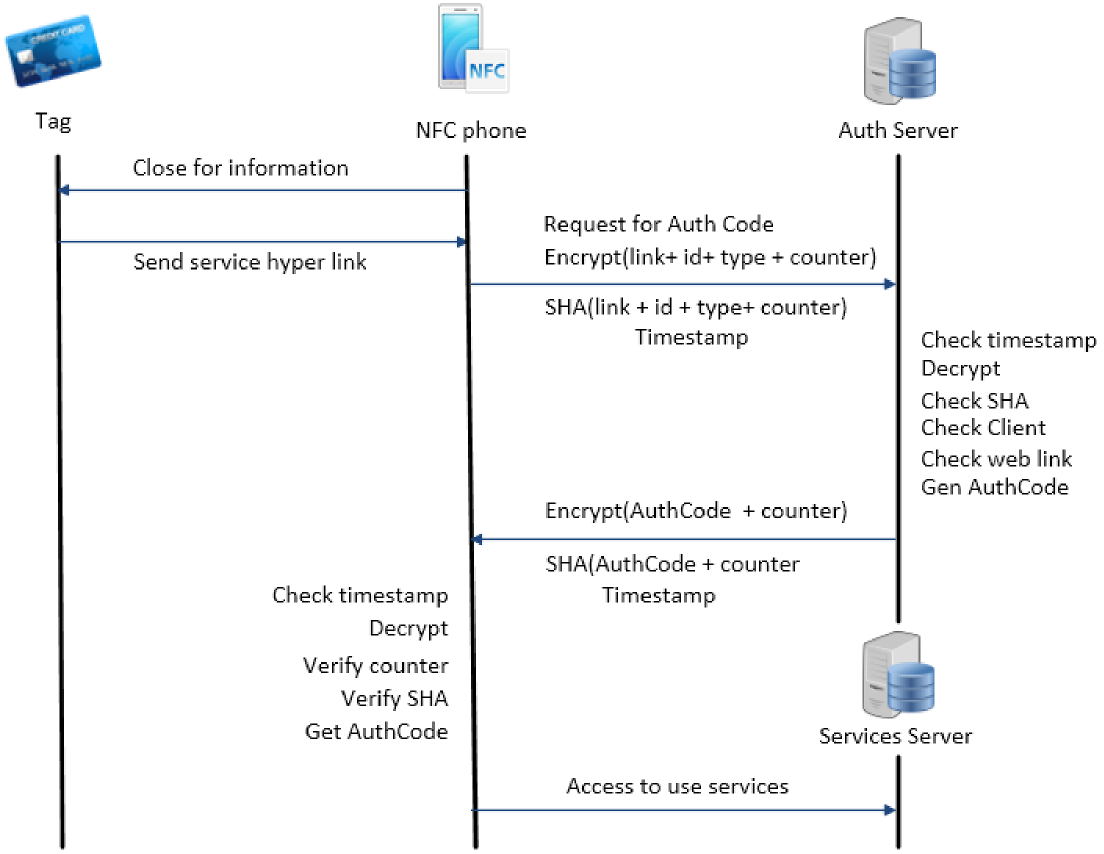


Figure 6. The protocol for securing website in NFC

The protocol process is described in Figure 6 above and includes following steps:
1. The consumers will close their NFC-enabled smartphone to the NFC tag to get the link to access to the services. Then they will make the request to ensure that the link is valid and officially from the services department of the manufacturers. The package comprises of three main parts which are the encryption of link, client identification (id), type of client like general, gold or vip member and the counter, the hash code SHA of the content like plaintext in above encryption and the timestamp. The package will be sent secretly to authentication server.
2. After receiving the data message from the client. The authentication server will check the timestamp. By using timestamp technique, we define a specific threshold to make sure that the particular request can not be used than one. It is for fight against replay attack. When the

timestamp check is done, the package will be decrypted, then used the decrypted content to be input of generating SHA to check whether the data is modified or not.
3. The server will check the client identification and their typing member. Specifically, if the client type is general, they only can see list of promotions for general clients. If they are Gold members, they can see both list of promotions for general and gold members. If they are VIP consumers, they can check and take part in all items in all the promotion list.
4. The server will check whether the link that consumer got by their NFC-enabled smartphone is their official link or others.
5. Based on the results of above consecutive four steps, the server will generate a suitable authentication code and make as part of content to send back as a response to client.
6. The responding package will be made. It includes the encryption of authentication code and counter that server received, the hash code of authentication code and counter and the timestamp.
7. The client receives response from the server. The timestamp will be check first to ensure that is just be made from the server. The decrypt activity is carried out as following. Then on client side, the counter will be compared with the counter they sent to server before. The counter is used as factor for verifying server. Because only server and client know it. And it will be changed every time. There is another way the client can verify the server is the client can generate a random number then encrypted and sent to server.
8. After verifying timestamp and counter successfully, the hash code will be created to ensure that the content is not modified by other party. The input for making hash code is the decrypted text they receive after decrypting the encrypted package.
9. As the final step, the client can receive the authentication code. Based on the code, the program will generate the information in text as a notice, warning and so on for client easy to read and understand. Then they can use the service in a safe manner and need not to worry about phishing or malicious website.

The different point between Kerberos and our method is Kerberos publishes the ticket to access to service server. In our method, we give a role of link validity to authentication server. The server checks out the link throughout the white lists which includes a list of valid site addresses and then give a notice to client whether it is right or wrong. However, in our protocol, we do not check only website link but also client authorization. And client identification checking will be carried out first before checking the link.

3.3 Evaluation

In this section, we will discuss about the previous works on preventing malicious NFC tag by authentication scheme and achieved results in our protocol.

3.3.1 Related NFC Protocols

As NFC technology has many undeniable advantages, it has been become a vitally inherent part of Internet of Things (IoT). It has been used widely in many areas in our life and, it is nowadays more convenient for users since it can be integrated seamlessly to smartphone because many people have their own smartphone today. In this paper, we only mention about advertisement using NFC. It can be easily seen in supermarket for client can check promotion program, product information or in cinema for client can check film information, watch film trailers or advertisement in subway and so on.

As used for client services, advertising smart poster is not be cared enough about security matter, there are not many works about it. For example, to against illegal use in smart poster, a protocol of securing mCoupon authentication based on low-cost NFC has been proposed. They however did not have source code of previous scheme, and it has not been compared in term of performance yet [5]. Another work on preventing malicious NFC tags is [6]. They designed a functional hardware shield named “Engarde” to protect user smartphone from malicious NFC tags that try to compromise. In [7], an offline NFC-enabled ticketing system for small events has been proposed, they used trusted service manager (TSM) as insurance for users.

Currently, for avoiding phishing, users often have to protect themselves against it. Not only in NFC advertising poster but also in personal email, attackers do this by sending fraudulent URLs to email or write it into a NFC tag and put somewhere. When user access to that link, it will direct users to a websites which have specifically been set up to steal user’s personal data, commonly passwords or banking information. For that reason, we would like to introduce a good protocol to help users avoid phishers in NFC-adopted applications.

3.3.2 Protocol Evaluations

The protocol can satisfy almost requirements of a smart poster system. Here are a list of achievements that our proposed method got:

- Confidentiality: all of data is encrypted when transferring through network
- Replay attack: to prevent replay attack or playback attack in which a valid data transmission is maliciously or fraudulently repeated or delayed, we use timestamp technique. The sent data package is always include timestamp in both client and server side.
- Data integrity: to verify the received data whether is corrupted or not, we use SHA to generate hash code. By that way, after decrypting the data, both server and client side can generate hash code again and check data corruption.
- Server Verifiability: by using counter in message request, when the client receive the authentication code from the server, they can verify this message is from authentication server or not.
- Denial-of-service: timestamp is also useful to prevent DoS attack. Furthermore, we can set up IDS (Intrusion detection system) or IPS (Intrusion prevention system) in server to fight against DoS attack.
- Prevent URI spoofing: before opening URI in client smartphone, the content will be sent to authentication server to both authenticate client and the web link. So client no need to care about URI spoofing attack. The server also authorize the client permission to use to their specific delivered services.

The drawback of our protocol is we use counter instead of random number procedure and used it in part of common key which is more secure. However, it will cost more time. It is believed other financial systems such as NFC payment or m-coupon should achieve highest security level as possible. It is more necessary than advertisement application in which performance is more necessary. Another drawback is we just used and deployed server side on PC computer which is different from real server. In order to apply proposed method in practical system, we should modify to suit depend on specific cases. For instance, in laboratory we use file system as a database and implement in Java platform, but in larger case such as big company or government organizations, they can use better and more professional database such as

Access, DB2, No SQL, Hadoop, Oracle and so on depend on amount of data and development fees.

4. Demonstration

In this section, we show the implementation of our proposed protocol shown in part 3 above. The communication between user smartphone and server is describing the both client and server sides. In this demonstration, we used UDP network protocol for communication and LEA (Lightweight Encryption Algorithm) cryptography [4] to encrypt and decrypt data. Both of them were used for high performance under smart phone environments.

4.1 Deployment environments

In order to deploy the demonstration, a NFC tag, NFC-enabled smartphone with Android OS version 4.0 or later and a Personal Computer (PC) in which Java environment (JDK) is installed are needed. Particularly, we use a NFC white card that is often used for developers, smartphone Samsung Galaxy S2 which is NFC-enabled, Android version 4.0.3, model SHW-M250S and a computer has installed Window 7 and JDK 7.0 on it. Both smartphone and PC need to connect to network.

4.2 UDP communication between NFC-enabled smartphone and PC server

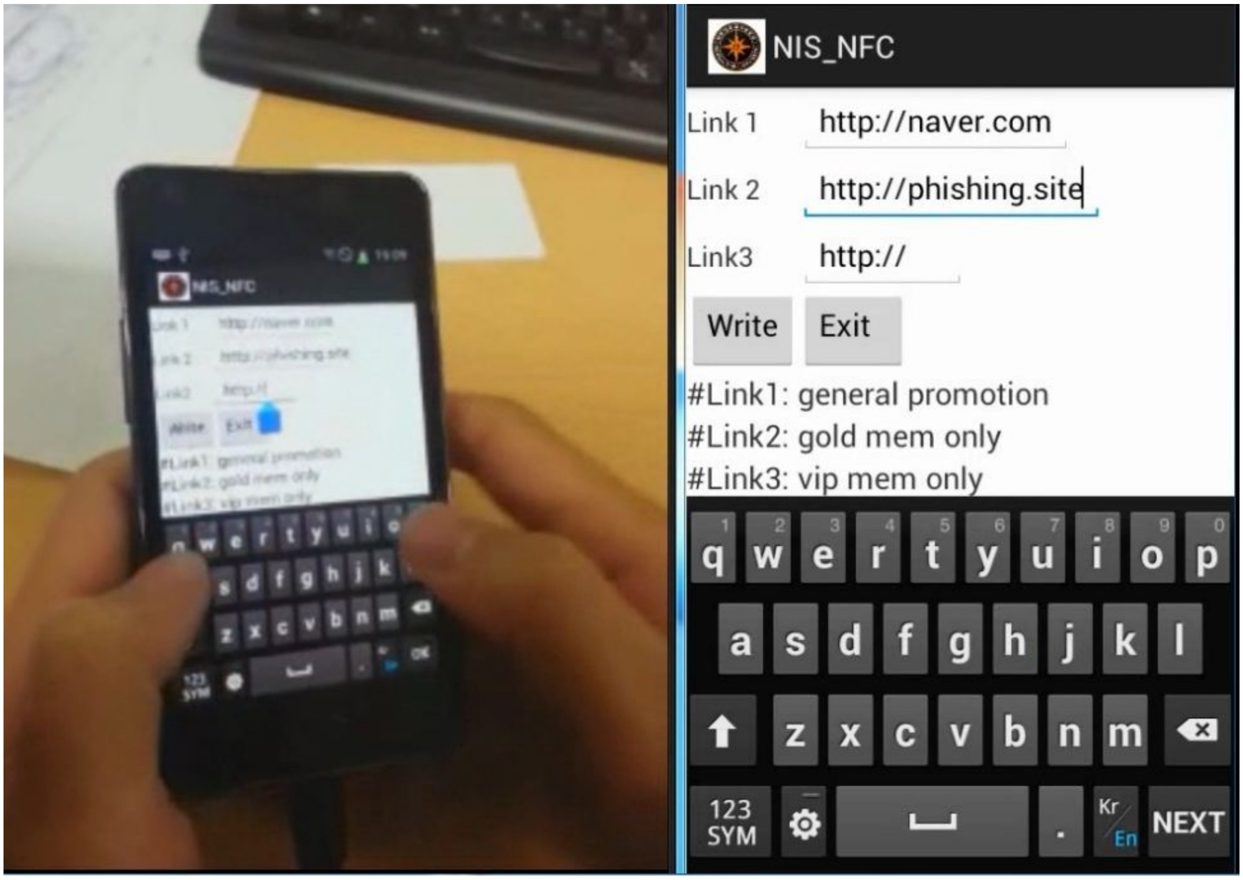
The User Datagram Protocol (UDP) is one of network protocols in transport layer used for the Internet. Compare to Transmission Control Protocol (TCP), UDP is a simpler message-based connectionless protocol that do not set up a dedicated end-to-end connection. Communication are achieved by transmitting information in one direction from source to destination without verifying the readiness or receiver's state [3]. Therefore, it is unreliable. However, the advantage of UDP network protocol is its lightweight property. For this proposed client-care system, we use UDP protocol due to this advantage.

The Android NFC-enabled smartphone is used for client side. When clients close their smartphone near to the NFC tag to get promote information. In order to be sure that the link they receive is originally released from the services party, they can check it by sending their client identification and that link to authentication server. After that, they will receive authentication code from service manufacturers. The benefits that company gains by issuing this policy are persuasion and client data. Finally, they can create some other product consumer strategies.

4.3 Client side

In our advertisement diagram, the NFC-enabled smartphone will play role as client in client-server model. When the people close it to near promotion tags. I will catch content which is some link and description. In order to ensure, it is a healthy and original from manufacturer, consumer can check the link by sending it to authentication server.

The Figure 7 below shows the screen of client side when writing links to tag. In our demonstration, there are three types of clients who are general client, gold client and vip client with level from low to high respectively. Below is the case that the input for general link is http://naver.com, the input for gold link is http://phishing.site which is a phishing website and the input for vip client is http://infosec.pusan.ac.kr.



NIS_NFC

Link 1 http://naver.com

Link 2 http://phishing.site

Link3 http://

#Link1: general promotion

#Link2: gold mem only

#Link3: vip mem only

Figure 7. Screen of client side in writing content to tag

All clients can access to the general link. The gold clients can access to gold link or general link. The vip clients can access and use all services.

4.4 Server side

As a pilot project, we use PC window 7 with Java platform installed as a server to deploy. We will open some port and it always listen out requests from client side which are client's smartphones. We implement it as console application, and use text file as database. As mention before, database type can be chosen depend on the amount of data we want to store and the fee to use and maintain it. The structure of database is as follows:

Table Link

Link	Text	Not null

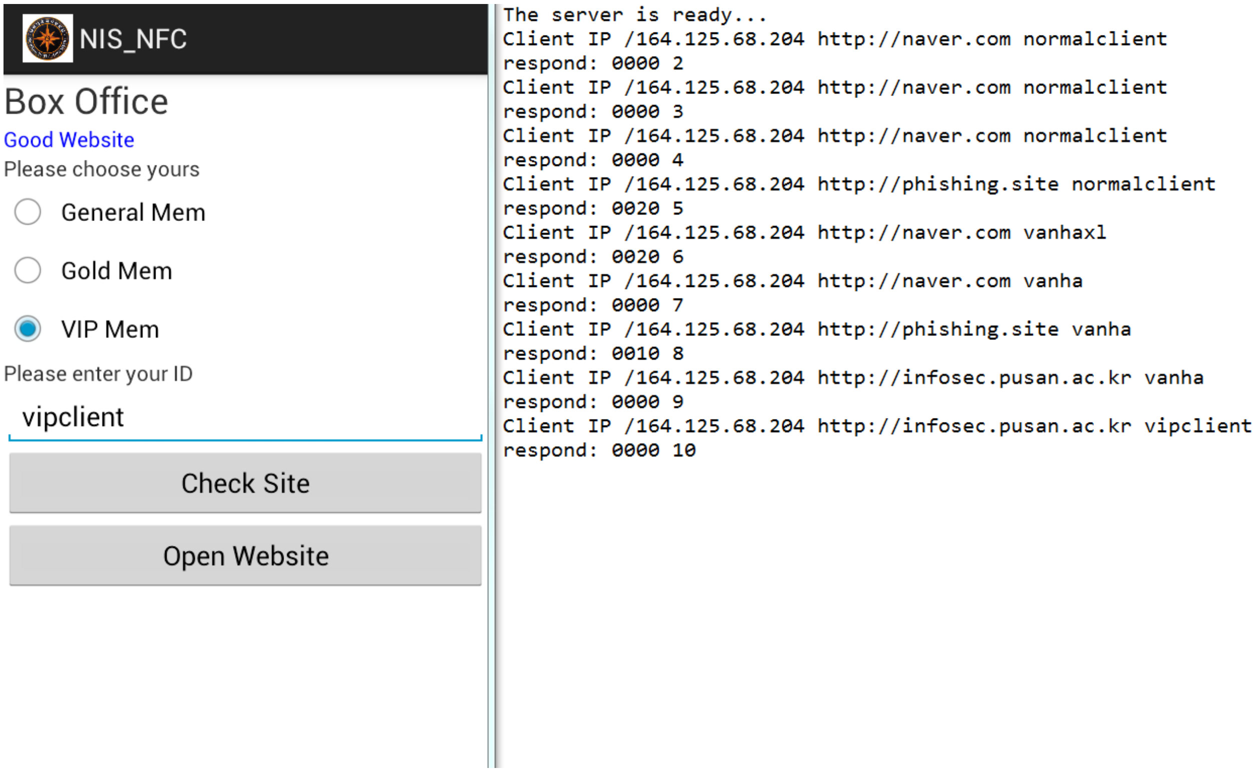
Table Client

clientID	Text	Primary key
clientType	Text	Not null

After checking timestamp and verifying hash code, the encrypted data package will be decrypted. The client identification and client type will be checked in database. Then the link will be checked. If it exist in database, it is the official link from manufacturer.

In server, the log activity also can be made to log all client access time. It would be really helpful data for company to analyze to get better marketing campaign.

The Figure 8 below shows screen of client in the left and server in the right. This case is when a vip client check services for vip members. They receive the authentication is 0000 which is a good website. The server also can back log all activities and used in the future.



Box Office

Good Website

Please choose yours

○ General Mem

○ Gold Mem

● VIP Mem

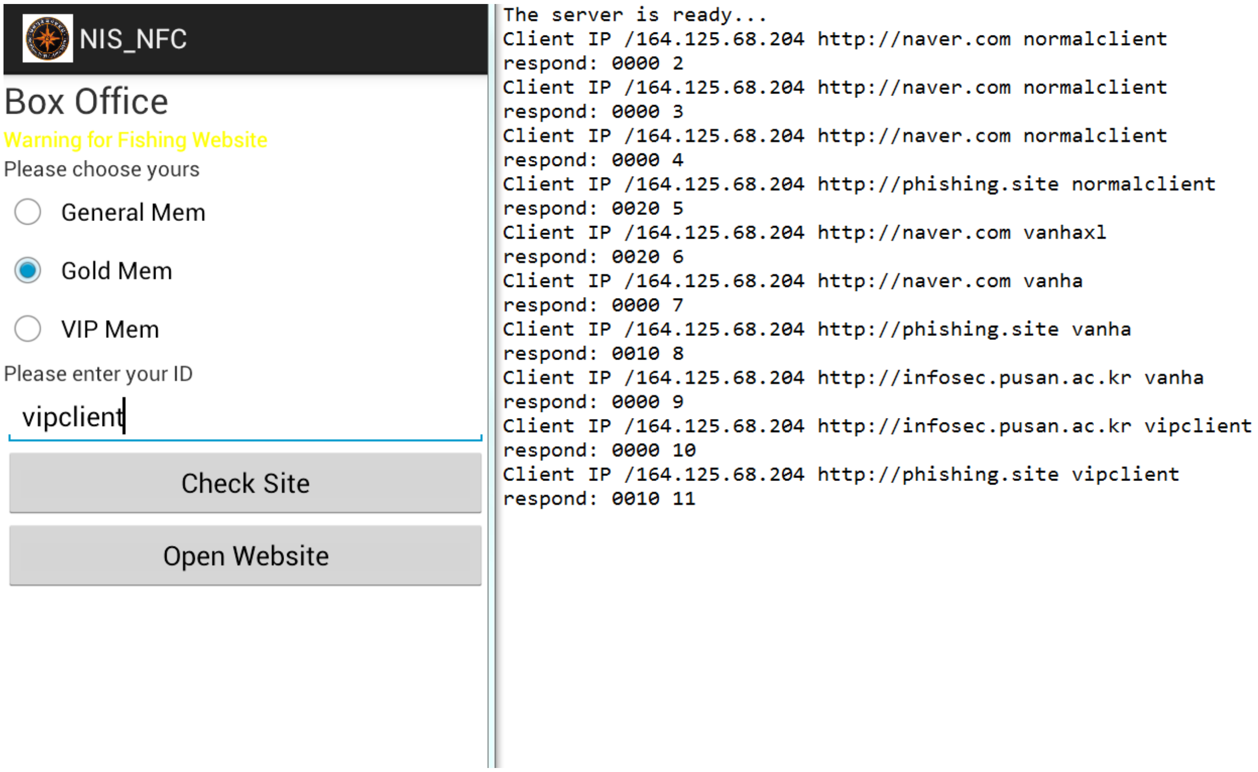
Please enter your ID

vipclient

```
The server is ready...
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 2
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 3
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 4
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 5
Client IP /164.125.68.204 http://naver.com vanhaxl
respond: 0020 6
Client IP /164.125.68.204 http://naver.com vanha
respond: 0000 7
Client IP /164.125.68.204 http://phishing.site vanha
respond: 0010 8
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vanha
respond: 0000 9
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vipclient
respond: 0000 10
```

Figure 8. Screen of client side (left) and server side (right) with response of Good Website

The Figure 10 describes a case of when vip client check the service for gold members. As mention previously, the vip client can use all the service. However, the link for gold member has been modified by attacker. So the client will receive the status warning about it.



Box Office

Warning for Fishing Website

Please choose yours

○ General Mem

● Gold Mem

○ VIP Mem

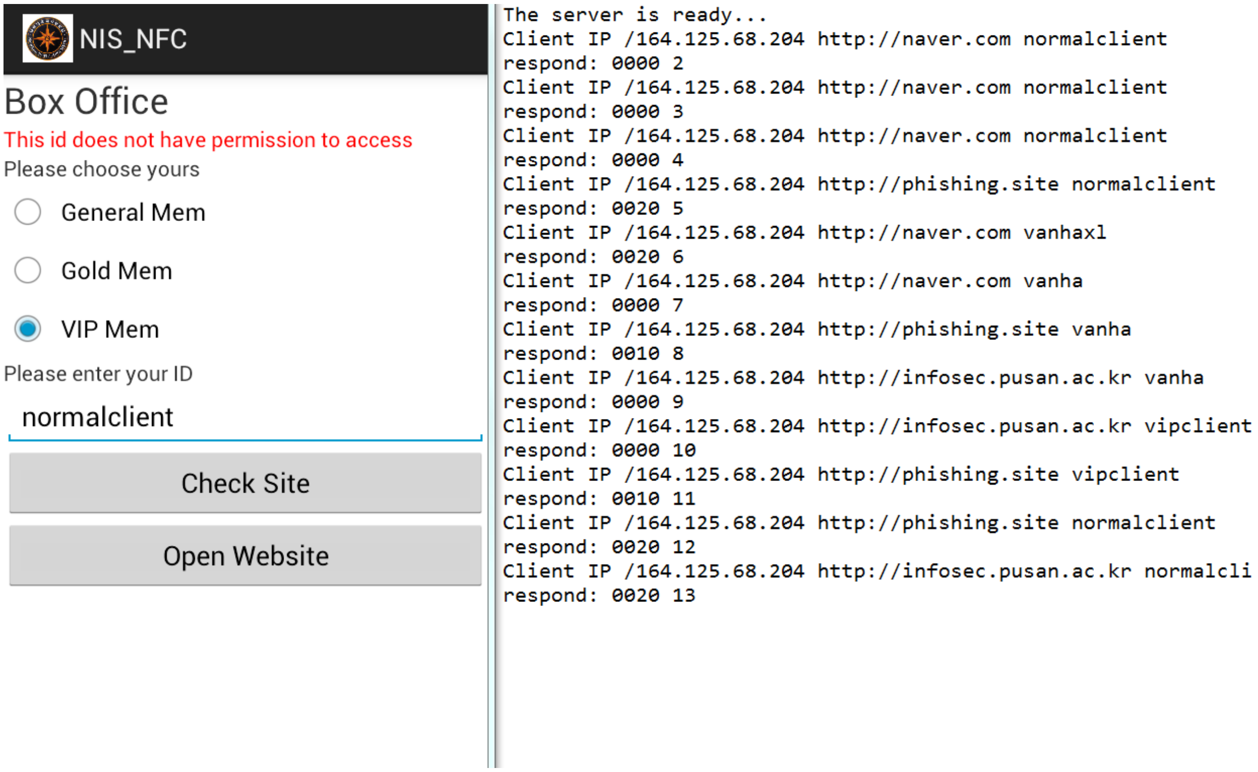
Please enter your ID

vipclient

```
The server is ready...
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 2
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 3
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 4
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 5
Client IP /164.125.68.204 http://naver.com vanhaxl
respond: 0020 6
Client IP /164.125.68.204 http://naver.com vanha
respond: 0000 7
Client IP /164.125.68.204 http://phishing.site vanha
respond: 0010 8
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vanha
respond: 0000 9
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vipclient
respond: 0000 10
Client IP /164.125.68.204 http://phishing.site vipclient
respond: 0010 11
```

Figure 9. Screen of client side (left) and server side (right) with response of Warning Fishing

The Figure 10 shows a case of a normal client want to use the service for vip member. As a result, they will have no access permission to use it.



Box Office

This id does not have permission to access

Please choose yours

○ General Mem

○ Gold Mem

● VIP Mem

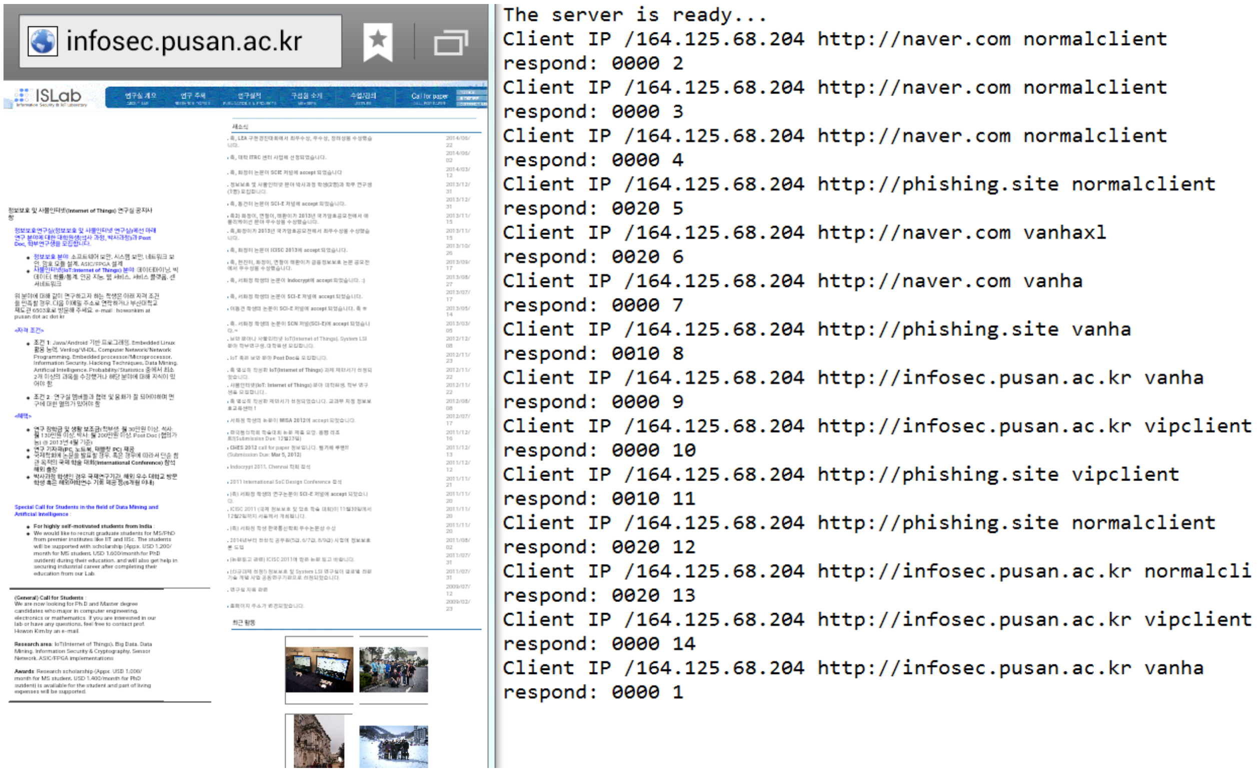
Please enter your ID

normalclient

```
The server is ready...
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 2
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 3
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 4
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 5
Client IP /164.125.68.204 http://naver.com vanhaxl
respond: 0020 6
Client IP /164.125.68.204 http://naver.com vanha
respond: 0000 7
Client IP /164.125.68.204 http://phishing.site vanha
respond: 0010 8
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vanha
respond: 0000 9
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vipclient
respond: 0000 10
Client IP /164.125.68.204 http://phishing.site vipclient
respond: 0010 11
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 12
Client IP /164.125.68.204 http://infosec.pusan.ac.kr normalcli
respond: 0020 13
```

Figure 10. Screen of client side (left) and server side (right) with response of No Access Permission

After a good authentication code from server, the clients can use the services they desire. The Figure 11 show a case in which the client open the service link and use it.



```
The server is ready...
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 2
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 3
Client IP /164.125.68.204 http://naver.com normalclient
respond: 0000 4
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 5
Client IP /164.125.68.204 http://naver.com vanhaxl
respond: 0020 6
Client IP /164.125.68.204 http://naver.com vanha
respond: 0000 7
Client IP /164.125.68.204 http://phishing.site vanha
respond: 0010 8
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vanha
respond: 0000 9
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vipclient
respond: 0000 10
Client IP /164.125.68.204 http://phishing.site vipclient
respond: 0010 11
Client IP /164.125.68.204 http://phishing.site normalclient
respond: 0020 12
Client IP /164.125.68.204 http://infosec.pusan.ac.kr normalcli
respond: 0020 13
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vipclient
respond: 0000 14
Client IP /164.125.68.204 http://infosec.pusan.ac.kr vanha
respond: 0000 1
```

Figure 11. Screen of client side (left) and server (right) using the service by open the link

5. Conclusion

In this paper, we presented a secure NFC advertisement protocol. Traditional NFC link access is dangerous for consumers when attackers put some malicious NFC tags somewhere in subway station, supermarket or cinema. Current NFC system does not ensure secure service distribution out of its lacking authentication process. We challenge to these vulnerabilities by referring Kerberos system. Unlike Kerberos, we use authentication server as a link validity checker which points out whether the link is officially from the service providers or not. As shown in part 3 above, the protocol satisfies essential requirements in term of security and simple, fast in in term of performance manner. It is believed that the proposed protocol could contribute to not only in advertising and client-care services but also in wider secure and robust NFC services. The future work is optimizing, upgrading suitably in applying the protocol depend on specific aimed systems.

Reference

[1] Kerberos, available at http://web.mit.edu/kerberos/

[2] V.Coskun, K. Ok and B. Ozdenizci. “Professional NFC application development for Android”, 1st Edition, John Wiley & Sons, 2013

[3] UDP, available at http://en.wikipedia.org/wiki/User_Datagram_Protocol

[4] K. H. Ryu and D.-G. Lee. “Lea: A 128-bit block cipher for fast encryption on common processors. Information Security Applications,” WISA’13.

[5] S. W. Park and I. Y. Lee “Efficient mCoupon Authentication Scheme for Smart Poster Environments based on Low-cost NFC”, International Journal of Security and Its Applications, Vol. 7, No.5, pp 131-138, 2013.

[6] J. Gummeson, B. Priyantha, D. Ganesan, D. Thrasher and P. Zhang. “EnGarde: Protecting the mobile phone from malicious NFC interactions”, Proc. 11th annual international conference on Mobile systems, applications and services, pp 445-458, 2013

[7] S. Chaumette, D. Dubernet, J. Ouoba, E. Siira and T. Tuikka. “Architecturer and Evaluation of a User-centric NFC-enabled Ticketing System for Small Events”, Lecture Notes of the Institute for Computer Science, Social Informatics and Telecommunication Engineering Vol. 95, Springer, pp 137-151, 2012.