International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:11, 2013

User Behavior Based Enhanced Protocol (UBEP) for Secure Near Field Communication

Vinay Gautam, Vivek Gautam

***Abstract*—**With increase in the unauthorized users access, it is required to increase the security in the Near Field Communication (NFC). In the paper we propose a user behavior based enhanced protocol entitled 'User Behavior based Enhanced Protocol (UBEP)' to increase the security in NFC enabled devices. The UBEP works on the history of interaction of a user with system.The propose protocol considers four different factors (touch, time and distance & angle) of user behavior to know the authenticity or authorization of the users. These factors can be same for a user during interaction with the system. The UBEP uses two phase user verification system to authenticate a user. Firstly the acquisition phase is used to acquire and store the user interaction with NFC device and the same information is used in future to detect the authenticity of the user. The second phase (recognition) uses analysis of current and previous scenario of user interaction and digital signature verification system to finally authenticate user. The analysis of user based input makes a NFC transaction more advance and secure. This security is very tactical because it is completely depends on usage of the device.

***Keywords*—**Security, Network Field communication, NFC Protocol.

I. Introduction

THE Near Field Communication (NFC) is a technology for contactless short-range communication based on the Radio Frequency Identification (RFID). It uses magnetic field induction to enable communication between electronic devices. The number of short-range applications for NFC technology is growing continuously, appearing in all areas of life. Especially the use in conjunction with mobile phones offers great opportunities. The specification details of NFC can be found in ISO 18092[1], [2]. The NFC is characterized as a very short-range radio communication technology with a lot of potential, especially when applied to mobile handsets. It is a short-range radio technology that operates on the 13.56 MHz frequency, with data transfers of up to 424 kilobits per second. The NFC communication is triggered when two NFC-compatible devices are brought within close proximity, around four centimeters. The interface can operate in several modes. The modes are distinguished whether a device creates its own RF field or whether a device retrieves the power from the RF field generated by another device. If the device generates its own field it is called an active device, otherwise it is called a passive device. Active devices usually have a power-supply passive device usually don't (e.g. contactless Smart Card). Three different configurations of NF devices are shown in Table I.

TABLE I
Communication Configurations

DeviceA	DeviceB	Description
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF filed is generated by Device B only

There are different security issues related with the NFC as described below:

A. Why Enhanced NFCP

- NFC technology combines the speed and ease of use of a contactless card, such as the Oyster Card with the convenience and flexibility of a smart phone. With other new service technologies, along with NFC come new opportunities for fraud. This work provides an insight into the technology and the services that are expected to be deployed through NFC and gives a high--level review of the information security risks associated with the NFC device, along with an introduction to the countermeasures expected to be embedded in the services.
- Phishing attacks could easily be performed by modifying or replacing tags. This is a simple and inexpensive way to mislead the user. Using signatures on tags and transporters would be suitable way to overcome this issue.
- Eavesdropping is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can use an antenna to receive the transmitted signals. If the attacker has required knowledge on how to extract the transmitted data out of the received RF signal. There is no special equipment required to decode the RF signal.

The NFC communication is usually done between two devices in close proximity. This means they are not more than 10cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable an RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more [3], [10].

- RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB,

V. G. is an Assistant Professor in CSE department of Desh Bhagat University. He is also Doctoral Research Scholar in School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India (e-mail: vinaykkr@gmail.com).
V. G. is working as Software Developer of IT Wing of Path InfoTech Pvt. LTD. Noida.

the environment)

- Characteristic of the attacker's antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device

Additionally, it is of major importance in which mode the sender of the data is operating. This means whether the sender is generating its own RF field (active mode) or whether the sender is using the RF field generated by another device (passive mode). Both cases use a different way of transmitting the data and it is much harder to eavesdrop on devices sending data in passive mode. In order to not leave the reader without any idea on how big the eavesdropping distances are, we give the following numbers, which as stated above are not valid in general at all, but can only serve to give a rough idea about these distances. When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1m.

- Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device. Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.
- In data modification the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption. The feasibility of this attack highly depends on the applied strength of the amplitude modulation. This form of attack is possible for some bits under different coding schemes. There are a number of ways to provide protection against this form of security attack. It is impossible for an attacker to modify all the data transmitted at the 106 Baud data rate in active mode. As a result, the 106 Baud data rate, active mode would be required for data transfer in both directions.
- This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.
- In the classical Man-in-the-Middle Attack, two parties which want to talk to each other called Alice and Bob are tricked into a three party conversation by an attacker Eve.

In the paper we propose a new protocol User Behavior based Enhanced Protocol (UBEP) for secure communication between devices. The protocol considers different factors of user behavior to authorize or authenticate users.

The rest of the paper is organized as follows. The different ways in which the security is implemented in conjunction with NFC is described in Section II. Section III explains complete working of User Behavior Based Enhanced Protocol (UBEP) adopted by us. In Section IV explained the implementation and analysis of protocol in context of previous protocol. Section V is the concluding section.

II. Related Work

Different ways are used to secure communication using NFC devices and are discussed below in [4]-[9], [11]-[14].

A secure channel is established in [4] over NFC to protect communication against eavesdropping or data modifications. This can be done very easily, because the NFC link is not susceptible to the Man-in-the-Middle attack. Therefore, well known and easy to apply key agreement techniques without authentication can be used to provide a standard secure channel. This resistance against Man-in-the-Middle attacks makes NFC an ideal method for secure pairing of devices.

The Signature Record Type Definition added in [5] to integrate the protection and authenticity to the NFC Data Exchange Format, it also opens up for several security vulnerabilities. The problem of establishing trust in signed data and its origin. Further, in this a new class of attacks against signed NDEF records, which called as the "Record Composition Attack".

The first generic practical implementation of a contactless relay attack using only NFC-enabled mobile phones and software applications given in [6]. They build a passive proxy-token, a proxy reader and a suitable communication channel between the proxies by using only publicly available platform APIs. Our relay attack demonstrates the reduced complexity of attack as it did not require special hardware. The attack implementation required no unlocking of devices or secure elements, no hardware or software modification to the phone platform, and minimal knowledge of the data that was to be relayed. Neither was there any need to access the mobile network or any related services, and we utilized devices of a form factor accepted by merchants. The attack implementation was application independent so would work against a number of conventional contactless systems. For example, we experimentally verified that the implementation work against both test payment and e-passport systems. The attack therefore holds implications for all contactless systems and can be implemented against any system using NFC or compatible technology, with a few exceptions as discussed above in Section I. Research work on relay attacks, preceding this paper, have often been dismissed by system implementers as a complicated attack that is unlikely to be used in the real world. The 'software-only' nature of this relay attack implementation increases the likelihood of it being used in practice (e.g. an attacker simply downloads the applications), and so represents

a potential threat to real-world systems.

The cross-layer approach is taken in [7], [8] to enhance today's standardized NFC protocol. The enhancements in the protocol are more efficient than the standard handshake sequence, and have more affinity with the Internet. The enhanced protocol contributes to wireless access convergence while keeping backward compatibility. The enhanced NFC protocols are proposed and evaluated in terms of performance and complexity.

The novel NFC technology used in [9] for enabling secure mobile applications and demonstrate it through the proposal of a NFC peer-to-peer mobile application, founded on NFC Forum rules and Android NFC APIs. Many solutions were experimented and evaluated but this was the best to demonstrate a proposal to solve this problem because it turns simple a bored task to perform. User does not need to write many instant messages to request his/her network operator for change money to another person. With a simple touch of two NFC enabled devices it is possible to create a safe, reliable, and trusted operation for money exchange. Secure operations among devices were also demonstrated. Then, this technology offers the possibility to create a huge amount of other type of applications supporting secure communications among mobile devices. This application was also proposed because some network operators want to simplify the credit transfer operation. Given the available solutions in terms of mobile operating systems, it was deployed on Android mobile operating system. However, it can easily be extended to other operating systems with NFC support. Then, the migration of this application to other operating systems device belongs to future interests, improving and also creating new solutions.

A secure NFC is described in [11] for a service-oriented environment, which provides the needed data protection without requiring costly changes to the payment processing infrastructure. In the payment transaction, a personal mobile phone is viewed as a single, user-trusted touch point. This approach better protects user credentials, provides better user control over the transaction, and supports both proximity and remote transactions. The prototype has been integrated with an in store kiosk application and a HP multi-channel banking platform to demonstrate its value in the retail environment.

A low cost security framework is proposed in [12] which include a PKI based security protocol to secure NFC transactions. This is used to integrate transactions involving external contact-based smart cards, for the purposes of e-identification, e-payment, e-ticketing, and communication services. A secure Communications Protocol Translator Interface (CPTI), which allows an NFC enabled mobile phone to access and use, over a contact less interface, any additional smart cards (or secure elements (SE)).Using CPTI, it is now possible to have communication and interaction between passive security tokens as well as to use external contact based security tokens in the NFC environment.

A system of virtual coupons (so-called mCoupons) described in [13] to protect against illicit use. The NFC used inexpensive passive tags to prevent attacks in a decentralized approach. From a user's perspective, the system is based on the very intuitive usability of NFC, by simply touching NFC targets with a mobile device for pick-up and cash-in of mCoupons.

A middleware is proposed in [14] using actual NFC hardware and Symbian-based mobile phones to secure transition in NFC enabled devices.

In this paper, our aim is to enhance security in communication with NFC devices. So, in this work we have enhanced the capability of NFC protocol with user interaction history to authenticate a user. The security is maintained with a user unique capabilities and procedures for accessing NFC and protecting her/his potentials.

The main contribution of paper is in two-fold

- To propose a new protocol User Behavior based Enhanced Protocol (UBEP) for secure access of NFC devices.
- Increase the Quality of Service (QOS) to the user in respect to Near Field Communication.

III. User Behavior Based Enhanced Protocol (UBEP) for Near Field Communication

The improved NFC considers user inputs to make decision on authenticity of user. This makes a NFC device more advance and secure from any unauthorized user from the existing model. This security is very tactical because it is totally depend upon user behavior.

The protocol uses two phases: (i) the acquisition, that collects user interaction data and stores it in repository; (ii) the recognition, that reads from the interaction files, and classifies the user as imposter or genuine,to identify user authenticity.

When user interacts with any NFC enable device then different factor of a user can be used to distinguish between authorized or unauthorized users. In this paper we consider four different factors: touch, time, angle and distance to know authenticity of the user.

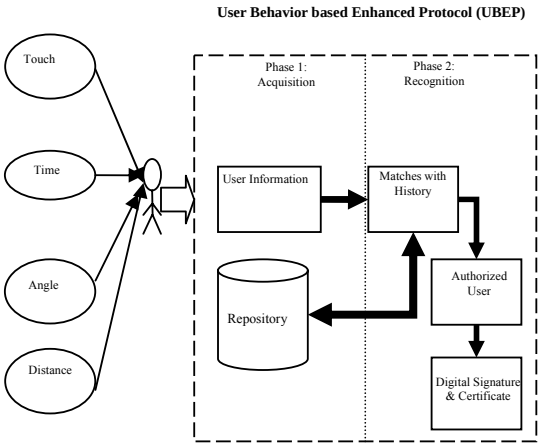

Fig. 1 User Authentication Using User Behavior based Enhanced Protocol (UBEP)

A. Acquisition (Touch, Time, Angle & Distance)

This phase considers four different factors of user which

are touch, time, angle and distance. These factors show the behavior of a particular user which can vary from one to other during communication with electronic machine such as ATM. These factors can be used to distinguish between authorized and unauthorized users. Every time when user interacts with system protocol keep the information for further use.

- Touch can be different for different users.
- Time taken by user to input.
- Angle could be different during touching NFC enabled devices.
- Distance can vary for different users.

The particular inputs are used to map with history information available in phase 2 to give access to the user. The same inputs are used for further user authentication and kept in repository for further use.

B. Recognition & Digital Signature Check

The recognition phase uses the user interaction data and data stored in the repository. The data in the repos and starts a feature extraction procedure, by applying some mathematical operations to decides to accept or reject the user as genuine. In this phase, the global sets of extracted features are used in an algorithm that selects a set of "best "features for each user, using the equal error rate as performance measure. The complete process is explained below:

1. Information Extraction

The input to the recognition phase is the interaction data from the users. The device extracts four different features as defined above. The different parameters with the absolute values are used by this phase to authenticate user. Firstly, the extracted information is checked with history available if user is interacting with same values (little error is permissible) then he/she is authentic user. Detailed process of feature extraction is given below:

Each pattern passes through several processing phases in order to generate the complete set of features. In a preprocessing phase, signals are cleaned from some irregularities via a cubic spline smoothing process. The second phase concerns the extraction of spatial and temporal information, leading to intermediate data representation vectors. A final step generates the features by exploring some statistical information from these vectors, and other general properties of the patterns.

Extraction is based on the spatial and temporal vectors. The vectors x′, y′, μ, c, ¢c, vx, vy, v, v˙ , v¨, and w are statistically analyzed, and 5 values are computed per vector: the minimum,maximum, mean, standard deviation, and range (maximum - minimum). Two other features are computed related to the path of the stroke: the straightness, defined as the ratio of the Euclidean distance between the starting and ending points of the stroke, and the total path distance; the jitter, related to the tremor in the user movement, defined as the ratio between the original path length and the smoothed path length.

The curvature vector c is processed searching for high curvature points, that we call critical points. Wesearch for zeros in the derivative of select the points that have absolute curvature higher than a constant:

$$\alpha = \pi^* \text{ rad}/10^* \text{pixel}^2$$

The number of critical points constitutes an additional feature. We consider a pause in the user interaction when two consecutive events have a time interval greater than a constant =0.1 sec.

- Error Estimation

The error estimation is most important here to authenticate user. The algorithm to estimate error is explained below:

The algorithm is as follows:

1. Create an empty feature subset fsubset.
2. Initialize the best equal error rate of the previous interaction, EERlast = 1.
3. For each feature fi, i = 1...nfeatures:
   (a) Create the vector with the features to test, ftest = fsubset∪fi.
   (b) Set the feature equal error rate (fEERi) equal to the result of the recognition system test, using the subset ftest. fEERi= TEST(ftest).
4. If mini fEERi>EERlast exit and return fsubset.
5. Set EERlast = mini fEERi .
6. Set the best feature fbest = argminifEERi .
7. Set fsubset = ftest∪fbest.
8. Go to 3.

2. User Authentication and Digital Signature Verification

After information extraction this part of protocol maps extracted information with the new information which generate due to current interaction. This is a very crucial part in which a 3rd party will verify the OEM (Original Equipment Manufacturer) and its MAC address and the digital signatures will verify the key encryption. Therefore if all the four stages are cleared properly then the user may access the resource.

According to INFC Protocol the user should have to remember his behavioral activity and usage for NFC device as he has done it at the first time of pairing. The above three activities are stored in the PN65 chip [8]. At the first stage this protocol will compare the actual touch sensitive response by the genuine user with the false user, if the differences varies too much then it will lock the system otherwise the second stage will starting identify time period for reacting with resource either aggressively or slowly, similarly if the differences is too much it will further lock the system otherwise the third stage will open and starting identifying the appropriate distance and angle of the NFC devices with the resource, similarly if the distance and the angle having a large tolerance value as compared with the genuine user it will lock the system, if the user clears all these three stages that's mean he clears 50% of enhanced NFC Protocol. Thus pending job will be identified at the last step of digital signature with hash codes crunched with the user private key to the device and the Certificates by the authorized 3rd party, where the OEM will verify genuinely of a user and his credentialed.

IV. Implementation Result and Analysis

The GUI is implemented using Java and NFC part is implemented with a NFC chip which is used to detect signal The analysis of new protocol provide good result as compared with previous protocol as shown in Fig. 2.

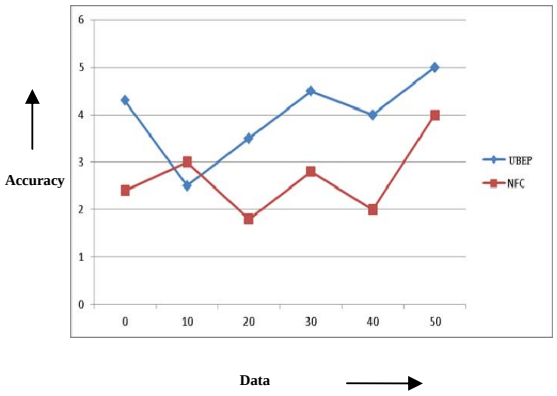

Fig. 2Analysis of User Behavior Based Enhanced Protocol (UBEP)

V. Conclusion

We have presented a novel user behavior based Improved NFC protocol to provide access to authentic user. The protocol uses different user behavior factors such as touch, time and distance & angle to authenticate a user. On the basis of these four different factors protocol detect authenticity of user. The protocol uses two different phases to check the authenticity of the user. The User Behavior Based Enhanced Protocol (UBEP) works on inputs from user. The propose protocol considers four different factors (touch, time and distance & angle) of user behavior to know the authenticity or authorization of the users. The UBEP uses two phase user verification system to authenticate a user. Firstly the acquisition phase is used to acquire and store the user interaction with NFC device and the same information is used in future to detect the authenticity of the user. The second phase (recognition) uses analysis of current and previous scenario of user interaction and digital signature verification system to finally authenticate user. One can touch NFC device with different speed, with different angle. These parameters are used here to give access to NFC device.In future work we will check the fuzziness of the user inputs and try to implement a new system which will work on the user inputs with fuzziness. In future we will work for a formal model of proposed work.

References

[1] Annika Paus, "Near Field Communication in Cell Phones",*in Chair for Embedded Security*, 24.07.2007.

[2] Ernst Haselsteiner and KlemensBreitfu, Security in Near Field Communication (NFC), *in Workshop on RFID Security RFIDSec*, 2006.

[3] C.Mulliner, "Attacking NFC mobile phone", *SIT Fraunhofer - EUSecWest* - 85.10.227.147, http://www.mulliner.org/collin/acad emic/, 2008

[4] David M. Monteiro, Joel J. P. C. Rodrigues and Jaime Lloret, "A Secure NFC Application for credit Transfer Among Mobile Phones."*International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1 – 5 ISBN: 978-1-4673-1549-4, doi:10.1109/CITS.2012.6220369*, 2012.

[5] Michael Roland, Josef Langer and Josef Scharinger, "Security Vulnerabilities of the NDEF Signature Record Type." *3rd International Workshop on Near Field Communication (NFC)*, pp. 65 – 70, ISBN:978-1-61284-176-2, doi: 10.1109/NFC.2011.9, 2011.

[6] Lishoy Francis, Gerhard Hancke, Keith Mayes, KonstantinosMarkantonakis, "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones." *IOS press*, doi: 10.32.33/978-1-61499-143-4-2-1, 2012

[7] A. Arutaki, D. Cavendish, H. Sakai, A. Matsumoto and Y. Oie, "Direction of Wireless Access Convergence; Can Near Field Communication (NFC) Be a Member of Future Internet."*ICMU*, 2012.

[8] H. Sakai and A. Arutaki, "Protocol Enhancement for Near Field Communication (NFC); Future Direction and Cross-Layer Approach," *IEEE INCoS2011*, November 2011, Fukuoka, Japan.

[9] Information technology – Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1), ISO/IEC 18092, Second edition, 2013-03-15.

[10] PN65 Chip, http://www.nfc.cc/technology/nxp-nfc-chips/,2012

[11] Kiran S. Kadambi, Jun Li and Alan H. Karp,"Near-field communication-based secure mobile payment service", *in ICEC '09 Proceedings of the 11th International Conference on Electronic Commerce,* pp. 142-151, 2009.

[12] Francis, L., R. Holloway, Egham, Hancke, G., Mayes, K. and Markantonakis, K.,"A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions", *in Telecommunications (AICT)*, pp. 452 – 461, 2010.

[13] Aigner, M., Dominikus, S. and Feldhofer, M.,"A System of Secure Virtual Coupons Using NFC Technology", *In Pervasive Computing and Communications Workshops, PerCom Workshops '07. Fifth Annual IEEE International Conference*, pp. 362 – 366, *2007*.

[14] Z. Antoniou and D.N. Kalofonos, "NFC-based Mobile Middleware for Intuitive user Interaction with Security in Smart Homes", *in Communication Systems and Networks*, 2006.