A Design of Electronic Payment Authentication Method based on NFC Smartphone

Seolhwa Han, Okkyung Choi*, Kangseok Kim, Hongjin Yeh, Taesik Shon

Dept. of Knowledge Information Security, Graduate School of Ajou University, Suwon, Korea
{ hsh3440, okchoi, kangskim, hjyeh, tsshon}@ajou.ac.kr
*Author to whom correspondence should be addressed; E-Mail: okchoi@ajou.ac.kr

Abstract. Unlike the phones from the past, Smartphone holds greater performance like that of PC and it is also true that riskier security threat comes along. Also, with the rapid development of mobile NFC payment services, an importance of the mobile security is growing rapidly but currently, the security-related technology is a very secure manner. Therefore this paper aims to propose an electronic payment authentication method using vibration cues, which will be then utilized for design and implementation. The proposed method enables an efficient, secure mobile payment service by analyzing security issues likely to occur in payments using NFC Smartphone and by proposing payment protocols with an authentication method using vibration cues to resolve such issues.

Keywords: NFC(Near Field Communication), User Study, Mobile Phones, Vulnerability Analysis, Authentication, Shoulder Surfing Attack, Relay Attack, MITM Attack, Vibration Cue.

1 Introduction

NFC, short for Near Field Communication, literally means a short-range wireless interaction. It makes life easier and more convenient for consumers around the world by making it simpler to make transactions, exchange digital content, and connect electronic devices with a touch[1].

It is important to provide a simple method for designing and implementing NFC payment systems that offer both reasonable security protection as well as ease of use for the user[2]. Therefore this paper aims to propose an electronic payment authentication method using vibration cues, which will be then utilized for design and implementation. Furthermore, the existing NFC payment system has some weakness of low efficiency and difficulty in the aspect of usability but those problems were solved in this study by developing a method that can be easily used in the Smartphone environment.

2 Proposed Method

The method proposed in this study, intended to cover such vulnerability, is possibly dedicated to preventing data forgery through the use of a biotouch vibration cue like a method for the lock on a safe, coding and storing the payment information in the DB registry to enable strengthening user authentication and getting prepared for personal information leakage.

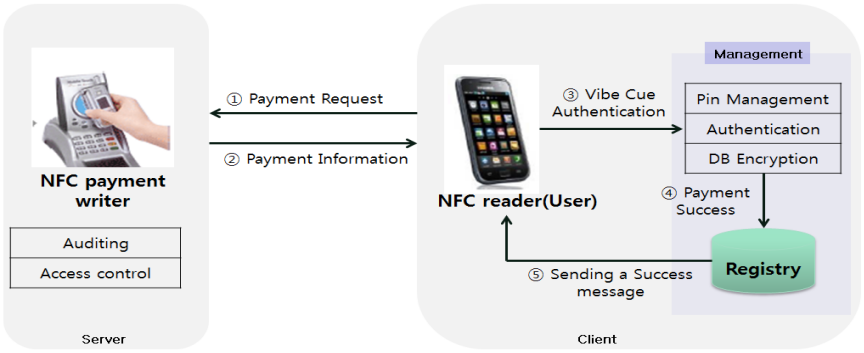

Fig. 1. Flow chart of proposed method.

Fig. 1 shows the staged process of the overall flowchart for the proposed method.

① User puts the NFC reader to contact the NFC payment writer for payment.

② The NFC payment writer transfers payment information to the NFC reader.

③ The NFC reader upon receipt of payment information performs a vibration cue authentication which then enters a pin value in the completed pin setting in a vibration way. Security factors used here include : 1) pin management that prevents pin number from leaking through periodical renewal, re-coding process and continuous management of the first registered pin number, 2) an authentication that uses the vibration cue recognized by biotouch to prevent pin number from leaking due to SSA, and 3) the DB encryption that encodes significant personal information such as pin number and payment information using AES256 and SHA1, strengthens personal information by comparing hash values.

④ If the vibration cue authentication is successful, payment information is encoded and stored in the registry. If the vibration cue authentication fails over 3 times, the process is forcibly closed so no further payment process can develop. Making repayments is possible only by moving to the initial screen for pin number setting, going through the user authentication process and setting the pin number again.

⑤ Lastly, a success message is delivered to the NFC reader and the payment process is closed.

3 Conclusion

With the growing popularity of Smartphone, electronic payment services using Smartphone are rapidly gaining traction. Therefore, mobile NFC services market combining with communication and payment is growing rapidly and they are becoming an alternative computing approach to provide lots of convenient services to users. This paper proposed the mobile payment service using NFC based on vibration cues to prevent Reply attack, MITM attack and SSA that are likely to occur in NFC payment service. The proposed method can deter an attack from an outside attacker that can take place in payment process by applying security factors such as Authentication, PIN management and Access Control to banking security techniques. On top of this, while the existing method held disadvantages such as inefficiency and inconvenience in terms of usability, this method considered a matter of security and complemented it for a better use in smartphones.

Acknowledgments. This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the "Employment Contract based Master's Degree Program for Information Security" supervised by the KISA(Korea Internet Security Agency).

References

1. Near Field Communication, http://www.nfc-forum.org (2006)
2. Anokwa, Y., Borriello, G. Pering, T. Want, R.: A User Interaction Model for NFC Enabled Application. In: 5th Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 357--361. IEEE Computer Society, New York (2007)
3. Haselsteiner, E., Breitfuss, K.: Security in Near Field Communication. Proceedings of Workshop on RFID Security, pp. 3--13 (2006)
4. Mulliner, C.: Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In: 1st Workshop on Sensor Security, Proceedings of the International Conference on Availability, Reliability and Security, ARES 2009, pp. 695--700. Fukuoka, Japan(2009)
5. Chen, W.D., Hancke, G.P., Mayes, K.E., Lien, Y., Chiu, J.H.: Using 3G Network Components to Enable NFC Mobile Transactions and Authentication. In: 2010 IEEE International Conference on Progress in Informatics and Computing (PIC), pp. 441--448. Shanghai (2010)