**Improvement on a lightweight security protocol for NFC-based mobile payments**

 Hung-Pin Chiu 1, Yalin Chen2, Kuan-Lun Wu3 , Jue-Sam Chou 4\*

2Institute of information systems and applications, National Tsing Hua University

2 corresponding author:Yalin78900@gmail.com

1,2,3,4\*department of Information Management, Nanhua University, Taiwan

jschou54@gmail.com

**Abstract**

  Recently, Mohamad Badra et al. proposed a lightweight security protocol for NFC-based mobile payments, by assuming that the customer and the devices are trust. Their proposed solution includes two cases: 1) the PoS has an Internet connection, and 2) it doesn’t have an Internet connection. They pointed out that their approach maintains the required security for NFC communications, and is not only simple, scalable, cost-effective, but also with minimal computation overheads. However, after examination, we found both of the cases are problematic. They suffer active attacks. We will explain the situations in this article.

**Keywords**: authentication, session key, NFC interface, point of sale, host controller, mobile payment, secure element, attack

# **1. Introduction**

 The near field communication (NFC) applications emerged drastically, recently. It had been widely adopted in many applications to increase the convenience of our daily life, such as e-Passport, digital wallet, ticket, billing, etc [1-3]. Hence, the security and privacy had become an important issue for us to tackle with carefully.When it works, the two NFC-enabled objects must be close enough (within 4 to 10 cm) to manipulate properly. They work in three modes: 1) peer to peer mode, 2) reader/writer mode, and 3) card emulation mode. Normally, a generic NFC mobile phone usually contains several special hardwares: 1) a controller, 2) an antenna, and 3) a secure element (SE). The SE does not protect the data in transmission; it only protects the data on the phone. Another NFC technology, which does not need SE, is Host Card Emulation (HCE). In HCE, the application running on the mobile host carries out the card emulation transaction together with the external reader.

There have been many cryptographic scientists working in NFC secure protocol design [4-28]. In 2016, after reviewing the related work [17-21,29-32], Mohamad Badra et al. [16] stated that these literature all use certificate-based method to authenticate the SE and the PoS. The processing time required to achieve the public-key cryptographic operations will thus influence the performance of NFC communications, because it is well known that mobile devices always have the memory and battery-life limitations. Therefore, by assuming both the customer and the devices are trust, they proposed a lightweight security protocol for NFC-based mobile payments to get rid of the public-key cryptographic operations between the SE and PoS. Although, they successfully remove the certificate-based operations performed on the SE. However, upon a closer examination, we discovered that it does not support the desired security requirements of NFC transactions. It suffers from active attacks. To enhance its security, we modified their scheme to exclude the vulnerability. We will demonstrate both the active attacks and our enhancement in this article.

## **2. Review of Mohamad Badra et al.’s Scheme**

Mohamad Badra et al.’s lightweight security protocol for NFC-based mobile payments [16] consists of three roles: 1) a trusted third party TTP, 2) the point of sale (PoS), and 3) a SE on an NFC mobile phone. In their design, although the authentication process between the PoS and trusted third party (TTP) is certificate-based, it is shared-secret-based between the PoS and NFC enabled device to decrease the computation overhead on the mobile phone. They makes a series of assumptions: 1) the secret key SKTTP\_SE shared between the TTP and the mobile is securely stored in SE, 2) the cryptographic computations are performed inside SE, 3) SE offers good tamper-resistant, and 4) a certain physical hardware and software protections are used in SE to make it difficult for extracting or modifying the secret information stored.

To illustrate the weaknesses below, we review the two cases in the scheme and also show them briefly in Figure 1 (which were presented in Figure 4 in the original article). As for the of the used definitions notations, please refer to the literature [16].



 Fig. 1. (a) Case 1, (b) Case 2.

**Case (1): authentication solution when PoS has an Internet connection**

Step 1: SE sends its user identity and a random value, IDSE and RVSE , to PoS.

Step 2: PoS produces a random value RVPoS , and sends this random value together with its certificate, and the received message, CertPoS, RVPoS, RVSE, and IDSE to TTP.

Step 3: TTP verifies PoS’s certificate and generates a secret key SKPoS\_SE. It then computes the session\_key by applying a Pseudo Random Function PRF on the of concatenation RVPoS, RVSE, IDSE , and the XORing result of SKTTP\_SE and SKPoS\_SE. TTP then computes E which is the encryption of SKPoS\_SE concatenated with the session\_key by using PoS’s public key, PubPoS , and sends it to PoS.

Step 4: After receiving E, PoS decrypts it by computing AsymD (E, PrPoS) using its private key PrPoS, obtaining session key|| SKPOS\_SE. Then, PoS symmetrically encrypts the session\_key by using SKPoS\_SE, and sends the result F=E session\_key (SKPOS\_SE) and RVPoS to SE.

Step 5: SE computes the session\_key and then uses it to symmetrically decrypt F to obtain SKPoS\_SE, which is thereafter used as a shard key to securely exchange data between the itself and the PoS.

**Case (2): authentication solution when PoS has no Internet connection**

Step 1: PoS transfers its certificate CertPoS and a random value RVPoS to SE.

Step 2: SE generates a random value RVSE and a secret key SKPoS\_SE, and then symmetrically encrypts the concatenation of RVSE, RVPoS, and SKPoS\_SE by using the key SKTTP\_SE which is shared between TTP and itself, obtaining F. SE then sends F along with its IDSE and the received CertPoS to TTP.

Step 3: TTP verifies PoS’s certificate and symmetrically decrypts F using SK TTP\_SE. Then, TTP encrypts the concatenation of SKPoS\_SE and RVSE by using PoS’s public key PubPoS, obtainingE. It then sends E to SE.

Step 4: SE forwards E to PoS.

Step 5: Upon receiving E, PoS asymmetrically decrypts it by computing

AsymD(E, PrPoS) to obtain E, where Prpos is its private key. Next, PoS computes G by symmetrically encrypts RVSE using SKPoS\_SE and sends the result G to SE. SE then symmetrically decrypts G and compares the result for qualifying the random value RVSE which it initially generated. If the two random values equal, then PoS is authenticate.

## **3. Weakness of the proposed scheme**

In this section, we point out the weaknesses in both cases.

##  **Case (1): authentication solution when PoS has an Internet connection**

 Due to the parameter SKPoS\_SE is generated by TTP in step 3, it is impossible for SE to compute the session key without the knowledge of SKPoS\_SE for decrypting F in step 5. That is, without the knowledge of SKPoS\_SE, SE cannot compute session\_key by applying a Pseudo Random Function (PRF) on RVPoS, RVSE, IDSE,and the XORing result of SKTTP\_SE and SKPoS\_SE. Moreover, if an active attacker Eve intercepts message 2 sent to TTP by PoS, and replaces CertPoS with his own CertEve,he can decrypt E, and then compute F and send it with RVPoS to SE without SE’s awareness. That is, Eve can masquerade as PoS successfully.

## **Case (2): authentication solution when PoS has no Internet connection**

The attack in this case is similar to that in case (1). That is, if an active attacker Eve intercepts message 2, sent from SE to TTP, and replaces CertPoS with his own CertEve,he can decrypt E, and then compute and send Gto SE without SE’s awareness. That is, Eve can successfully masquerades as PoS, too.

**4. Modification**

From the weaknesses found in both cases, we note that the key point is the active attacker Eve can intercept message 2 and replace the legal certificate with his own, without the victim SE’s awareness, as described in Section 3. To remedy this problem, we first add an additional assumption (other than the ones in the original scheme) that the secret key SKTTP\_PoS shared between the TTP and the PoS is securely stored in PoS and TTP. We then modify both cases in the following and show them in figure 2 and 3, respectively.



Figure 2. The modification of case (1)

## **a). Case (1) ：Pos has an internet connection**

Step to 2 are the same as in the original paper. We just modify the messages in steps 3 through 5.

step 3: TTP verifies PoS’s certificate, generates a secret key SKPoS\_SE. It then computes the session\_key=PRF( CertPoS‖RVPoS‖RVSE‖IDSE, SKTTP\_SE). TTP then computes D=encrypt(SKPoS\_SE) using SKTTP\_PoS, and E=encrypts(D ‖(SKPoS\_SE $⊕$session\_key) ) by using PoS’s public key PubPoS. It then sends E to PoS.

step 4:After receiving E, PoS decrypts it by using his private key, obtaining D. He then decrypts D, obtaining SKPoS\_SE. And then usig SKPoS\_SE, PoS can calculate the session key by computing SKPoS\_SE⊕session\_key. After this, he computes F=encrypt(SKPoS\_SE) by using the session key. PoS then forwards F and RVPoS to SE.

step 5: SE computes the session key= PRF(CertPoS‖RVPoS ‖RVSE‖ IDSE, SKTTP\_SE) to decrypt F, obtaining SKPoS\_SE.

**b). Case(2)：PoS has no Internet connection**

We modify the messages in steps 1 through 3.

Step 1: PoS computes A=h(SKTTP\_PoS⊕CertPoS). He then sends A along with his certificate and a random value RVPoS to SE, where h is a hash function.

 

 Figure 3. The modification of case (2)

Step 2: SE generates a random value RVSE and a secret key SKPoS\_SE, and computes F=encrypts((A ⊕ CertPoS ⊕ RVPoS) || RVSE || SKPoS\_SE) by using SKTTP\_SE.

SE sends F along with A, RVPoS, IDSE, and Cert PoS , to TTP.

Step 3: TTP verifies the received PoS’s certificate by comparing it with the one in the symmetrically decrypted F using SKTTP\_SE. Then, the TTP computes E=encrypt(SKPoS\_SE‖RVSE) using the PoS public key PubPoS, and sends E to SE.

The remaining steps 4 and 5 are the same as the original ones.

## **5. Security Analyses**

##  **Case (1)：Pos has an internet connection**

Due to the session\_key = PRF ( CertPoS‖ RVPoS‖ RVSE ‖ IDSE, SKTTP\_SE), D=encrypt(SKPoS\_SE) by using SKTTP\_PoS, and E=encrypts(D ‖ (SKPoS\_SE ⊕ session\_key) ) by using PoS’s public key PubPoS. For impersonating POS, if an attacker intercepts and modifies the certificate of PoS in message 2, although he can decrypt E , obtaining D|| (SKPoS\_SE ⊕ session\_key). However, due to that D=E SKTTP\_POS(SKPOS\_SE), without SKTTP\_PoS he can not decrypt D to obtain SKPoS\_SE. And without SKPoS\_SE, he can not calculate out the session key in E to compute F = session\_key(SKPOS\_SE)successfully, which will be decrypted by SE to obtain SKPoS\_SE.

## **Case (2)：PoS has no Internet connection**

Due to A=h(SKTTP\_PoS⊕CertPoS) and F= encrypts((A⊕CertPoS⊕RVPoS)||RVSE|| SKPoS\_SE) by using SKTTP\_SE, if an attacker Eve intercepts and modifies the certificate in message 2 to his own CertEve, he will definitely be identified by TTP, because without the knowledge of SKTTP\_SE, he cannot compute a valid F to be decrypted by TTP for passing the verification of CertPoS. Even if SE wants to fool TTP, he changes CertPoS to Certeve and computes F= encrypts((A⊕CertEve⊕RVPoS) || RVSE || SKPoS\_SE) by using SKTTP\_SE; however, he cannot pass TTP’s verification of A=h(SKTTP\_POS ⊕CertPos) by using CertEve ,without the knowledge of SKTTP\_PoS.

## **6. Conclusion**

In this paper, we showed that Mohamad Badra et al.’s scheme is flawed, because both cases suffer from active attacks. We, therefore, modify the scheme to avoid these weaknesses. From the analyses shown in Section 5, we see that we have corrected the security problems.

## **References**

[1] Sabella, Robert P. et al., NFC For Dummies, John Wiley & Sons, Inc., 2015

[2] Ahson, Syed A., and Mohammad Ilyas, eds. Near field communications handbook.

CRC Press, 2011

1. Ok, K., V. Coskun, and B. Ozdenizci, Near Field Communication: From Theory

to Practice, Istanbuh NFC Lab-lstanbul, ISIK University, 2012

1. Roland, Michael, Security Issues in Mobile NFC Devices, Springer International Publishing, 2015
2. Rawat, Danda B., Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, IGI Global, 2013.
3. Chen, Hsing-Chung. "A multi-issued tag key agreement with time constraint for homeland defense sub-department in NFC environment." Journal of Network and Computer Applications 38 (2014): 88-98.
4. Alizadeh, Mojtaba, et al. "Authentication in mobile cloud computing: A survey." Journal of Network and Computer Applications 61 (2016): 59-80.
5. León-Coca, Jose Maria, et al. "Authentication systems using ID Cards over NFC links: the Spanish experience using DNIe." Procedia Computer Science21 (2013): 91-98.
6. Dragusha, Kushtrim. "Center for Electronic Payments NFC Payment"

International Stability. Vol. 15. No. 1. 2013.

1. Grassie, Kai. "Easy handling and security make NFC a success." Card Technology Today 19.10 (2007): 12-13.
2. Urien, Pascal, and Selwyn Piramuthu. "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks." Decision Support Systems 59 (2014): 28-36.
3. Alexiou, Nikolaos, Stylianos Basagiannis, and Sophia Petridou. "Formal security analysis of near field communication using model checking."Computers & Security 60 (2016): 1-14.
4. Das, Raghu. "NFC-enabled phones and contactless smart cards 2008–2018."Card Technology Today 20.7 (2008): 11-13.
5. Pacific, Asia. "On-card fingerprint matching secures NFC paymentsbiometric." Biometric Technology Today (2011): 2.
6. Jambusaria, Utsav, Neerja Katwala, and Dharmeshkumar Mistry. "Secure Smartphone Unlocking Using NFC." Procedia Computer Science 45 (2015): 465469.
7. Badra, Mohamad, and Rouba Borghol Badra. "A Lightweight Security Protocol for NFC-based Mobile Payments." Procedia Computer Science 83 (2016): 705711.
8. Frisby W, Moench B, Recht B, and Ristenpart T. Security Analysis of Smartphone Point-of-Sale Systems. USENIX Workshop on Offensive Technologies. 2012; p. 22-33.
9. Dierks T and Rescorla E. Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246; 2008
10. Rosati T and G., Zaverucha G. Elliptic Curve Certificates and Signatures for NFC Signature Records. Research In Motion, Certicom Research; 2013.
11. Urien P. LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things. IEEE Consumer Communications and Networking Conference; 2013. p. 845-846.
12. Ahamad SS, Udgata SK, and Nair M. A Secure Lightweight and Scalable Mobile Payment Framework. International Conference on Frontiers of Intelligent Computing: Theory and Applications; 2013. p. 545-553.
13. Luo, Jia Ning, Ming Hour Yang, and Szu-Yin Huang. An Unlinkable Anonymous Payment Scheme based on near field communication. Computers & Electrical Engineering 49 (2016): 198-206.
14. Rubio, Óscar J., et al. Analysis of ISO/IEEE 11073 built-in security and its potential IHE-based extensibility. Journal of biomedical informatics 60 (2016): 270-285.
15. Alizadeh, Mojtaba, et al. Authentication in mobile cloud computing: A survey. Journal of Network and Computer Applications 61 (2016): 59-80.
16. Sánchez-García, J., et al. On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks. Future Generation Computer Systems 64 (2016): 50-60.
17. Mayes, Keith E., Konstantinos Markantonakis, and Gerhard Hancke. Transport ticketing security and fraud controls. information security technical report 14.2 (2009): 87-95.
18. Chen, Yu-Yi, Meng-Lin Tsai, and Fong-Jia Chang. The design of secure mobile coupon mechanism with the implementation for NFC smartphones. Computers & Electrical Engineering (2016).
19. Chatzigiannakis, Ioannis, Andrea Vitaletti, and Apostolos Pyrgelis. A privacy-preserving smart parking system using an IoT elliptic curve based security platform. Computer Communications (2016).
20. Norbert Druml∗, Juergen Schilling, Walther Pachler, Bernhard Roitner, Thomas Ruprechter, Holger Bock and Gerald Holweg. Secured miniaturized system-in-package contactless and passive authentication devices featuring NFC (2017).
21. Jalayer Khalilzadeh, Ahmet Bulent Ozturk and Anil Bilgihan. Security-related factors in extended UTAUT model for NFC based mobile payment in the restaurant industry (2017).
22. Yu-Yi Chen, Meng-Lin Tsai and Fong-Jia Chang. The design of secure mobile coupon mechanism with the implementation for NFC smartphones (2017).
23. Torsten J. Gerpott, Phil Meinert. Who signs up for NFC mobile payment services? Mobile network operator subscribers in Germany (2017).