INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Efficient and Robust Pseudonymous Authentication Using NFC

C. L. Vijaikumar
Department of ECE, Prathyusha Institute of Technology and management, Tamil Nadu, India
T. S. Sofia
Department of ECE, Prathyusha Institute of Technology and management, Tamil Nadu, India
T. S. Valarmathi
S. A. Engineering College, Tamil Nadu, India

Abstract:
In recent years, various mobile terminals equipped with NFC (Near Field Communication) have been released. The combination of NFC with smart devices has led to widening the utilization range of NFC. It is expected to replace credit cards in electronic payment, especially. In this regard, security issues need to be addressed to vitalize NFC electronic payment. The NFC security standards currently being applied require the use of user's public key at a fixed value in the process of key agreement. The relevance of the message occurs in the fixed elements such as the public key of NFC. An attacker can create a profile based on user's public key by collecting the associated messages. Through the created profile, users can be exposed and their privacy can be compromised. In this paper, we propose conditional privacy protection methods based on pseudonyms to solve these problems. In addition, PDU (Protocol Data Unit) for conditional privacy is defined. Users can inform the other party that they will communicate according to the protocol proposed in this paper by sending the conditional privacy preserved PDU through NFC terminals. The proposed method succeeds in minimizing the update cost and computation overhead by taking advantage of the physical characteristics of NFC1.

Key words*: NFC security, Pseudonym, privacy protection*

1. Introduction

NFC (Near field Communication) is a short-range wireless communication technology whose technology distance is around 4 inches, and it operates in the 13.56MHz frequency band at a speed of 106Kbps to 424Kbps. The combination of the NFC with smart devices resulted in widening the range of NFC, which includes data exchange, service discovery, connection,e-payment, and ticketing. It is expected to replace credit cards in electronic payment, especially. According to Gartner, a market research company, the number of NFC- To use NFC in electronic payment, security is a prerequisite to be addressed. Presently, NFC security standards define data exchange format, tag types, and security protocols, centering on NFC forum. It is expressly stipulated in the NFC security standards that key agreement is required for secret communications between users. In the process of key agreement, both users should exchange their public keys. The public key is received from CA (Certificate Authority), and it uses a fixed value until reissued.

In this paper, we propose privacy protection methods based on pseudonyms to protect privacy.

Malicious internal attackers can create profiles of users through the acquisition of public keys of other users in the process of key agreement. If NFC is used in e-payment in this way, the privacy of users can be infringed through profiles created by attackers. Suppose Alice purchase items such as clothes, food, and medicine several times at a supermarket, the supermarket can get information about her tastes, preferences, and health conditions. The collected information can help her to purchase products more efficiently, but it may contain information that nobody wants to announce to others such as his or her health conditions.

The proposed methods provide conditional privacy in which the identity of users can be verified by the TTP (Trusted Third Party) to resolve disputes when necessary. In addition, the PDU (Protocol Data Unit) for the conditional privacy is proposed in this paper. The data used to help a future purchase uses protected PDU of NFC-SEC, and data not wanted to be recorded uses conditional privacy PDU selectively, which makes it possible to remove the connectivity with the existing messages. This paper is the extended version. It covers background, security requirements, and differences between pseudonym-based method and the proposed method. According to survey conducted so far, this paper has its significance in the sense it is the first research on the conditional privacy protection of users in the NFC.

In this paper,describes standards and privacy protection methods related to NFC, and the NFC environments that are currently applied are introduced. An analysis of the security threats that can occur in the current NFC environment is conducted, and the security requirements necessary for NFC are deduced. In section 5, the conditional privacy methods for NFC are proposed.

2. Proposed Method

The conditional privacy method has widely been studied in the light of pseudonyms when the privacy protection is required. In this paper, conditional privacy protection methods tailored to the NFC environment are proposed. Since the proposed method can reuse NFCIP-1 and NFC-SEC, the NFC standards in most cases, more efficient production is possible in the implementation and the chip design sector. Let us suppose that a user stores the long-term public key issued by TSM in the SE.

3. Algorithm

QA'|| QA''||NA
Generate *NB*
Generate *rB*
Compute *Q'B=rBQB*
Compute *Q''B=rBdBQS+QB*
QB'||QB''||NB

P=rAdAQ'B		P=rBdBQ'A
Compute z from P		Compute z from P
Compute MK		Compute MK
=KDF(NA, NB, IDA, IDB, z)		=KDF(NA, NB, IDA, IDB, z)
Compute MacTagA		
=f(MK, IDA, IDB, QA", QB")		
	MacTagA	
		Check MacTagA
		Compute MacTagB
		=f(MK, IDB, IDA, QB", QA")
	MacTagB	
Check MacTagB		For SSE,
For SSE,		Set SharedSecret=MK
Set SharedSecret=MK		

Table 1: Proposed Key Agreement And Confirmation Protocol Using The Selfupgradable Pseudonym Based Method

4. Analysis

MuPM needs additional storage to maintain the pseudonym set and communication cost for issuance of pseudonym. SuPM does not need any communication cost for the issuance of pseudonyms, but it needs additional computation time and transfer time. In this section, the proposed methods are analyzed in terms of additional cost for maintaining and using the pseudonyms.

- Additional storage to maintain the pseudonyms
  A pseudonym is composed of a public key, private key (encrypted with a long-term key of the user), ID of TSM, and signature on the message. TSM should generate a number of pseudonyms and send to user. The size of the fields generally used in NFC protocol is shown in Table .

	Table
	SIZE OF THE FIELDS
Field	**Size**
IDTSM	16bits
NX, rX	96bits
MacTagX	96bits
	128bits
dMX,Kz	192bits
QX, QX', QX″	200bits
Enc(QA, dA)	352bits
QX	384bits
STSM	448bits

Table 2

The size of single pseudonym is computed as follows:
Size of *PN* = Public key + Encrypted Private Key + ID of TSM + Signature = 1200 bits

5. Additional Transference Time

SuPM requires each user to transfer points on the elliptic curve additionally in the key agreement process. Therefore, 200 bits are additionally transmitted by user. In comparison with the transfer time based on the lowest 106 kbps NFC, the standard method requires 2.727 ns, and 4.569 ns is needed for the proposed method. In the assumption that the transfer time required by each user is the same, transfer of 3.628 ns is additionally required. Even when random value rX and updated public key are created, additional time is required, but it does not have an effect on the transfer time itself since pre-computation is possible. On the other hand, user A and user B cannot be allowed to calculate point P in advance. The doubling operation takes 0.08 ms in Pentium III process of 548 MHz [20]. The proposed method takes 7.680003628 ms, because it performs 288 doubling operations to calculate point P. When compared with NFC-SEC, 7.68 ms turned out to be increased. Accordingly, since conditional anonymity is provided, the additional transfer time required is 7.680003628 ms.

6. Conclusion

With the recent release of various terminals equipped with NFC (Near Field Communication), e-payment market using NFC is expected to be activated. In such situation, the user's transaction information leaks can lead to the invasion of privacy. In this paper, the conditional privacy protection methods are proposed to solve the aforementioned problems. The proposed method uses random public key like pseudonyms. Since the public key is updated, fewer burdens are imposed on the administration. The update is made based on the long-term public key issued from TSM (Trusted Service Manager), and safe management is achieved by storing the long-term public key in the SE (Secure Element). Unlike VANET (Vehicle Adhoc NETwork) environment in which pseudonym methods have been studied for a long time, NFC is a short range-one-to-one communication technology, and it has the robust characteristics to MITM (Man in the Middle) attack. Due to its design based on NFC features, the proposed method can provide conditional privacy with less overhead.
The proposed methods follow standard systems additionally can hide the user's identity, and if necessary, the user's identity can be confirmed by the TSM. Also the user can get personalized service by the selective use of our proposed method. In conclusion, it is expected that the proposed method will help users to protect their privacy and use personalized services. It will contribute to the promotion of mobile payment services through NFC.

7. References

1. Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.
2. Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.
3. ISO/IEC 15946-1:2008, "Information technology – Security methods – Cryptographic methods based on elliptic curves – Part 1: General," Apr. 2008.
4. ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 1: NFC-SECNFCIP-1 security service and protocol," ISO/IEC, May 2010.
5. ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange between systems – NFC Security – Part 2: NFC-SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.
6. H. Eun, H. Lee, J. Son, S. Kim, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-381, Jan. 2012.
7. ISO/IEC 18092:2004, "Information technology – Telecommunications and information exchange between systems – Near field Communication Interface and Protocol (NFCIP-1)," ISO/IEC, Apr. 2004.
8. J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.
9. E. Haselsteiner and K. Breitfuß, "Security in near field Communication (NFC) – Strengths and Weaknesses –," RFIDSec 2006, Jul. 2006.
10. IEEE Std. 1363-2000, IEEE Standard Specifications for Public-KeyCryptography, Jan. 2000