IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 6, Dec-Jan, 2014
ISSN: 2320 - 8791
www.ijreat.org

Efficient And Robust Pseudonymous Authentication Using NFC

C.L. Vijaikumar[1], T.S.Sofia[2], T.S.Valarmathi[3]
Department of ECE
Prathyusha Institute of Technology and Management[1, 2]
S.A. Engineering College[3], 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.

Index Terms — NFC security, Pseudonym, privacy protection.

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 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.

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 purchases items such as cloths, food, and medicine several times at a supermarket, the supermarket can get information about her tastes, preferences, and health conditions. The collected

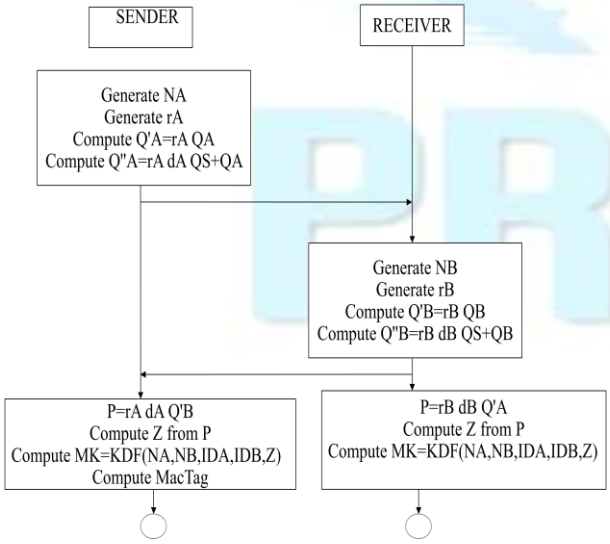
information can help her to purchase products more efficiently, but it may contain information that nobody wants to announce to others such as his or her health conditions.

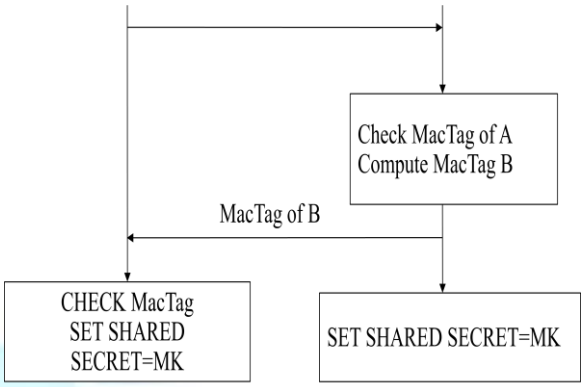
In this paper, describes standards and privacy protection methods related to NFC, and the NFC environments that are currently applied are introduced. An analysis on the security threats that can occur in the current NFC environment is conducted, and the security requirements necessary for NFC are deduced.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

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.

ALGORITHM





. The size of the fields generally used in NFC protocol is shown in Table.

SIZE OF THE FIELDS

Field	Size
IDTSM	16bits
NX, rX	96bits
	96bits
MacTagX	128bits
dMX,Kz	192bits
QX, QX', QX"	200bits
Enc(QA, dA)	352bits
QX	384bits
STSM	448bits

The size of single pseudonym is computed as follows:

Size of *PN* = Public key + Encrypted Private Key + ID of TSM + Signature = 1200 bits

CONCLUSION

With 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 thelong-term public key in the SE (Secure Element). Unlike VANET (Vehicle Adhoc NETwork) environment in which pseudonym method have been studied for long time, NFC is a short rangeone-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.

Also the user can get personalized services 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.

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.