An Efficient Arbitration Mechanism for Secure Data Exchange with NFC

Ming-Tsung Kao^{a,*}, Yu-Hsin Cheng^b, Shang-Juh Kao^a

^aDepartment of Computer Science and Engineering, National Chung Hsing University, No.145, Xingda Rd., South Dist., Taichung, 402, Taiwan

^bDepartment of Information Networking and System Administration, Ling Tung University, No.1, Lingdong Rd., Nantun Dist., Taichung, 408, Taiwan

*Corresponding Author: kevinkao@cs.nchu.edu.tw

Abstract

With the provision of both point-to-point transmission and remote sensing, Near Field Communication (NFC) has been getting popular in the short-range wireless communication. Due to its nearness characteristics, NFC is effective in securing communication between peer users. To further ensure the security of the data exchanged, we propose a simple efficient arbitration mechanism to confirm the data transmission, especially in the application of an attendance system. In the propose mechanism, communication peers are required to register to a third authority party in advance to get a security key. During the session of data exchange, both peers use their own security keys to encrypt the message without the third party being involved. If one peer is in question of the identity or the attendance record, he can ask the designated third party for verification. Hence, the correctness of data transmitted can be confirmed and the dispute of attendance can be resolved.

Keywords: NFC, security key, data exchange, arbitration.

1. Introduction

Near field communication (NFC) ⁽¹⁾ resembles radio frequency identification (RFID) ⁽²⁾ in the applications of object identification and remote sensing. However, NFC devices are beneficial over RFID in facilitating for computation capability, hence it is possible to perform the verification procedure for security mechanism. Currently, attendance systems commonly adopt RFID for controlling entrance and departure statuses. By taking the advantages of the computing capability on NFC devices, we are able to develop an arbitration system to guarantee the validity of attendance. Due to the limited memory capacity available on

RFID devices, the monitored data should be forwarded to the backend management system. Either the communication faults or the malfunctions of RFID readers may result in incorrect records or data loss. To avoid the argument because of the system faults or the control card lost, we need an arbitration mechanism.

When there exists an inconsistent record, such as a mismatch between both peer devices, the attendance proof of a peer participant will require the help from a third authority party. In this paper, we present an arbitration mechanism to resolve the problem due to the data inconsistency. In the following, we will briefly introduce NFC and review the mutual authentication technology. Then, the operating phase and the security arbitration mechanism are presented. Finally, achievement the brief conclusions are included.

2. Preliminaries

2.1 Near Field Communication (NFC)

Near Field Communication (NFC) is a short-range and a wireless communications technology based on radio frequency at 13.56 MHz. It can transmit data up to 10 cm with the maximum transmission speed of 424 kbps. NFC devices can perform fast pairing with others under low energy consumption. With the advantages mentioned above, NFC is currently widely used for transmitting a small amount of data within short range. NFC devices are generally portable devices, such as Mobile phones and tablets. It works similar to RFID (Radio Frequency Identification) in terms of using radio frequency for transmission, but they are different in the way that NFC provides two-way, proximity coupling technology based on to the smart card standard ISO14443 or ISO 18092 communications whereas RFID provides one-way communication. However, RFID is longer than NFC in

the transmission range.

2.2 Host-based Card Emulation

The Host-based Card Emulation ⁽⁷⁾ allows any Android application to emulate a card and talk directly to the NFC reader. When an NFC card is emulated using host-based card emulation, the data is routed directly to the host CPU on which Android application is running, instead of routing the NFC protocol frames to a secure element as shown in Fig.1. In our experimental environment, we will apply Host-based card emulation technology for the implementation of NFC data exchange.

Fig. 1. NFC card emulation without a secure element ⁽³⁾.

2.3 Mutual Authentication

Most previous NFC applications focused on the real-time data exchange without considering the security, especially the mutual authentication. Recently, there are several research papers discussed the mutual authentication issue. Lee et al ⁽⁸⁾ argued that the protocol is capable of preventing replay and man-in-the-middle attack, and also provides authentication. Lu et al ⁽³⁾ proposed an authentication method for smart-living NFC applications. Thammarat et al ⁽⁴⁾ and Ceopidor et al ⁽⁵⁾ also presented mechanism to ensure the information to be correctly exchanged between NFC devices and the point of sales (POS). A framework ensuring the availability and safety of data transmission among NFC applications was also proposed by Luo and Qiu ⁽⁶⁾.

Since there are occasions that data is lost or a peer device is failure after completing the mutual data exchange, a verification mechanism to prove the appearance (or attendance) of the application user has to be supported. Among the mutual authentication proposals found so far, the study about arbitration mechanisms is still far away from

enough. Hence, we need a system which can protect exchanged data as well as can verify the communication records when an unexpected error occurs.

3. The Arbitration System Architecture

In this paper, we propose a simple arbitration mechanism using a third party authority to prove the validity of data transmission between peer NFC devices in attendance systems. Instead of simple recording and reacting by the RFID reader and connecting to the backend information processing system, we replace RFID with NFC and include a third party authority server for arbitration purpose. The two-way communication characteristic allows us to build a secure data exchange mechanism by providing mutually authenticated operations. As shown in Fig.2, all NFC reader connect to the Internet, particularly MIS/ERP server and arbitration server. Once peer communications are in progress between a NFC reader and a NFC device, the message from a mobile NFC device is sensed and recorded at the NFC reader and is encrypted, if necessary. The received message is then forwarded to the MIS/ERP server for management processing. Whenever there is a controversy about the attendance record, the arbitration server may get involved in verifying the transmitted message to make sure the participation history.

To work in the proposed arbitration system, all peer devices must register to the arbitration server in advance. Arbitration procedures are necessary only when there is an argument about the attendance. The system consists of three phases: device registration phase, data exchange phase and arbitration phase, which are described in the followings.

3.1 Device Registration Phase

Fig. 2. The system architecture.

In order to join the arbitration system, both the NFC reader and NFC mobile device are required to register to the arbitration server. The client, either the NFC reader or the mobile NFC device, sends the unique user identifiable (NFC UID) to the arbitration server. The arbitration server then creates an authentication ID (AID) and an encryption key to the requesting device. Once the requester has received both ID and key, he responds with an acknowledgement. The registration procedure is completed when the arbitration server has successfully received the acknowledgement. The communications between the arbitration server and client are accomplished using a secure channel e.g. TSL (Transport Layer Security). The communication flows of the registration phase are shown in Fig. 3.

Fig. 3. Device Registration Phase.

3.2 Data Exchange Phase

When a mobile device, m , is ready to make contact with the NFC reader, r , it enters the data exchange phase, as described in Fig.4. The mobile device m initiates a data transmission, it uses the key, K_m , which is obtained during the device registration phase, to encrypt the data, D , including the clock time, T_m . Then, the mobile device, m , transmits the encoded data, $E(m)$, its arbitration ID (AID_m), D , and the timestamp T_m to the NFC reader, r . Upon data being received by r , it encrypts $E(m)$ and Tr using the key K_r to obtain the encrypted code $E(r)$, and sends back, together with AID_m , AID_r , D , T_m , and Tr , to the mobile device. The mobile device then performs the same encryption procedure (e.g. Advanced Encryption Standard, AES⁽¹⁰⁾) as it works for the first time, but this time the data to be manipulated has changed to the received D and T_m . The newly generated data is then compared with the previous

encoded data, if both are the same, then we are sure that the transmitted data has not been altered during the communication. Otherwise, the data has been changed and should be aborted. The final step in the data exchange phase is to save the exchange data which includes AID_m , AID_r , D , T_m , Tr and $E(r)$. These data will be applied whenever there is a need to verify the communication during the data arbitration phase.

Fig. 4. Data Exchange Phase.

3.3 Data Arbitration Phase

In the case that either side of communication ends needs to verify the contents of previous exchanges, the arbitration phase is taken place. Either a NFC reader or a mobile device may start the data arbitration phase. The verification procedure is initiated by the requester sending the data saved in the last step of the data exchange phase to the arbitration server. That is, the data of AID_m , AID_r , D , T_m , Tr and $E(r)$ are sent to the arbitration server.

When the arbitration server receives the request from a client, it discovers K_m and K_r from AID_m and AID_r . Once K_m and K_r are ready, arbitration server with obtain the $E'(m)$ and the $T'r$ by decrypting $E(r)$ with K_r . Then D' and $T'm$ are derived by using K_m to decrypt $E'(m)$. Eventually, logical comparisons are performed on D and D' , T_m and $T'm$, and Tr and $T'r$. If they are all the same, the arbitration result is positive and a successful return is back to the requester. If K_m and K_r can't be calculated or any one of the comparisons fails, the arbitration failure will return to the initiator.

Fig. 5. Data Arbitration Phase.

3.4 Security Analysis

Two security features are guaranteed in our proposed mechanism. One is the assurance of data transmission. The other one is the capability of device authentication.

(a) Assurance of data transmission

Since each device participating the communication gets a unique key and arbitration ID (AID) from the arbitration server during the registration, all data-transmitted in the exchange phase can be encrypted accordingly. The encrypted data together with its to-be-transmitted data, key, AID and time stamp are sent to the NFC reader. As the receiver, the NFC reader will send back the sending data, the sender can verify the data integrity. Hence, this mechanism can ensure the data correctness of data transmitted. Consequently, it can effectively avoid from data alteration during the exchange phase.

(b) Capability of device authentication

At the beginning of participating the arbitration system, each device has to register at the arbitration server. The device, either the NFC reader or mobile device, is associated with an arbitration ID (AID), which is authorized by arbitration server. During the peer communications or whenever an arbitration request is issued, the device can be effectively verified by consulting its associated AID. Hence, communicating devices can be authenticated successfully.

4. Conclusions

With the punch card attendance system, equipment failures or system faults are possible. If an error occurred

after an employee has successfully completed his sensing procedure, a controversy will be resulted. The current solution to resolve the dispute between the company and the employee is to enhance the monitoring system, such as image recording, so that an auxiliary verification can be accomplished by examining the monitored data. This could be a time-consuming and expensive task. In this study, we propose an arbitration system by adopting the NFC P2P technology as well as by introducing a secure data exchange mechanism. Our system requires all participated users to register to a third authority party, so that security keys and arbitration request can be offered safely. We also take the advantage of the computing power on the NFC devices to improve the security during data transmission. Once as disagreement between communication peers, either side can issue a request to the arbitration server for the attendance judgement. When there is no argument over the attendance record, the arbitration server can be idle during the regular communications. Hence, the proposed system can provide secure data exchange as well as can resolve the inconsistent attendance record problem.

As the NFC devices are getting widely deployed, more and more applications become possible. Mutual data exchanges of two near field devices are getting popular, such as between a POS and a mobile phone, between an ATM machine and a mobile phone, or even between two mobile phones. As a result, the demand for security guaranteed, either for the contents of transmitted data or for the assurance of data admitted, is increasing. How to enhance the security, to improve the efficiency and to develop useful NFC applications are among the potential topics for the future study.

References

- (1) nfc-forum.org, 'What Is NFC? - NFC Forum', 2015. [Online]. Available: <http://nfc-forum.org/what-is-nfc/>. [Accessed: 24- Nov- 2015].
- (2) Wikipedia.org, 'Radio-frequency identification - Wikipedia, the free encyclopedia', 2015. [Online]. Available: https://en.wikipedia.org/wiki/Radio-frequency_identification. [Accessed: 24- Nov- 2015].
- (3) Lu, Yung-Feng, et al. "An NFC-phone mutual authentication scheme for smart-living applications." Information Science, Electronics and Electrical Engineering (ISEEE), 2014 International Conference on. Vol. 2. IEEE, 2014.
- (4) Thammarat, Chalee, et al. "A secure lightweight

protocol for NFC communications with mutual authentication based on limited-use of session keys." Information Networking (ICOIN), 2015 International Conference on. IEEE, 2015.

- (5) Ceipidor, Ugo Biader, et al. "KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions." Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on. IEEE, 2012.
- (6) Luo, Jianchao, and Zhijie Qiu. "A Framework for Secure NFC Applications." International Journal of Multimedia and Ubiquitous Engineering 10.3 (2015): 147-160.
- (7) Android.com, 'Host-based Card Emulation', 2015. [Online]. Available: [http://developer.android.com](http://developer.android.com/intl/zh-tw/guide/topics/connectivity/nfc/hce.html)
- (8) /intl/zh-tw/guide/topics/connectivity/nfc/hce.html. [Accessed: 24- Nov- 2015].
- (9) Lee, Yun-Seok, Eun Kim, and Min-Soo Jung. "A NFC based Authentication method for defence of the Man in the Middle Attack." 3 rd International Conference on Computer Science and Information Technology (ICCSIT'2013). 2013.
- (10) Wikipedia.org, 'Advanced Encryption Standard - Wikipedia, the free encyclopedia', 2015. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 24- Nov- 2015].