Journal of Computer Science

Original Research Paper

Design and Development of an Advanced Authentication Protocol for Mobile Applications using NFC Technology

Reham Abdellatif Abouhogail and Ahmed H. Ali

Department of Electrical Quantities Metrology, National Institute of Standards (NIS), Egypt

Article history
Received: 01-09-2019
Revised: 03-12-2019
Accepted: 24-12-2019

Corresponding Author:
Reham Abdellatif Abouhogail
Department of Electrical Quantities Metrology, National Institute of Standards (NIS), Egypt
Email: rehlatif@yahoo.com

Abstract: In this paper, we proposed a new Authentication Protocol for Mobile Applications using NFC technology (AP for MAN). The proposed protocol minimizes the required time to complete the authentication process between the shared entities with a high level of privacy. According to the main security measures, the proposed protocol is evaluated. The current paper presents a new idea for preventing denial of service attack and preserves the limited mobile device capability. The proposed protocol is checked using BAN logic and established that it has no redundancy, the mutual authentication property between the shared parties is verified. The implementation of the proposed protocol shows that it works as designed and it is practical.

Keywords: NFC, Authentication Protocols, Integrity, Mobile Transactions, Denial of Service Attack

Introduction

Near Field Communication (NFC) is a wireless technology that operates in a short range of about ten centimeters for communication. NFC is based on the technology of Radio Frequency Identification (RFID) (Timalsina *et al*., 2012). For communication, an NFC initiator or transmitter device starts to generate a radio frequency at a frequency of 13.56 MHz. NFC receiver can receive the sent message if it exists in close proximity. NFC feature is a small chipset embedded in wireless devices such as PS (Point of Sale), mobile phones, cards posters and many other wireless devices (Timalsina *et al*., 2012).

Moreover, NFC can operate in three modes, the first mode is a Card emulation mode. In this mode, NFC acts as an RFID tag embedded in a portable device, the second mode is a Reader/Writer mode. In this mode, a mobile device with NFC acts as an NFC reader and writer similar to RFID tags and the last mode is Peer-to-peer (P2P) mode. In this mode, two NFC technologies can communicate directly between two NFC phones or NFC can exchange data directly by touching each other (Thammarat *et al*., 2015).

NFC is a bidirectional and a proximity coupling technology that based on standard ISO14443 of the smart card (Ukalkar, 2017). The physical and data link layer for NFC modes are based on standard ISO18092, but applications, device architecture and related topics standards are still discussed by the NFC-Forum (Ukalkar 2017).

These days, many smartphones as well, as mobile devices, have embedded NFC to enable data transfers between devices to speed communication in a short-range (Ukalkar, 2017). Moreover, it is widely used as a wireless communication media in a mobile payment system (Ukalkar, 2017). This means that a consumer can purchase goods from a seller easily and conveniently way by using his mobile device. By using this payment, the customer has been allowed to transfer money to the merchant using the mobile device (Ukalkar, 2017). In addition, it can be used on transportation tokens/tickets in addition to access badges or keys to restricted locations (Thammarat and Kurutach, 2019; El Madhoun *et al*., 2016).

Furthermore, NFC increases the capability of mobile phones and it is predicted to have the potential to do more functions. However, there are many serious concerns in different factor as privacy, the satisfaction of the user, speed of data transfer, the usability of functions, etc. Moreover, the NFC feature is replacing various popular devices communication technologies such as RFID tags (Timalsina *et al*., 2012). Therefore, it is very important to measure and evaluate the performance of the NFC technology security protocol and where it stands. In this paper, we proposed a new and lightweight authentication protocol using NFC technology and analyzing its performance compared with other authentication protocols in terms of various factors.

Also, due to the rapid development of short-range wireless communication technology, there is an increasing demand to design secure and efficient mobile applications

(Levy *et al*., 2015). Thus, security is a prerequisite for NFC applications. Moreover, NFC technology transmission capacity is limited as its operating frequency is 13.56 MHz and its transmission speed starting from 106 Kbps up to 424 Kbps cm (Odelu *et al*., 2016). As a result, authentication protocol should ensure high security in addition to low computation and communication time (Levy *et al*., 2015).

During the last years, there are many types of research presented for authentication protocols that are based on NFC. However, most of these proposed NFC protocols have some weaknesses in information security and fairness. And as a result, these protocols face a problem with many attacks (Ukalkar, 2017). In addition, the missed of fairness prevents the trust among all NFC system parties and without trust, no NFC applications are to be used that lead to a failure of the mobile NFC proposed system (Ukalkar, 2017).

In this paper, a new authentication protocol (AP for MAN) allowing to overcome weaknesses of existing corresponding protocols. The proposed protocol depends on online communication with an authentication Application Server (*AS*) that considered a representative of the confidence and security of issuing and acquiring data from other systems. Moreover, it depends on two devices support NFC application. So The proposed protocol has three main entities as shown in Fig. 1, the main component of driver entity is the application server that handles all authentication and registration processes, second and third entities are NFC mobile device and Point-of-Sale (PS), finally, all the data processed will be stored in a database. The main security target for these types of protocols is to satisfy the mutual authentication between these three mentioned shared parties.

The main contribution of this paper is: First the proposed protocol is free from the most security drawbacks that other similar protocols suffer from. Second, comparing with other comparable authentication protocols, the proposed one satisfies low processing time, because it's based on Keyed Hash Message Authentication Code (HMAC) function. The HMAC function verifies the integrity and authenticity. Therefore, the mobile device doesn't need to run heavy processing functions to be authenticated making the proposed protocol more practical. Third, the proposed protocol uses pseudonyms instead of the real identity of the users to preserve their privacy. These pseudonyms are updated periodically for more privacy preservation. Moreover, the mobile device in the (AP for MAN) has a great immunity against denial of service attack which preserves its limited resources.

This paper is organized as follows the following section reviews the related work, the proposed protocol is described in Section3. The proposed protocol is evaluated in Section4. Section 5 presents performance analysis compared with other similar protocols. Implementation for (AP for MAN) is presented in Section 6. Finally, Section 7 concludes the paper.

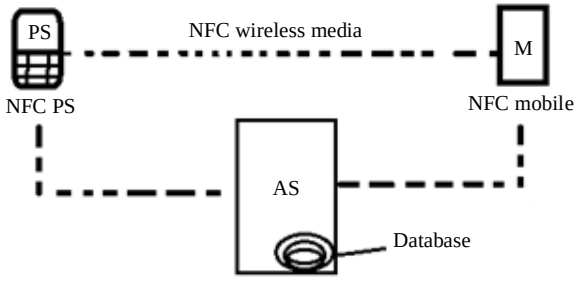

Fig. 1: Mobile payment system based on NFC technology

Related Work

Number of efficient and secured protocols are proposed for payment system using NFC application (Thammarat and Kurutach, 2019; Badra and Badra, 2019; Ahamad *et al*., 2013; Tung and Juang, 2017; Al-Fayoumi and Nashwan, 2018; Nashwan, 2017; (Thammarat *et al*., 2015; Ceipidor *et al*., 2012; Kungpisdan and Metheekul, 2009; Ahamad *et al*., 2012; Bojjagani and Sastry, 2019). As proposed by (Thammarat *et al*., 2015), Thammarat *et al*. proposed two protocols, NFCAuthv1 and NFCAuthv2. NFCAuthv1 is the authentication protocol between an *M* mobile device and the *AS* server. NFCAuthv2 is the authentication protocol between *M* mobile device, *PS* device and the *AS* server. In the NFCAuthv1 protocol, each mobile user needs to install an application. Then, *M* makes registration through a secure channel. After the registration process, the *AS* server and the *M* mobile can create a set of session keys, $SK_{N\text{-}ASj}$, where $j = 1, \ldots, m$, as mentioned in (Kungpisdan and Metheekul, 2009). This method for session key generation is used to prevent sending the session keys over the internet. However, it may cause a data desynchronization attack. These proposed protocols use six messages. Another protocol called SAP-NFC protocol proposed in (Nashwan, 2017) and its performance analysis is presented in (Al-Fayoumi and Nashwan, 2018). The SAP-NFC protocol's structure consists of the *AS* server and two NFC devices. In SAP-NFC protocol, some assumptions are required like: Both of the *AS* and the NFC devices can generate their session keys using Key Derivation Function (KDF). To solve the problem of the data desynchronization attack, the *AS* saves the new and the old session keys of the NFC devices in its database. The *AS* updates the identity of the NFC user for each authentication and saves only the new and the old one as mentioned. Hence, it may not satisfy the non-repudiation problem. The authentication phase needs five messages. Another protocol is presented by Tung and Juang (2017), which is called "Secure and Efficient Mutual Authentication Scheme for NFC Mobile Devices". In this protocol, the system is divided into three entities, two NFC devices and one *AS* server. It's divided into two

DOI: 10.3844/jcssp.2019.1809.1819

phases, the registration phase and authentication phase. After the registration phase, the NFC device will have its required session key. This session key has a limited lifetime as mentioned. However, the method of updating the session key is not mentioned. Thus, this protocol satisfies forward and backward secrecy. Its computation overhead is better than other because it uses the only number of MAC functions. However, it lacks privacy property. The storing of old identities is not mentioned in this protocol. Therefore, it can't satisfy the non-repudiation property. Tung and Juang's proposed protocol needs five messages in the authentication phase.

Furthermore, one of the recent research in NFC mobile payment systems is proposed in (Ali *et al*., 2017), in this research, a proposed payment system was presented using NFC technology, in this system a web application was developed using java programming language and for data storage a database was used. A mobile system was developed using android software development technology that installed in both customer mobile and point of sale NFC reader. The registration and authentication phases of the proposed system totally depend on mobile identification and serial number that hashed to create a system identifier and registration data for both POS and mobile (Ali *et al*., 2017).

The Proposed Protocol

In this section, we propose a new authentication protocol for NFC mobile payment communications to resolve the previous problems and to resist the weak points of existing protocols. The proposed (AP for MAN) protocol consists of two phases, namely, registration phase and authentication phase as shown in Fig. 2 and 3 respectively. Table 1 presents the used notations in our scheme.

Registration Phase

Registration of the NFC Mobile Device

Through a secure communication channel, the NFC mobile device (M_i) performs the registration procedures with the Authentication Server (*AS*) as follows:

MSG#1: $M_i \rightarrow AS$: ID_M^i $R1$

MSG#2: $AS \rightarrow M_i$: I_M^i , $R2$, K_M^i , T_M^i ,C; where; I_M^i is the pseudonym of the NFC mobile and I_M^i = $H(ID_M^i \| R^i)$. It is valid during the valid life time T_M^i. Note: I_M^i is unique as the real identity of the mobile device is unique due to the preimage resistance of the hash function. *C*: Is a random number used for the denial of service check in the authentication phase given to each registered mobile device. After the NFC mobile device receives MSG#2, it stores I_M^i , K_M^i , C and T_M^i in its database and prepares MSG#3.

MSG#3: $M_i \rightarrow AS$: $HMAC(R2, K_M^i)$

After receiving MSG#3, *AS* calculates $HMAC(R2, K_M^i)$ and compares the calculated value with the received one to verify the integrity of K_M^i. Hence, most of the authentication operation will depend on this key. The *AS* stores I_M^i , K_M^i and T_M^i in its database. Note that I_M^i and K_M^i are updated after the life time period T_M^i. The *AS* still keeps I_M^i and K_M^i after T_M^i expired to prevent non_repudiation as will be clarified later.

Table 1: Notations

AS	The Authentication Server
M_i	The NFC mobile device *i*
PS_j	The point of sale *i*
ID_M^i, ID_{PS}^j	The identity of the NFC mobile and the identity of the point of sale, respectively.
I_M^i and I_{PS}^j	The pseudonym of the NFC mobile and the point of sale; where *i, j* = 0, 1,.....*n*, respectively.
C	Random number used to prevent denial of service check.
K_M^i and K_{PS}^j	The NFC mobile key and the point of sale key generated by the authentication server; where *i, j* = 0, 1,.....*n*, respectively.
R1, *N1*	Nonce random numbers generated by the NFC mobile.
R2, *N2*	Nonce random numbers generated by the point of sale.
T_m^i, T_{PS}^j	The valid life time for the NFC mobile and the point of sale; where *i, j* = 0, 1, ...*n*, respectively.
$H(x)$	Hash function of the message *x*.
$HMAC(x, k)$	Keyed Hash Message Authentication Code function (MAC) for the message *x* using the key *k*.
$E_s/D_s(x)k$	Symmetric encryption/ Decryption function for the message *x* using the key *k*.
MSG#*i*	Message number *i*.
V_M, V_{PS}	Verification messages.
A_M, A_{PS}	Authorization messages.

DOI: 10.3844/jcssp.2019.1809.1819

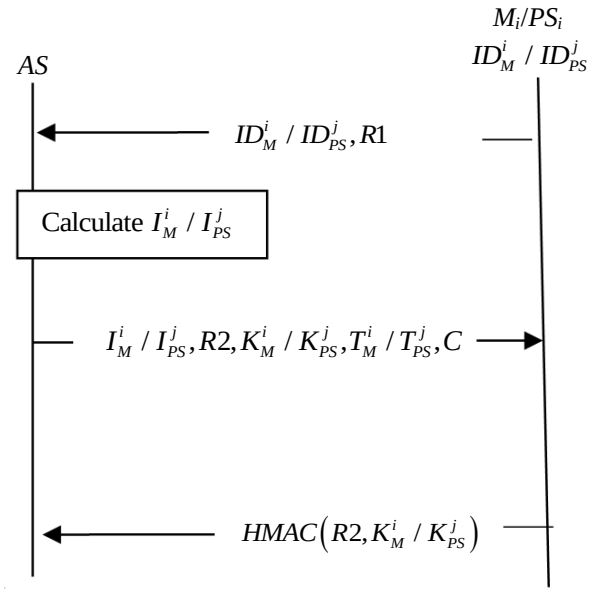

Fig. 2: The Registration phase in the proposed protocol (AP for MAN)

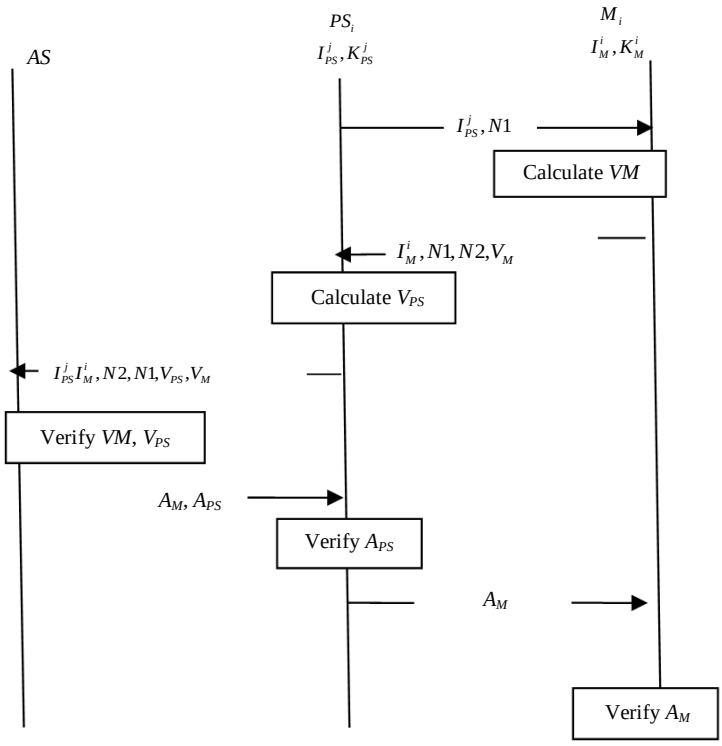

Fig. 3: The authentication phase in the proposed protocol (AP for MAN)

A. 2 Registration of the Point of Sale

The Point of Sale (PS_j) performs similar sequences of operations for registration, under a secure channel. As follows:

1. MSG#1: $PS_j \rightarrow AS$: ID_{PS}^j, R1
2. MSG#2: $AS \rightarrow PS_j$: I_{PS}^{ji}, R2, K_{PS}^j, T_{PS}^j, C; where; I_{PS}^j is the pseudonym of PS_j and $I_{PS}^j = h\left(ID_{PS}^j \| R^j\right)$. It is valid during the valid life time T_{PS}^j. C: is a

DOI: 10.3844/jcssp.2019.1809.1819

random number used for the denial of service check

3. MSG#3: $PS_j \rightarrow AS : HMAC\left(R2, K_{PS}^j\right)$

After the PS_j receives MSG#2, it stores I_{PS}^j, K_{PS}^j and T_{PS}^j. Note that I_{PS}^j and K_{PS}^j are updated after the life time period T_{PS}^j.

AS stores I_{PS}^j, K_{PS}^j and T_{PS}^j in its database. After T_{PS}^j expired, the *AS* still keeps I_{PS}^j and K_{PS}^j to prevent non_repudiation. Then, *AS* sends a message to the user (either the NFC mobile device or the Point of Sale) asking him to take the new pseudonym and the new key. In the following Subsection, the authentication phase is declared.

B. Authentication Phase

After the registration phase, each one of the NFC mobile M_i and the PS_j has the required data to start the authentication operation as follows.

The PS_j sends MSG#1 to M_i contains a generated random number $N1$ and the NFC *PS* pseudonym I_{PS}^j.

MSG#1: $PS_j \rightarrow M_i$*:* I_{PS}^j*,N1,H(C||N)*

After M_i receives MSG#1, it calculates the hash function for the stored C number concatenated with the received random number. Then it compares the result with the received value. If there isn't any match. M_i closes the session with this sender and doesn't continue the authentication process. This fast check protects the mobile device from the possibility of occurrence of denial of service attack by sending, receiving and preparing number of fake messages. So it gives the mobile device the ability to differentiate between the legitimate and illegitimate received messages. If M_i finds the required match, it generates $N2$, computes V_M as a verification message. Then, M_i sends MSG#2 to PS_j as a response. Note that:

$$V_M = HMAC\left(I_M^i \| N1 \| N2, K_M^i\right)$$

MSG#2:Mi$\rightarrow$ *PSj:* I_M^i*,N1,N2,*V_M

After PS_j receives MSG#2, it computes V_{PS} as a verification message; where:

$$V_{PS} = HMAC\left(I_{PS}^j \| N1 \| N2, K_{PS}^j\right).$$

Then, PS_j sends MSG#3 to *AS*.

MSG#3: $PS_j \rightarrow AS$*:* $I_{PS}^j I_M^j$*,N2,N1,* V_{PS}*,*V_M

After receiving MSG#3, *AS* extracted from its database the stored data, K_{PS}^j, K_M^i, T_M^i and T_{PS}^i related to the received I_{PS}^j and I_M^i. Then, *AS* starts to compute V_M and V_{PS} and checks if the results are the same as the received values to verify the identification of the NFC mobile M_i and the point of sale PS_j. If the verification is passed, *AS* authenticates *M* and *PS*. Then, *AS* prepares A_{PS} and A_M as authorization messages; Where, $A_{PS} = HMAC\left(I_{PS} \| I_M \| N1 \| N2, K_{PS}^j\right)$ and $A_M = HMAC\left(I_{PS} \| I_M | N1 \| N2, K_{MS}^i\right)$. Then *AS* sends A_M and A_{PS} to PS_j. Otherwise, *AS* terminates the session.

MSG#4:AS$\rightarrow$*PSj:*A_M*,*A_{PS}

After PS_j receives MSG#4, it computes A_{PS} and checks if the computed value equals the received one. If the check is passed, PS_j authenticates *AS* and M_i. Then, sends A_M to M_i.

MSG#5: $PS_j \rightarrow M_i$*:*A_M

After receiving MSG#5, M_i computes A_M and checks if the computed value equals the received one. If the check is passed, M_i authenticates *AS* and PS_j *and* the authentication phase is finished.

Security Analysis

In this section, the security analysis is presented, the analysis is based on the main security measures. Furthermore, the security features of the proposed protocol have been compared with other similar NFC mobile payment authentication protocols.

Mutual Authentication

The (AP for MAN) uses about four *MAC* values to accomplish the mutual authentication between the three entities. To authenticate the point of sale PS_j and the NFC mobile M_i, the *AS* checks if the received I_M^i / I_{PS}^j in the pseudonym list or not. So, the *AS* can determine the required keys K_M^i / K_{PS}^j for the following steps. After that, the *AS* calculates VPS or V_M to verify the received ones. If the received pseudonym is not in the list or the calculated verification function doesn't equal the received values then the *AS* will consider the NFC mobile or the point of sale is not legitimate and the *AS* terminates the authentication session. The PS_j verifies if the received A_{PS} value equals the calculated value. If they are not equal, the *AS* will be considered not legitimate and the PS_j terminates the session. In the same way, The M_i mobile checks whether the calculated A_M equals the received A_M. If they are not equal, then the M_i terminates the session and the *AS* will be considered not legitimate. Note that the PS_j device and the M_i device authenticate each other indirectly by the *AS*. So we can say that the proposed protocol accomplishes the mutual authentication between the three entities.

Data Integrity

Data integrity property is satisfied by using MAC functions, which are generated by the users' own keys.

Privacy

The privacy property or preserving the anonymity of the users are very essential property. Especially, according to the payment application. The proposed protocol ensures that the adversary can't trace the users. The user's real identity like: ID_M^i , ID_{PS}^j ,.....etc. are involved inside their corresponding pseudonyms: I_M^i and I_{PS}^j ,.....etc. Moreover, These pseudonyms are changed after their corresponding valid life times: T_m^i, T_{PS}^j .....etc. have expired. So the proposed protocol satisfies the required privacy property.

Immunity against Attacks

In this section, we assume that the adversary can obtain and retransmit the mutual authentication messages. Then, we will make an analysis for the important types of attacks to test the possibility of occurrence of them.

Man in the Middle Attack

The proposed protocol satisfies the mutual authentication between the involved entities. Therefore, the adversary can't impersonate the legal users.

Replay Attack

The adversary can't impersonate the legal users and open a session with them by replaying the messages because he doesn't know the legal keys with the corresponding pseudonyms. So the proposed protocol is secure against the replay attack.

Denial of Service Attack

The proposed protocol presents a fast method to check the authorization. The mobile user starts the authentication phase by calculating a simple hash function and comparison as declared in the previous section. The result of this comparison determines whether the mobile will continue in the authentication process or not. Therefore, the required time to neglect the fault messages is minimized. So the proposed protocol has a great immunity against denial of service attack which preserves its limited resources.

Desynchronization Attack

The proposed protocol doesn't use time synchronization. Therefore, it's free from the data desynchronization attack.

Forward and Backward Secrecy of the Key

Forward and backward secrecy of the user's key means that the attacker can detect the session keys (Nashwan, 2017) and therefore, he can know all the mutual messages either old messages (to penetrate the backward secrecy) or forward messages (to penetrate the forward secrecy) between the legal partners. In the proposed protocol, the user's session keys are sent through a secure channel. Moreover, the user's session keys expire after a valid life time. After the expiration period, the users contact the server to take a new session key. Hence, the new keys are independent on the previous keys. Therefore, penetration of the forward or backward secrecy is improbable.

Non-repudiation

The proposed protocol satisfies the non-repudiation property, which means that the mobile user can't deny that he performed this operation. Because the *AS* server stores the previous identity of each user for a certain time period. This time period is determined according to the database storage and what suits the provisions and legislation.

Formal Analysis

In this subsection, a formal analysis using BAN logic (Burrows *et al*., 1990) is presented. BAN logic is a logical analysis method for authentication protocols. Using BAN logic gives the ability to determine the unnecessary functions in the protocol. Moreover, it gives the required trust between the shared parties by proving the mutual authentication property. Before making our analysis using BAN logic, the important notations and logical rules which are used in BAN logic will be presented.

Notations (Burrows *et al*., 1990)

$P \in X$	*P* believes *X*.
$P \triangleright X$	*P* sees *X*.
$P \mid\sim X$	*P* once said *X*.
$P \Rightarrow X$	*P* has jurisdiction over *X*.
#(*X*)	The formula *X* is fresh.
$\{X\}_K$	The formula *X* is encrypted under the key *K*.

Logical Rules (Burrows *et al*., 1990)

1. R1: $\dfrac{P \mid\equiv p \xleftrightarrow{k} Q, P \triangleleft [X]_K}{P \mid\equiv Q \mid\sim X}, P \neq Q$. This rule is called the interpretation rule.
2. R2: $\dfrac{P \mid\equiv (Q \mid\sim (X,Y))}{P \mid\equiv (Q \mid\sim X), P \mid\equiv (Q \mid\sim Y)}$. This rule is called the message meaning rule.
3. R3 : $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \sim X}{P \mid\equiv Q \mid\equiv X}$. This rule is called the nonce verification rule.
4. R4: $\dfrac{P \mid\equiv Q \Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$. This rule is called the jurisdiction rule.

DOI: 10.3844/jcssp.2019.1809.1819

5. R5: $\frac{P|\equiv\#(X)}{P|\equiv\#(X,Y)}$. This rule is called the freshness rule.
6. R6: $P|\equiv(Q|\sim X)\rightarrow P|\equiv(Q|\sim(X,Y))$. This rule is called the synthetic rule.
7. R7: $\frac{P|\equiv(X,Y)}{P|\equiv(X)P|\equiv(Y)}$

This is called the belief rule.

The proposed protocol will be transformed into the following formulas. MSG #1 will be neglected, because it's consisted of plaintext.

To prove that the mutual authentication between the shared parties is satisfied we have to prove:

- First: For certain data X, $AS\in PS\in X$ and $AS\in X$; where; AS is the Authentication Server and PS is the Point of Sale.
- Second: For certain data Y, $AS\in M\in Y$ and $AS\in Y$; where M is the mobile user:

$$M\rightarrow PS: I_M,\#N1,\#N2,(I_M,\#N1,\#N2)_{K_m} \quad (1)$$

$$PS\rightarrow AS: I_M, I_{PS},\#N1,\#N2,\ (I_M,\#N1,\#N2)_{K_m},(I_{ps},\#N1,\#N2)_{K_{ps}} \quad (2)$$

$$AS\rightarrow PS:(I_M,I_{PS},\#N1,\#N2)_{K_m},(I_M,I_{PS},\#N1,\#N2)_{K_{ps}} \quad (3)$$

$$PS\rightarrow M:(I_M,I_{PS},\#N1,\#N2)_{K_m} \quad (4)$$

We have some Initial assumptions:

A1: $AS\in AS\xrightarrow{K_m}M$
A2: $M\in AS\xrightarrow{K_m}M$
A3: $PS\in AS\xrightarrow{K_{ps}}PS$
A4: $AS\in AS\xrightarrow{K_{ps}}PS$
A5: $AS\in\#N1$
A6: $AS\in\#N2$
A7: $AS\in PS\Rightarrow I_{PS}$
A8: $AS\in M\Rightarrow I_M$
A9: $M\in AS\Rightarrow I_M$
A10: $PS\in AS\Rightarrow I_{PS}$
A11: $PS\in\#N1$
A12: $M\in\#N2$

Using Equation (1), A1 and R2, we obtain:

$$AS\in M|\sim(I_M,N1,N2) \quad (5)$$

Using Equation (2), A4 and R2, we obtain:

$$AS\in PS|\sim(I_{PS},N1,N2) \quad (6)$$

Using Equation (6) and R1, we obtain:

$$AS\in PS|\sim(N1,I_{PS}) \quad (7)$$

Using Equation (7) and R5, we obtain:

$$AS\in\#(N1,I_{PS}) \quad (8)$$

Using Equation (7 and 8) and R3, we obtain:

$$AS\in PS\in(N1,I_{PS}) \quad (9)$$

From Equation (9) and R7:

$$AS\in PS\in I_{PS} \quad (10)$$

From Equation (9 and 10) and R4, we obtain:

$$AS\in I_{PS} \quad (11)$$

From Equations (10 and 11), we prove that AS authenticates PS.

Using Equation (6) and R4, we obtain:

$$AS\in M|\sim(N2,I_M) \quad (12)$$

Using Equation (12) and R5, we obtain:

$$AS\in\#(N2,I_M) \quad (13)$$

Using Equations (13 and 12) and R3, we obtain:

$$AS\in M\in(N2,I_M) \quad (14)$$

From Equation (14) and R7, we obtain:

$$AS\in M\in I_M \quad (15)$$

Using Equation (15), A8 and R4, we obtain:

$$AS\in I_M \quad (16)$$

From Equations (15 and 16), So AS authenticates M.

By dividing Equation (3) into three parts and by using Equation (4) we can get the following three Equations:

$$AS\rightarrow PS:(\mathrm{I_m},I_{ps},\#N1,N2)_{K_m} \quad (17)$$

$$AS\rightarrow M:(\mathrm{I_m},I_{ps},\#N1,N2)_{K_m} \quad (18)$$

$$AS\rightarrow PS:(\mathrm{I_m},I_{ps},\#N1,N2)_{K_{ps}} \quad (19)$$

From Equation (18), A3 and R2, we obtain:

$$M \in AS \mid\sim \left(I_M, I_{PS}, N1, N2\right) \tag{20}$$

Using Equation (20) and R1, we obtain:

$$M \in AS \mid\sim \left(I_M, N2\right) \tag{21}$$

Using Equation (21), A12 and R5, we obtain:

$$M \in \#\left(I_M, N2\right) \tag{22}$$

Using Equations (21 and 22) and R3, we obtain:

$$M \in AS \in \left(I_M, N2\right) \tag{23}$$

From Equation (23) and R7, we obtain:

$$M \in AS \in I_M \tag{24}$$

From Equations (24), A9 and R4, we obtain:

$$M \in I_M \tag{25}$$

From Equations (24 and 24), we prove that *M* authenticates *AS*.

From Equation (19), A3 and R2, we obtain:

$$PS \in AS \mid\sim \left(I_M, I_{PS}, \#N1, \#N2\right) \tag{26}$$

Using Equation (26) and R1, we obtain:

$$PS \in AS \mid\sim \left(I_{PS}, N1\right) \tag{27}$$

Using Equation (27), A11 and R5, we obtain:

$$PS \in \#\left(I_{PS}, N1\right) \tag{28}$$

Using Equations (28 and 29) and R3, we obtain:

$$PS \in AS \in \left(I_{PS}, N1\right) \tag{29}$$

From Equation (29) and R7, we obtain:

$$PS \in AS \in I_{PS} \tag{30}$$

From Equations (30), A10 and R4, we obtain:

$$PS \in I_{PS} \tag{31}$$

From Equations (30 and 31), we prove that *PS* authenticates *AS*. From the previous analysis and the properties of BAN logic, we prove that the mutual authentication property between the three entities *AS*, *PS* and *M* is verified. Moreover, our proposed protocol is free from redundancy.

Performance Analysis

In the proposed protocol, the mutual authentication property is satisfied by four MAC functions. No public or symmetric encryption operations are required. No excessive processing operations are required from the mobile user side, which considered suitable for its limited capability. In this section, we select a number of recent and lightweight computations NFC authentication protocols for comparison, that is described in Section 2 (Tung and Juang, 2017; Al-Fayoumi and Nashwan, 2018). The performance comparison is according to the following important parameters: Computation overhead, Computation cost (*ms*), the number of required messages through the authentication phase, *M*. The comparison is performed for the authentication phase only. The processing time for updating the session key after each period is ignored. The computation time for different cryptographic operations listed in Table 2 is used in our comparison to calculate the computation cost.

According to the results that are appeared in Table 3, we can notice that NLA protocol has an intermediate result between the other compared protocols.

Table 2: The computation time for different cryptographic operations (Abouhogail, 2016)

Cryptographic function	The used algorithm	Time (ms)
MAC	HMAC	0.015
H	SHA-2	0.009
Epub	RSA	1.420
Es	AES	2.100
Dpub	RSA	33.300
Ds	AES	2.200

Table 3: Performance comparison among different NFC payment authentication protocols

	Tung and Juang's protocol (Tung and Juang, 2017)	SAP-NFC protocol (Al-Fayoumi and Nashwan 2018)	AP for MAN
Computation overhead	8MAC	$2E_s+2D_s+10H$	9HMAC+ H
Computation cost (ms)	0.12	8.69	0.144
Number of messages through the authentication phase.	5	5	5

DOI: 10.3844/jcssp.2019.1809.1819

Simulation and Protocol Evaluation

The proposed protocol was developed using the Java Software Development Kit (SDK) and mobile virtual machine simulator in additional to the Java Application Programming Interface (API) to verify and evaluate the proposed protocol (Coskun *et al*., 2013). The implementation was simulated on a local host. The language used to write the protocol is a Java tool which is a platform-independent tool (Cheon, 2019). Figure 4 shows the used component and the development environment consists of two Integrated Development Environment (IDE): One platform-specific IDE and one for developing NFC mobile proposed protocol. Thus, a combination of many tools is used for multiplatform application development.

A Custom application was configured in the development environment by composing platform-specific IDEs and tools as shown in Fig. 4. The proposed prototype consists of two developed applications as shown in details in Fig. 4, the first application is an android application that developed using android studio tool and this application will be installed into customer mobile application, the second application was developed using Java technologies that developed using java IDE tool , this program will be installed at system servers to generate needed keys as per proposed protocol, the proposed system was developed based on java pre-define library and used to develop NFC based applications.

We performed a small case study to evaluate the proposed protocol, as the proposed protocol totally depends on the hash function for all its variables, so we used NFC Message-Digest Algorithm 5 (MD5) API to develop the proposed hashing mechanism (Kasgar *et al*., 2013). Table 4 shows the protocol variables for the test scenario as per the abbreviations that presented in Table 1.

The proposed protocol was implemented and evaluated using the most recent Java API taking into consideration the time consumption for each part of the code to enhance the authentication process time. The implementation and evaluation of the proposed protocol show the efficiency of the protocol.

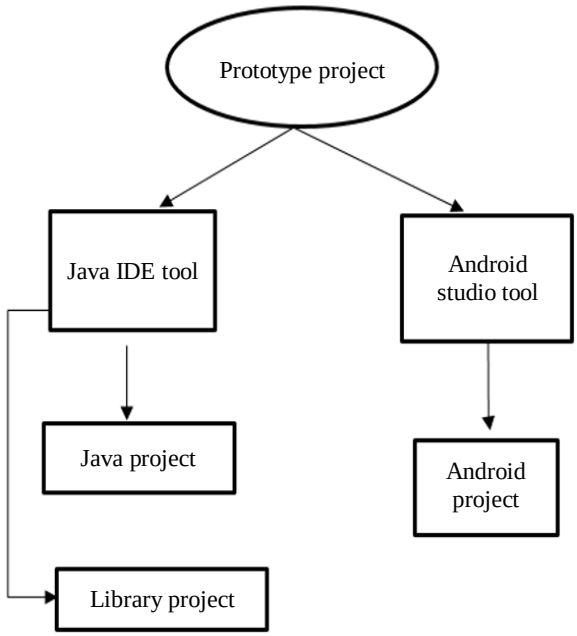

Fig. 4: Project development environment

Table 4: Protocol variables for the test case.

Variables	Test case value	NOTE
ID_M^i,	C7CWF0CQJC6M	It can be mobile serial number
ID_{PS}^i	NE1GAM0750907202	It can be POS serial number
I_M^i	da8eee2f864555f65 e0f6dbc6597f95f	Calculated using MD5 hash function
I_{PS}^i	064bec6493a42a3f383 c176401f48766	Calculated using MD5 hash function
K_M^i	MOBILE8	It is a concatenation between word “POS” in case of point of dale or
K_{PS}^i	POS5	“MOBILE” in case of mobile and incremental number
$R1$	2zyxy	Auto generated random variable
$N1$	71358925	
$R2$	yy11z	
$N2$	95286547	
T_{PS}^i	11062019	Its value equal to registration date plus one day in format of ddMMyyyy
T_m^i	11062019	

Conclusion

In this paper, a new authentication protocol for mobile payment is proposed. The proposed protocol has some important features as it uses a pseudonym to preserve privacy. It's simple and has low computation time comparing to similar authentication protocols. The proposed protocol depends on a number of HMAC functions that are used to preserve the integrity and minimize the time of authenticity. Moreover, using the HMAC function making our protocol more appropriate for the limited mobile device capability. Because the HMAC function is more light in its computation processing with respect to other cryptographic algorithms, which are used in the other comparable authentication protocols. The proposed protocol presents a new idea to minimize the possibility of happening a denial of service attack, which consumes the mobile resources by simple check at the beginning of the protocol. A comparison between the proposed protocol and the similar NFC authentication protocol is presented, which proves that the proposed protocol satisfies low authentication time. The proposed protocol is analyzed and tested using the BAN logic tool, which proves that the required security parameters are satisfied as the mutual authentication between the three shared entities. Furthermore, the proposed protocol is implemented using the Java tool which proves that it works as required.

Author's Contributions

Reham Abdellatif Abouhogail: Proposed and designed the new protocol, participated in the literature review and made the security and performance analysis.

Ahmed H. Ali: Proposed the field of the research, participated in the literature review, made the simulation and the data evaluation for the new protocol.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that no ethical issues involved.

References

Abouhogail, R.A., 2016. Improving the handoff latency of the wireless mesh networks standard. Int. J. Security Applic., 10: 73-86. DOI: 10.14257/ijsia.2016.10.5.07

Ahamad, S.S., S.K. Udgata and M. Nair, 2013. A secure lightweight and scalable mobile payment framework. Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications, (CTA' 13), Springer, Cham, pp: 545-553. DOI: 10.1007/978-3-319-02931-3_62

Al-Fayoumi, M. and S. Nashwan, 2018. Performance analysis of SAP-NFC protocol. Int. J. Commun. Netw. Inform. Security, 10: 125-130.

Ali, A.H., R.A. Abouhogail, I.F. Tarrad and M.I. Youssef, 2017. A new design of mobile payment system based on NFC technology. Int. J. Eng. Technol., 17: 7-18.

Badra, M. and R.B. Badra, 2016. A lightweight security protocol for NFC-based mobile payments. Proc. Comput. Sci., 83: 705-711. DOI: 10.1016/j.procs.2016.04.156

Bojjagani, S. and V.N. Sastry, 2019. A secure end-to-end proximity NFC-based mobile payment protocol. Comput. Standards Interfaces. DOI: 10.1016/j.csi.2019.04.007

Burrows, M., M. Abadi and R. Needham, 1990. A logic of authentication. ACM Trans. Comput. Syst., 8: 18-36. DOI: 10.1145/77648.77649

Ceipidor, U.B., C.M. Medaglia, S. Sposato and A. Moroni, 2012. KerNeeS: A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions. Proceedings of the 9th International ISC Conference on Information Security and Cryptology, Sept. 13-14, IEEE Xplore Press, Tabriz, Iran, pp: 115-120. DOI: 10.1109/ISCISC.2012.6408203

Cheon, Y., 2019. Multiplatform application development for android and java. 7th IEEE/ACIS International Conference on Software Engineering Research, Management and Applications, May 29-31. IEEE Xplore Press, Honolulu, Hawaii. DOI: 10.1109/SERA.2019.8886800

Coskun, V., K. Ok and B. Ozdenizci, 2013. PROFESSIONAL NFC Application Development for Android. 1st Edn., John Wiley and Sons, ISBN-10: 9781118380093, pp: 308.

El Madhoun, N., F. Guenane and G. Pujolle, 2016. An online security protocol for NFC payment: Formally analyzed by the scyther tool. Proceedings of the 2nd International Conference on Mobile and Secure Services, Feb. 26-27, IEEE Xplore Press, Gainesville, FL, USA. DOI: 10.1109/MOBISECSERV.2016.7440225

Kasgar, A.K., M.K. Dhariwal, N. Tantubay and Hina Malviya, 2013. A review paper of Message Digest 5 (MD5). Int. J. Modern Eng. Manage. Res., 1: 29-35.

Kungpisdan, S. and S. Metheekul, 2009. A secure offline key generation with protection against key compromise. Proceedings of the 13th World Multi-conference on Systemics, Cybernetics and Informatics, (SCI' 09), Orlando, USA.

Levy, K., R. Katz, T. Mane and R. Stahl, 2015. Multiple NFC card applications in multiple execution environments. United States Patent, Patent NO US 8977195 B2.

Nashwan, S., 2017. Secure authentication protocol for NFC mobile payment systems. Int. J. Comput. Sci. Netw. Security, 17: 256-263.

Odelu, V., A.K. Das and A. Goswami, 2016. SEAP: Secure and efficient authentication protocol for NFC applications using pseudonyms. IEEE Trans. Consumer Electron., 62: 30-38. DOI: 10.1109/TCE.2016.7448560

Thammarat, C. and W. Kurutach, 2019. A lightweight and secure NFC-base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification. Int. J. Commun. Syst., 32: e3991-e3991. DOI: 10.1002/dac.3991

Thammarat, C., R. Chokngamwong and C. Techapanupreeda, 2015. A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys. Proceedings of the International Conference on Information Networking, Jan. 12-14, IEEE Xplore Press, Cambodia, pp: 133-138. DOI: 10.1109/ICOIN.2015.7057870

Timalsina, S.K., R. Bhusal and S. Moh, 2012. NFC and its application to mobile payment: Overview and comparison. Proceedings of the 8th International Conference on Information Science and Digital Content Technology, Jun. 26-28, IEEE Xplore Press, Jeju, South Korea.

Tung, Y.H. and W.S. Juang, 2017. Secure and efficient mutual authentication scheme for NFC mobile devices. J. Electronic Sci. Technol., 15: 240-245. DOI: 10.11989/JEST.1674-862X.60804031

Ukalkar, G.V., 2017. Survey on NFC in healthcare sector. Int. J. Innovative Res. Comput. Commun. Eng., 5: 1823-1826.