2017 8th International Conference on Information Technology (ICIT)

Online Security Protocol for NFC Mobile Payment Applications

Mayada Al-Tamimi and Ali Al-Haj
Department of Computer Engineering
Princess Sumaya University for Technology
Amman, Jordan
eng.mayada84@gmail.com, ali@psut.edu.jo

***Abstract*—Near Field Communication (NFC) is a short range wireless technology that allows exchange of data between devices communicating within a short distance. Recently, the NFC functionality has been integrated inside mobile devices to allow them act as identifiers for customers, credit cards, and access cards. Payment transaction using NFC-enabled Mobile devices is continuously increasing because of its speed, convenience, and ease of use. However, a widespread of NFC-based payment can be guaranteed, if and only if, the payment transactions are made in a secured wireless environment. Unfortunately, the Europay, Mastercard and Visa (EMV) protocol, which is currently used to provide the required security, has some serious vulnerabilities which could lead to obvious risks for users of NFC-based payments. This paper presents an effective solution to enhance the security of NFC payments by solving the vulnerabilities of the EMV protocol. The proposed protocol adds a security layer to the EMV protocol in order to ensure confidentiality of the transmitted banking data and to provide mutual authentication between the different actors of the NFC payment transactions.**

Keywords—NFC-based mobile payme;, EMV protoco; mutual authentication.

I. INTRODUCTION

During last decade, the number of mobile devices users has grown rapidly due to a fast emergence of wireless communication technologies which have contributed hugely in the development of advanced, interactive, and smarter applications. Of particular interest is the NFC short range wireless technology which has been developed to facilitate conducting daily tasks through communication between NFC-enabled devices. NFC operates at frequency 13.56 MHz; all that through simple-touch technology and in short distance, less than 10 cm. Supported data rates are 106, 212 or 424 Kbit per second [1,2,3]. The NFC functionality has been developed and implemented on single chip that can be integrated inside mobile phones other objects and devices.

Many applications, such as mobile contactless payment application, can be implemented on the NFC-enabled mobiles. Payment transaction using NFC-enabled mobile devices payment is continuously increasing because of its speed, convenience, and ease of use. However, a widespread of NFC-based payment can be guaranteed, if and only if, the payment transactions are made in a secured wireless environment. Unfortunately, the Europay, Mastercard and Visa (EMV) protocol, which is currently used to provide the required security, has some serious vulnerabilities which could lead to obvious risks for users of NFC-based payments. In turn, those risks may lead in the slow adoption of NFC technology for making mobile payment transactions. To provide the needed secured wireless environment, few protocols have been proposed in literature [4, 5, 10, 11, 12, 13, 14, 15]. These protocols provide some degree of the required security; however, the computational requirements of the proposed protocols remain high.

This paper presents a unique protocol to enhance the security of NFC payments by solving the vulnerabilities of the EMV protocol. The proposed protocol adds a security layer to the EMV protocol in order to ensure confidentiality of the transmitted banking data and to provide mutual authentication between the different actors involved in the NFC payment transactions. The protocol been developed following a lightweight design so that they can be easily implemented on the constrained hardware resources of the NFC-enabled mobile devices. The added security layer in the mobile network operator is responsible for the management, authentication and authorization of the transaction by connecting with its subsystem issuing bank. The proposed protocol offloads the verification of the point of sales authenticity and cryptogram generation from the mobile device to the mobile network operator. It also ensures the validity of banking data that are not revoked while executing the payment' even if there is no Wi-Fi or 4G available in NFC-enabled Mobile.

The remainder of this paper is organized as follows. First, the operation of the standard EMV protocol is described in section two. This is followed by a detailed description of the operational steps of the proposed protocol in section three. The performance of the protocol is evaluated in section four. Concluding remarks and future research work directions are presented in section five.

978-1-5090-6332-1/17/$31.00 ©2017 IEEE

II. THE NFC-BASED MOBILE PAYMENT APPLICATION

Many applications, such as mobile contactless payment application, can be implemented on the NFC enabled mobiles. As a matter of fact, the NFC technology has been already experimented in many countries for contactless payment systems through integrating it into mobiles, bank cards, and points of sales. In contactless payment systems, the payment transaction can be performed immediately. It does not require physical contact, or using a PIN code or a signature.

The EMV protocol is a security protocol that is used for both contact and NFC contactless systems [6,7]. It involves a group of security regulations that control the payment transaction between the involved parties. In order to perform an EMV payment transaction, either with or without physical contact, the involved actors are shown in Fig. 1.and their interaction is described briefly hereafter.

Operation of the EMV protocol. In a standard transaction, a buyer holding a card (cardholder) (A) purchases goods or services from a merchant (B) with the card. The Issuing Bank (D) authorizes and allows this transaction using EMV network, and then the Acquiring Bank (C) pays the cost of purchase, after discount, to the merchant. This discount is called the merchant discount. After that, the Issuing Bank (D) pays the Acquiring Bank (C) an amount after deducting any interchange fee from the value of transaction. At the end, the Issuing Bank (D) posts the amount in the account of the buyer holding the card (cardholder). According to EMV specifications [6], depending on the availability of internet connection in the Point of Sale, each EMV phase has two different applications, the online mode and the offline mode. The online mode requires an online connection between the Point of Sale and the Acquiring Bank, and between the Acquiring Bank and the Issuing Bank. In the offline mode, the Point of Sale executes the EMV security procedures since all the security measures are performed in the Point of Sale.

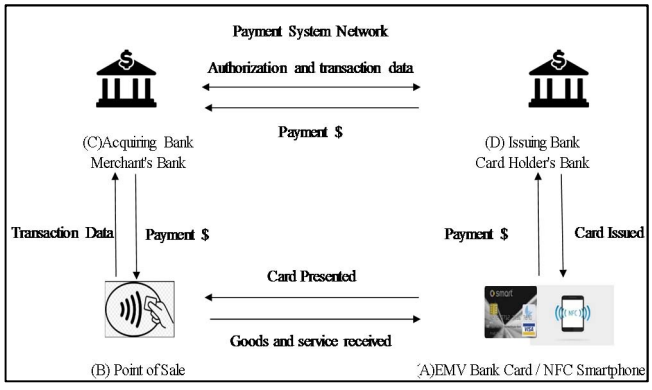

Fig. 1. Actors of the EMV protocol.

EMV security vulnerabilities. When using the EMV protocol for contactless NFC mobile payments, it should be noted that two security vulnerabilities exist between user payment devices and point of sales. These two security vulnerabilities must be treated to guarantee secured NFC mobile payment transactions. One of these vulnerabilities is nonexistence of mutual authentication between the Point of Sale and the user's payment device (i.e. NFC-enabled mobile phone), and the other vulnerability is non-encryption for banking payment data [8, 9].

Proposed Solutions. The widespread of NFC-based payment can be guaranteed, if and only if, the payment transactions are made in a secured wireless environment. To provide the needed secured wireless environment, few protocols have been proposed in literature [4, 5, 10-15].

The reported protocols employed different mechanisms to provide the required security properties which include mutual authentication, non-repudiation, confidentiality of banking information, integrity, and validity of banking data. The proposed protocol, which will be presented in the next section, will take into consideration filling the security gaps and deficiencies found in the reported protocols.

III. THE PROPOSED PROTOCOL

In this section, a security protocol is proposed to enhance the security of the EMV exchanged messages by adding a new security layer called Mobile Network Operator (MNO) while taking the NFC Mobile constrained resources into consideration. The Mobile Network Operator (MNO) is responsible for the management, authentication and authorization of the transaction by connecting with its Subsystem Issuing Bank through TLS. The proposed protocol offloads the verification of the POS authenticity and cryptogram generation from the Mobile device to the operator (MNO). The proposed protocol focuses on the advantage of having the 4G or Wi-Fi interface in POS to communicate with MNO via TLS secure channel. This protocol ensures the validity of banking data that are not revoked while execute this protocol payment even if there is no Wi-Fi, 4G available in NFC enabled Mobile. One important feature of this protocol is that it is considered a lightweight protocol since it applies only symmetric cryptographic operations AES and avoids the disadvantages of using certificates. The mutual authentication between the mobile device and Point of Sale is established by applying the PRF function with a key on exchanged data between the communicating parties.

A. The Proposed Protocol Actors

The proposed protocol consists of three actors as shown in Fig. 2. The protocol controls the type and content of the messages exchanged among these actors so that secured payment transactions are achieved between M and POS. Communication between the three actors can be direct or indirect. For example, POS can communicate directly with the MNO, but the NFC Mobile can communicate with MNO only through POS. The three actors are described below in details.

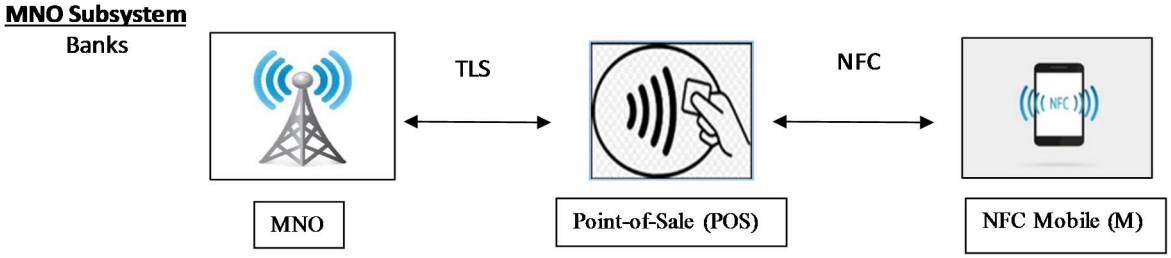

Fig. 2. Actors of the proposed protocol.

• NFC-enabled Mobile (M): the NFC-enabled mobile is the main device for conducting contactless NFC mobile payment transactions. It is assumed that the NFC-enabled Mobile trusts the mobile network operator (MNO) and both achieves mutual GSM authentication via POS. It is also assumed that the NFC interface of the mobile has a cryptographic unit that will be utilized to provide mutual authentication between M and POS. To allow for communication between the mobile and the MNO and Issuing Bank, the mobile has two identifiers: Temporary Mobile Subscriber Identity (TMSI) and Local Area Identifier (LAI). An NFC-based payment transaction is made by a client by presenting his or her NFC-enabled Mobile to the shops NFC-enabled POS.

• Point-of-Sale (POS): is an actor which performs contact and contactless NFC payment transactions. POS has three wireless interfaces: Wi-Fi, 4G, and NFC. The Wi-Fi and 4G interfaces are used to allow POS communicate via a secure channel (TLS) [14] with the mobile network operator (MNO). On the other hand, POS's NFC interface is used by POS for the wireless NFC communication with the mobile device. The MNO and POS must authenticate each other and exchange a new session key for each NFC payment transaction. The POS is registered with one or more operators, and the bank details of the shop are registered with the MNO for monetary transactions.

• Mobile Network Operator (MNO): the mobile network operator (MNO) plays the role of a trust entity that communicates with POS via TLS secure channel. It is responsible for ensuring secured NFC-based payment transactions by providing management, authentication and Authorizations functionalities. The NFC Mobile trusts and authenticates MNO after achieving the GSM Authentication.

B. Protocol Description

In what follows we describe the operational steps of the proposed security protocol in details. The operational steps are described in terms of the messages exchanged between the different actors.

• Message 1: Authentication request for POS (M->POS)

The Mobile (M) sends to the POS a message containing: the identifiers TMSI and LAI (this contains the network code which is uniquely code for Mobile Operator) as its ID, an Authentication request for POS (ReqPOS), and Random M (in order to prevent reply attack). It is assumed that M will not send the Authorization Request directly to POS as in the online EMV, but it contacts its trust entity (MNO) through POS to check the authenticity of POS.

• Message 2: Authentication request for M + Session Key Request (POS->MNO)

After receiving Message (1), the POS terminal extracts the user's mobile network operator from LAI's network code, which is unique for each operator. Next, the POS will not send its transaction data (TData) to the Mobile in clear text, as it is the case in EMV's online mode. Instead, POS will communicate securely with its linked operator (MNO) via the secured TLS channel. The aim of Message (2) is to request the respective MNO to provide mobile authentication and POS identification.

• Message 3 and Message 4: Mobile authentication to MNO

Messages 3 and 4 achieve Mobile authentication to MNO through a challenge and response scenario, and therefore they're described together. The operator (MNO) authenticates the NFC-enabled Mobile device (M) as follows. The MNO identifies M its TMSI and produces an authentication triplet (R, S, Kc). Then, it transmits R to M as a challenge (Message 3). The mobile responds to the challenge by calculating the value of Kc using the formula: Kc = EKi(R) [15]. The mobile generates a random number (Rs), concatenates with R, encrypts with key (Kc), and then send it to the MNO as a response to the challenge: {R|| RS} kc (Message 4). The operator decrypts the message using the key (Kc) and compares R in the authentication triplet with the R received in the response. If they are equal, M is authenticated for a valid SIM.

• Message 5: Confirmation of POS and M authenticity

After successful mobile authentication, the MNO swaps R and Rs, encrypts it with the key (Kc), and send it to M within a ticket sent to M. It is this swap step ({RS || R} Kc which authenticates MNO to M. Then, the MNO responds to the pending requests MNO's response ReqM, MNO's response ReqPOS, MNO's response ReqK.

• Message 6: Forward Ticket M and TData to M (POS->M)

After successfully receiving the POS ticket from the MNO, POS will forward to M, via the NFC link, the ticket Mobile which is encrypted by Kc. After that, POS sends Transaction Data to M encrypted with the Session-Key: T= {TData} Session-Key. Ensuring non-repudiation of origin is done by hashing the TData with the shared key between POS and MNO as follows: H (TData, SKMNO-POS). The Mobile receives Mobile ticket and decrypts it with the key (Kc). Next, it makes a comparison between R and Rs. If they are equal, then the MNO is authenticated. After successful authentication, M ensures the POS authenticity by calculating the Session-Key to check if equal with the received Session-Key from MNO.

• Message 7: Send Mobile Authorization request to MNO

The Mobile sends the request ReqM2 to its operator (MNO) through POS in order to provide the POS with the M authorized payment data received from MNO. The M authorization process is offloaded to the MNO since POS could not verify ARQC, random M, and TData since the message is encrypted with the key (kc). The MNO decrypts the authorization message with the key (kc). Then, it responds to Req2 by generating a cryptogram (ARQC)which is the hash of (TData, Random M, Random MNO, Banking Data) signed with the Cryptogram Key. ARQC can be represented as: ARQC=H (TData, Random M, Random MNO, Banking Data, ConfirmPOS)} Cryptogram Key.

• Message 8: Providing the NFC transaction with authorization result and data

The MNO operator sends authorization message to POS via the secured TLS channel. The authorization message includes: TData, Random M, Random MNO (to prevent replay attacks), and Data (Banking Data, ARQC). This message can be either a confirmation message, ConfirmM, or a rejection message, RejectM. If ARQC and ARQC1 are equal, the ConfirmM message is sent to confirm: M authenticity, authorization and non-repudiation, integrity of the message contained in ARQC and specifically for BankingData. Otherwise, the message RejectM is sent to imply that the payment transaction between POS and M must be terminated.

IV. PROTOCOL ANALYSIS

In this section, the performance of the proposed protocol will be evaluated in terms of achievement of the general security requirements and robustness to malicious attacks.

A. Achievement of the general security requirements .

When the customer and the shop perform the exchanged messages during an NFC payment transaction, the mutual authentication and confidentiality, which have been the EMV vulnerabilities, will be guaranteed as described hereafter. Other security requirements have also been achieved as shown in Table I.

• Mutual Authentication: the proposed protocol solves EMV's first vulnerability since the mutual authentication between the Mobile M and POS, is established. This has been achieved by applying the PRF function which provided a session key to allow secured exchange of data between these two parties. Messages 5 and 6 achieved the mutual authentication by computing the Session-Key and comparing it with the key received from MNO.

• Confidentiality: the transaction messages exchanged among the different actors are encrypted with shared session keys. Therefore, only senders and receivers who share the same symmetric key will be able to encrypt and decrypt messages. The operator transmits the payment data encrypted to the POS via the secured TLS channel. After that, POS decrypts the message. All M-POS transaction messages are encrypted with shared keys (session-key, symmetric session key of the TLS or Kc). The confidentiality of M-POS communications will be guaranteed. Messages 6, 7 and used to ensure the confidentiality of M-POS communications.

Table I. Achieved general security requirements in the proposed protocol.

Security Requirements	Steps in which requirements have been Achieved
Mutual Authentication	5, 6
Non-Repudiation	6,8
Integrity	6,8
Confidentiality	6,7,8
Data Privacy	8
Validity of Banking Data	8

B. Robustness to the malicious network attacks.

Since payment transactions are carried out in a wireless environment, malicious network attacks could interrupt the NFC payment transactions and manipulate its data contents. Therefore, the proposed protocol has been evaluated with respect to its ability to prevent these attacks in order to ensure the security properties of the payment. Possible malicious network attacks include impersonation attack, reply attack, session key manipulation attack, brute force attack, man-in-the-middle attack, modification attack, among many other types of attacks. A selected set of the prevented attacked are described below and summarized in Table II.

• Replay attack prevention: an attacker cannot launch a replay attack, as this is prevented by the proposed protocol by employing random session keys.

• Session Key Security and Brute force attack: a brute force attack that aims to find the right session may not succeed. This is achieved by virtue of the fact that MNO provides a unique session key to M and POS for each NFC payment transaction.

• Man-in-the-middle attack: an attacker takes public information which used by the communicating legal users to intercept the messages and impersonate these users. An attacker cannot masquerade as M or POS to launch Man-in-the-Middle attack since mutual authentication between the two parties is required before transactions, and because message integrity is guaranteed, as described earlier. As a result, the proposed protocol is secured against Man-in-the-Middle attack.

Table II. Robustness of the proposed protocol to selected security attacks.

Possible Attacks		Protected by Message #
Replay Attack	Dishonest Shop Impersonation as MNO	6
	Dishonest Shop Impersonation as a client	4
Session Key Security and Brute force attack		5
Modification attack		6 and 8
Man-in-the-middle attack		Because it is protected from impersonation replay attacks and guarantee mutual authentication and message integrity

C. Comparison with relevant protocols.

The performance results of the proposed protocol are compared here with the performance of relevant protocols. The comparison is made in order to show the effectiveness of the proposed protocol for achieving the security requirements and for providing robustness against a set malicious network attacks. The following performance issues are compared: utilization of mobile resources, computational requirements, providing secured communication channel, ensuring non–repudiation of origin, ensuring validity of banking data, and finally performance evaluation method. Table III summarizes the computational requirements of the proposed protocol compared to [4, 5, 15]. The proposed protocol achieved mutual authentication and online authorization with less number of operations compared to protocols [4, 5, 15]. It can be noted that the same number of cryptographic operations used by the proposed protocol is also used by protocol [4] to achieve the authentication only. Moreover, protocol [15] used asymmetric cryptographic methods in addition to symmetric techniques which lead to more consumption of NFC resources compared to low computational requirement of the proposed protocol.

D. Protocol Verification using the Scyther Tool.

The Scyther tool [16] enables formal analysis of security protocols by demonstrating potential attacks and vulnerabilities. Therefore, the Scyther tool has been used to evaluate the performance of the proposed protocol by showing the undesirable attacks which occur in the NFC communication channel. Fig. 3 shows Scyther claims results. It can be seen from figure that the protocol successfully ensures all Scyther claims (Nisynch, Niagree, Alive, Weakagree) for POS, M, MNO, and thus no attacks have been reported.

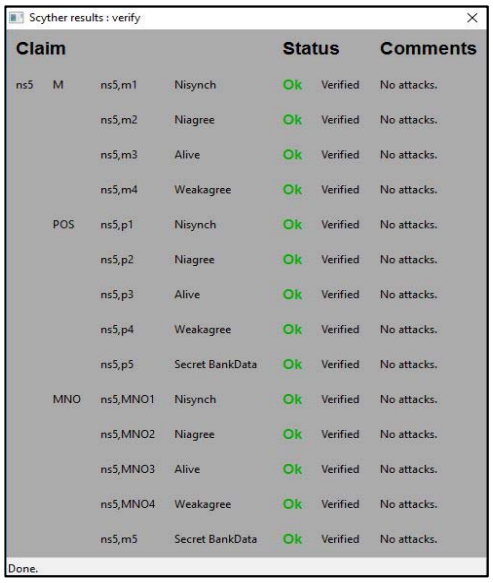

Fig. 3. Scyther claims results report.

V. CONCLUSIONS AND FUTURE WORK

The NFC technology has the advantage of allowing the integration of services from various applications into one single mobile. In this paper an effective security protocol has been proposed to provide more secure NFC mobile online payment transactions between NFC-enabled mobile devices and payment terminals. The protocol aims to solve the EMV security vulnerabilities by improving the classical EMV exchanged messages and adding a new security layer called the Mobile Network Operator (MNO) while taking into account NFC constrained resources. The MNO is responsible for the management, authentication, and authorization of the transaction by connecting with its Subsystem Issuing Bank through TLS. The performance analysis demonstrated that the proposed protocol provides the security needed to perform safe NFC communications. The protocol successfully prevents malicious network attacks such as the impersonation and replay attack, session key security attack, the brute force attack, and the Man-in-the-middle attack. Moreover, the results obtained from the Scyther tool verify the robustness of the protocol against these attacks. Finally, the protocol offers other advantages such as scalability, simplicity, cost-effectiveness, and low computational processing overheads. For future work, a potential extension of the reported research is to carry out a prototype hardware implementation of the proposed protocol in order to achieve fast payment transactions in real-time.

Table III: The computational requirements of the proposed protocol compared to the protocols in [4, 5, 15].

	Symmetric Encryption Operations	**Symmetric Decryption Operations**	**Asymmetric Encryption Operations**	**Asymmetric Decryption Operations**	**Hash Functions**	**Exchanged Messages**
[4]	7	7	-	-	-	7
[5]	10	10	2	2	4	11
[15]	5	5	1	1	2	6
Proposed Protocol	7	7	-	-	2	8

REFERENCES

[1] NFC Forum. Logical Link Control Protocol. Technical Specification, LLCP 1.1. 201.

[2] K. Ok, M. N. Aydin, V. Coskun and B. Ozdenizci, B. "Exploring Underlying Values of NFC Applications," In Proceedings of the Third Int. Conf. on Inf. and Financial Engineering, Singapore, pp. 290–294, 2011.

[3] V. Coskun, B. Ozdenizci, and K. Ok, "A survey on near field communication (NFC) technology," Wireless Pers. Commun., Vol. 71, no. 3, pp. 2259-2294, 2013.

[4] U.B. Ceipidor, C.M. Medaglia, S. Sposato and A. Moroni, "A protocol for mutual authentication between NFC phones and POS terminals for secure payment transactions," Proceedings of the Information Security and Cryptology (ISCISC), 9th International ISC Conference on Digital Object, pp. 115 – 120, 2012.

[5] P. Pourghomi, M. Q. Saeed, and G. Ghinea, "A proposed NFC payment application," International Journal of Advanced Computer Science and Applications. SAI, Vol. 4, no. 8, pp. 173 – 181, 2013.

[6] Integrated Circuit Card Specifications for Payment Systems: EMV Books, book 1: Application Independent ICC to Terminal Interface Requirements, book 2: Security and Key Management, book 3: Application Specification, book 4: Cardholder Attendant and Acquirer Interface Requirements, Version 4.3, EMVCo, http://www.emvco.com/, 2011.

[7] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," RFC 5246 , 2008.

[8] M. Emms and A. V. Moorsel, "Practical attack on contactless payment cards," in HCI2011 Workshop-Heath, Wealth and Identity Theft, 2011.

[9] R. Lifchitz, "Hacking the NFC credit cards for fun and debit,"Hackito Ergo Sum conference, 2012.

[10] L. Yun-Seok, K. Eun and J. Min-Soo, "A NFC based Authentication method for defense of the Man in the Middle Attack," Proceedings of the 3rd International Conference on Computer Science and Information Technology (ICCSIT'2013), Bali, Indonesia, 2013.

[11] C. Thammarat, R. Chokngamwong, C. Techapanupreeda, S. Kungpisdan "A Secure Lightweight Protocol for NFC Communications with Mutual Authentication Based on Limited-Use of Session Keys," In Proceedings of the Int. Conference on Information Networking, pp. 133–138, Siem Reap, Cambodia, 2015.

[12] P. Pourghomi and G. Ghinea "Managing NFC payments applications through cloud computing," IEEE 7th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 772–777, 2012.

[13] N. El Madhoun, F. Guenane and G. Pujolle, "A cloud-based secure authentication protocol for contactless-nfc payment," IEEE 4th International Conference on Cloud Networking (CloudNet), pp. 328–330, 2015.

[14] N. El Madhoun, F. Guenane and G. Pujolle, "An Online Security Protocol for NFC Payment: Formally analyzed by the scyther tool ," IEEE Second International Conference on MobiSecServ), pp. 1-7, USA, 2016.

[15] N. El Madhoun and G. Pujolle, "Security Enhancements in EMV Protocol for NFC Mobile payment," IEEE 15th International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), Tianjin, China, 2016.

[16] C. J. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," In Proceedings of the 20th international conference on Computer Aided Verification (CAV '08), Berlin, Germany, pp. 414–418, 2008.