International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

A Challenging Solution for Man-in-Middle Security Issues through Near Field Communication (NFC)

Meenaketan Sarangi , Debabrata Singh, Mitrabinda Khuntia

Abstract: ***NFC (Near Field Communication) integration with mobile devices does provide a huge space where it opens gateway for easy transactions, of money and data. Thus, NFC can be used by banks, and applications that regulate under initiating some action or to keep a record of something. NFC provides easy update facility of any kind of regular log application. This property will also give a consumer or a user an ease to access and keep a track on everyday update and have correct check on their record consumption or payment trail. Use of NFC gives the best ease in communication that can be used to keep an up to date record. NFC provides the ease of communication and easy transactions which leads our interest to the vast area where we need to discuss its challenges, like man-in-middle issue, relay attack and eavesdropping. This paper primarily focuses on how to solve the attacks like man-in-middle security and then put some light on how to create the whole system of NFC module to be utilized for a complex system. The use of NFC provides one of the smallest, shortest and the best cost efficient communication that can help to transfer data, update data, and various other tasks. Though being one of the shortest communication modules where the distance between two operating devices is the shortest, yet it does give space to vital challenges.***

Index Terms: NFC, Radio Frequency, Single Wire Protocol, UICC, Attacks & Authentication.

I. INTRODUCTION

Near-Field Communication that gives access to use of contactless-transactions and contactless-messages exchange that can be done between two devices which are in the range of less than few centimeters. In the architecture of NFC communication, a certain number of devices like Smartphone's do execute the NFC standard [1]. These devices can only exsist in two modes active mode or passive mode. In the active mode, a Radio Frequency (RF) field is generated by both the devices (among which communication is to be established) and data exchange starts (Initiator's role), and in the passive mode (e.g., NFC-tag or contactless card), the communication sessions can only be initiated by the active device and the passive device's role is known as target (e.g., ticket counter, code bar, etc.). There are three modes in which NFC can operate:

(i) reader/writer - Communication is done by an active device along with a passive device,
(ii) peer-to-peer - Communication is done by an active device along with passive or active devices,
(iii) Optional card emulation modes - device imitates a passive element, such as a contact-less card.

The integration of NFC technology with a mobile device depicted as in Fig.1 below. Multiple integrated circuits like Secure Elements (SE) and NFC interface are the basic and most important elements of this device. The NFC devices can communicate over the NFC interface. The compositions of the NFC interface are,

(i) NFC antenna
(ii) NFC Contactless Front-end
(iii)NFC controller.

The SE is integrated with the NFC-enabled devices to,

a) to confirm the secure storage of information that maintains the confidentiality,
b) to confirm the connection of the NFC controller which makes the reliable vicinity proceedings with external NFC devices happen.

An interface called Single Wire Protocol (SWP) is distributed between the NFC controller and Secure Elements which enables communication between the contactless readers (PoS (Point of Sales)) and the log application installed on SE through the NFC interface. The processing of interchanging the information and laying association surrounded by the Secure Elements and the NFC controller (managed by host controller) which is a part of the NFC system. Over the single wire protocol interface, Host Controller Interface (HCI) allows communication between SEs and NFC controller, and also provides connection between host controller and NFC controller [1]. In order to exchange the data from the remote server Universal Integrated Circuit Card (UICC) uses ISO 7816 interface. By the help of ISO 7816 includes the set of data packets i.e. Application Protocol Data Unit (APDU) to execute reading, writing, and data exchange between the Host and UICC card.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Meenaketan Sarangi*, Department of CSE, ITER, SOA Deemed to be University, BBSR, Odisha **,**
Debabrata Singh, Department of CSIT, ITER, SOA Deemed to be University, BBSR, Odisha**,**
Mitrabinda Khuntia, Department of CSE, ITER, SOA Deemed to be University, BBSR, Odisha,

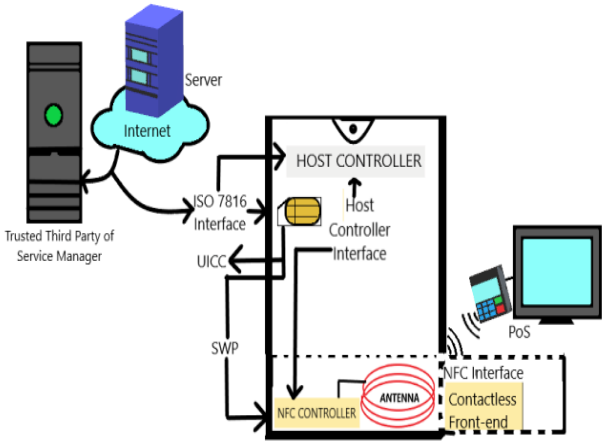

Fig.1 NFC integrated Mobile Device Architecture

Link-level security primitives are not supported by the lower layers of NFC [2]. This provides a void for the unethical attackers, who engage in exploitation of vulnerabilities such as,

a) eavesdropping
b) drop (delete) the data
c) taking over the device completely

This also raise concerns which are related to the user's privacy as the third parties can watch-over the consumer's current activities and gain knowledge about the consumer's behavior.

In section 2 we discuss about the challenges, vulnerabilities of NFC and security issues. It's very essential to take account of all the known vulnerabilities that are known till now, to which solution can be discussed. In section 3, we provide our proposed solution for "man in middle" issue which also acts as prevention from relay attacks and replay attacks. The section 4 throws light on what the solution exactly provides and how it acts as prevention to the attacks. The analysis of the solution i.e., comparison between a previously provided solution and this proposed solution and how it is better and gives proper result on the security issue. In section 5 we discuss the performance analysis and section 6 concludes the paper with some references.

II. VULNERABILITIES OF NFC

In spite of the numerous applications that presently could be manipulated using the NFC technology, with the evidence that gains the concern is that communication security primitives are not included in the lower layers of NFC does make the technology defenseless against a diversified range of attacks and vulnerabilities. In this paper, the assumption is made that the customer as well as the devices are honored. The involvements of precaution identified have connection with the transaction and update of log file (in Fig.1) over the NFC radio interface is the prime focus. It did come to notice that there are different possible angles for ambushing NFC, which primarily consist of,

(1) Malware applications instead of legitimated and authorized applications which are malicious in nature are connected on the NFC approved devices,
(2) side channels over shared the hardware components for instance smart cards are over shared by side channels selection or modify the secret and authority-only instruction that are gathered into the cards,
(3) Operating System which is malicious, where the attacker can avail himself/herself authorized access to the device and then exploits vulnerabilities.

In [3], the authors throw light on hazards for Smartphone's like accidental reveal of data, exposure of hidden data, attacks on devices which are demilitarized, supervision, etc. The solutions [3, 4] can be used to alleviate the previously mentioned issues. Like Internet, browsers contain malicious URLs the NFC tags could contain malicious threats. For example, the content of NFC tags can be hoaxed by an attacker or redirect users to the attacker website by replacing the original tags, send Short Messages (SMS), initiate phone calls, and secretly install malwares (malicious codes) (e.g., Worms and Viruses) on the NFC-enabled device without getting user's authorization or consent. An attacker can passively eavesdrop on the communication between the NFC-enabled devices without any modification to the data that is being exchanged between the devices (Fig. 2). As the data of NFC is passed through radio transmission, and by itself it is difficult to protect against eavesdropping. With the use of an antenna the attackers can sniff the data that is being exchanged between NFC-enabled devices.

Instead of being a passive element, an attacker can be an active eavesdropper who is capable of intercepting and modifying the data that is being exchanged between NFC-enabled devices and to shoot new data (Fig. 2). Replay attacks are like a passive man-in-the-middle attack, here the attacker gets to record an authentic NFC signal for later purpose.

Relay attack can also be installed in order to lay a bi-directional communication channel between two authentic NFC-enabled devices [9]. This is done to create a relay between a reader and a tag or between two authentic NFC-enabled devices. The most effective solution should be the one that can provide resistance to maximum number of discussed security issues by laying sessions that are secured over the NFC radio interface[10][11].

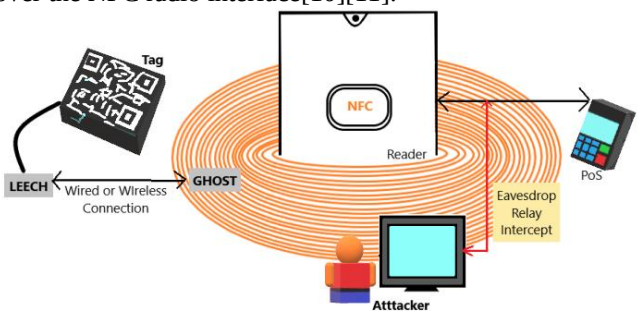

Fig.2 Possible attacks on NFC payment and update system.

2.1 NFC Security Attacks

NFC deals with various security attacks because of its perilous procedure of operating the communication and its unreliable sensors. We will discuss each attack associated with NFC to get proper perceptive of what each attack deal with and what entity they affect.

1. Eavesdropping- The NFC communication is a wireless communication. So, it becomes easier for an attacker to eavesdrop the communication. This attack is observed only in peer to peer mode and card emulation mode. When the communication is done in peer to peer mode without any security, attacker can easily eavesdrop and get the data. When the NFC devices are not in use and are in card emulation mode, the attacker can read the data in card by introducing a virus or a harmful code.
2. Faking ID- All NFC tags and cards have unique ID. It is required to avoid collision while reading more than one card. The attacker can copy the ID and use in another smart card as there no authenticity clearance checks of the ID. So more than one card can have one ID because one card uses only one ID.
3. Cloning of Ticket- E-tickets have become common in many cases like e-movie tickets, e-bus tickets, e-metro tickets, e-parking tickets, etc. Cloning of tickets is done when the tickets are shared to someone else by the ticket owner before the ticket verification is done. Now anyone who has the shared ticket can avail the service which was only supposed to be for the ticket owner till the expiration of the ticket.
4. Spoofing- It is a process where the attacker sniffs the target signal get into it and extracts the data. This can be done in more than one ways.
5. The attacker can get a malicious code into the card of the NFC-enabled device which provides the data of the card. The attacker now uses the data and makes a duplicate card which can intercept the signal from the original card.
6. The attacker can use radio receivers that are to sniff the closed by signal, intercept it and extract the data. For this attacker has to be at a 2 feet distance from the original receiver or the original sender.
7. The attacker can intercept the signal from more than a meter distance, using a simple reader which is associated with an Adriano micro-controller.
8. Man in middle attack (Modification of data)- The attacker gets in middle of the two communicating entities and modifies data (according to the purpose of attack) and passes it to the other entity at receiving end. The attacker has to be knowledgeable enough in field radio technology and wireless communication for handling the transmission modifications.
9. Corruption of Data- This happens when the attacker intercepts the signal and makes changes to the data as well as its format. After this the receiver receives a corrupted data as the NFC tag corrupted which cannot be used any further. The device has to start the data retrieving procedure again.
10. Insertion of Data- The attacker inserts undesirable data during the communication session of the NFC devices. The inserted data can be a malicious code that can corrupt the receiver's device.
11. Relay Attack- Relay attack or relay version of man in middle attack, the attacker does more than just passing data between two devices. It extracts data private data without being noticed. ISO14443 as well as ISO18092 are non-resilient to relay attacks. This attack is done by creating a bi-directional path between two devices. This two devises (ghost and leech) are the main entities of the relay attack system. The ghost hoaxes the card/tag to the reader and the leech hoaxes the reader to the card/tag. Relay attack uses Application Protocol data unit commands through a malicious application.
12. Denial of Service- Denial of Service or DOS attack, is observed when the NFC secure chip is flooded with infinite requests to access. It basically makes the device go into a loop of accessing infinite URLs simultaneously providing with a result, "browser is not responding". It can also use a simple malicious application which would stimulate all the other applications present in the device and to a point which the device fails to provide memory resource anymore. This either makes the device corrupt or the device has to be restarted [12].
13. Phishing- This attack is used when a collective credential has to be stolen like data, ID, passwords, credit card credentials. The attacker first pretends to be a trusted entity and asks the user to open any kind of pop-up, message or an e-mail. This then leads to opening of a link which then installs malware which or a ransomware. This gives the attacker full access of all the data that are present in the device. The attacker can demand ransom, expose private details, or corrupt the device. This is normally used on big companies or government related network systems to get access of private data and credentials.

III. PROPOSED SOLUTION

Shared key authentication or Shared secret key authentication, it is a verification methodology mostly used by cryptographic security mechanism. It implements the Wired Equivalent Privacy protocol to utilize a network. The authentication procedure is simple,

Step 1: The device at client end pings the access point in order to initiate the communication.

Step 2: The Wired Equivalent Private protocol sends and confidential private key.

Step 3: The access point sends a message. The client now has to provide the available private key that it received from Wired Equivalent Private protocol to encrypt the message. The message is then sent back to access point.

Step 4: The access point checks the message and does a equality comparison between the sent message and received message.

Step 5: If the comparison provides true result, it grants the device authentication, and communication path is created between the two. Certificate based authentication: It provides authentication to a genuine user or client by using digital certificate cryptography. It is a more secure cryptography security module than share key authentication. It is user friendly that makes any architecture much easier to implement. Its policy of issue of certificates, revoke of certificates and dumping of certificates makes it more secure and user friendly. In Figure 3, a clear view of how the communication engagement is done in a NFC-integrated module of authentication. A point here has to be noted, that the TTP access is a cloud-based access, for which internet is required.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

3.1 SKCB authentication (proposed solution):

Our solution SKCB (Shared Key and Certificate Based) authentication module depends upon how the PoS is used. So it is divided in two cases,

i. Internet access is provided to the reader or PoS.
ii. Internet access is not provided to the reader or PoS

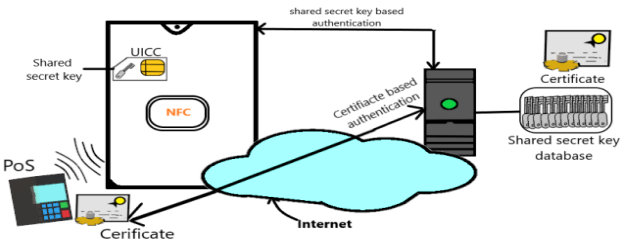

Fig.3 The certificate based and shared secret key based authentication (Di-authentication)

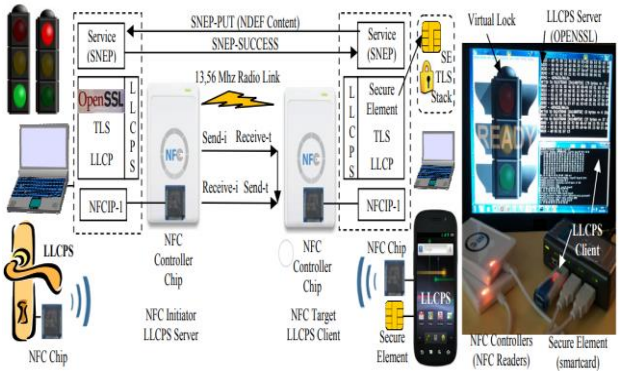

Fig .4 The architecture of LLCPS platform used in [6]

3.1.1. SKCB authentication when PoS has access of Internet connection

Level 1: R_{SE}, an arbitrary value generated by SE and UID_{SE}, the client ID in SE are sent to the reader.

Level 2: R_{PoS}, an arbitrary value generated by reader, $Cert_{PoS}$, certificate credentials generated by the reader along with R_{SE} and UID_{SE} are sent to TTP.

Level 3: A K_{PoS-SE}, key generated by the TTP after evaluating the $Cert_{PoS}$. Exclusive OR of K_{TTP-SE} and KPoS-SE is done in order authenticate the key equality. The above Exclusive OR function along with other entities (R_{SE}, UID_{SE} from step 1 and R_{PoS} from step 2) are used as parameters for generating a session key (sess key) by implementing the Pseudo Random Function on the parameters. Another entity, i.e. $Public\_key_{PoS}$ along with the sess_key are set as parameters for asymmetrical encryption to get the Res_1. (All the above operations are performed by TTP).

Level 4: The reader or PoS now has the Res_1. Res_1 needs to decrypted asymmetrically, for which the PoS uses $Private\_key_{PoS}$. The sess_key along with K_{PoS-SE} is encrypted symmetrically in order to achieve Res_2 , which is passed to SE. (All the above operations are performed PoS)

Level 5: The SE now bears the Res_2, it now evaluates the sess_key. Decryption of Res_2 is done. After decrypting the Res_2 the SE finally gets access of K_{PoS-SE} which was initially generated by the TTP as depicted in Fig. 5.

3.1.2. SKCB authentication when PoS cannot access Internet connection

Level 1: R_{PoS}, an arbitrary value generated by PoS and $Cert_{PoS}$, the certificate issued by PoS are sent to the SE.

Level 2: R_{SE}, an arbitrary value generated by SE and K_{PoS-SE}, a key that is achieved after evaluating the $Cert_{PoS}$ along with K_{TTP-SE} and R_{PoS} are assigned as parameters for a symmetric encryption. The result of the encryption procedure, i.e. Res_1 along with $Cert_{PoS}$ and UID_{SE} are passed to the TTP (all operations in Level 2. are done by SE)

Level 3: The TTP receives and evaluates the $Cert_{PoS}$. The Res_1 received in an encrypted form. The TTP uses the and the K_{TTP-SE} to do the symmetrical decryption of the Res_1. The R_{SE} along with K_{PoS-SE} is to be passed to SE. The asymmetrical encryption of these entities is done with the help of a Public_keyPoS. This encrypted message is Res_2 (all the above operations are done by TTP).

Level 4: The SE upon receiving the encrypted message passes it to the reader.

Level 5: The Res_2 is now with PoS. Asymmetrical Decryption of Res_2 is done using the $Private\_key_{PoS}$. The K_{PoS-SE} and the R_{SE} that is received from SE, confirms the equality at reader part. These entities are encrypted symmetrically to achieve Res_3 and pass it to the SE. The SE now compares the equality of the R_{SE} received from TTP and the R_{SE} received from PoS. If true, then the access of communication is allowed.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

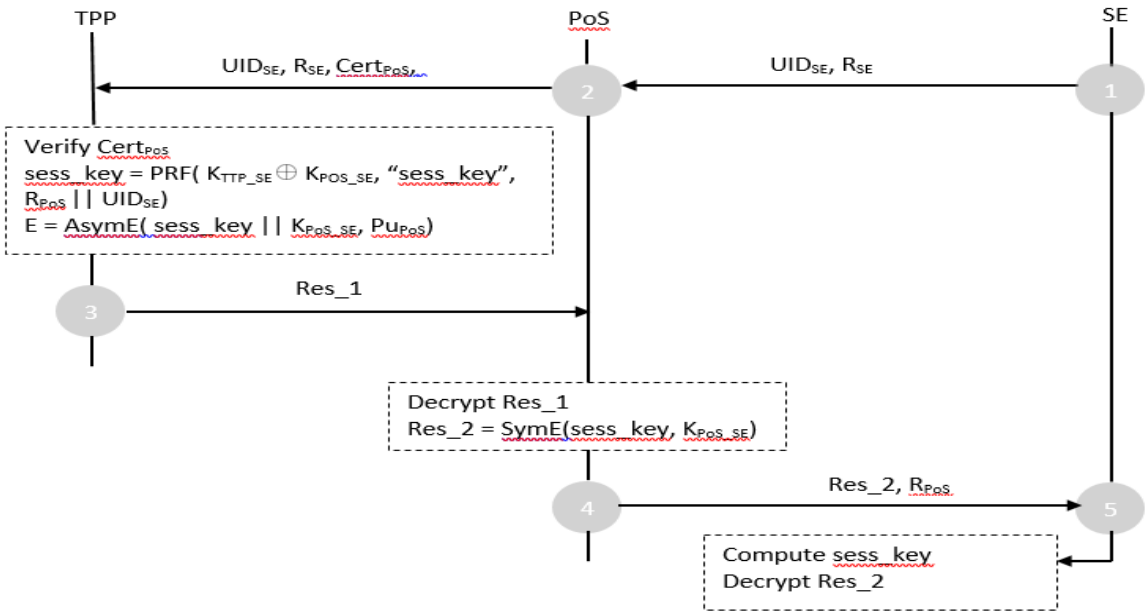

Fig.5 SKCB Authentication Case-1 (when Internet connection is accessible by PoS)

As soon as the authentication of the PoS is successful, the PoS and SE compute an encryption key which is received from K_{PoS_SE} to do the encryption of the subsequent session traffic as depicted in Fig.6.

I. ANALYSIS OF THE SKCB AUTHENTICATION

The performance analysis is done in the next section, that the SKCB authentication less expensive and more secure than some of the previously provided security protocol. As per the algorithm and figures protocol presented in previous Section, the use of session key shuts the attacker from access the communication credentials.

The decryption of session key becomes next to impossible because of its asymmetrical encryption nature. The session key uses the Pseudo Random Function (PRF), the sole-entity which confirms the mutual authentication of the reader and SE. An attacker can act as malicious/bad PoS to a SE. The solution against man-in-the-middle attack that was described earlier is very difficult for man-the-middle-attacks to decrypt the sess_key (session key) in the first place where it can be asymmetrically encrypted.

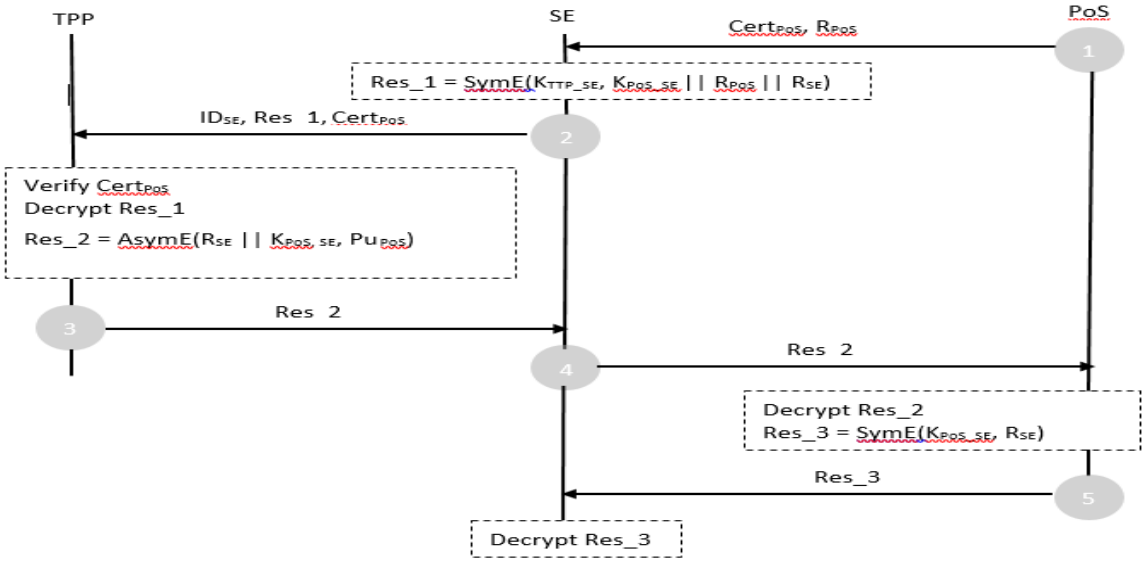

Fig.6 SKCB Authentication Case-2 (when Internet connection is not accessible by PoS)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

On the second hand, the module also provides an authentication between SE and PoS which is mutual and also with the TTP. The use of PRF function which is associated with a key establishes the mutual authentication between SE and PoS, when the exchange of data is done between the two entities. Now we provide a brief discussion on how the protocol proves to be a barrier against the security attacks.

i. Eavesdropping- Eavesdropping is avoided easily due the shared key authentication protocol. The attacker cannot decrypt the session key. The session key holds the encryption keys during the
data transfer. Hence eavesdropping is successfully avoided.

ii. Manipulation of Data or man-in-middle attack- As discussed earlier the attacker here can intercept the signal and get the encrypted session key. But it goes in vain because session key cannot be decrypted because of the encryption keys that are associated with it while encrypting in a PRF function.

iii. Relay and Replay attacks- The relay and replay attacks proves to useless due to the very same reason as the other attacks. There is no point of intercepting the signal and save it for future utilization, because the decryption of session key cannot be done at any point of time.

NFC cannot be protective against eavesdropping by itself [8-9]. But, eavesdropping can be prevented by the encryption of the exchanged data with the help of an encryption key that is achieved from the sess_key as previously described.

I. PERFORMANCE ANALYSIS

From [5] we can get the idea of implementing the Logical Link Control Protocol or LLC protocol with the TLS protocol as a security module for communication between two NFC-integrated devices. The author in [6] coined the security protocol as LLCPS authentication as depicted in Figure 4. Before going further, we must discuss about LLCP in brief.

5.1 Logical Link Control Protocol:

It is generally used when there is need of multi-signal communication. It delivers data between two Service Access Providers, if one of them is a Source Service Access Provider another has to be a Destination Service Access Provider. In Open Systems Interconnection model, this protocol layer lies in the just above the data link protocol layer [6].

Our proposed solution uses the key-encryption authentication protocol to confirm the authenticity between the NFC-integrated device which contains Secure Elements and Trusted Third Party device or server [7]. The certificate based authentication protocol is used to confirm the authenticity between the NFC-integrated reader (PoS) and Trusted Third Party device or server. In LLCPS protocols it is impossible for user/client to identify protection without renegotiation of a new TLS session. Although, in renegotiating a new TLS session there rises requirement of more asymmetric cryptographic computations that are the rate limiting step in TLS. The renegotiation of TLS gives negative impact on the performances consequences. We provide a genuine comparison of cost of computation for the three entities that we have used in SKCB authentication protocol. The three entities are PoS/reader, SE and TTP in Table 1 and Table 2. The comparison is to prove why SKCB protocol is better than LLCPS protocol are:

i. The LLCPS protocol does not show any association with TTP authentication, where as in SKCB protocol it is TTP which confirms and performs the encryption with help of encryption keys.

Table 1. The variables used for comparison between SKCB and LLCPS authentication

Time for symmetric encryption	tse
Time for decryption	td
Time for signature verification	tsig
Time for evaluating the computation	tec
Time for asymmetric encryption	tae

Table 2. Comparisons between the SKCB authentication and the LLCPS

Entity	Di-authentication 1	Di-authentication 2	Solution in [6]
SE	$1t_{se} + 1t_{PRF}$	$1t_{se} + 1t_{d}$	$1t_{PRF} + 1t_{ae} + 1t_{sig}$
PoS	$1t_{se} + 1t_{d}$	$1t_{se} + 1t_{d}$	$1t_{PRF} + 1t_{d} + 1t_{vc}$
TTP	$1t_{vc} + 1t_{PRF} + 1t_{ae}$	$1t_{vc} + 1t_{d} + 1t_{ae}$	NA

ii. The number of symmetrical encryption performed by SE in LLCPS protocol case is three and in case of SKCB protocol it is two. The author in [6] uses authentication and encryption of certificate signature, making the cost of computation more.

iii. The SKCB protocol associated the TTP, it maintains anonymity manner in encryption of session whenever required. If an attacker intercepts the communication, The TTP drops the encrypted credential (which cannot be decrypted) and simultaneously establishes a new communication with a different random encryption key which is totally different from the previous communication. But in case of LLCPS, if an attacker intercepts it drops session and re-establishes a new TLS protocol session which makes it more expensive due to increase in number of asymmetric operations.

II. CONCLUSION

Association of NFC with mobile payment and mobile log update system has made us look the vulnerabilities and voids for unethical hackers. It provided growth to the interest that is related to the security issues of the NFC users'. The fact that, all the security issues have been proven with improve of technology each day the attacks get another angle of finding vulnerability.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

So, to this view the proposed solution not only does provide security to the transactions that are performed through NFC but also to the private data of the account of the user. It is proven to be better than the all the previously given solutions in terms of computation cost as well as communication. It does provide a future scope for digging more towards sharing the solution with TLS protocol.

REFERENCES

1. Divyashikha Sethia, Daya Gupta, Huzur Saran, "NFC Secure Element-Based Mutual Authentication and Attestation for IoT Access", IEEE Transactions on Consumer Electronics, vol. 64, issue: 4, pp. 47-479, IEEE, November 2018.
2. Fan Dang, Pengfei Zhou, Zhenhua Li, Yunhao Liu, "NFC-enabled attack on cyber physical systems: A practical case study",IEEE Conference on Computer Communications Workshops Electronics", IEEE, November 2017.
3. Gummeson J, Priyantha B, Ganesan D, Thrasher D, and Zhang P, "EnGarde: Protecting the Mobile Phone from Malicious NFC Interactions", 11th International Conference on Mobile Systems, Applications, ad Services, pp. 445-458. MobiSys, 2013.
4. Rieback, Melanie R., Georgi Gaydadjiev, Bruno Crispo, Rutger FH Hofman, and Andrew S. Tanenbaum, "A platform for RFID security and privacy administration", USENIX LISA, pp. 89-102.USENIX, December 2006.
5. Badra, Mohamad, and Ibrahim Hajjeh, "Key-exchange authentication using shared secrets", Computer, vol. 39, issue: 3, pp.58-66. IEEE, March 2006.
6. Urien, Pascal, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things", 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC), pp. 845-846. IEEE, January 2013.
7. Elminaam, Diaa Salama Abdul, Hatem M. Abdul Kader, and Mohie M. Hadhoud, "Performance evaluation of symmetric encryption algorithms on power consumption for wireless devices", International Journal of Computer Theory and Engineering, vol.1, issue: 4, p.343, Semantic scholar, 2009.
8. M. k. Sarangi, D. Singh, "Supply and Monitoring the Municipality Drinking Water through NFC and SCADA System", IEEE Conference on Applied Electromagnetic, Signal Processing & Communication (AESPC-2018), 2008.
9. Ong D.D.W. & Mahinderjit Singh M. , "A secure near field communication (NFC)-enabled attendance on android mobile for higher education", Knowledge Management International Conference (KMICe), pp.111-115, 2016.
10. Vermaas R., Tervonen T., Zhang Y. & Siljee J., "The security risks of mobile payment applications using Near Field Communication", Rotterdam: Erasmus University Rotterdam, 2013.
11. Velasquez M. & Hester P.T., "An analysis of multi-criteria decision making methods", International Journal of Operations Research, 10, 2, pp.56-66, 2013.
12. D. Singh, B.K. Pattanayak, "Ambient Energy Harvesting and Management on the Sensor Nodes in a Wireless Sensor Network", International Journal of Renewable Energy Research (IJRER), Volume 7(4), pp. 1869-1879,Dec-2017.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)