PEER TO PEER TRANSACTION AND USER PRIVACY PROTECTION IN NEAR FIELD COMMUNICATION

Neeta Thorat and Prof. Chaitali Laulkar

Department of Computer Engineering, Sinhgad college of engineering, Vadgaon bk, Pune.

ABSTRACT:
Near Field Communication is a short range wireless communication technology. It is also used as contactless identification which is evolved from RFID. NFC is using with smart phone increases range of applications of NFC. Today peer to peer communication of NFC is not secure in term of data privacy and data integrity. Also currently NFC use their fixed value public key at the time of key agreement, but this is also not secure because attacker can create profile based on user profile, so there is issue of user privacy. The smart phone equipped with NFC replaces credit card to the electronic payment can be able to do payment transaction processing in automated manner, also able to respond in real time for automated checkout in retail shopping environment. This paper focuses on authentication protocol with the envelope of LLCPS (Secure logical link control protocol) for NFC peer to peer secure payment processing in a retail store environment means provide security to NFC transaction. Also provide privacy protection for user in which the identity of users can be verified by the TTP (Trusted Third Party) to resolve disputes when necessary. The proposed method can solve the problem of privacy information leakage of user and works with strong mutual authentication, and enforces privacy and integrity features for peer to peer transaction over NFC.

Keywords: NFC Security, LLCPS, Physical Retail store, Payment, RFID.

[1] INTRODUCTION

Today the rapid development and adoption of information technologies is changing the way of doing business significantly. The growing interest on electronic commerce to perform business transactions brought vital improvements, especially in contact less technologies. Near Field Communication (NFC) has become one of the promising technological developments in IT industry. Near Field Communication is a combination of contact less identification and interconnection technology.

NFC is short range wireless communication technology. It is evolved from RFID (Radio Frequency Identification). It uses principle of magnetic induction coupling. The frequency of NFC is 13.56 MHz and data transfer rate is 424 kilobits per second. Maximum range is up to 10 cm. The functionality of NFC is divided into three modes reader/writer, card emulation, peer to peer. Each operating mode has a different technical infrastructure as well as advantages for the users. Only one mode can be selected at a time, which means that, for example, when the reader/writer mode is on, the card emulation mode cannot be used.
A. Reader/Writer: The NFC device behaves as a reader for NFC tags, such as the contactless smart cards and RFID tags.

B. Peer-To-Peer: This mode enables two NFC devices to exchange data with each other.

C. Card Emulation: NFC device acts as a contact less smart card. It is compatible with existing smart card infrastructure.

Now a day’s many smart mobile terminals equipped with NFC. There are various applications of NFC with smart phone like data exchange, service discovery, connection, e-payment, ticketing. Due to NFC enabled mobile phone the seamless processing of retail store transaction is possible with using the tap of smart phone. Secure framework with authentication protocol for retail store transaction is also necessary for it. Every customer is not regular, so there is key distribution problem which we can solve by public key cryptography, but it required more space to store. Elliptical curve based authentication protocol is used at the place of public key cryptography because it required less memory and also required less computational resources. Consider the item presents at the physical retail store for selling is identified by NFC tag.

When NFC use in electronic payment then security is more important. Key agreement is required for secure secret communication between two NFC devices. This paper presents privacy protection methods to protect privacy of user with authentication protocol based on elliptical curve cryptography with the envelope of secure logical link control protocol (LLCPS) for payment processing in physical retail store based on smart phone. In this paper, section 2 gives the detail background information about NFC interface, NFC security standards, elliptic curve cryptography, and related literature. Section 3 presents proposed method. Section 4 shows algorithm used proposed method. Section 5 presents results for proposed method. Finally section 6 concludes the paper.

[2] BACKGROUND AND RELATED LITERATURE

There are different security threats for NFC such as MIME (Man In the Middle attack), eavesdropping, data corruption, data modification, privacy which is shown by Haselsteiner and Breitfu in [17]. Due to such security threats NFC security protocol satisfies some properties or some requirement. The security requirement for NFC security protocol is data confidentiality, data integrity, unlink ability, traceability. There is also issue due to use of fixed ID. There are not much work regarding security of NFC was available.

Security protocols of NFCIP-1 are standardized in ECMA 385 as NFC-SEC (NFC Security) and ECMA 386 as NFCSEC-01. It defines a protocol stack that enables application independent encryption function on the data link layer. NFCSEC-01 specifies cryptographic mechanisms for key agreement, data encryption and integrity. It create a secure channel for peer to peer communication of NFC [2]. Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkata N. Padmanabhan, proposed in [18] Dhwani : Secure Peer-to-Peer Acoustic NFC provides security at the physical layer using a novel selfjamming technique, JamSecure, wherein the receiver intentionally jams the signal it is trying to receive, thereby stymying eavesdroppers, but then uses selfinterference cancellation to successfully decode the incoming message. The security thus obtained is information-theoretic, i.e., Dhwani inherently prevents the leakage of information to an eavesdropper. Hasoo Eun, Hoonjung Lee, Heekuck Oh proposed in [3] Conditional Privacy Preserving Security Protocol for NFC Applications. The method of conditional anonymity is based on dynamic ID. NFC does not provide security there is no security in today’s LLCP
sessions. NFC-SEC and also some researcher introduce some security method to different layer of NFC, as shown in [Table-1].

**Table: 1 Different security methods for NFC**

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>Name</th>
<th>Layer of NFC</th>
<th>Algorithm or technique use</th>
<th>Support to mobile phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NFCSEC</td>
<td>Top on NFCIP-1</td>
<td>ECDH, AES</td>
<td>NO</td>
</tr>
<tr>
<td>2</td>
<td>Conditional privacy</td>
<td>NFCIP-1</td>
<td>ECDH, Anti collision, MacTag, Hardware use</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Dhwani</td>
<td>Physical layer</td>
<td>Self jamming technique</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Similarly when NFC enabled mobile phone use for seamless transaction in physical retail store then for key distribution there are two options RSA and Elliptic curve. Several researchers have studied elliptic curve cryptography for wireless applications. For example, [14] design and illustrate an elliptic curve based public key authentication of RFID tags. Hoa et al. use elliptic curve cryptography (ECC) to develop a protocol for mutual authentication. Martinez et al. propose to develop a feasible and scalable zero knowledge authentication protocol with privacy guarantee using elliptic curve cryptography. Godor et al. present a mutual authentication protocol based on elliptic curves and public key infrastructure (PKI). They consider attacks related to authentication, verification, integrity, traffic analysis, and non-repudiation and design their protocol based on resistance to these attacks [2]. The [Table-2] shows comparison between RSA and ECC.

**Table: 2. Comparison of RSA and ECC.**

<table>
<thead>
<tr>
<th>Sr. No</th>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Key size is large</td>
<td>Key size is small</td>
</tr>
<tr>
<td>2</td>
<td>Slower Computation</td>
<td>Faster computation</td>
</tr>
<tr>
<td>3</td>
<td>Power consumption is high</td>
<td>Power consumption is less</td>
</tr>
<tr>
<td>4</td>
<td>waste memory space and bandwidth</td>
<td>Save memory space and bandwidth</td>
</tr>
</tbody>
</table>

[3] PROPOSED METHOD

The proposed peer to peer transaction and user privacy in NFC system model basically designs for the physical retail store which uses the NFC enabled sign in and sign out terminal and NFC tag present on items. The system targets mainly on security and also key distribution problem for the customer in retail store. The proposed system is divided into three phases. 1) Customer sign in. 2) Shopping. 3) Customer signs out successfully.
Sequence of processes in the system architecture shown in [Figure-1] is as follows: In the first phase Smart phone and sign in terminal generate keys then exchange those key and store key when customers comes at sign in terminal and tap his smart phone to sign in terminal. At that time shopping cart get activate. In the second phase, read and add value present on NFC tag when smart phone taps on the NFC tag which is present on item. At the end make total. In third phase first verify the keys and then make secure payment by using LLCPS and get sign out when smart phone taps on the point of sale terminal.

1. **Sign in module**

   The sequence of procedure of sign in module is as shown in [Figure-2]. The sign-in protocol begins when the customer’s smart phone is tapped on the Sign-in Terminal at the store entrance. It goes from three steps: 1) Key Generation. 2) Key exchange. 3) Activate shopping cart.

   Elliptical curve cryptography is used for key generation (details in 4 B). The standardized curve name as secp160k1 is used for algorithm. Property of curve is SECG curve over a 160 bit prime field. The algorithm generates 160 bit key. The public key is calculated as multiplication of private key and generator of curve G. This multiplication is called as scalar multiplication.
In step 2, generated public key gets exchange. Both generate shared secrete by using self private key and others public key. From the shared secrete we cannot calculate the private keys of any of them. Both agree on shared secrete for that session. Once authentication is done then sign in terminal set signal to activate shopping cart in smart phone. Proposed sign in protocol required minimum messages and shorter key size. When complete sign in protocol the atomic transaction start for shopping in distributed manner.

2. Shopping cart module

Shopping cart module is as shown in [Figure-3]. Shopping cart module get activate at the time of sign in module. When smart phone taps on tag present on the item then tag reading algorithm is running and shopping cart read information from the tag. Add the value to the cart and finally make total of it. The information stored on the tag is in the form of NFC data exchange format(NDEF).

![Figure: 3 shopping cart module](image)

3. Point of sale module

The sequence of procedure of PoS module is shown in [Figure-4] PoS module start with smart phone taps on PoS terminal then both are validate to each other by comparing the store message in sign in module, if message are invalid then abort transaction. Then by using database and transaction processing system payment is done in the envelope of LLCPS and generates bill and then customer get sign out.

![Figure: 4 Point of sale module.](image)

4. Payment by LLCPS module

As shown in [Figure-5] this procedure follows message sequence from top to bottom. It contains NFC initiator and NFC target. Both have four software layers. (1) A NFCIP-1 layer provides radio framing and MAC facilities [21] (2) A LLCP (Logical Link Control Protocol) layer manages P2P sessions[10], (3) A TLS stack using the well-known OPENSSL library on the Initiator side, and running in a secure element (a java card, see) on the Target side. (4) A SNEP service used by the Initiator to collect data from the Target [11].

Neeta Thorat and Prof. Chaitali Laulkar
Here, the proposed method of authentication protocols is used instead of SNEP. When user taps a NFC mobile due to above all layer passes key value securely.

[4] METHODOLOGY AND ALGORITHM

A. Tag Reading Algorithm
1) User starts NFC Shopping application.
2) User scans the tag containing item information.
3) ReaderActivity class is launched.
4) getNdefMessages() method is invoked.
5) if NDEF message is present then parsed it and display message in text form else show text scan a tag
6) The product is added to the shopping cart.

B. ECDH Generator Algorithm
1) Take standardized curve.
2) Set or initialize the parameter of the curve.
3) Take any integer as private key which is less than n. N is the largest number on curve.
4) Generate public key.- a) Take private key b) Take curve generator as G. c) Do scalar multiplication of private key and G. d) Retrieve public key.
5) Generated keys for smart phone and sign in terminals are:
   private key of smart phone = sS. public key of smart phone = sP = sS*G. private key of sign in terminal = tS.
   public key of sign in terminal = tP = tS*G.
6) Smart phone send sP to sign in terminal.
7) Sign in terminal send tP to smart phone.
8) Both generate shared secrete M= tS*G_sS by using self private key and others public key.
9) Agree on shared secrete.
10) Save the generated key

C. LLCPS Algorithm
1) It uses secure element at end of POS service & uses open SSL library at bank server which protect bank server
2) Algorithm working in 5 processes
   a) Connection process - Secure session get initiated.
   b) Sending process - Server and client can send PDU
c) Receiving Process - Server and client can receive PDU
d) Disconnection process - It is optional due to distance; otherwise any of server or client send DISC PDU to disconnect.
e) Inactivity process - It continuously run when both client and server can’t send any message.

[5] RESULT AND DISCUSSION

The Proposed system is one secured application for physical retail store. In proposed system there is a secure envelope which secures the whole application and key distribution for authentication and shopping in distributed environment for each customer. The PoS module collects payment from every user and every user do payment and logout with security. Security Levels are a formalization of ‘strengths’ of security, Security Bits estimate the computational steps or operations required to find a solution to the problem in the problem’s domain. For key distribution in application for authentication of user the key size should be small but providing security is more. So that here key length is also very important security parameter. The [Figure-6] shows generated key sizes for the same level of security which is recommended by NITS in [4].

Figure: 6 Security level with key size.

For the same security level ECC required less key size than RSA. If key size is small then its required storage space is also minimum. The key generation time is the time required to generate the key by specific algorithm. It should be minimum to reduce the execution time of the application to increase the efficiency of application.

<table>
<thead>
<tr>
<th>Security level In bits</th>
<th>ECC key size(in Bits)</th>
<th>Key generation time(in milliseconds)</th>
<th>RSA key size(in Bits)</th>
<th>Key Generation time(in milliseconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>160</td>
<td>80</td>
<td>1024</td>
<td>160</td>
</tr>
<tr>
<td>112</td>
<td>224</td>
<td>180</td>
<td>2048</td>
<td>7470</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>270</td>
<td>3072</td>
<td>9800</td>
</tr>
<tr>
<td>196</td>
<td>384</td>
<td>640</td>
<td>7680</td>
<td>133900</td>
</tr>
<tr>
<td>256</td>
<td>512</td>
<td>1440</td>
<td>15360</td>
<td>679060</td>
</tr>
</tbody>
</table>
The above [Table-3] shows for same security level the RSA take more time to generate key with more size and ECC take less time to generate key with small size. Time to break the security is measured in MIPS-years. MIPS-years is a one Million Instructions Per Second in one year. Fig shows what key lengths of each algorithm will provide a level of security measured in the time in MIPS-years to break the security.

![Figure: 7 key size of ECC & RSA for same security level.](image)

The above [Figure-7] shows that security of ECC is break in similar time as compare to RSA but with minimum size. The security must be stronger where the money transaction involved in the application. The proposed system provides the security to Peer to peer transaction in NFC.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>NFC</th>
<th>NFC-SEC</th>
<th>LLCPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Secure channel establishment</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Used security Algorithm</td>
<td>No</td>
<td>ECDH, AES</td>
<td>TLS Open SSL</td>
</tr>
<tr>
<td>Supported to mobile phone</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Link level security</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The [Table4] shows the comparison between the proposed system and previous system. It shows that NFC with LLCPS provides the link level security so that any data transfer in application layer is secure.

### [6] CONCLUSION

Consider uses of smart phone enable with NFC increasing day by day and also it provides number of services. Also Automation in retail store increases like self check out, So it is important that NFC is strongly secure. This project stage-I conclude that the proposed system is basically designed for the secure seamless transaction in physical retail store environment. Mostly modules are designed for the authentication and atomic transaction in retail store in the envelope of LLCPS. LLCPS module provides security related to data integrity and privacy for peer to peer communication between two NFC devices so that securely payment is done.
ACKNOWLEDGMENT

I would like to thank my teachers and also I want to thank my family and friends for their support.

REFERENCES

