NFC Enabled Car Key in WSN Secure Crypto Mediated_RSA

Siddharth Shankar Pandey

Abstract- Near Field Communication (NFC) technology is one of the most promising technologies in the field of mobile application. The integration of NFC technology and smart mobile device stimulates the daily increasing popularity of NFC-based mobile applications which having proliferated in the mobile society.NFC is the latest wireless technology which works on the principle of Radio Frequency Identification (RFID). The data is moved over charismatic field within the closeness of about 4-5 cms. Though RFID has been around for a long time, it does not provide personalized facilities to authorized person according to the random key producer. NFC is as long as facilities which no technology has offered so far. NFC is basically executed into smart phones. Here we need to identify the key splitting in two shares with the use of mediated RSA algorithm.

Keywords— NFC hardware, RSA key, Identity encryption, Security mediator.

I. INTRODUCTION

NFC enabled SIM is a totally new concept in the mobile telephony outline. The specific new era SIM is known as UICC For the UICC we can control into secure key if we able to take UICC key then it is not totally secure key, in the event that we detail it into auto produced key as an uneven key which is act as secret word ensured key [3]. It is the most Secure Element (SE) possible in the mobile phone devices. It provides extended facilities and security to the receiver. It likewise offers enhanced scope and limit for end clients [5].

In the event that we need more secure for UICC key we will enter the irregular key that Sem(security mediator) Will handle the key, the complete data about the UICC key nobody have, which will give more security to the UICC [9].

UICC includes ISIM (IP multimedia Facility s Identity Module) which lets user have a unique digital identity and gain access to non telecom applications which in this case is the NFC enabled car keys. We utilize 'TAP and GO' characteristic to satisfy different undertakings [10]. It joins using IP (Internet Protocol), the same standard which is used in Internet thus providing unique digital self to each device UICC key will split into two part as far security media and end user. Which will transfer the SMS also in between the SEM and user as well.

Actors and Roles

1) *Key Mediater* - basically it's a virtually key handler for particular period of time) - Manages the split key accounts of every user. Also sends the decrypting code to the delegated user upon administrator's request. Security concern is that key mediator also has 50% key.
2) *Administrator* - User who owns the car and is the sole owner of the car key.
3) *Delegated User* - User who has been granted key which will have random key and it will be auto generated code .
4) *Chip Manufacturer* - This entity basically manufactures the NFC chips/UICC with unique identifier.

   The Administrator will open the car using 'TAP AND GO' feature, sit inside the car and put his phone in the center console. When the telephone is set in the middle support, the circuit for motor ignition is finished [5]. Here placing the phone in center console acts the same as putting the key in the cars now[8]. However the telephone will in any case request secret key which must be entered by the executive when he/she enter the watchword it will try for security mediator and it match with half key with security mediator [2]. In the event that three times the wrong watchword is entered the caution message is sent to the enrolled numbers [13].The registered numbers could be those which the administrator has listed with the system administrator. The extra password might end up being valuable in case the phone is stolen. At the point when key affix with sender key in the event that its right ,charge try for begin else it will try for administrator client as a robbery client [12].

   such data on a large scale. Another shortcoming is that today's Web lacks an efficient mechanism to share the data when applications are developed independently. it is important to stretch out the Web to make information machine-justifiable and incorporated and reusable crosswise over different applications[2].

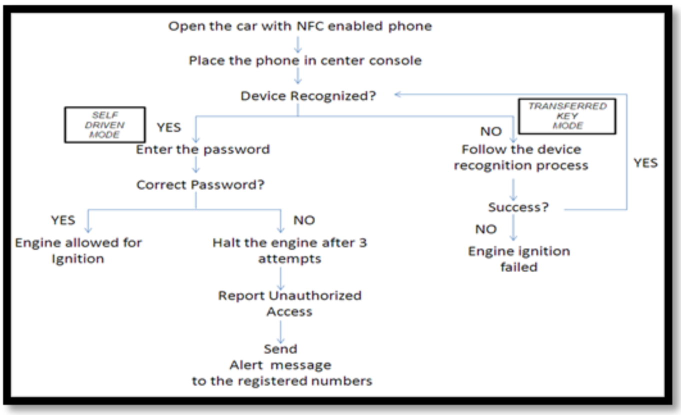
Open the car with NFC enabled phone
Place the phone in center console
Device Recognized?
SELF DRIVEN MODE
YES
Enter the password
Correct Password?
YES
Engine allowed for Ignition
NO
Halt the engine after 3 attempts
Report Unauthorized Access
Send Alert message to the registered numbers
TRANSFERRED KEY MODE
NO
Follow the device recognition process
YES
Success?
NO
Engine ignition failed

Fig. Example of open the car with NFC enabled phone

CASE STUDY: HYUNDAI INTRODUCES NFC ENABLED CAR KEYS

Hyundai is also using a similar concept and making cars which support NFC enabled keys (using smart phones). The proposed system will take some time to come around as it is being tested for implementation. The expected features are:

1. Authorized access
2. Prevention of Theft
3. Find location of the car(moving or parked)
4. Transferring the key over the air (OTA)
5. Immobilizing the car in case unauthorized access is detected.

To realize the given features, NFC must be embedded into phone. There are two possible ways to embed NFC in mobile:

1) NFC chip integrated into mobile device with the suitable antenna[1].

2) NFC application incorporated into the SIM

II. RELATED WORK AND MOTIVATION

Identity based encryption (IBE) is an open key encryption advancement that allows an open key to be figured from an identity and a set of open numerical parameters and that considers the corresponding private key to be computed from a character, a set of open numerical parameters, and a domain-wide secret value. An IBE open key may be calculated by any individual who has the necessary open parameters; a cryptographic mystery is required to figure an IBE private key, and the estimation must be performed by a trusted server that has this mystery [1].

A novel blind signature scheme based upon security of ECDLP. The proposed plan is untraceable. The proposed plan is also generally verifiable. The proposed plan can withstand some of the dynamic ambushes like falsification assault, key-just ambush, and known-message strike, picked message ambush [4].

Results: The scheme also satisfies untraceability property. They have demonstrated that their plan is generally. verifiable. The proposed scheme has low computational overhead and proved to be resistant against active attacks. The proposed scheme is suitable for applications, for examples e-banking, e-commerce and e-voting.

Another ID-based mark plan utilizing bilinear pairings. This plan is secure against existential impersonation on flexible picked message and ID strike with the assumption that the Cdhproblem is immovable [6].

Results: They have proved that the proposed scheme is unforgeable in the random oracle model with assumption that the CDH problem is intractable[14].

In this paper They propose another secure key issuing meeting in which a private key is issued by a key period center and after that its security is guaranteed by various key protection powers[7].The proposed secure key issuing convention issues a true ID-based private key, henceforth it may be utilized with any ID-based cryptosystems defending the purpose of enthusiasm of ID-based cryptography [4].

Results: In cryptography the proposed technique is another methodology to devide a power into various parties. This methodology will be valuable in numerous provisions where the power is truly compelling and a control or perception is required. It will help to make this present reality power be more distributed ones [4].

III. PROBLEM WITH SOLUTION

i. If the phone is lost or stolen.

The enemy will still need to enter the password after placing the phone in the center console.

ii. The challenger can't try to copy the key from the phone because the code will be generated.

The key placed inside the phone is encrypted and needs a decrypting code from the key mediated which is not the fully identifier of the key . Without the decrypting code the encrypted key is rendered useless. The decoding code must be made accessible when the owner converses with the key director and gives him the commissioning secret password [3].

iii. The adversary may try to corrupt the key.

The encrypted key is placed inside the secure element which is isolated and cannot be accessed easily. Following security elements are realized in the Secure Element using cryptography:

1) Access Security (i.e. unapproved access to read/write data, control of prepared information).
2) Data Integrity (determined information might not be controled, separately control should be distinguished and may be counter measured).
3) Major disadvantage is if key lost the recoverable process is long behind the reason is key will change every login unless more security point of view.

IV. EXPERIMENT DESIGN AND METHODOLOGY

ALGORITHM FOR IB-mRSA in NFC encrypted Code Generation

- e→IB- mRSA.key(recipient's identity)
- n is saved from organization certificate;
- Message m is encoded utilizing standard RSA encryption with (e; n) as the general open key

The beneficiary's open key guaranteeing is not needed for the sender to encode.

Since the key is resolved from the beneficiary's emerge identifier, the sender does not oblige an declaration to assurance that the proposed recipient is the right open key holder. ALGORITHM FOR IB-mRSA DECRYPTION

First step:

- USER: m' →encrypted message
- USER: send m'to SEM

Second step:

- In parallel:
- SEM :
- If USER revoked return (ERROR)
- PDsem→$m'^{dx,sem}$ mod n
- Send PDsem to USER
- USER:
- PDu→$m'^{dx,u}$ mod n

Third step:

- USER: m→(PDsem * PDu) mod n
- USER: return (m)

Along these IB-mRsa provides identity based encryption alongside revocation. Additionally use of mRsa decoding strategy offers security to the message. Presently we will perceive how this method could be stretched out to electronic transactions.

The merchant, Admin and SEM together check for the authentication of the mouthpiece and get the required messages after decryption. The merchant and the Admin verify the signature of the mouthpiece on the order and payment details.

The merchant sends the goods/facility s to the receiver and the receiver acknowledges with the transaction id with a signature as above. Then the merchant sends this acknowledgment along with a capture request consisting of payment amount and transaction id to the payment Admin. The Admin confirms the signature of the recipient and matches the transaction id with the prior message. At that point the installment is made to the dealer [9].

Thus, the receiver sends the encrypted order details and payment details along with the corresponding signed messages. The merchant decrypts the order details and verifies the signature.

The Admin decrypts the payments points of interest and checks the signature for the same [11]. The order details are not known to the Admin and payment details are not known to the merchant. The two are sent together to avoid any confusion regarding the order and payment combination. The Security Mediator takes care of the payment through the payment Admin to the merchant once the order is released. Also, the SEM authenticates the receiver as well as the merchant.

V. RESULTS

The purchaser gets the payment card issued by a Admin. Then he goes through the Internet to purchase certain goods. Once he goes through various retailers' information, he decides on a particular retailer to place the order. He sends the order list to the retailer and after going through the order, the merchant accepts the order and sends an acknowledgment. Then the purchaser sends the information about the order placed by him along with the payment details to the mercantile. However, the merchant should not get the credit card details of the purchaser, which is sent lengthwise the payment details. To make sure that the purchaser does not lie about the order, the order and the corresponding expense information are to be sent together. The security outline takes care of the issue that, the merchant gets only the order information and the Admin gets the payment information. The purchaser using the individual public keys of the merchant and the Admin encrypts the order details and payment details. He then connects the two alongside an arbitrary number and sends to the dealer. The dealer sends the same to the SEM. The SEM verifies the validity of the merchant and the Admin. The SEM using the part of the private keys of the merchant and the Admin decrypts the order details and payment details and sends them to the merchant and the Admin, respectively. The merchant makes use of the part of his private key and decrypts the order details and uses it to get the order details along with the decrypted message received from the SEM. Similarly the Admin gets the payment details after decrypting the payment details with partial private key and making use of the decrypted message from SEM. So the scheme takes care that the merchant gets the order details only and the Admin gets the payment details only. Also they are sent together by the purchaser to avoid conflict. The scheme also uses the Identity based cryptography.The actual working of the scheme is described below.

VI. CONCLUSION

NFC is captivating for customers who love technology in their routine life. But sometimes it may go out that person stealing your phone may end up stealing your car as well. Further more in many case where the phone's battery dies out or the phone is dropped into water the smart key may be rendered useless.

On the contrary it would a little hard to give that kind of power to the handset.

However the main alarm is the role of the mobile network as they will be the ones who have to bear the cost of UICCs. Definitely the cost of UICCs will be higher than the simple SIMs. The cost can be divided between different facility provider such as MNO, OP and RP. While the user adds more facility s to his card (i.e. UICC) the cost will be further divided. Facility providers have always been willing to expand their facility s hence multi-application capability of UICC has the potential to add a large number of functions. The new combination of NFC and SIM can enable the realization of many new use cases which have not been pulled off till date. UICC has opened gates to limitless opportunities.

Main coordination in between the user admin and SEM ,they don't identify the key , some combination depend on the append the security key .Which is security point of view more higher in future scope we can follow up how to recover the key as administrator side when he get lost the key.

VII. ACKNOWLEDGMENT

We are truly grateful to the idea reviewers for their accommodating plans and remarks for the empowerment for composing this paper.

REFRENCES

[1] Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Sandeep Tamrakar, and Christian Wachsmann '
[2] SmartTokens : Delegable Access Control with NFC-enabled Smartphones'
[3] X.509 Internet Public Key Substructure Online Certificate Status Protocol (OCSP), IETF
[4] RFC2560, http://www.ietf.org/rfc/rfc2560.txt.
[5] Annual PKI Research Workshop, 2002.
[6] Boneh, D. and M. Franklin, 2001. Identity based encryption from weil pairing. Adv. Cryptol. Crypto, 2139: 213-229.
[7] Boneh, D., X. Ding and G. Tsudik, 2002. Identity-based encryption using mediated RSA. Proceedings of the 3rd Workshop on Information Security Applications, Aug. 28-30, Jeju Island, Korea.
[8] Choon, J.C. and J.H. Cheon, 2003. An identity-based signature from gap diffie-hellman groups, public key cryptography. PKC, 2567: 18-30
[9] Diffie, W. and M. Hellman, 1976. New directions in cryptography. IEEE Trans. Inform. Theory, 22: 644-654.
[10] Rivest, R.L., A. Shamir and L. Adelman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Common. ACM., 21: 120-126.

[11] A. Karatsuba and Y. Ofman. Multiplication of Many-Digital Numbers by Automatic Computers. Proceedings of the USSR Academy of Sciences, 145:293–294, 1962.

[12] Michael LeMay and Jack Tan. Acoustic surveillance of physically unmodified PCs. In SAM '06: Proceedings of the 2006 International Conference on Security and Management, pages 328–334. CSREA Press, 2006. [Min] MinGW. Minimalist GNU for Windows. URL: http://www.mingw.org.

[13] MITRE. Common vulnerabilities and exposures list, entry CVE-2013-4576, 2013. URL: http://cve.mitre.org/cgibin/cvename.cgi?name=CVE-2013-4576.

[14] Peter L. Montgomery. Modular multiplication without trial division. Mathematics of Computation, 44(170):519–521, 1985.