Security of NFC

Mrs. Shreya Parikh
Assistant Professor,
Department of Computer Engineering,
Atharva College of Engineering,
Mumbai University, India

Abstract: **Security is an important aspect for the success of Near Field Communication technology. Due to high interoperability, protection of the NFC data requires combination of suitable mechanism and popular collection of standards.NFC does not provide reliable security against privacy protection or protection against a device being vulnerable to coincidental reception of malicious data. Since no kind of authentication is involved before an NFC transaction, transfer of malware applications could also be a major threat to the user. Hence a secure NFC Application to implement the available features of NFC not only efficiently but also securely is more than important to make the fullest use of this technology.The paper reviews two system which focuses on protection of the data transferred between two NFC enabled devices using combination of RSA and AES and another combination which uses combination of AES and Deffie Hellman encryption algorithms and trying to secure the transferred data from various possible attacks.**

Keywords: Near Field Communication (NFC), Security, Data Transfer, RSA, AES, Deffie Hellman Attacks

I. INTRODUCTION

Near field communication, also known as NFC is a form of wireless communication technology between modern mobile devices such as smartphones and tablets. Two mobile devices are tapped close to each other together to exchange information. It is a short-range radio technology that operates on the 13.56 MHz frequency, with data transfers of up to 424 kilobits per second. NFC is basically an evolution of radio-frequency identification (RFID) technology. It uses magnetic field induction to enable communication between two active devices which are close together.This feature makes it easy to exchange variable form of data such as contact cards, photos etc.

Three communication modes are available as illustrated below:

Peer to Peer mode: Device to device link level communication

Read/Write mode: Allows applications to transfer forum defined messages

NFC card emulation mode: Allows handset to behave as a smart card[1].

NFC potential is enormous and includes things like:

- Contactless credit cards. Making payments without taking the card out of the wallet.
- Public transport fare systems, tickets in general.
- Bonding and establishment of trust relationships, like Bluetooth pairing, without the need of PIN codes since the close contact is the security factor.
- E-money stored in your cell phone, use your phone as the credit card or pre-paid card. Many cell phones already support NFC.
- Communication with medical devices in a very ergonomic fashion, since the act of touching e.g. a blood pressure monitor with the cell phone is a strong indication that the user wants to transfer measurements. The proximity adds to security.
- NFC technology is designed to increase convenience when learning, shopping, and sharing data.

II. LITERATURE REVIEW

The possibilities are limited only by the imaginations of those manufacturing this technology. NFC can replace barcodes with more intelligent NFC tags and allow smartphone users to interact with objects to find out information such as a bus schedule or learn more about a product they want to purchase. The principal objectives to pursue for data protection are: Authenticity, Integrity and Confidentiality [2].

With media exposing major security breaches and the compromising of sensitive data due to the activity of hackers, there are growing concerns about the security and safety of private stored information when carrying out NFC-based mobile transactions. The NFC communication is usually done between two devices in close proximity. This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more.

•RF field characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)

•Characteristic of the attacker’s antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)

•Quality of the attacker’s receiver

•Quality of the attacker’s RF signal decoder

- •Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- •Power sent out by the NFC device

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.

The possible breaches that can occur while transferring data from one NFC device to another are as follows:

Eavesdropping

Eavesdropping is when a criminal "listens in" on an NFC transaction. The criminal does not need to pick up every single signal to gather private information. One way of preventing it is secure channels. When a secure channel is established, the information is encrypted and only an authorized device can decode it.

ii. Data Corruption and Manipulation

Data corruption and manipulation occur when a criminal manipulates the data being sent to a reader or interferes with the data being sent so it is corrupted and useless when it arrives. To prevent this, secure channels should be used for communication.

iii. Interception Attacks

Similar to data manipulation, interception attacks take this type of digital crime one step further. A person acts as a middleman between two NFC devices and receives and alters the information as it passes between them. To prevent it, devices should be in an active-passive pairing. This means one device receives info and the other sends it instead of both devices receiving and passing information.

iv.Theft

No amount of encryption can protect a consumer from a stolen phone. If a smartphone is stolen, the thief could theoretically wave the phone over a card reader at a store to make a purchase. To avoid this, smartphone owners should be cautious about keeping tight security on their phones. Through data encryption and secure channels, NFC technology can help users make payments quickly while keeping their information safe at the safe time [3].

Secure channels are used for sending sensitive information, making them hard to access. In the event that a hacker did crack it past these security measures to steal the information, the information itself is encrypted. Encryptions prove very difficult to crack and the information would likely be useless to the hacker.
http://www.nearfieldcommunication.org/nfc-security-risks.html

When a device is sending data in active mode, eavesdropping can take place up to a distance of about 10m [4].

Cryptographic methods

There are three different basic encryption methods, each with their own advantages

Hashing

Hashing creates a unique, fixed-length signature for a message or data set. Each "hash" is unique to a specific message, so minor changes to that message would be easy to track. Once data is encrypted using hashing, it cannot be obtained back or deciphered. Hashing, not technically an encryption method as such, is still useful for proving data hasn't been tampered with.

ii. Symmetric Methods

Symmetric encryption is also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encodes the data with one key, sends the data (the ciphertext) and then the receiver uses the key to decdoe the data.

iii. Asymmetric Methods

Asymmetric encryption, or public-key cryptography, is different than the previous method because it uses two keys for encryption or decryption. With this method, a public key is openly available to everyone and is used to encrypt messages, and a different, private key is used by the recipient to decrypt messages[5].
In this paper we are going to use combination of asymmetric and symmetric encryption algorithms.

III. AES, RSA AND DEFFIE HELLMAN

The Advanced Encryption Standard (AES) is a cryptographic algorithm that is used to protect electronic data. The AES algorithm is asymmetric block cipher that can encipher and decipher information. Encryption converts data to a coded form called ciphertext, decryption of the ciphertext converts the data into its original form, called plaintext. The AES algorithm has a quality of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. We use cryptographic methods to ensure confidentiality. AES uses keys of 128, 192 or 256 bits, instead 128 bit keys provide sufficient strength today. Blocks of 128bits are used by AES, and is efficient in both software and hardware implementations. The main weakness of DES is it uses a 56 bit encryption key. It also has a structure of Feistel network which divides the block into two halves before starting with the encryption steps. Whereas, AES uses permutation-substitution, which involves a series of substitution and permutation steps which creates the encrypted block.
Public-key cryptography, which is also known as asymmetric cryptography, uses two different but such keys which are mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key is kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the other key from the one used to encrypt a message is used to decrypt it. This is one of the

reason of RSA becoming the most widely used asymmetric algorithm: It defines a method of assuring the confidentiality, integrity, authenticity and non-reputability of e-communications and data storage [6].

One of the architecture includes encrypting the data using combination of AES and RSA. The data can be a text file or an image that is transferred via NFC is selected and encrypted. The encryption process is carried out on the data using public key generated by AES algorithm and the same key is again encrypted using the public key generated by the RSA. The transfer of data takes place between two NFC devices immediately as the phones are tapped with each other. The other NFC device receives the data and stores it in the device folder. The data can be accessed by the application and then decrypted in the reverse process of encryption i.e. it decrypts the key and obtains the AES key and then using that key it decrypts the encrypted data and obtains original data in same format as it was sent by the receiver. Now, if the data received by the receiver device is malicious, the application won't decrypt the data. This can be verified by installing an malicious application in the senders device and sending malicious data to the receiver's end.

The other architecture includes Diffie-Hellman Key Negotiation Algorithm which is a method that lets two parties communicate over an insecure channel (in our case NFC) to agree upon a random number only known to them. Though during execution of the Diffie-Hellman key negotiation algorithm the parties exchange information over the insecure channel, it is computationally infeasible for an attacker to deduce the random number they agree upon by analyzing their network communications.

A prime number p and primitive element g is selected by both the sender and receiver. The sender chooses a secret key 'a' and computes A as A = ga mod p. Similarly receiver chooses a secret key 'b' and computes B as B = gb mod p. Both A and B are exchanged. Both the sender and receiver compute the shared key as
Sender: k = Ba mod p
Receiver k = Ab mod p

IV. COMPARISION BETWEEN RSA AND DEFFIE HELLMAN

RSA and Diffie-Hellman are both based on supposedly perverse problems, mainly the difficulty of factoring large numbers and exponentiation and modular arithmetic respectively, and with key lengths of 1,024 bits, give comparable levels of security. Both have been subjected to examination by mathematicians and cryptographers, but given correct implementation, neither is significantly less secure than the other.

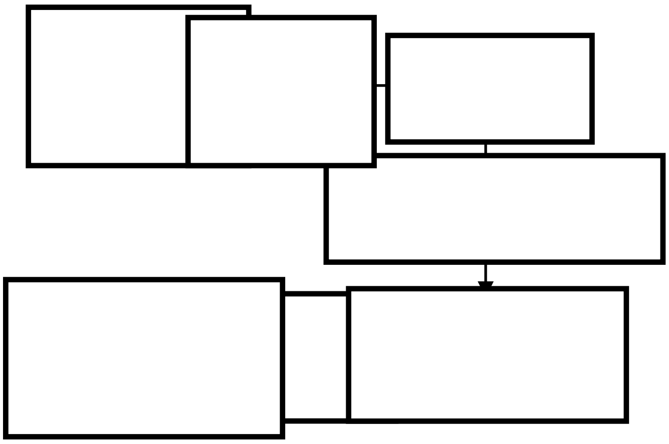

Fig.1. Block Diagram of secured data transfer between two NFC devices

1. The application is installed and launched in an NFC enabled mobile phone.

2. The application provides an interface to choose a file from the existing files in the phone memory which is extracted to the application.

3. The file is then encrypted using AES algorithm.

3.1 Encryption is done using 128bit key for 10 rounds of processing.

3.2 Each round consists of substitute bytes, shiftrows, mix columns, add round key.

3.3 The output fron the previous three steps and four words from the key are XORed.

4. The target mobile phone is tapped for file transfer via NFC.

5. The data file is received by the target device and stored in device folder in encrypted form which can be accessed via the same application.

6. The data file is then decrypted to extract the original information.

6.1 Decryption is carried out using 10 rounds of processing.

6.2 Each round consists of inverse shift rows, inverse substitute bytes, add round key, inverse mix columns except the last round which doesnot include mix column stepand inverse mix column step respectively.

7. The original information is then read by the receiver.

For every NFC transaction the NFC tag is assigned a unique id number. This unique id number can be used as the key for encrypting the message intended to be sent as it is absolutely random and changes continuously. The sender can extract the receiver's tag id during the tap after which the message can be encrypted using the tag id of the receiver’s device at that instant and send to the receiver who can use the tag id of his own device to decrypt and read the message. Hence this method ensures security as the tag id is unique at the instant when a transaction takes place and changes continuously, preventing possible attacks which might arise due to the use of a public key.

V. ANALYSIS

Both the system aim at securing the data which is transferred via NFC so that the data received at the receiver end is in its original format and can be achieved successfully by encryption and decryption process via an application. The transfer of the data selected in one NFC device which is encrypted is successfully received by the other NFC device in encrypted form. We can verify it by introducing another malicious application in the same device. Data is transferred using that malicious application and the receiver device does not decrypt the data and is able to detect the vulnerability of the data.

On an average NFC transfers data at the speed of 141.33Kbits/s. For time complexity, when NFC transfers data via the proposed application it will take little more time due to encryption and decryption process. In general it takes O (m) complexity, where m is the message size, as there are O(m) blocks of data to encrypt. In term of space complexity, suppose a plain text of size 240KB is selected then after encryption it gets converted to text of size 847KB. Even though there is an increase in overall complexity, it fulfills the need for security of data transfer through NFC.

VI. CONCLUSION

To put the innovative and growing NFC technology to its best use, it is essential to ensure security in its transactions even though there is an increase in complexity especially because it involves important data, files and images. Our proposed solution attempts to secure the data/files/images during transfer through NFC technology. Since NFC being a new technology, to the best of our knowledge there are not many attempts to resolve the security issues concerned with it, our idea is a primitive scheme to make NFC transfer a secure one. As a future plan we would be further analyzing the scheme to evaluate its effectiveness in mitigating other forms of attacks and reduced complexity of computations that would make it much more efficient.

REFERENCES

[1] http://www.oracle.com/technetwork/articles/javame/nfc-140183.html
[2] http://www.nearfieldcommunication.org/using-nfc.html
[3] http://www.nearfieldcommunication.org/nfc-security.html
[4] http://www.nearfieldcommunication.org/nfc-security-risks.html
[5] http://www.smartcardalliance.org/resources/webinars/NFC_Tags_Webinar_FINAL_041813.pdf
[6] http://datashieldcorp.com/2013/06/04/3-different-data-encryption-methods/
[7] http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/
[8] http://simple.wikipedia.org/wiki/RSA_(algorithm)
[9] http://www.ijstr.org/final-print/june2014/Vulnerability-Analysis-And-Security-System-For-Nfc-enabled-Mobile-Phones.pdf
[10] http://newscience.ul.com/wp-content/uploads/sites/30/2014/04/New_Science_TS_Case-Study_NFC_Implementation_Model.pdf
[11] https://globaljournals.org/GJCST_Volume13/4-A-Study-of-Encryption-Algorithms.pdf
[12] http://lifehacker.com/5943006/what-is-nfc-and-how-can-i-use-it