# Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones

S.Kavya, K.Pavithra, Sujitha Rajaram, M.Vahini, N Harini

**Abstract:** An encryption system for NFC enabled applications using a combination of AES cryptography algorithm and Diffie-Hellman key negotiation scheme which when implemented prevents data modification, man in the middle attack and eavesdropping has been proposed in the paper. A timestamp based Protocol where the size of the file and time at which it is sent is retrieved to calculate the estimated time of reception which will be compared with actual reception time is also proposed to prevent relay attacks. A complete study of authentication methodologies in NFC technology and a critical analysis of our proposed system with the existing systems showing how it can resist all the possible attacks on the data exchanged between mobile phones through NFC technology.

**Index Terms:** Authentication, Decryption, Encryption, NFC tag, Security, NFC technology

## 1 INTRODUCTION

In today’s era of technical advancements people prefer mobile devices as they provide unprecedented level of convenience, flexibility and portability. One of the main features of smart phones is the easy transfer of data and communication between various electronic devices. Of all the technologies developed for wireless communication one of the most recent and innovative technologies is NFC (Near Field Communication). NFC [2] is a set of standards for smart phones and similar devices to establish Radio Communication with each other by touching them together or bringing them into close proximity. Communication between NFC enabled devices is based on inductive coupling where loosely coupled inductive circuits share power and data over a distance of few centimeters, incorporating RFID Technology.

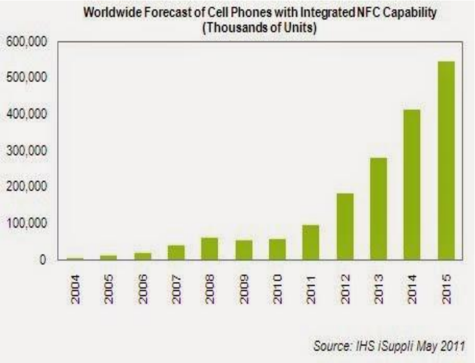


**Fig 1:** Increase in use of NFC enabled mobile phones

NFC based transactions, file sharing and data transfer are the primary applications built on the basis of this technology. Though many applications have proved to be effective considering speed and consistency of the transfer, the most potential application for wide use would be payment using mobile phones at NFC enabled payment portals as it would make the process simple and elegant. NFC enabled payment systems are not widely used all over the world, the infrastructure required to accept NFC-enabled payments are present in MasterCard’s PayPass network and Visa payWave. These modes of payment are beginning to be perceived as a technology with a huge scope in the near future.

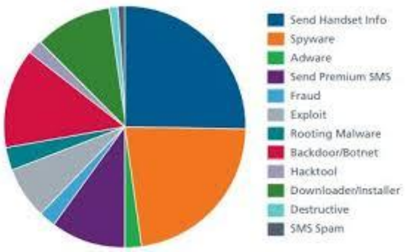


**Fig 2:** Security concerns in mobile phones

NFC provides no reliable security against privacy protection or protection against a device being vulnerable to inadvertent reception of malicious software or data [Fig 2]. The NFC protocol has very few safeguards against data sniffing and data modification. And since one of the most popular applications implementing this technology is ‘Contactless Payment System’[4], security is a very important concern. Since any sort authentication is not involved before an NFC, transfer of malware applications could also be a major threat to the user. Hence a secure NFC Application to implement the possible features of an NFC enabled application not only efficiently but also securely is more than necessary to make the fullest use of this technology.

## 2 RELATED WORK

### 2.1 Tag Authentication

NFC enabled mobile phones contain NFC tags which are useful in retrieving information from other NFC enabled mobile phones. The integrity of the data stored in these tags is maintained using digital signatures. However there is no guarantee on the authenticity of these tags. These tags can be replaced with illegitimate tags by the attacker leading to security breaches. There are various mechanisms to verify and authenticate these NFC tags.

**Off –line authentication:**
When there is no shared secret between the tag and the reader, any reader can access the tag and read its contents. The process of authenticating NFC tag or the reader or both is called off-line authentication. But in general only the authentication of the tag is necessary. NFC tags can be used for identifying products. The information stored in the NFC tag

is product specific and can be useful to an off-line user to know about the specification and legitimacy of the product. The data on the tag is protected by the signature record and a valid signature is an indication of an authentic product [5]. The disadvantage in this type of authentication is the low computation power of RFID tags leading to difficulty in authentication process.

**On-line authentication:**

In this case some information is to be shared between a tag and reader. The reader will have access to a server containing the information. The reader gains access to the database to obtain the tag's information and then check whether the tag knows the information. Since the attacker doesn't know about the information, a duplicate tag can be easily identified as it will not contain the secret information [5]

### 2.2 Cryptographic Methods

Although NFC communication range is restricted to few centimetres, but still NFC does not ensure secure communication. To ensure confidentiality, we use cryptographic methods. AES is the successor of DES as standard symmetric encryption algorithm for US federal organizations. AES uses keys of 128, 192 or 256 bits, although, 128 bit keys provide sufficient strength today. It uses 128 bit blocks, and is efficient in both software and hardware implementations. The inherent weakness on DES is it uses very short 56 bit encryption key. It also has a structure of Feistel network which divides the block into two halves before going through the encryption steps. AES on the other hand, uses permutation-substitution, which involves a series of substitution and permutation steps to create the encrypted block. For Key Management scheme we use Diffie-Hellman key negotiation algorithm .This is a method that lets two parties communicating over an insecure channel to agree upon a random number known only to them. Though the parties exchange information over the insecure channel during execution of the Diffie-Hellman key negotiation algorithm, it is computationally infeasible for an attacker to deduce the random number they agree upon by analysing their network communications. For every NFC transaction the NFC tag is assigned a unique id number which will be used as the key for encrypting the message sent by the sender by extracting the receiver's tag during the tap, the receiver can hence use the unique id number assigned to his tag to decrypt the message and this method ensures security as the tag id changes every time a transaction takes place.

### 2.3 Summary of Findings

**Security concerns:**

#### 2.3.1 Eavesdropping:

The RF signal for the wireless data transfer can be picked up by an antenna. The attacker need not pick up every signal to gather private information, and can typically eavesdrop within 10 metre and 1 metre for active and passive devices respectively. With the use of a patch loop antenna it is possible to place a receiver close to the target and disguise it. This Security concern can be resolved using the proposed technique.

#### 2.3.2 Data Modification:

Data transferred across NFC-enabled devices can be captured and modified by an attacker's radio frequency device, which will be able to inhibit the NFC data exchange briefly but long enough to alter the binary coding. The most common method to interfere with an NFC data exchange is to use a RFID jammer. This Security concern can be resolved using the proposed technique.

#### 2.3.3 Data Corruption:

This type of attack is a 'Denial of Service' attack in which an attacker interferes with data transmission, disturbing or blocking data such that the receiver is not able to decipher the data. The attacker transmits radio signals to reduce the signals to random noises destroying the information content. This Security concern can be resolved using the proposed technique.

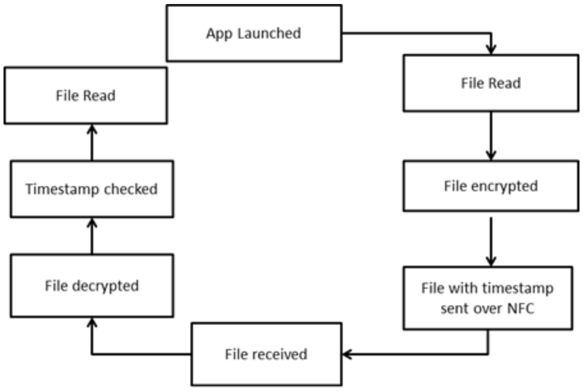
#### 2.3.4 Man in the Middle Attack:

Despite the fact that NFC standard requires proximity of devices during data transfer it is still susceptible to MITM attacks. An attacker can intercept information, manipulate it and relay it to the receiving device. This Security concern can be resolved using the proposed technique.

#### 2.3.5 Relay Attack:

The attacker forwards the request of the reader to the victim and relays back its answer to the reader in real time in order to carry out task pretending to be the sender. This attack focuses on the extension of the range between NFC token and the reader, two NFC devices on acting as a reader and other as a card emulator will be required. The victim can't detect this as it will appear like a card in front of it. The attacker holds the NFC reader near the victim's card and relays the data over another communication channel to a second NFC reader placed in proximity to the original reader that will emulate the victim's card. This Security concern can be resolved using the proposed technique.

## 3 ARCHITECTURE OF THE PROPOSED APPLICATION



**Steps:**

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 encrypted using AES algorithm.

**3.1** Encryption is done using 10 rounds of processing of 128 bit key.
**3.2** Each round consists of substitute bytes, shift rows, mix columns, add round key.
**3.3** The output of the previous three steps is XORed with four words from the key.

4. The target mobile phone is tapped for file transfer via NFC.
5. The timestamp of the start of the transfer is sent along with the file.
6. The file is received by the target device which can be accessed via the same application.
7. The file is then decrypted to extract the original information.
   **6.1** Decryption is done using 10 rounds of processing.
   **6.2** Each round consists of inverse shift rows, inverse substitute bytes, add round key, inverse mix columns. The last round for encryption does not involve the mix columns step. The last round for decryption does not involve the inverse mix columns step.
8. The size of the file is calculated by the application.
9. An estimated time of receiving the file is calculated using the file size.
10. The estimated time is verified with the calculated time.
11. The original information is then read by the receiver.

## 4 DIFFIE-HELLMAN KEY NEGOTIATION ALGORITHM

Diffie-Hellman Key Negotiation Algorithm is a method that lets two parties communicating over an insecure channel (such as NFC) to agree upon a random number known only to them. Though the parties exchange information over the insecure channel during execution of the Diffie-Hellman key negotiation algorithm, it is computationally infeasible for an attacker to deduce the random number they agree upon by analyzing their network communications. Oracle Advanced Security uses the Diffie-Hellman key negotiation algorithm to generate session keys.

**Steps [6] involved are:**

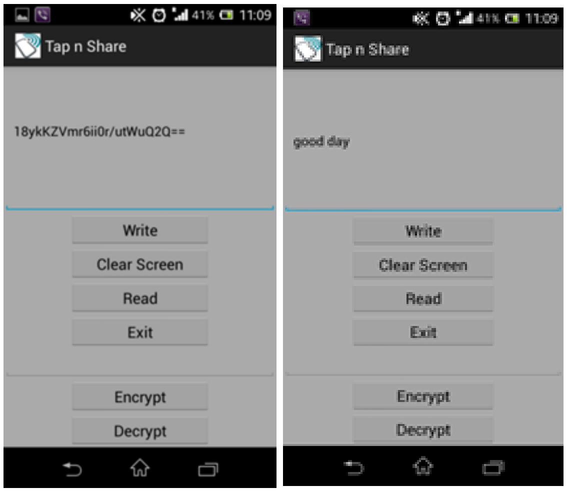
**4.1** A prime number p and primitive element g is selected by both the sender and receiver.
**4.2** The sender chooses a secret 'a' and computes A as $A = g^a \bmod p$ .
**4.3** Similarly receiver chooses a secret 'b' and computes B as $B = g^b \bmod p$.
**4.4** Both A and B are exchanged.
**4.5** Both the sender and receiver compute the shared key as

Sender: $k = B^a \bmod p$
Receiver $k = A^b \bmod p$
Proposed method for secure Key Management for Transfer via NFC for the proposed Application Architecture:

NFC enabled devices have a hardware chip that is called the NFC Tag. 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. The following lines of code represent the java code for using the tag id in the programming of the application:

```
Tag myTag = (Tag)
intent.getParcelableExtra(NfcAdapter.EXTRA_TAG);
Log.i("tag ID", myTag.getId().toString());
```

Example:
This gives an ID "[B@40521c40"
And the ID changes every time it is read.



18ykKZVmr6ii0r/utWuQ2Q==

good day

**Fig 3:** sample screenshots of the android application after encryption and decryption

## 5 Critical Analysis

On an average NFC transfers data at the speed of 141.33 Kbits/s. In terms of 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, a plain text of size 240KB after encryption 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.

### 5.1 Eavesdropping:

The RF signal for the wireless data transfer can be picked up by an antenna and can typically eavesdrop within 10 metre and 1 metre for active and passive devices respectively. NFC requires very close proximity of the devices. A secure channel is established using a strong encryption system in our proposed application architecture. Even if the attacker is able to get the encrypted message, it will be impossible for him to decrypt the same as the key is the tag which is random and continuously changing.

### 5.2 Data Modification:

The most common method to interfere with an NFC data exchange and modify the data is to use a RFID jammer. So the data to be sent is encrypted using the AES algorithm and the key that is used is the NDEF tag ID [1] .The NDEF tag ID changes for every exchange of data so extracting the key is also not possible which ensures that the data cannot be modified.

### 5.3 Relay Attack:

Relay attack is an attack in which the attacker relays the data to be sent to the valid receiver. So the timestamp that is generated along with the data that is encrypted can be used to prevent relay attack .The proposed application will calculate the length of the data that is sent and it will check it along with the timestamp to make sure that it has not taken significantly more time to get transferred than the estimated time.

### 5.4 Man in the Middle Attack:

Man in the middle attack is the one in which the attacker creates connection with the victims and relays the messages between them making them believe that they are communicating with each other, when in fact their communication will be completely controlled by the attacker. Man in the middle attack can be corrected using the Encryption mechanisms which can be used for secure communication so that intercepted information can't be decrypted by the attacker.

**Table 1**
Analysis of the proposed solution

| Type of attack | Proposed Solution |
|---|---|
| Data Modification | √ |
| Data Corruption | X |
| Eavesdropping | √ |
| Man in the middle attack | √ |
| Relay attack | √ |
| Spoofing | X |

Notations used in the table :
√ - Secure and X – Insecure

## 6 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 payment related applications. Our proposed solution attempts to resolve the critical attacks possible during data transfer through NFC technology. Since it is 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 more efficient.

## REFERENCES

[1]. CollinMulliner ,Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones , Fraunhofer Institute for Secure Information Technology

[2]. http://www.nfc-forum.org/aboutnfc/nfc

[3]. http://www.maintag.fr/chiers/pdf-fr/nfcforum-ts-ndef-1-0.pdf, June 25, 2012

[4]. David M. Monteiro1, Joel J. P. C. Rodrigues, and Jaime Lloret ,A Secure NFC Application for Credit Transfer Among Mobile Phones Instituto de Telecomunicações, University of Beira Interior, Portugal

[5]. Muhammad Qasim Saeed, Colin D.Walter, Offline NFC Tag Authentication

[6]. http://www.thegeekstuff.com/2013/01/diffie-hellman-key-exchange-algorithm/