NEAR FIELD COMMUNICATION, IT'S VULNERABILITY AND COUNTER MEASURES

[1]Suhas Rahul, [2]Sangeetha, [3] Mercy Flora Pratheba

[1] Dept. of Computer Sciences and Engeineering, Dr. T. Thimmaiah Institute Of Technolgy (VTU), KGF, Karnataka, India
[2,3] Assistant Professor, Dept.of Computer Science and Engeineering, Dr. T. Thimmaiah Institute Of Technolgy (VTU), KGF, Karnataka, India

---

ABSTRACT

. A NFC-enabled mobile phone operates in a similar manner to traditional contactless cards, which are widely used in credit cards, public transit tickets, and other forms of electronic commerce. In this research, we examined various attacks in the context of NFC, as well as the fundamental principles of hacking. We conducted experimental analyses to uncover various aspects of NFC attacks. Additionally, our study identified a counter measure security approach to overcome attacks, which could enable users to protect secure systems through NFC-Near Field Communication technology is a rapid instantaneous communication between two devices. It is a short-range high-frequency wireless communication technology that allows data exchange between devices through a distance of around 10 cms (almost 4 inches).

The uptake of Near Field Communication (NFC) technology is rapidly increasing their phone's user interfaces.

Keywords: NFC, Wireless short range communication, NFC attacks, NFC security

1. INTRODUCTION

The Near Field Communication Forum was founded in 2004 by Nokia, Philips, and Sony. Radio frequency identification Devices (RFID), that's where NFC originated. A passive electronic tag can be identified and tracked using RFID by allowing a reader to transmit radio waves to it. Mobile phone use utilising NFC is primarily intended. The enhanced protection offered by the NFC phone allows the user to safeguard secure systems through the phone's user interface features of 13.56 MHz. It supports data speeds of 106 or 424 Kbit/s. NFC utilizes magnetic field induction each other, communicate besides forming an air-core transformer out of two loop antennas that are connected directly. For a device to work using NFC, a chip is installed into a mobile phone. If the application involves payments, the chip is linked to a credit or debit card account so that money can be charged to the user's account. To make a payment using the NFC enabled mobile, the user swipes the mobile over a contactless pay point, from a distance not exceeding 10 cms **[1][2]**

1.1 UNIQUE FEATURES:

Support for passive communication is a core part of NFC devices. Mobile phones and other rechargeable batteries devices can use it. The Passive mode of NFC communication allows the communication to be powered from one side only in a power-saving mode since it does not require both devices to generate the Radio Frequency field **[3]** To choose devices and automate connection setup, the protocol is straight forward to use in conjunction with other protocols connections with a longer range. Selecting the right device from among several the devices in the range and establishing the appropriate connection parameters are difficult while using long-range protocols like Bluetooth or Wireless Ethernet .

1.2 ADVANTAGES OF WIRELESS SHORT RANGE COMMUNICATION

NFC is favourable to Bluetooth and 802.11 due to their long-distance capabilities and since it allows for relatively easy wireless network configuration. NFC is designed for short-distance wireless communication **(Fig.1)** NFC provides a communication channel-related for non-self-powered devices and can be utilised in unsafe circumstances and does not require line of sight **[4]**

Fig:1.Wireless short range communication

1.3 NFC STANDARDS

NFC operates at a high frequency band of 13.56 HMZ, received ISO/IEC 18092 (NFC IP-1) accreditation in December 2003. The interface and protocol for basic wireless communications between closely-coupled devices that transfer data at speeds of 106, 212, and 424 kbps are specified by this standard. In 2005, NFC also acquired the additional ISO/IEC 21481 accreditation. NFC is a certified International standard, consequently it is bound to become an extensively utilised technology that is accepted **[5]**

1.4 OPERATING MODES OF NFC

The devices work in two modes: Active and Passive mode. This works on the concept of a message and reply. The Active or Initiator device sends a message to the Passive, or Target device. The Target device then responds, but can only do so once it has received the message from the Initiator. The code that is transmitted between the two devices uses Manchester coding. It is possible for the Active device to take on both active and passive roles, but the Passive device is always the Target. The initiator will send a message to the target and then wait for a response **[6].** NFC Devices are capable of three different operating modes **:**

I.Peer-to-Peer mode (NFC):

This NFC mode allows for data transmission rates of up to 424 Kbit/sec.Electromagnetic characteristics and the NFCIP-1 protocol are specified in ISO 18092 and ECMA 320/3409 **(Fig: 2)**

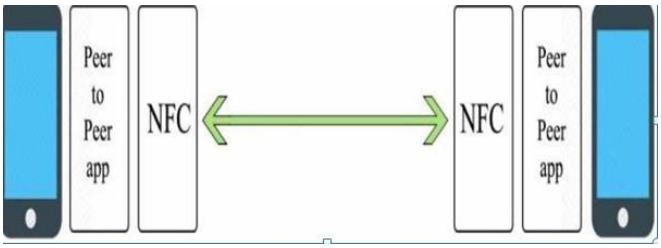

Fig: 2. Peer to Peer Mode NFC

II.Reader/writer mode (PCD): Tags and smart cards can potentially read and written through NFC devices**.** In this case, the passive tag is the target and the NFC device serves as the initiator **(Fig.3**)

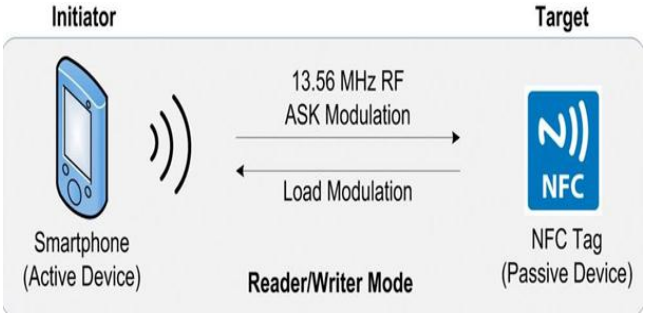

Fig:3.Reader/Writter Mode

III. Tag Emulsion Mode: Here antenna of the NFC module is attached to a smart card chip integrated within mobile devices or an ISO 14443 smart card that the NFC device emulates (fig 4)

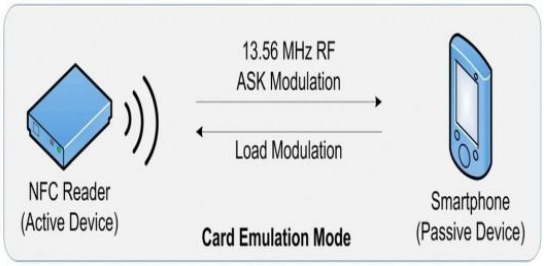

Fig.4. Tag Emulsion Mode

1.5. NFC Applications

The applications of NFC are under 4 categories: i) Touch and go ii) Touch and Confirm, iii) Touch and Connect and iv) Touch and explore **[2] i)Touch and go application** : Users need to tap or bring the NFC devices close to the NFC reader so as to use the application's touch-and-go feature. The use of public transit ticketing is an example of an NFC touch-and-scan application, where NFC users scan and touch their NFC devices to access the transportation system**. ii)Touch and Confirm application:** This requires user's password confirmation or approval of the payment transaction for verifying the interaction to the system. **iii)Touch and connect application** : Enables connection between two NFC devices which render peer-to-peer exchange of data such as image sharing between two NFC-enabled smartphones. **iv) Touch and explore application:** Allows user to find and explore applications and devices capabilities. For examples : NFC enables users to browse to a website for more information about a product or service of interest and allows for the transmission of a URL to the target device. Consumers may utilise smartphones with NFC capabilities to compare prices before making purchases, which is quite handy. Additionally, they can be used to exchange tokens at airports, doing away with the need for boarding cards. At the departure gate, the traveller would swipe their

phone once again to confirm their check-in using their mobile device. Furthermore, they might be able to store biometric data, which is being developed more and more for airport security. For displaying photographs very fast, NFC devices can be used in conjunction with image display devices like digital photo frames. Just clicking on the picture frame with the image ready to send creates the connection and sends the picture over Bluetooth. Since NFC and RFID are backward compatible, using an NFC-enabled device as an RFID key is entirely feasible **[7][8]**

1.6 . Risks and attacks on NFC- Sites

Risk in NFC targets 4 basic sites that constitute NFC technology components, these sites are: **i)Hardware**: Includes all physical components, equipments, and tools that composed NFC chip, etc.ii)**Software**: Applications or instructions arranged in a specific format for carrying out an NFC task, they are either stored the information or autonomous information within the NFC systems.iii) **Data**: It is considered as the main target for systems crimes.Input or output, stored or transmitted throughout networked system. Iv) **Communication**: Wireless communication has been employed to link the technological gadgets together. The overwhelming majority of dangers include attacking the system and overcoming it by using the vulnerabilities of communication to their advantage. If any one of the components are damaged, the entire system could be impacted. Therefore, consumers should take into account all of those factors and identify that attackers might target any of them [**9]**

1.7. Types of Attacks on NFC

Modern times have seen a boom in the use of NFC enabled technologies. The attacks may be executed without physical access for the reason to the growing popularity of these technologies and the nature of wireless communication, involving no physical touch between the hardware units. The technology has become more customised, and there are several ways for attackers to mask their attacks. based on the security standards they violated**.** The attacks encountered by NFC systems are summarized as follows: (i) Attacks that affect Integrity, (ii) Attacks that effect confidentiality, (iii) Attacks that affect availability**[8][9]**

(i)Attacks those effects on Integrity:**(a)**

Data Manipulation: In this type of attack,

the attacker changes and manipulates the data. The main methods of this attack involve interrupting and changing the NFC device's service provider. This attack affects the integrity of NFC data and takes place through a wireless medium. **(b**) Data insertion - During communication of data between NFC devices, any unwanted information may be inserted into the messages by an attacker. Before the authorised device is ready to start communicating, the attacker reacts to the device. The received data would simultaneously be spoofed with damaged data being sent. **(c**) **Deception**: NFC devices can be tricked by providing false information. Integrity is impacted by this kind of attack**. (d) Man in the Middle**: An attacker might intercept the data, alter it, and transmit it to the receiving device**[10][9]**

ii)Attacks that effect confidentiality:

(a)Eavesdropping: Since NFC functions by means of wireless transmission, it is quite simple to eavesdrop on conversation. Peer-to-peer and card emulation NFC operating types are vulnerable to eavesdropping. Peer-to-peer communication is susceptible to eavesdropping since information is sent in an unencrypted manner. If the NFC device's function is inactive, attackers may be able to access the information content while it is in card emulation mode. **(b) Rely attack**: This attack takes advantage of NFC's compliance with the protocol. The attacker attempts to get the victim's card details while masquerading as the card's owner. The victim's access system may not be able disclose the attacker's identity since it will believe a card is in front of it**.(c) High distance read:** The NFC device has been impacted by this attack. It boosts the High Frequency (HF) field's range, letting an attacker to read tags from a secure distance. This type of attack threatens the system's secrecy.

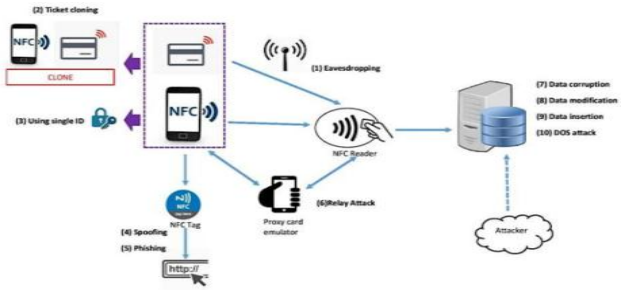

Fig:5. Types of NFC Security Attacks

(iii) Attacks that affect availability

(a)Denial of Service/Data corruption Attack: A Denial of Service (**DOS**) attack hits the memory or server resources of a network. The licenced user is in this particular instance restricted from information or services. The attack's most evident patterns involve hacking into the system gaining it control, then endeavour to steal valuable information like credit card details**.(b) Destroy Attack** - Destroy attack is the simplest attack that could happen to the NFC tag. After this attack, the tag is not able to communicate any longer with an NFC device. It destroyed by cutting the

connection to its antenna or destroying the electrical circuits of the tag. This type of attack will affect the availability of the system. **(c)Removed attack - A removed** attack is happening to NFC tag where the tag is removed from the carrier object. This kind of attack will affect the availability of an NFC system.**(d) Jamming attack** - Jamming the NFC system by sending a disorder signal and must be near to the system or it can use antennas and power rates.[**8]** This attack happens over the Wireless Medium. and it causes system unavailable. (**Fig.5**)

2. METHODOLOGYAND ANALYSIS

Impact estimation and Likelihood estimation calculated using Common Vulnerability Scoring System (CVSS)Version 3.0 Calculator.

Impact estimation is calculated using base metrics group and environmental metrics group of CVSS. Likelihood estimation is calculated using base metrics group and temporal metrics group of CVSS. The result derived from survey data from each case study for each security risk. Ten case studies are designed for each security risks that identified in the research. S**urvey** data were organized and assigned to discrete probability distributions. Individual outcome probabilities for Low, Medium, and High rating groups CVSS. Probability calculated by equation :

$(x)=\sum ngroup/N$

P(x)=probality distribution. N= No. of participants. - An open source JAVA program was implemented for SMAA-TRI method.

3. RESULT

By Accessing the CVSS method to find the state of vulnerability for different cyber attacks on NFC technology. We can observer that for Data Corruption and DOS attack are in high risk category, others fall into medium category of NFC. Since risk is a function of probability times impact, risk level is determined by probability and impact estimates. There are two case studies that show higher risk as a result of the risk assessment process-Data corruption and DOS have high risk attack.

4. DISCUSSION

NFC COUNTER MEASURE SECURITY

Data can be encrypted, with the key being stored securely in the memory of the device and the NFC device supports the authentication. In order to offer secure data storage, Secure NFC incorporates smart-card technology with NFC technology. In a nutshell, information may be encrypted, and as the NFC device permits authentication, the key can be securely stored in the device's memory. This secure storage is of the utmost importance to the NFC-enabled technology since it will be used to store private information, encryption keys, electronic money, etc**.** With enhanced NFC, a transaction can still be accomplished even if the phone is off or the battery is low, which is critical for circumstances like ticket purchases.

4.1. Counter measure security on NFC

The most and simple countermeasure to combat the NFC attacks is by turning ON/OFF the NFC functionality, when not in use. This simple technique helps to combat most of the NFC based attacks such as Phishing, Spoofing, Relay attacks easily with using complicated algorithms and expensive hardware to protect the NFC hosted device and NFC services**[10]**

4.2. Counter measure for Data Corruption attack & Denial of Service attack

Data corruption involves manipulation of data by attackers interfering with NFC communications or transmission through NFC interfaces and devices. The data is corrupted and cannot be read by other NFC devices. NFC devices can probe and observe radio frequency fields during data transmission, thus preventing data corruption. This attack can be detected by NFC devices that detect all transmitted data that consumes significantly more power during data transmission. DOS attack occurs when the NFC device distressed an empty or damaged NFC tag, and an error information employed the NFC device until exposed. It can also occur through malicious applications on NFC-enabled smartphones. Precautionary measures to minimize the risk of data corruption and DOS attacks include signing tags with appropriate cryptographic techniques, using cryptographic tag authentication protocols, and establishing secure channels between NFC devices. Securing the NFC channel is the best way to secure NFC communications and defend against all kinds of attacks on data in transit[10]. MCDM Analysis using AHP Approach**:** AHP method is used to select the highest priority of NFC risk countermeasures. AHP is use to develop priorities for alternatives and the criteria is used to judge the decision alternatives**.[11]**

4.3 Other counter measures on attacks

(i) Integrity counter measures: **Data Modification:** To protect from data modification the NFC devices should check the RF field while sending data. **Data Insertion:** To protect from data insertion there is more than one way. **(a)**Answering device answers without delay**.(b)**via answering device to channel throughout the time**.(c)** Applying algorithm such as RSA, SHA, 3DES insecure

channel. **Man-in-the Middle:** To protect from the man-in-the middle is the encryption of data using a shared secret and Assuming attack by time delay.

(ii) Confidentiality counter measure: **Relay attack**: To protect from Relay attack it can be different way countermeasures**.(a)**By using a container that made of mineral it is impossible to impenetrable via radio signals. This way is called "Faraday Cage" **(b)**By using the distance bounding protocol to adds an extra security limit to the system .**Eavesdropping Attack:** To protect from eavesdrop is to establish a secure channel.

(iii) Availability countermeasure: **Denial-of-Service:** To protect from this attack, it should be several kinds of techniques that controlled by a consumer to switch ON and OFF reader/writer function of the NFC. **Jamming**: To protect from jamming is by increasing the signal power of the device to be over the power of the attackers. **Destroy and remove**: To protect from this attack by encrypted or incorporate a form of data validation controls**[10][11]**

5. CONCLUSION

NFC has become an integral part of our day-to-day lives. It provided a simple way to make data available and transmit information by embedding NFC tags in most technology that was used, readable with NFC-enabled mobile devices. Waving your card or phone at the checkout makes paying more convenient. However, there are risks associated with most data transfers that are unencrypted, unsecured hardware, unsecured software or communication. Communications in the centimeters range may appear more secure. However, technologies like these are highly vulnerable to security attacks because they require minimal to no authentication. The attacks on NFC can be solved using the mentioned approaches

REFERENCES

[1] Vedat Coskun, Busra Ozdenizci, Kerem," A Survey on Near Field Communication (NFC) Technology" Wireless Personal Communications Volume 71, Issue 3 pp 2259-94.

[2] Doaa Abdel-Gaber and Abdel-Aleem Ali, "Near-Field Communication Technology and Its Impact in Smart University and Digital Library: Comprehensive Study," Journal of Library and Information Sciences, 3, no. 2 (December 2015): 43-77

[3] Ed, "Near Field Communication vs Radio Frequency Identification," accessed March 10, 2019.

[4] Apuroop Kalapala, "Analysis of Near Field Communication (NFC) and other Short Range Mobile Communication Technologies" (Project Report, Indian Institute of Technology, Roorkee, 2013), accessed March 19, 2019

[5] C. Ruth, "NFC Forum Calls for Breakthrough Solutions for Annual Competition," accessed March 21, 2019

[6] Ekta Desai and Mary Grace Shajan, "A Review on the Operating Modes of Near Field Communication" In proceedings of International Journal of Engineering and Advanced Technology (IJEAT), December 2012.

[7] Shyamal Pampattiwar," Literature Survey on NFC, Applications and Controller", International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012.

[8] Esko Strommer, Juha Parkka, Arto, Ilkka Korhonen ,Ylisaukooja, " Near Field Communication for Health Monitoring in Daily Life" 28th IEEE EMBS ANNULA International Conference , Febuary 2006.

[9] Hutter, M., Mangard, S., Feldhofer, M.: Power and EM Attacks on Passive 13.56 MHz RFID Devices. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 320–333. Springer, Heidelberg 2007.

[10] Ernst Haselsteiner and Klemens Breitfuß, "Security in Near Field Communication (NFC) Strengths and Weaknesses"

[11] NFC Security Available: http://www.radioelectronics.com/info/wir wireless/nfc/nfc-near-fieldcommunications-security.php