International Journal of Engineering & Technology, 7 (4.31) (2018) 298-305

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures

Manmeet Mahinderjit Singh*[1], Ku Aina Afiqah Ku Adzman[2], Rohail Hassan[3]

[1] School of Computer Sciences, Universiti Sains Malaysia, Penang, Malaysia
[2]University Teknologi Petronas, Perak, Malaysia
**Corresponding author E-mail: manmeet@usm.my*

Abstract

Nowadays; the adoption of Internet of things (IoT) technologies and applications in everyday is rising. IoT technology such as Near Field Communication (NFC) is vastly adopted due to its short range frequencies, making it a good candidate for token based security access control applications such as door systems and attendance systems. However, due to the miniature size of NFC tags; its clear text contents and unprotected communication channel between tag-reader-database; NFC technology is prone to security attacks such as the man in the middle; denial of services (DOS) and etc. These attacks lead to leakage of user critical data which could impact any organization adopting NFC applications and technologies. In this paper; NFC vulnerability, causing both security and privacy attacks studies in depth. By focusing on attacks such as DOS and data corruptions; existing risk assessment models are evaluated using Analytical Hierarchy Process (AHP) approach. Best practice in mitigating these attacks is presented as well. A case study on an existing NFC access control application is then used to demonstrate the effectiveness of best practice solutions proposed.

Keywords: *Analytical Hierarchy Process (AHP); Attendance System; Near Field Communication (NFC); NFC Security Taxonomy; Risk Assessment; Security*

1. Introduction

Near Field Communication (NFC) is a wireless communication technology extension of Radio Frequency Identification (RFID) technology that operates in short range communication[1, 2]. RFID mainly used for tracking and identification by transmitting the radio waves. NFC operates on low-range 13.56 MHz frequency within distance from 4cm to 10cm and has a maximum data rate of 424 kilobits per second (kbps) [2-4].

NFC applications can be categorized such as touch and go, touch and confirm, touch and connect, and touch and explore. The usage of NFC in real life applications does not really ensure a secure application. Thus, NFC technology has its own challenges to face such as RFID security threats are applicable to NFC because NFC is a counterpart of RFID and all NFC devices act as readers or writers which could create various threats.

Another factor leading to security vulnerability in NFC is due to lack of an NFC specification which covers all the countermeasures for x.800 security services such as authentication and access control. Current specification is only to provide guideline for NFC developers of applications to secure data and communications within NFC devices. Next the privacy issues raised when using NFC such personal information of users that stored in NFC devices could be leaked to malicious attacks. For instance, user using NFC as a digital wallet to store their bank account information are prone to data privacy attack when information on wallet are captured by attacker without any knowledge of user at anytime and anywhere [5]. As NFC technology faces challenges, security concerns are rising for a secure environment.

There are many NFC applications are developed with a contactless payment application that works in 2 ways which are in touch and confirm, and touch and go application. The examples of contactless payment application are Google Wallet [6] and Visa Paywave [7]. Google Wallet is an NFC touch and confirm application that require PIN code confirmation to perform the transaction [6, 8]. While, Visa Paywave is a type of NFC touch and go application that enables Visa cardholders to simply wave their card or NFC-enabled smartphone at a contactless payment terminal to make a payment without making any confirmation of the payment. Previous research has identified the vulnerability of the contactless payment in Visa contactless card that the card does not recognize foreign currency outside United Kingdom and lead to fraudster in the contactless transaction [9]. Thus, security becomes a concern in contactless payment of NFC particularly in touch and go application that perform tasks without any confirmation during the transaction.

Thus the aim of this paper is to identify security risks occurring in touch and go application particularly. The objectives identified in this research are: (1) to identify related security vulnerability for NFC-enabled smartphone in covering NFC security challenges in depth; (2) to evaluate and test the vulnerability risk assessment occurring in NFC touch and go application by using risk modeling tools and gaining insight and awareness of experts; (3) to propose a secure NFC-enabled smartphone architecture of touch and go applications based on risk modeling outcome and NFC attacks solutions guidelines. The main significant of this research is the ranking of various security attacks by using CVSS framework and AHP model and to provide guideline in tackling attacks which have the highest risk level. The rest of the paper is organized as follows. In Section 2, a taxonomy of NFC technology is presented. Next, a risk assessment and MCDM methods are described. In section 4, the research methodology to conduct the research is described. In 5 and 6 section, the results of risk assessment analysis and MCDM analysis are presented. Finally, in section 7 the conclusion and future work of this research is presented.

2. Background

In this section, an NFC taxonomy is presented. The taxonomy is designed by covering few main factors such a NFC vs RFID, different types of operation modes and application, ISO standards and security attacks. Next, the taxonomy will be presented by describing each factor in depth.

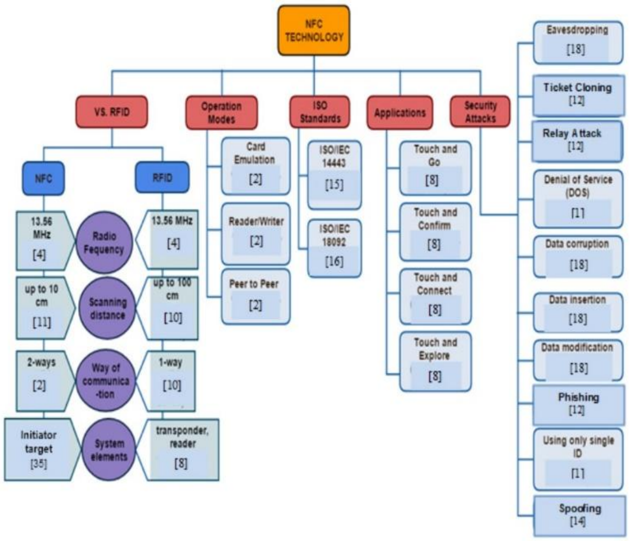

Fig. 1: NFC Technology Taxonomy

2.1 NFC and RFID

NFC is closely related to RFID as it an extension of RFID technology. RFID is used for the purposes of identification and tracking RFID tags attached to objects from distance. Both NFC and RFID operate at the 13.56 MHz frequency. NFC works when NFC devices touch to each other to establish communication between the devices. Two main differences between these technologies is scanning distance and method of communication. The NFC system consists of two modes operations, similar to RFID, which are active mode and passive mode. In active mode, both NFC devices generate their own radio frequency to carry data. In passive mode, only one NFC device generates the radio frequency field. According to NFC Forum [2, 10], NFC communicate in two way communication or peer to peer communication, meanwhile RFID only has one way communication which operates only between active and passive.

2.2 NFC Operation Modes

There are three operation modes of NFC [2]:

Card Emulation Mode: This mode enables NFC-enabled device to act like smart cards. It allows users to perform transactions such as purchases, ticketing, and transit access control.

Reader/Writer Mode: NFC-enabled device is capable to read information stored on NFC tag embedded in smart posters and displays. User can retrieve tag information that stored in the tag for further uses.

Peer-to-peer Mode: This mode enables two NFC-enabled devices communicate with each other to exchange information and share files.

2.3 NFC Applications

NFC applications can be categorized into the behavior of NFC communication. There are four categories of NFC applications involved, which are i) touch and go, ii) touch and confirm, iii) touch and connect and iv) touch and explore [8]. The functionality of the application are as the following:

Touch and go application - requires users to bring close or touch the NFC devices to the NFC reader to run the tasks that implemented in the application. The example of NFC touch and go application is public transportation ticketing where NFC users scan and touch their NFC devices to access the transportation system.

Touch and confirm application- requires user to confirm the interaction by entering password or accepting the payment transaction for system confirmation.

Touch and connect application- provides a connection between two NFC devices to enable peer-to-peer data transferring such as exchanging images between two NFC-enabled smartphones.

Touch and explore - allows user to find and explore applications and devices capabilities.

2.4 NFC Security Attacks

The security attacks and risks that could occur in NFC are due to the physical nature of the NFC sensors and its operating mechanism which uses the insecure communication channel [3]. Figure 2 illustrates the security attacks that occur in NFC technology. Next, each attacks will be discussed in depth.

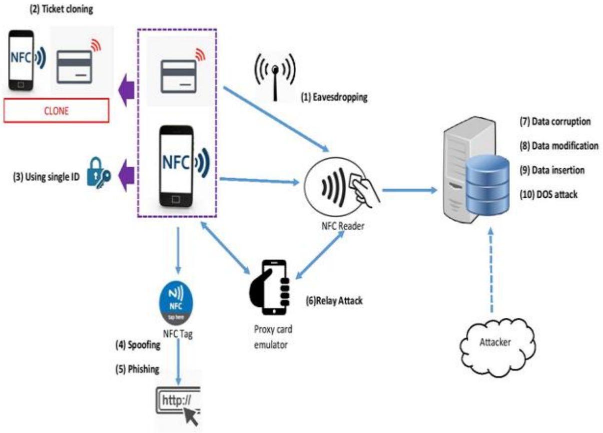

Fig. 2: Types of NFC Security Attacks

Eavesdropping: As NFC communication takes place in wireless communication, the communication can be easily get attacked and enable the attackers to eavesdrop the NFC communication out of their reach [11, 12]. Eavesdropping can happen in card emulation mode and peer to peer mode of NFC operation mode [12]. In card emulation mode, the data content can be read by malicious attacker if the function of NFC devices is not in use. While in peer to peer mode, if the data is transmitted without secure protection, the communication is risked for eavesdropping by an attacker.

Ticket Cloning: NFC technology is useful in ticketing service such as e-ticket or digital ticket. Ticket cloning from NFC can happen if the tickets have been copied and shared to other before verified [12, 13]. Everyone can use the cloning ticket as new ticket such as for getting discount in purchasing products. If the ticket has been verified, it can be used until the ticket expired. The cloning case can occur in two different ways which is depending on the ticketing system design. The goal of the ticket cloning is to share the ticket until its expiration.

Use Only Single ID: Each contactless smart card chip has a unique ID. The ID is needed for collision avoidance during the process of contactless reading [1, 12] The ID could be used for identification as it is unique. There is neither encryption nor authentication to read the ID with the NFC reading device. An attacker can capture or copy the unique ID to gain access to the ID since only one ID is used.

Spoofing: Attacker can spoof the tag content by supplying false information such as fake domain name, false URL or email [3]. Smart poster URI spoofing allows for attacks against web browser, URLs and mobile telephony services using SMS URIs, telephony URIs and etc [14].

Phishing: Phishing attacks could easily be performed when the NFC tags were modified or replaced with the other tags. Phishing in NFC is done by social engineering. Attacker tries to mislead NFC users by social engineering. If the tags are altered, it is easy to deceive the users to reveal their personal information by mislead them into malicious applications [1, 12].

Relay Attack: Both standards ISO14443 and ISO18092 are open to relay attacks which can neither be recognized by the card nor by the reader [1, 15, 16]. Smart card functionality could be relayed if the battery of NFC device is removed. When the battery is removed, the communication could not be occurring unless the functionality without the device being powered on should be considered. The attack can be achieved by using Application Protocol Data Unit (APDU) commands [3]. Malicious application can get the APDU commands from network socket. A basic relay attacks system that builds using two devices such as ghost and leech [17] The ghost is a device that fakes a card to the reader; meanwhile the leech is a device that fakes a reader to the card. Bidirectional communication channel was created by the ghost and leech and providing transparent communication channel through reader and tag.

Data Corruption: Data corruption may happen if the data transmitted over an NFC interface are modified by attacker [11, 18]. The data corruption can be considered as denial of service when the attacker changes the data into unrecognized format. The communication between user and receiver can be disturbed. If the data stored on NFC tag is corrupted, the tag will be useless and the device need to retrieve the data again. Data corruption can be performed by malicious software that running on a smartphone.

Data Modification: The attacker can manipulate and change the actual data to incorrect data especially during data transmission of NFC devices [11, 18]. The manipulated data could be received during the data transmission between NFC devices. This type of vulnerability requires expertise from the attackers in the field of wireless and radio communication which can handle the amplitude modulations of the transmission.

Data Insertion: Any unwanted data can be inserted by attacker in the form of messages especially during data exchanged between NFC devices [11, 18]. The attacker needs to respond to the device before legitimate device wants to establish its communication. The received data would be corrupted when both devices of legitimate and spoofed transmit data at the same time.

Denial of Sevice(DOS): DOS attack in NFC happens when there is incoming of continuation of flooding access request to NFC secure chip and malicious application in mobile phone [1, 12]. The function for access the secure chip will be locked until attacks stops to send massive asking message. All the installation process of the application will be aborted. At that time, the secure chip could not be used for transaction and it may lose its function. Besides that, DOS could happen when NFC device is touched with empty tag [1]. When the empty card of NFC is touched to NFC reader, there is possible a flooding error messages to occur that can affect NFC devices or services to go into suspended status.

Next, various techniques regarding Risk Assessment and MCDM methods will be discussed in Section III.

3. Risk Assessment & Multi-Criteria Decision Techniques

In this section, risk assessment and MCDM techniques will be discussed. Comparison between various types of risk assessment and multi-criteria decision making is done thoroughly.

3.1 Risk Assessment Methods

Risk assessment is a scientific and technologically based process which consisting steps of risk identification, risk analysis and risk evaluation [19].

Table 1: Risk assessment method/tool Comparison

Method	Description	Advantages	Disadvantages
CVSS [20]	An open framework for communicating the characteristics and severity of software vulnerabilities [20].	Usable by anyone, easy to understand and can be improved by anyone to score vulnerabilities [21].	Does not reduce number and severity of possible attack [22].
OCTAVE [23]	A methodology for identifying and evaluating information security risks [23].	Help a large organizations with 300 or more employees [23].	Large and complex as many worksheets and practices to implement [22].
TRIKE [24]	A conceptual framework that use for security auditing which view from risk management perspective [24].	Good as communication methods [24]. Designed to support automation to the greatest [24]	In experimental stage as not been fully tested against real systems [24].
STRIDE [25]	A classification scheme for characterizing known threats (spoofing identity, tampering with data, repudiation, information disclosure, DOS and elevation of privilege) [22].	STRIDE look for threats and consider the effect the threats [19]	can be very challenging and frustrating to categorize threats using STRIDE [25].
TARA [26]	Risk assessment methodology that was developed by Intel Information Technology (IT) [26].	Analyse and prioritize the most critical risks and narrow down to most likely attacks. [26].	Only list of likely possible attack. [26]

Table 1 displays the example of risk assessment method based on its advantage and disadvantages.

Accordingly, CVSS stand as the best option for risk assessment due to the fact of its capability which is focused in calculating various different types of scores such as temporal, base and environment. This is applicable to be adopted as a risk assessment for a technology based applications such as NFC. Meanwhile, OCTAVE only focuses on organizational risk as it is designed for organizations instead of technological risk and, it is hard to implement because there are many practices that need to implement. Although, CVSS does not reduce the number of attack, it evaluates the attacks with rating score.

3.2 Multi Criteria Decision Making (MCDM) Methods

MCDM is a decision making technique that make best decision among a set alternative decisions [27]. The aim of MCDM is to rate and determine the priority among different alternatives of decisions. MCDM for risk assessment have been applied to solve many issues of risk in e-business development, software development, healthcare and etc. Based on study, AHP and MACBETH support pairwise comparisons between criteria and options but AHP is evaluated on ratio scale while MACBETH use interval scale. TOPSIS can be used when only ideal and anti-ideal options are required. ELECTRE and VIKOR are based on similar principles on concordance analysis such as consideration of a certain global measure (concordance and global utility) and the other minority criteria is not too strong to oppose (non-discordance). SMAA determines if the information of decision is accurate as to protect wrong decision due insufficient information.

For MCDM method, [28] describes that application of AHP as a highly flexible and powerful method for a guidance to those who responsible in making decisions especially for better implementation of information security policy. So, AHP is selected because it able to handle larger problem and has control on the consistency of judgment while comparing to TOPSIS that has difficulty to keep the consistency of judgement. [29] SMAA able to handle flexibly the whole range of uncertain, imprecise or partially missing information and provide accurate information for decision making. So, SMAA is selected because it can handle ignorance in parameter values through probability distribution or ordinal information such as ranking information. 10 security attacks that have been listed previously happen in NFC payment application and those attacks are evaluated using a risk assessment method, ETSI TISPAN TVRA and an MCDM method of SMAA-TRI that resulted on risk acceptability for each security attack in NFC.SMAA-TRI produces category acceptability indices for all pairs of alternatives and categories by allowing uncertainty on parameter values [30]. Past research had presents a CVSS risk level estimation model to estimate security risk level by combining frequency and impact estimates from CVSS [31].

4. Research Methodology

A case study for each security risk is designed and included in the survey questionnaire. The purpose of the survey is to evaluate the vulnerability by using the risk assessment method. Then, the interview is conducted as to achieve the objective of this research which is to gain views from NFC experts in the NFC security for this research.

There are 32 participants involved in the survey and 2 individual of NFC experts for the interview. All the participants are knowledgeable in the security field. This include 2 employees of a well-known NFC organisation which tackle the NFC technology development and maintenances of high end projects. The risk assessment process for this research has been designed by referring to [19], risk assessment framework that provide risk determination and control measures. The security risks of NFC in this research are determined by evaluation of CVSS and SMAA-TRI method. After the higher risk is determined through the evaluation, a few of preventive measures are suggested to avoid the security risks according to the study. AHP method is used to select the best preventive measures for the risk.

5. Result and Discussion of Risk Assessment Analysis

This section describes the result and discussion on the risk assessment in the research.

5.1 Likelihood and Impact Estimation of Vulnerabilities using CVSS

Likelihood estimation is calculated using base metrics group and temporal metrics group of CVSS meanwhile impact estimation is calculated using base metrics group and environmental metrics group of CVSS [31]. The result of likelihood and impact estimation are derived from survey data that requires respondents to evaluate each case study for each security risk. There are ten case studies are designed for each security risks that identified in the research. The data of the survey is composed into discrete probability distribution that assigned probabilities for each individual outcome for each rating group of Low, Medium and High of CVSS. In order to respect the score inputs from all participants, the scores are aggregated in a probability distribution since the participants score the CVSS with different values for each CVSS metric. The process to calculate the probability, P(x) is presented as follows [32, 33]:

(i) Step 1: Determine total n value, $\sum n_{group}$ for each rating group (Low, Medium, High) and total number of participants, N

(ii) Step 2: Calculate probability using equation,

$$P(x) = \frac{\sum n_{group}}{N} \quad (1)$$

After the probabilities for each rating group are calculated, the SMAA-TRI method is used to calculate and produce category acceptability indices for all pairs of alternatives and categories. The SMAA-TRI method is calculated and simulated through JSMAA, an open source JAVA program that implement the SMAA-TRI method. The results for the SMAA-TRI method are displayed in Table 2 and Table 3 and illustrated in Figure 3 and Figure 4.

Table 2 displays the results from the likelihood estimation for each case study. There are many case studies that evaluated from survey's participants are categorized in Medium as they are likely to occur in NFC according to participants' evaluation. The case studies that evaluate in Medium category are included eavesdropping (0.7628), modified data (0.8135), spoofing (0.9282), ticket cloning (0.7684), relay attack (0.7227), phishing (0.7227), using a single ID (0.8214) and insertion of unwanted data (0.5201). There are 2 case studies that most likely to occur in NFC, in High category, according to participants evaluation which are DOS attack (0.7438) and data corruption (0.512).

Table 2: Likelihood estimation for each case study

Alternatives	Low	Medium	High	Likelihood
Eavesdropping	0.0758	0.7628	0.1614	Medium
Data corruption	0.0000	0.488	0.512	High
Modified data	0.0000	0.8135	0.1865	Medium
Spoofing	0.0000	0.9282	0.0718	Medium
Ticket cloning	0.0353	0.7684	0.1963	Medium
DOS	0.0000	0.2562	0.7438	High
Relay attack	0.0160	0.7227	0.2613	Medium
Phishing	0.0801	0.7227	0.1731	Medium
Using Single ID	0.0369	0.8214	0.1417	Medium
Insertion of unwanted data	0.0000	0.5201	0.4799	Medium

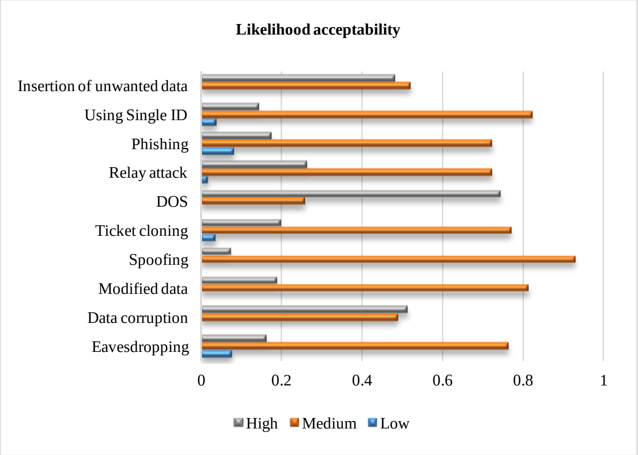

Fig. 3: Likelihood acceptability

Table 3: Impact estimation for each case study

Alternatives	Low	Medium	High	Impact
Eavesdropping	0.0849	0.7537	0.1614	Medium
Data corruption	0.0000	0.4581	0.5419	High
Modified data	0.0000	0.7955	0.2045	Medium
Spoofing	0.0000	0.9282	0.0718	Medium
Ticket cloning	0.0438	0.7165	0.2397	Medium
DOS	0.0000	0.2562	0.7438	High
Relay attack	0.0160	0.7227	0.2613	Medium
Phishing	0.0900	0.7369	0.1731	Medium
Using Single ID	0.0476	0.8545	0.0979	Medium
Insert of unwanted data	0.0000	0.5373	0.4627	Medium

Table 3 displays the results from the impact estimation for each case study. The case studies that are likely to happen in NFC are included eavesdropping (0.7537), modified data (0.7955), spoofing (0.9282), ticket cloning (0.7165), relay attack (0.7227), phishing (0.7369), using a single ID (0.8545) and insertion of unwanted data (0.5373). There are 2 case studies that most likely to occur in NFC according to participants evaluation which are DOS attack (0.7438) and data corruption (0.5419). The acceptability of likelihood and impact are calculated from the participants' evaluation of case studies in the online survey.

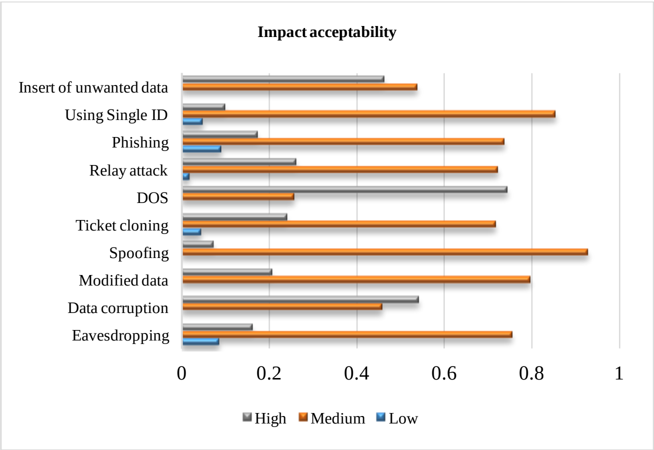

Fig. 4: Impact acceptability

Table 4: Risk level for each case study

Case Study	Likelihood	Impact	Risk
Eavesdropping	Medium	Medium	Medium
Data corruption	High	High	High
Modified data	Medium	Medium	Medium
Spoofing	Medium	Medium	Medium
Ticket cloning	Medium	Medium	Medium
DOS	High	High	High
Relay attack	Medium	Medium	Medium
Phishing	Medium	Medium	Medium
Using Single ID	Medium	Medium	Medium
Insert of unwanted data	Medium	Medium	Medium

5.2 Risk Assessment Analysis Outcome

The risk level in Table 4 is determined by likelihood and impact estimation (Table 3 and Table 3) since risk is a function of likelihood multiply with impact. From the result of the risk assessment process, there are two case studies that have higher risk which are data corruption and DOS attack. Case studies for data corruption and DOS attack display high likelihood and impact which indicate that the case studies have high risk. The other case studies such as eavesdropping, modified data, spoofing, ticket cloning, relay attack, phishing, using single ID and insert of unwanted data are categorized into medium risks as they have medium likelihood and impact.

The results in Table 4 are concluded by the evaluation results from the participants of the survey. Different participants involved could have impacted the results on the risk determination as each participant has their own interpretation to evaluate for each case study, so there is a possibility that likelihood and impact are rated as low, or likelihood is rated high and impact is rated as medium, or vice versa.

6. Dos Attack & Data Corruption Attack Countermeasures & Selection Using Mcdm

Data corruption involves data manipulation as attacker disturbs the NFC communication or transmission through NFC interfaces and devices. Since data is corrupted, the data is unreadable to other NFC devices. Data corruption can be prevented as NFC devices can check and observe the radio frequency field while transmitting data. This attack can be detected because higher power is needed to corrupt data than sending data, so NFC devices can detected any sending data that use power significantly higher during data transmission [34]. DOS attack occurred when an NFC device touches empty or corrupted NFC tag and error messages will occupy the NFC devices until suspended. It also could happen from malicious application in NFC-enabled smartphone [12]. The preventive measures to minimise the risks of data corruption and DOS attack are by signing tags appropriate encryption technique, using cryptographic tag authentication protocols and establish secure channel between NFC devices [3, 18]. Securing NFC channel is a best approach to secure NFC communication and defend against all types of attacks on data during communication [11].

6.1 MCDM Analysis is AHP Approach

AHP method is used to select the highest priority of NFC risk countermeasures. AHP is used to develop priorities for alternatives and the criteria is used to judge the decision alternatives. AHP procedure consists of [35]:

(i) Step 1: Develop the weights for the criteria by developing a single pairwise comparison matrix for the criteria;

(ii) Step 2: Develop the ratings for each decision alternative for each criterion by developing a pairwise comparison matrix;
(iii) Step 3: Calculate the weighted average rating for each decision alternative. Choose the one decision alternative with the highest score.

The pairwise comparisons are used to establish relative priority for each criteria against criteria or even against decision alternatives. It uses the AHP scale rating from equal importance to extreme importance as shown in Table 5.

Table 5: Scale rating using AHP

Scale (Intensity of importance)	Explanation
1	Equal importance
3	One is slightly important to the other.
5	One is important to the other.
7	One is very much more important to the other.
9	One is absolutely more important to the other.
2,4,6,8	When compromise is needed

A decision hierarchy had been designed to decide the highest priority of NFC countermeasures as presented in Figure 5. On the comparison to provide confidentiality, establishing secure channel is very much more important than using cryptography and authentication protocol. Establish a secure channel also absolutely more important than using the protocol. Meanwhile, using the protocols is slightly important than signing tag with encryption.

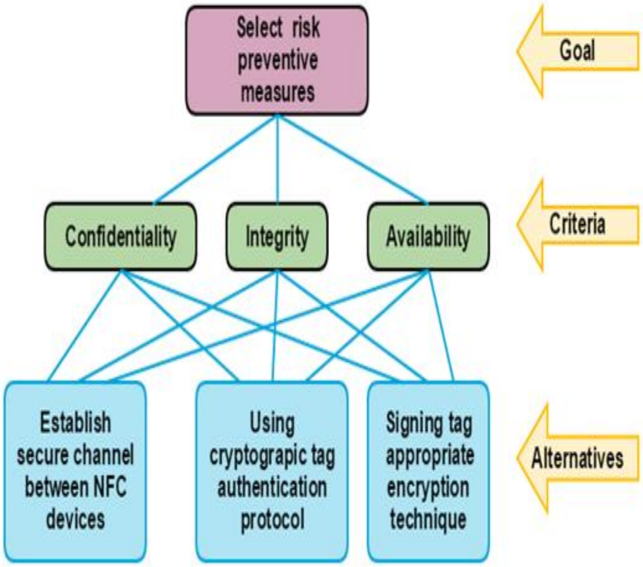
Select risk preventive measures
Goal
Confidentiality
Integrity
Availability
Criteria
Establish secure channel between NFC devices
Using cryptograpic tag authentication protocol
Signing tag appropriate encryption technique
Alternatives

Fig. 5: Decision hierarchy to select preventive measure of data corruption and DOS attack

The priority resulted from the comparison shows that establish secure channel have priority is 0.7611, using the protocols is 0.1663, and using a tag with encryption is 0.0726.On the comparison to provide integrity, establishing secure channel is very much important than using cryptography and authentication protocol. Establishing a secure channel also absolutely more important than using the protocol. Meanwhile, using the protocols is slightly important than signing tag with encryption. The priority to establish a secure channel is 0.7503, using the protocols is 0.1714, and using a tag with encryption is 0.0782. On the comparison to provide availability, establishing secure channel is more important than using cryptography and authentication protocol. Establish a secure channel also more important than using the protocol. Meanwhile, using the protocols is slightly important than signing tag with encryption. The priority to establish a secure channel is 0.7172, using the protocols is 0.1947, and using a tag with encryption is 0.0881.

Table 6: Overall priority of AHP calculation to select preventive measure

Alternatives	Confidentiality	Integrity	Availability	Overall priority
P1	0.7611	0.7503	0.7172	0.7429
P2	0.1663	0.1714	0.1947	0.1775
P3	0.0726	0.0782	0.0881	0.0796

The AHP overall priority for each alternative in Table 6 is calculated with all the pairwise comparison of alternatives with respect to CIA. The highest weight or priority that obtained through the AHP calculations is to establish a secure channel that has a priority of 0.7429 which is 74.29%. Preventive measures such as using cryptography and authentication protocol has priority at 0.1775 (17.75%), signing tag appropriate encryption techniques has priority at 0.0796 (7.96%). Thus, from the overall priority, establish secure channel has higher priority at 74.29% that makes it is the best solution for risk countermeasures to prevent data corruption and DOS attack in NFC.

From the AHP result, the solution to prevent data corruption and DOS attack is to establish a secure channel which has the highest priority of 74.29%. From the study, securing channel in NFC communication is the best way to prevent all type of attacks, eavesdropping and also included to protect from DOS attack [18, 34]. Protocols that could be used to establish secure channel in NFC are Diffie-Hellman (DH) based on RSA or Elliptic Curves Cryptography (ECC) [18]. Asymmetric keys like 3DES or AES for key sharing and provide confidentiality, integrity and authenticity. From interview data that obtained through research, the NFC participants suggested to use 3DES or AES algorithm for a shorter transaction which is shorter response time, and RSA is applied when longer time of transaction is needed. An AHP method has been approached to weight and score the priority among the cryptography algorithms. The factors or criteria have been considered for the AHP method such as key size, speed, complexity, security and cost. The alternatives for the AHP method are the cryptography algorithms such as AES, 3DES, RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC).

The highest priority for key agreement protocol is using ECC which has priority at 0.788 (78.8%) than DF that has priority at 0.212 (21.2%). Meanwhile, the highest priority to use key sharing technique is using AES which has priority at 0.761 (76.1%), 3DES at 0.183 (18.3%), and RSA at 0.056 (5.6%). All the priority vector for each alternative have been considered by taken into factors such as key size, speed, security, complexity and cost. From decision making of AHP, for key agreement protocol, ECC is the best key agreement protocol compared to DH because it has shorter key size, faster speed, more secure and cheaper in cost, although ECC is more complex than DH. For key sharing algorithms, AES is chosen as the best algorithm because it uses low key size, has faster speed than other algorithms, more secure, less complex, and cheaper in cost. Meanwhile, RSA is the worst among AES and 3DES because it use longer key size, that make its speed become slower, less secure, has complexity and expensive in cost. Thus, ECC and AES are the best solution to establish secure. Based on the finding to establish a secure channel in the NFC, the cryptography algorithms that selected from the AHP approach in this research are similar and correlated to ECMA-386 standard. The ECMA-386 standard specifies cryptographic mechanisms to use the elliptic curve Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm for data encryption and integrity as to establish secure channel in NFC [36].

7. Case Study – Multi-Factor Identification Attendance System (Midas)

After risk countermeasures are determined from AHP approach, a solution guideline is proposed by designing a secure NFC application architecture to prevent the most likely security attacks that could happen in NFC. The existing NFC touch and go application that has been selected is Multifactor Identifications Attendance System (MIDAS) [37]. The aim of using a case study for NFC touch and go application is to prevent data corruption and DOS attack using MIDAS as solution essential. MIDAS is a prototype of attendance system for university that using NFC and authenticate biometric via face. It can be accessed through web-browser and Android based mobile application. The target users of this system are included student and lecturer in university. Student use NFC card as student's identity card and NFC-enabled smartphone to take attendance. Lecturer only can check students' attendance in MIDAS system using smartphone or internet browsers. The devices that are used in this system are involved NFC-enabled smartphone for face authentication and mobile application, NFC card as student identity, NFC reader to scan and read NFC card and computer laptop as local server and NFC reader application.

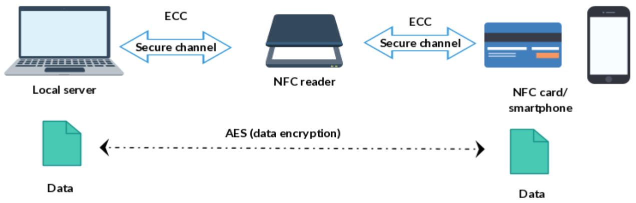

Fig. 6: Secure channel in MIDAS

Secure channel of NFC devices are establish from the interaction of NFC devices. Figure 6 shows secure channel that establish in the proposed NFC-enabled smartphone architecture of MIDAS prototype. All the channels between NFC devices are secure using ECC protocol and AES provide data encryption between the NFC card or smartphone to local server. NFC reader acts as a pinpoint to pass the data from NFC card to local server. All the communication channels between NFC-enabled smartphone, NFC reader and server are secured.

8. Conclusion & Future Work

There are two contributions in this research: (1) Based on significant of the study and research method, the likelihood of NFC security risks had been determined by evaluating the risks using the risk assessment method. Through the evaluation, the highest risks that had been determined are data corruption and DOS attack. The other security risks from the study had been classified as medium risks. (2) A guideline of solution is proposed using MIDAS system (a touch and go application) to secure the NFC application. From the findings in this research, ECC and AES algorithms are the best techniques to establish a secure channel in the NFC as well as to prevent data corruption and DOS in NFC. We found that the findings, results of cryptographic algorithms are similar and correlated to ECMA-386 standard for NFC cryptographic mechanism.

The limitation of this research involves the number of participants that participate in online survey and the number of NFC experts. The outcome results from risk assessment process is correlated to the number of sampling size. Different sampling size or group can impacted the outcome results. For further research, different risk assessment method can be used to evaluate the security risks in NFC. Other MCDM methods can be considered to implement in this research as to decide the best solution to prevent security attacks. Besides touch and go application of NFC, other NFC application can be tested as to determine the likelihood of its security risks.

Acknowledgement

This paper is supported by USM Grant no. 1001/PKOMP/8014003.

References

[1] Madlmayr G., Langer J., Kantner C. & Scharinger J. (2008), NFC Devices: Security and Privacy. Proc. Proceedings of the 2008 Third International Conference on Availability, Reliability and Security2008, 642-647.

[2] NFC Forum. Home. http://nfc-forum.org/. Accessed September 3, 2015.

[3] Coskun V., Ozdenizci B. & Ok K (2015), The survey on near field communication. Sensors, 2015, 15, (6), 13348-13405.

[4] Want. R (2011), Near field communication. IEEE Pervasive Computing, 10, 3, 4-7.

[5] Hoepman J.-H. & Siljee J. (2007), Beyond RFID: the NFC Security Landscape. Delft: TNO.

[6] Google, Google Wallet. https://www.google.com/wallet. Accessed February 23 2016.

[7] VISA Inc, Visa payWave - Consumer. https://usa.visa.com/pay-with-visa/featured-technologies/visa-paywave.html. Accessed February23 2016.

[8] Finkenzeller K. (2010), RFID handbook: fundamentals and applications in contactless smart cards. Radio frequency identification and near-field communication, John Wiley & Sons.

[9] Emms M., Arief B., Little N. & Van Moorsel A. (2013), Risks of offline verify PIN on contactless cards. International Conference on Financial Cryptography and Data Security, Springer, 313-321.

[10] Dawidowsky F., NFC, Bluetooth and RFID: Unraveling the Wireless Connections. https://nfc-forum.org/nfc-bluetooth-and-rfid-unraveling-the-wireless-connections/. Accessed 27 August 2015.

[11] Chattha N.A. (2014), NFC—Vulnerabilities and defense. Conference on Information Assurance and Cyber Security (CIACS), IEEE, 35-38.

[12] Chen C.H., Lin I.C. & Yang C.C. (2014), NFC Attacks Analysis and Survey. 2014 Eigth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 458-462.

[13] Ceipidor U.B., Medaglia C., Marino A., Morena M., Sposato S., Moroni A., Di Rollo P. & La Morgia M. (2013), Mobile ticketing with NFC management for transport companies. Problems and solutions. 2013 5th International Workshop on Near Field Communication (NFC), IEEE, 1-6.

[14] Mulliner C. (2009), Vulnerability analysis and attacks on NFC-enabled mobile phones. International Conference on Availability, Reliability and Security (ARES'09), IEEE, 695-700.

[15] International Organization for Standardization (2011), Identification cards - Contactless integrated circuit cards - Proximity cards - Part 1 to 4. ISO/IEC 14443-3:2011,2, April 2011.

[16] International Organization for Standardization (2013), Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1). ISO/IEC 18092:2013,2, 1-44.

[17] Kfir Z. & Wool A. (2005), Picking virtual pockets using relay attacks on contactless smartcard. First International Conference on Security and Privacy for Emerging Areas in Communications Network (SecureComm 2005), IEEE, 47-58.

[18] Haselsteiner E. & Breitfuß K. (2006), Security in near field communication (NFC). Workshop on RFID security, 12-14.

[19] NIST Special Publications (2002), Guide for Conducting Risk Assessments (800-30). National Institute of Standards and Technology, U.S. Department of Commerce, 1-95.

[20] Mell P., Scarfone K. & Romanosky S. (2006), Common vulnerability scoring system. IEEE Security & Privacy, 2006, 4, 6.

[21] FIRST (2016), CVSS. https://www.first.org/cvss/v2/faq. Accessed February 23 2016.

[22] OWASP (2015), Threat Risk Modeling. https://www.owasp.org/index. php/Threat_Risk_Modeling. Accessed 20 September 2015.

[23] Caralli R.A., Stevens J.F., Young L.R. & Wilson W.R. (2007), Introducing octave allegro: Improving the information security risk assessment process. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

[24] Saitta P., Larcom B. & Eddington M., Trike v. 1 methodology document [draft]. http://dymaxion.org/trike/Trike_v1_Methodology_ Documentdraft. pdf, 2005.

[25] Shostack A. (2014), Threat modeling: Designing for security, John Wiley & Sons.

[26] Rosenquist M. (2009), Prioritizing information security risks with threat agent risk assessment. Intel Corporation White Paper.

[27] Velasquez M. & Hester P.T. (2013), An analysis of multi-criteria decision making methods. International Journal of Operations Research, 2013, 10, 2, 56-66.

[28] Syamsuddin I., & Hwang J. (2010), The Use of AHP in Security Policy Decision Making: An Open Office Calc Application. JSW, 5, 10, 1162-1169.

[29] Lahdelma R. & Salminen P. (2010), Stochastic multicriteria acceptability analysis (SMAA): Trends in multiple criteria decision analysis. Springer, 285-315.

[30] Vermaas R., Tervonen T., Zhang Y. & Siljee J. (2013), The security risks of mobile payment applications using Near Field Communication. Rotterdam: Erasmus University Rotterdam, 2013.

[31] Houmb S.H. & Franqueira V.N. (2009), Estimating ToE risk level using CVSS. International Conference on Availability, Reliability and Security, 718-725.

[32] Houmb S.H., Franqueira V.N. & Engum E.A. (2010), Quantifying security risk level from CVSS estimates of frequency and impact. Journal of Systems and Software, 83, 9, 1622-1634.

[33] Chan C.W. & Mahinderjit Singh M. (2015), Standardized security metrics with CVSS framework for BYOD higher education. BSc. Thesis, Universiti Sains Malaysia.

[34] Coskun V., Ozdenizci B. & Ok K. (2013), A survey on near field communication (NFC) technology. Wireless personal communications, 71,3, 2259-2294.

[35] Kunz J. (2010). The Analytic Hierarchy Process (AHP). https://www.slideshare.net/lakshanasuresh/ahp-calculations?t=123. Accessed October 24 2016.

[36] ECMA International (2015). 385–nfc-sec: Nfcip-1 security services and protocol. ECMA International (European Association for Standardizing Information and Communication Systems), Geneva, Switzerland.

[37] Ong D.D.W. & Mahinderjit Singh M. (2016). A secure near field communication (NFC)-enabled attendance on android mobile for higher education. Knowledge Management International Conference (KMICe) 2016 , 111-115.