ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MITIGATING DATA SPOOFING RISKS IN NEAR FIELD COMMUNICATION (NFC) READ/WRITE MODE: AN INVESTIGATION INTO ACCESS CONTROL VULNERABILITIES AND POST-COMPROMISE RECOVERY STRATEGY

PUTERI SHARIZA MEGAT KHALID[1], NOR FAZLIDA MOHD SANI[2]
[1] Information Security, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
[2]Professor Madya, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
E-mail: [1]puterisha.megat@gmail.com, [2]fazlida@upm.edu.my

ABSTRACT

The rapid growth of Near Field Communication (NFC) technology has facilitated its widespread adoption in everyday activities, particularly in cashless mobile payments and access control among urban dwellers. However, this convenience is accompanied by significant security risks, including data spoofing, relay attacks, and unauthorized data access. Despite advancements in NFC technology, a critical gap persists in securing communications, particularly at the end-user level, where awareness and preventive measures are insufficient. This research aims to address those gaps by focusing on end-user vulnerabilities and providing tailored solutions through the development of an NFC End-User specific security policy. The study's primary contribution lies in the development of an information security policy tailored specifically for NFC End-Users. This policy serves as a comprehensive guideline aimed at enhancing the security posture of individuals who utilize NFC-enabled devices. Unlike previous studies that primarily examine technical countermeasures, this work emphasizes the human factors by assessing user awareness and NFC secure practices. By developing an NFC security policy specifically for end users, the study aims to bridge the gap between technological safeguards and NFC End User behavior.

Keywords: *Near Field Communication (NFC) End-User Security Awareness, Information Governance, Personal Data Security, Information Security Policy.*

1. INTRODUCTION

1.1 BACKGROUND OF STUDY

NFC technology is widely used for mobile payments, transit, and access control due to its convenience in enabling quick data transfers through short-range wireless communication. Despite its benefits, NFC faces significant security vulnerabilities, particularly affecting end users who often lack awareness and proper security practices. These vulnerabilities include risks like unencrypted data transmission, inadequate authentication, and susceptibility to attacks such as relay attacks, eavesdropping, and data spoofing. End-user negligence, like ignoring updates or using weak security settings, further exposes NFC communications to threats. Malicious actors exploit these gaps, potentially intercepting sensitive information or conducting phishing attacks via fraudulent NFC tags, underscoring the need for improved user education and security measures. NFC technology has many benefits, but as its use has grown, major security vulnerabilities have been revealed, especially at the end-user level where awareness and lack of preventative measures often pose as a gap in the security chain.

NFC vulnerabilities in general encompass the weaknesses in the design, implementation, and operation of NFC protocols and devices, as well as the gaps in user awareness and security practices, which can be exploited by malicious actors to compromise the security and privacy of NFC communications. From a technological standpoint, NFC vulnerabilities are intrinsic weaknesses and faults that can be used by threat actors to compromise NFC protocols and devices during their design, implementation, and operation. The vulnerabilities encompass potential dangers related to the transmission of unencrypted data, insufficient authentication methods, and vulnerability to man-in-the-middle attacks, eavesdropping, relay attacks, and data tampering [1]. The limited range of NFC communication is frequently misconstrued as a guarantee of security. However, individuals with advanced tools can exploit these technical vulnerabilities to gain unauthorized entry or interrupt communications [2]

[2] introduces a real-world relay attack on Near Field Communication systems, specifically targeting peer-to-peer communication on mobile devices. The authors illustrate how an assailant can take advantage of the limited distance capability of NFC by intercepting and transmitting communication between two devices that are not in immediate proximity. This is accomplished by creating and deploying malicious software on the attacker's mobile phones that have NFC capabilities. The attack does not necessitate access to protected program memory or code signing, and only makes use of publicly accessible APIs. The research also explores possible countermeasures, such as utilizing device position information, to reduce the danger of relay assaults in mobile situations.

NFC vulnerabilities at the end user level arise from a lack of awareness and understanding about the possible risks connected with NFC technology, resulting in gaps in the security chain. These gaps include insufficient user education about the secure utilization of NFC-enabled gadgets, inadequate security practices such as neglecting software updates or enabling security features, and the utilization of default or feeble security settings. The absence of user attentiveness and awareness fosters a setting in which attackers can readily exploit weaknesses in NFC technology. They can accomplish this by employing fraudulent NFC tags to carry out phishing attacks or pilfer sensitive information via data spoofing [3]. Eavesdropping attacks, for example, could allow an attacker to intercept sensitive information, such as payment card details, as they are transmitted between an NFC-enabled device and a reader. Moreover, the ability to associate a user's identity with their NFC-enabled devices could be exploited to build detailed profiles of their movements and spending habits, posing a significant privacy risk.

It is crucial for information security organizations to recognize that a significant number of working people lack familiarity with terminology such as phishing and ransomware. Making assumptions about their knowledge might have a detrimental effect on security awareness training efforts [4]. [5] as cited in [6] conducted a study on the vulnerabilities found in smartphones equipped with NFC capability. He developed an NDEF security toolkit specifically tailored to evaluate the security of the selected NFC-enabled smartphone. The finding revealed that the NFC (Near Field Communication) Data Exchange Format (NDEF) was vulnerable to basic manipulation. Another vulnerability lies in the potential misuse of NFC-enabled mobile phones with embedded security elements as contactless attack vectors. Although such attacks can also be implemented on other contactless platforms, the NFC-enabled mobile phone's legitimate form factor and widespread acceptance by merchants could make it a particularly attractive target for malicious actors. Since, these NFC-enabled devices resides within the boundary and ownership of the device owners, therefore, there is a need to address this gap in the security chain.

1.2 PROBLEM STATEMENT

Near Field Communication (NFC), a subset of Radio Frequency Identification (RFID) technologies operating on the 13.56MHz HF range, enables three operation modes: (i) reader/writer, (ii) card emulation, and (iii) peer-to-peer. In the reader/writer mode, NFC devices can both read data from and write data to NFC tags [7]. The initial step in NFC operations is the attestation process, which authenticates identities, endpoints, applications, and data. However, NFC systems inherently lack robust security mechanisms, making them vulnerable to frequency jamming, data tampering, eavesdropping, and relay attacks [8]. A significant security incident reported by [9] highlighted these vulnerabilities, where security researcher Josep Rodriques demonstrated the ability to hack ATMs and various POS terminals using an Android app that exploited NFC system firmware flaws. This incident underscores the critical vulnerability of NFC systems to information disclosure attacks. Specifically, when an attacker taps an NFC-enabled device with a smartphone, they can easily capture and reuse returned data, such as URLs, without detection [10].

Recent reports from the MITRE CVE and NIST NVD databases list numerous NFC-related vulnerabilities, including those that enable unauthorized data access, manipulation, and device control. In the case of CVE-2020-15001 [11] which is post-compromise recovery that is addressed in detail in the Yubico security advisory [12] further illustrates the potential severity of these vulnerabilities, revealing that even hardware designed for secure authentication can be compromised through NFC flaws. These vulnerabilities highlight the urgent need to address data spoofing or information leak risks at both the end-user and device levels. Mitigating these risks is crucial, as end-users often lack the expertise to recognize and respond to sophisticated NFC-based attacks. At the device level, ensuring that NFC systems are secure by design, with robust firmware and hardware protections, is essential to prevent unauthorized access and data manipulation. Effective mitigation strategies must include not only countermeasure policies but also comprehensive post-compromise recovery strategies to contain damage and protect the security and privacy of information owners.

The importance of an integrated post-compromise security policy that bridge the practical gap between Enterprise Security Practitioners and Public Individual End Users cannot be overstated, especially in a landscape where mobile devices, integrated with NFC chips, are ubiquitous. End users, often unaware of the potential risks associated with NFC technology, are particularly vulnerable. This study aims to address the practical gaps in existing NFC security by developing a comprehensive policy that not only includes proactive security strategies but also applicable post-compromise recovery that can be referred to by Public NFC End-Users. Such a policy is crucial to mitigating the risk of data spoofing and ensuring the privacy and security of information for End Users. The contribution of this study will bridge the current security gaps in NFC-enabled devices and wireless-based services.

1.3 RESEARCH OBJECTIVES

At the heart of the study, the objectives of the study are as followings:

a. To explore the security vulnerabilities and data security challenges associated with NFC operations.
b. To assess the level of awareness and security perceptions among NFC End Users regarding NFC technology.
c. To propose a security policy to protect the privacy and security of information of NFC End Users.

1.4 RESEARCH QUESTIONS

To meet the objectives of the study, the overarching research questions are:

a. What are the primary security vulnerabilities associated with NFC technology?
b. How aware of the End Users of these NFC Security Vulnerabilities?
c. What policy can be implemented to mitigate these risks and enhance NFC security?

1.5 SIGNIFICANCE OF THE STUDY

The research addresses several critical gaps in the existing literature on NFC technology security, particularly in the areas of end-user vulnerabilities post-compromise recovery strategies. Much of the existing literature on NFC security concentrates on enterprise-level solutions or general NFC technology vulnerabilities, but there is a lack of focus on the specific end-user vulnerabilities End-users often lack awareness of NFC risks, leaving them particularly susceptible to attacks like data spoofing, relay attacks, and phishing through fraudulent NFC tags.

This research directly addresses these individual-level risks, highlighting the need for personalized security guidelines. While many studies have examined ways to prevent NFC attacks, post-compromise recovery strategies are largely unexplored. In practice, once an NFC-enabled device is compromised, there is often limited guidance available on how end-users should respond. This research contributes by proposing a detailed post-compromise recovery framework that can help individuals mitigate the impact of a breach and restore security. Current literature often outlines general security recommendations for NFC systems, but these are not tailored to the unique behaviors and needs of end-users.

This study fills this gap by developing an NFC-specific security policy that considers end-user behavior and practical challenges, such as user knowledge limitations and device-specific vulnerabilities. Although NFC security vulnerabilities are well-documented, there is a significant gap in research focused on end-user education and awareness as key components of security. This research contributes by emphasizing the role of end-user awareness in enhancing NFC security and providing actionable recommendations to improve end-user education on NFC-specific risks and best practices. While frameworks like Microsoft's Zero Trust are robust, they are largely designed for enterprise environments and do not adequately cover personal NFC usage scenarios. This study bridges this gap by proposing an integrated approach that complements existing frameworks with NFC end-user-focused strategies, making NFC security applicable beyond enterprise-controlled devices and into personal use cases. By filling these gaps, the study not only enhances the understanding of NFC-specific risks at the individual level but also offers practical, user-oriented solutions that strengthen overall NFC security from both preventive and recovery perspectives.

2.0 LITERATURE REVIEW

For the purpose of understanding, the followings are the definitions used in this study:

a) **NFC Vulnerabilities:** NFC vulnerabilities are the inherent weaknesses and flaws in the design, implementation, and operation of NFC protocols and devices that can be exploited by malicious actors. These vulnerabilities encompass susceptibility to man-in-the-middle attacks, espionage, relay attacks, and data modification, as well as risks associated with unencrypted data transmission and insufficient authentication mechanisms. The short communication range of NFC is frequently presumed to provide security; however, attackers with sophisticated tools can exploit these technical flaws to disrupt communications or acquire unauthorized access [13].

b) **NFC End Users:** From [14], in the context of product development, a person who ultimately utilizes or is intended to use a product, is referred to as an end user. For this study, Near Field Communication (NFC) end users are individuals who use NFC-enabled devices. for a variety of purposes, including data exchange, public transportation, access control, and mobile payments. These consumers utilize NFC technology by means of their smartphones, smart cards, or other NFC-enabled devices.

2.1 VULNERABILITIES IN NFC OPERATIONS

The attestation process in NFC Read/Write mode is fundamental for validating the legitimacy of devices and the data they exchange. Attestation ensures that the devices involved in the communication are trusted entities and that the data has not been tampered with [15]. The NFC attestation process involves several steps to authenticate devices and secure data transmission:
(a) *Initialization:* Establishes a secure communication channel between NFC devices using cryptographic protocols, exchanging cryptographic keys to ensure encrypted communications.
(b) *Challenge-Response Protocol:* The initiating device (reader) sends a challenge to the responding device (tag). The responding device must generate a valid response based on the challenge and its stored cryptographic keys, verifying authenticity.
(c) *Data Integrity Check:* Involves using hash functions and digital signatures to ensure transmitted data has not been altered. Any discrepancies detected indicate potential tampering or data corruption.
(d) *Secure Data Transmission:* After authentication and data integrity verification, data is transmitted securely. Encryption prevents unauthorized access and eavesdropping, ensuring intercepted data cannot be deciphered without appropriate cryptographic keys.

[16] discusses the security risks associated with Near Field Communication technology, particularly in the context of business information systems. The authors argue that while NFC offers convenience, its read/write mode, often used for tasks like making payments or accessing information via tags, is vulnerable to various security threats. They propose a threat model based on the STRIDE methodology to identify vulnerabilities in NFC applications and suggest potential mitigation strategies. The study by [17] highlights the importance of understanding these security risks and encourages developers and users to implement appropriate security measures to protect sensitive data.

The security and reliability of data exchanges are improved by the integration of NDEF (NFC Data Exchange Format) within the NFC attestation procedure in Read/Write mode, which guarantees that all transmitted information is authenticated and protected against tampering. The NFC Data Exchange Format (NDEF) establishes a standardized format and guidelines for the exchange of data structures using NFC. NDEF records include application-specific data structures and type information. An NDEF message consists of many records. The Type, ID, and Payload fields of NDEF records are the only fields that the signature record signs. This is the most severe scenario, as [18] have stated that it only ensures a minimum level of integrity and authenticity for the signed records, but it permits the use of signatures when used with Java's Contactless Communication API. Accordingly, [18] conducted a more thorough examination of the Signature Record Type Definition and identified numerous practical attack scenarios that are the consequence of the NDEF Signature Record Type's vulnerabilities and the absence of instructions regarding the utilization and interpretation of signatures. These vulnerabilities are supported further by subsequent studies.

The frictionless operation of NFC technology, while enhancing user experience, presents significant security challenges, particularly in terms of spoofing threats. [19] explains that one of the primary vulnerabilities arises from the inability of typical users to distinguish between authentic and counterfeit NFC tags. This vulnerability can be exploited in several ways. Firstly, attackers can physically replace or destroy legitimate tags and place spoofed ones in their place. Methods for tag destruction include the use of devices like RFID zappers or simply making physical cuts to the tag's antenna, rendering it useless. Secondly, adversaries can shield original tags using metal-coated stickers or foils and place spoofed tags over them, effectively hijacking the communication.

[20] further highlighted that another prevalent spoofing method involves manipulating the data stored on NFC tags. Attackers can store malicious URIs in the NDEF data formats, leading to phishing attacks or other malicious activities such as stealing geo-location data, initiating client Denial of Service attacks, or exploiting browser vulnerabilities through outdated security patches. Additionally, spoofing can be conducted through rogue applications installed on a user's smartphone via phishing or social engineering. These applications can intercept and alter NFC tag contents before they are processed by the device's operating system, deceiving users into interacting with malicious content. Finally, NFC's capability for Wi-Fi connection handover can be exploited to spoof legitimate networks, redirecting user data through malicious access points. This attack can be particularly effective in areas where users commonly place their smartphones, leveraging deceptive SSID names to trick users into connecting to compromised networks.

NFC tags are typically passive, which means that they have limited computational capacity and storage. Consequently, the complexity of cryptographic algorithms that can be implemented for authentication is restricted, as explained by [21]. Given this technical setting, there are numerous security and privacy hazards associated with NFC. The first is eavesdropping where the data exchange between an NFC-enabled device and a reader is susceptible to eavesdropping by an individual with the appropriate apparatus, as NFC involves the use of radio waves to transmit information therefore it is susceptible to wave interception.

Second is Relay Attacks; by employing two intermediary devices, an assailant can exploit the short-range communication function of NFC technology. In this type of attack, communication between an NFC tag and a reader is facilitated by telecommunication devices, which function as relays, allowing for a distance that exceeds the distance requirement of NFC. From the End User's perspective, the proxy token exhibits the same behavior as the original token during the relay attack. This type of attack bypasses the security mechanisms of the application layer.

In experiments conducted by [22], it is demonstrated that data can be intercepted at a distance of up to 10 m using a publicly available spectrum analyzer and with just an improvised passive antenna that does not have any amplification or signal filtering circuity. Confirming that, NFC technology still faces several security threats that compromise its integrity and reliability. For example, spoofing which involves attackers creating counterfeit NFC devices to disseminate malware or steal information, and data corruption through denial-of-service (DoS) attacks can occur by altering the NFC interface. Additionally, the lack of robust encryption in NFC communication makes it vulnerable to surveillance. And ultimately is relay attack, where attackers can relay communication between two NFC devices without verifiable physical access, which further exacerbate security concerns because this type of attack can bypass existing security measures [23].

To address these vulnerabilities, researchers have proposed various security countermeasures, such as ensuring that NFC cards are unreadable when not in use and implementing robust authentication protocols to prevent unauthorized access to NFC-enabled devices. [24] proposes a new protocol for NFC mobile payments that ensures mutual authentication, security, and fairness. The authors argue that standard NFC protocols prioritize speed over security, leaving them vulnerable to attacks, especially when messages are exchanged over the air. The author aims to address this vulnerability by introducing a technique that uses a secure offline session key generation. This technique ensures; (i) mutual authentication that prevents replay and man-in-the-middle attacks, (ii) transaction security that can protects sensitive information during the transaction, and (iii) strong fairness that guarantees that both parties involved in the transaction fulfil their obligations. The author further validates the robustness and soundness of their protocol using BAN logic, the Scyther tool, and AVISPA, providing formal proofs for its security. The author also claim that their protocol is lightweight and can resolve disputes that may arise during a transaction.

In different area of NFC application, in recent years, there have been numerous experiments with NFC application services worldwide, with the micropayment service being the most frequently referenced. In a technical sense, micropayments simulate mobile devices, such as cell phones, into stored value cards through card emulation mode and deduct money from the external card readers of stored value cell phones. Read-write mode enables devices to read or write external cards, with the exception of simulating cell phones into stored value cards. Consequently, in the context of micropayments, cell phones can function as point-of-sale (POS) devices. It is capable of reading the balances of external cards, deducting money, and storing value. In addition to the reading and writing of NDEF information in cards, key management is a critical issue that must be addressed when considering the use of NFC cell phones as mobile POS devices [25].

In another study, [26] in their research demonstrates how NFC, designed for secure short-range communication, is vulnerable to relay attacks. The authors successfully implemented a relay attack on NFC-enabled mobile phones using publicly available APIs and without needing access to secure program memory or code signing. They achieved this by developing and installing specific MIDlets on the attacker's NFC-enabled phones. The paper further discusses potential countermeasures to these attacks, particularly focusing on device location-based solutions. These countermeasures could also be applied to prevent relay attacks on contactless applications using 'passive' NFC on mobile phones.

In securing the NFC-enabled devices, it is utmost important to understand the design of the NFC-enabled device. [27] explains that the Secure Element (SE) is the security mechanism that enables the establishment of trust between the service provider and the device on mobile phones that are equipped with NFC. Additionally, the SE offers a secure environment for the storage of cryptographic keys and the hosting of sensitive applications. At present, there are three primary architectures for NFC. First, a SE is integrated into the phone as a standalone IC (Integrated Chip), which is an "independent" embedded hardware module. In the second option, the SE is integrated into the Universal Integrated Circuit Card (UICC). The Subscriber Identity Module (SIM), Universal Subscriber Identity Module ((U)SIM), and Removable User Identity Module ((R)UIM) are among the existing Subscriber Identity Application (SIA) modules. The third option involves the SE being implemented on a removable memory component, such as a Secure Digital card (Se-cure SD) or Secure Multi-Media Card (Secure MMC). The scope of their research does not encompass the discussion that compares the advantages and disadvantages of the aforementioned architectures.

It is crucial to acknowledge that the NFC standards do not stipulate any security services beyond the Signature Record Type Definition, which means that the security design is the responsibility of the application developer. The Signature RTD only specifies the method by which data is to be signed in order to guarantee data integrity and facilitate data authentication. This emphasize the need for a due diligence by the application developer and service providers to ensure the device and the software is secure by design.

[28] examines security vulnerabilities of Near Field Communication technology, particularly in Internet of Things applications. They highlighted that while NFC's short-range frequency is great for access control, its small tag size, unencrypted data transmission, and open communication channel expose it to attacks. [29] explains that there are three operational modes of NFC. First, is the Card Emulation Mode. In this mode, it allows all NFC-enabled devices to function as smart cards. It permits users to execute transactions such as transit access control, ticketing, and purchases. Second, is the reader/writer mode, in this mode, an NFC-enabled device is capable of reading the information recorded on the NFC tags that are embedded in smart posters and displays. Tag information that is recorded in the tag can be retrieved by the user for future use. Third, is the peer-to-peer mode that facilitates the exchange of information and the sharing of files between two NFC-enabled devices.

Findings from [30] concur the findings of the recent research whereby NFC has in inherent vulnerability issues. Although technology provider boasts on the short-range communication as secured, however, short-range communication doesn't guarantee security. While NFC's limited range (4-10cm) might seem like a security feature, it doesn't inherently protect against determined attackers. This is because NFC has an Open communication channel, therefore, the lack of strong encryption and authentication mechanisms in NFC communication makes it susceptible to eavesdropping and data manipulation. In addition is the miniature size and clear text format. The small size of NFC tags often limits the implementation of robust security features. Additionally, storing data in clear text increases the risk of data breaches. This finding corroborated by the study conducted by [31].

[32] proposed a secured-element (SE) policy that helps to enhanced the security of NFC-enabled devices. The proposed NSE-AA protocol is designed to be both lightweight and efficient, rendering it appropriate for IoT devices that are resource-constrained. Additionally, the authors implement a formal security assessment to illustrate the protocol's resilience in meeting the IoT Security Requirements. The IoT Security Requirements lists seven (7) security requirements in ensuring a secured communication between IoT Devices; (i) Confidentiality, (ii) Data Integrity, (iii) Mutual Authentication and Attestation, (iv) Privacy, (v) User Anonymity, (vi) Proof of Locality, and (7) Secure Storage.

In their framework of NFC Secured Element-Based Mutual Authentication and Attestation (NFA-AA), [33] underscore the following critical components: (i) to incorporate secured element during system design of the Mutual Authentication and Attestation to ensure that both the user device and the IoT device are authenticated prior to performing any data exchange, (ii) to utilize Trusted Certified Authority (TCA) to manage cryptographic credentials. The credentials must be stored in Secure Elements and cloud-based Trusted Platform Modules that are impervious to tampering on the devices. Locality of Proof is a unique form of proof of custody that is intended to ensure that the data is stored in close proximity to the key in order to facilitate efficient computation. The framework reduces the probability of man-in-the-middle attacks by attackers by leveraging the short-range communication capabilities of NFC to facilitate locality proof. [34] suggest that their framework can be integrated with existing security infrastructure and protocols to enhance the overall security posture of IoT ecosystems. This implies a need for future research on compatibility and seamless integration with common IoT security standards.

[35] emphasizes the significance of incorporating privacy by design principles into NFC applications to reduce potential risks such as unauthorized service initiation, location monitoring, and unwanted data collection. [36] highlights the inherent security features of NFC, including the need for close proximity user-initiated interactions in establishing connection between two devices. In managing the residual security and privacy risk, [37] advocate for the necessity of disabling NFC capabilities when the device is locked and to exercise cautions when granting users control over data sharing.

[38] recommends a specific Privacy by Design protocol for end-to-end security protection. For this, [39] emphasizes several critical methods for safeguarding NFC devices: (i) In order to establish a connection, NFC necessitates that device be within a few centimeters of one another as this complicates the process of data interception or relay attacks by assailants operating from a distance, (ii) Implement User-Initiated Interactions where each NFC transactions will necessitate user consent such as the act of tapping a phone on a reader. This safeguards against the occurrence of unauthorized transactions without the user's knowledge, (iii) the NFC capability should be automatically disabled when the device's screen or keyboard is locked. This safeguards against unauthorized access to NFC functionality when the device is not in use, (iv) End Users should have the capacity to wholly disable NFC functionality through their device's settings. This provides users with complete autonomy regarding the timing and manner of NFC usage, and (v) implements the use of tamper-resistant seals and digital signatures on NFC tags to guarantee data authenticity and prevent manipulation. [40] also emphasized that, despite the inherent security features of NFC technology, no system is entirely impenetrable. Therefore, End Users should remain vigilant regarding potential risks and adhere to the most effective mobile security practices.

In another study, [41] raises concerns about privacy infringement due to the lack of unlinkability between user messages and public keys in NFC standards. This could potentially expose user data and compromise privacy. [42] provides an example of data spoofing and frequency cloning. Consider the scenario in which an End User is required to utilize his or her NFC card to gain entry to a building. A malicious attacker could affix a small receiver to the gate RF reader and record the signal transmitted by a legitimate NFC card. In this scenario, a genuine NFC card perceives that it is transmitting signals to the reader when it approaches. In reality, the "recorder" is the one that is listening to the signal and attempting to create a copy. The adversary could then exploit this replica to perform actions such as cloning an NFC card or gaining access.

Although [43] applauded the use of Secured Element to enhanced the security of NFC-enabled devices, [44] argued that, in the absence of any security mechanism to safeguard its communication channel, NFC-enabled devices can still expose its End Users' privacy to the air citing the situation in Google NFC Device. The Secure Element (SE), which was devised by Google to be integrated into a Google NFC device, is not as secure as it appears as it is still susceptible to malware hazard. The Android operating system (OS) has been demonstrated to be susceptible to malware attacks, particularly the embedded SE. This vulnerability is particularly evident when malicious software attempts to access information contained in the SE through the OS. SHA256 is employed to hash the SE access PIN for rooted devices, which is then stored on the device rather than in the SE. The SE can be accessed by an adversary who is able to brute-force the PIN.

The literature review provides an extensive information pertaining to the security issues, the inherent vulnerabilities of NFC, and types of attacks on NFC during the read/write operation mode in understanding the technicalities of NFC vulnerabilities. However, these findings need to also be understood from the industry practical perspective as there are more variables happening dynamically in the real-life environment, something, that may not yet be understudied by academic researcher. Therefore, the records from the MITRE Common Vulnerabilities and Exposures database provide an in-depth insight on NFC security and vulnerabilities.

For this study, CVE-2020-15001 is selected as the anchor case study that was analyzed in detail. A significant vulnerability in Yubico YubiKey 5 NFC devices has been identified (CVE-2020-15001). This vulnerability occurs when the OTP application fails to verify access codes during the configuration update process, potentially resulting in a loss of confidential information. This vulnerability enables malicious actors to circumvent security measures and obtain unauthorized entry to saved OTPs and passwords, thereby greatly affecting users who depend on these devices for secure authentication. In order to reduce this threat, Yubico has advised updating the firmware to secure versions and employing robust, distinct access codes.

[45] has remedied this vulnerability by advising consumers to update their firmware to releases that fix this issue. For the purpose of preventing unwanted access, users should make sure that their YubiKey 5 NFC devices are running the most recent firmware. In addition, the business issued a comprehensive security advice that outlines specific measures to protect vulnerable devices. These measures include installing the most recent updates and implementing robust, distinct access codes for OTP configurations. Nevertheless, the efficacy of these mitigation techniques is strongly dependent on user intervention, as users must actively install firmware upgrades to safeguard their devices. This highlights the crucial need of users being watchful and attentive in order to ensure the security of their devices. Neglecting to update the firmware exposes devices to this vulnerability, highlighting the continuous requirement for users to be knowledgeable and promptly take measures to protect their devices. From this case, it also illustrates the practical challenges associated with ensuring all users update their devices promptly. The reliance on users to apply firmware updates exposes a critical gap in the security chain.

From the industry security standard, The Microsoft Zero Trust Policy [46] is a modern security framework specifically developed to handle the intricacies of the current digital landscape, encompassing cloud migration, hybrid workspaces, and varied device utilization. The policy is based on the idea of "never trust, always verify," which means that any request, regardless of its origin, is considered a possible threat. The policy is grounded in three fundamental principles; (i) explicit verification, (ii) least-privilege access, and (iii) the presumption that a breach has occurred. The Microsoft Zero Trust Policy however, focuses more businesses, enterprises, and organizations, especially ones that are running their digital infrastructure on cloud-based infrastructure. Although the policy covers the governance of End-User Computing (EUC), these EUCs are mostly enterprise owned devices. For End-Users, only registered devices under Bring-Your-Own-Device (BYOD) program are being monitored and managed as part of the Zero Trust Policy implementation. Thus, the gap still persists between End User Level at personal level and End User Level at Enterprise Level. This is because the personal devices owned by individuals are not entitled the access to any sophisticated security operations.

Literature Gaps

There has been a significant amount of research that concentrates on identifying security breaches and how users respond to notifications, with the assumption that the remediation procedures shall work as planned. But, it's necessary to go further and look at the security and efficacy of the repair methods themselves, especially in terms of making sure that any access held by the attacker is terminated. Expanding research beyond password reset scenarios and encompassing a broader range of web services and remediation mechanisms are also crucial. Although there has been research on account recovery mechanisms, however, it often focuses on specific aspects like authentication schemes and password reset strategies, therefore, a broader understanding of the security implications of the entire remediation process is needed [47]. This includes examining the effectiveness of diverse remediation mechanisms in different contexts and identifying potential vulnerabilities in the remediation mechanisms provided by NFC-based service providers, in some cases, although there is a re-authentication procedure post-compromise rendering, some sessions are inaccessible and attacker access irreversible. This highlights the need for a more robust, user-centric recovery strategy.

Despite significant advancements in NFC security prevention strategies, post-compromise recovery is still largely unexplored in the research. Instead of providing NFC systems with defined recovery processes to follow after a compromise, the majority of research concentrates on preventing breaches. One of the significant gaps in post-compromise recovery for NFC systems is the need for incident response frameworks created especially for NFC environments. A significant gap in NFC security literature pertains to behavioral factors influencing user compliance with security protocols. While many studies focus on technical aspects of NFC security, fewer explore how end-user behavior impacts the effectiveness of these security measures.

In terms of encryption technique, compared to standard IT systems, NFC environments need more flexible and lightweight solutions due to their smaller scope and resource limitations. NFC technology, often used in mobile payments and access control, operates in resource-constrained environments, making lightweight encryption techniques crucial for balancing device security and device performance.

In addition, there is a lack of research on forensic investigation after an NFC system breach, with few articles describing methods for identifying the root cause of compromises to prevent future attacks of this kind. Finally, current research does not offer suggestions on how service providers should effectively communicate post-compromise risks and recovery actions to end users, which affects post-attack mitigation measures and user trust. Consequently, procedures for user support and notifications are not sufficiently handled. The development of formal post-compromise frameworks for NFC environments especially ones that are scalable and flexible enough to accommodate a range of use cases, such as access control and mobile payments is necessary to close these gaps.

Recent Advancement in Post-Compromise Recovery Security

Trusted Execution Environment (TEE) offers isolated environments for protecting sensitive computations and data. To counter the growing potential of Trusted Execution Environment compromises, [48] presented TokenWeaver, a new technology for secure remote attestation in TEEs by offering robust privacy guarantees in addition to Post-Compromise Security. TokenWeaver presents an innovative post-compromise recovery method featuring a dual token chain system. The linkable chain enables quick detection and revocation of compromises, while the unlinkable chain ensures user privacy during attestation. By using one-time authorization tokens, TokenWeaver reduces the risk of token theft, as stolen tokens become invalid for future authentication. It also employs blind signatures to secure privacy during certificate issuance, preventing the TEE provider from associating tokens with individual users. Furthermore, TokenWeaver includes clone detection and active revocation capabilities, utilizing an optional out-of-band channel to allow users to regain control of compromised TEEs.

Despite these strengths, TokenWeaver faces challenges, such as relying on external out-of-band (OoB) mechanisms for revocation, which may not always be dependable, and the risk of metadata leakage (e.g., IP addresses) during attestation, which could affect user privacy. While technical solutions like TokenWeaver offer robust protection for Trusted Execution Environments (TEEs), its effectiveness hinges on user practices. To ensure the efficacy of the technology, there is still a need for interactive security awareness programs and behavioral interventions are essential for enhancing user understanding and promoting secure device management to mitigate threats such as social engineering.

2.2 PROTECTION MOTIVATION THEORY (ROGERS, 1975)

[49] presented Protection Motivation Theory (PMT), initially proposed by [50] in their book. PMT is a psychological framework designed to understand the processes involved in individuals' motivation to protect themselves against perceived threats. The theory integrates concepts from both cognitive and emotional perspectives to explain how people decide to engage in protective behaviors. At its core, PMT suggests that the motivation to protect oneself is influenced by four key components: perceived severity, perceived vulnerability, response efficacy, and self-efficacy [51].

Perceived severity and perceived vulnerability are two threat appraisal processes central to PMT. Perceived severity refers to an individual's assessment of the seriousness of the threat, while perceived vulnerability denotes their perceived likelihood of experiencing the threat. Higher levels of perceived severity and vulnerability are thought to increase an individual's motivation to adopt protective behaviors. For instance, in the context of cybersecurity, if users perceive a high risk of identity theft and consider it a severe consequence, they are more likely to take actions to secure their personal information.

Response efficacy and self-efficacy are the coping appraisal processes in PMT. Response efficacy is the belief that the recommended protective action will effectively mitigate the threat, whereas self-efficacy refers to the individual's confidence in their ability to perform the protective behavior. Together, these factors determine whether an individual believes they can successfully implement the necessary protective measures. In the context of information security, if users believe that using strong passwords (response efficacy) and feel confident in their ability to create and manage them (self-efficacy), they are more likely to adopt such practices.

The theory posits that individuals are motivated to protect themselves based on four constructs: perceived severity, perceived vulnerability, response efficacy, and self-efficacy. In the realm of information security, PMT can be particularly effective in explaining and predicting how users respond to potential threats and the measures they adopt to safeguard their data and devices. In the context of NFC Vulnerabilities and NFC End Users, perceived severity and perceived vulnerability are critical elements of PMT that influence how NFC end users assess the potential impact of security threats.

Perceived severity refers to the users' assessment of the seriousness of the consequences if their NFC-enabled devices are compromised. For example, users who believe that their financial data could be significantly harmed by NFC vulnerabilities are more likely to engage in protective behaviors. Perceived vulnerability, on the other hand, is the users' perception of the likelihood of encountering such threats. In the case of NFC technology, users who perceive a high likelihood of being targeted by spoofing attacks or unauthorized data access are more likely to adopt stringent security measures. PMT thus provides a robust framework for designing interventions aimed at enhancing individuals' protective behaviors by addressing both their threat perceptions and their coping capabilities.

3. METHODOLOGIES

3.1 CONCEPTUAL MODEL OF THE RESEARCH

The conceptual model functions as a detailed plan for analyzing the dynamics of NFC vulnerabilities, security solutions, End-User awareness. Protection Motivation Theory (PMT) has been incorporated into the conceptual model to systematically study these aspects. PMT establishes a theoretical framework for comprehending the cognitive processes that motivate individuals to implement protective behaviors in response to perceived hazards. By including PMT, the model takes into account the psychological factors that influence user behavior in addition to the technical aspects of NFC security. Through this comprehensive methodology, comprehensive security solutions are developed with consideration for both technical and human factors. Figure 1 illustrate how the PMT is adapted for NFC End-Users. Self-efficacy refers to an individual's confidence in their ability to successfully perform a specific behavior. In the context of NFC security, an example of self-efficacy would be a user's confidence in their ability to configure and use NFC-enabled devices securely. This could involve setting up strong passwords, updating firmware regularly, and understanding how to recognize and avoid potential security threats. Whereas, response cost pertains to the perceived inconveniences or expenses linked to the protective behavior. An instance of response cost in the realm of NFC security may be the perceived inconvenience and time needed to consistently upgrade the firmware or software of the device in order to rectify security vulnerabilities. For example, a user may find it hard and time-consuming to regularly upgrade the firmware of their NFC-enabled devices. This could potentially discourage them from keeping their security measures up to date, despite the advantages. This PMT explains how response efficacy, self-efficacy, and response cost interact to influence the user's motivation to adopt protective behaviors in the context of NFC security.

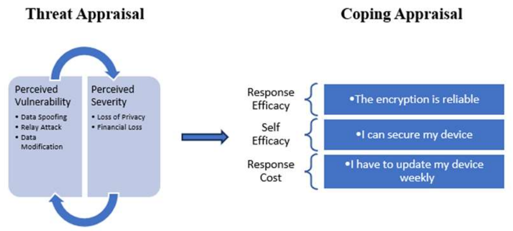


Figure 1: Protection Motivation Theory for NFC End User

The literature review has identified several vulnerabilities associated with Near Field Communication (NFC), such as spoofing, relay attacks, tag tampering, cloning, data corruption, and eavesdropping. These vulnerabilities provide substantial risks to the integrity and security of NFC communications. From the literature review, it has identified many security measures, including access control mechanisms, encryption techniques, and authentication procedures, that are crucial for mitigating these threats. Furthermore, the literature emphasizes how crucial user awareness are in influencing the adoption and efficacy of NFC security measures. The conceptual model functions as a detailed plan for analyzing the dynamics of NFC vulnerabilities, security solutions, End-User awareness.

Protection Motivation Theory (PMT) has been incorporated into the conceptual model to systematically study these aspects. PMT establishes a theoretical framework for comprehending the cognitive processes that motivate individuals to implement protective behaviors in response to perceived hazards. By including PMT, the model takes into account the psychological factors that influence user behavior in addition to the technical aspects of NFC security. Through this comprehensive methodology, comprehensive security solutions are developed with consideration for both technical and human factors. Figure 2 depicts the Research Conceptual Model of this study. The key elements in this research conceptual model are (i) NFC Vulnerabilities, (ii) Security Measures, (iii) User Perceptions, and (iv) post-compromise recovery policy for NFC End-Users. The Protection Motivation Theory inter-connects the themes, illustrating how threat appraisal and coping appraisal influence users' protective behaviors.

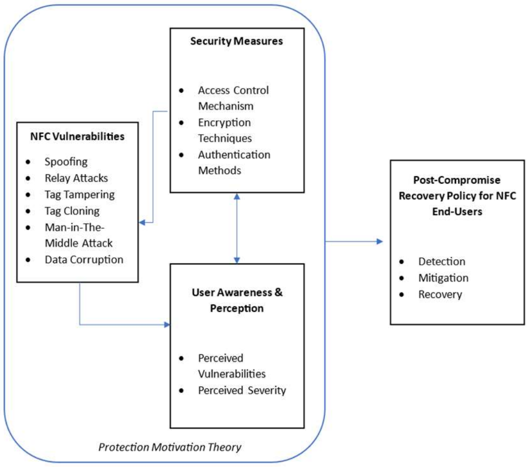


Figure 2: Research Conceptual Model for the Study

For the research methodology, Figure 3 depicts the conceptual framework of research methodology that underscore this study, which outlines the primary components and how the integration from the two components constructs the security awareness and vulnerabilities concerning NFC technology's security. The research methodology is structured around a conceptual framework that integrates security awareness and vulnerabilities in NFC technology. This framework guides the study by exploring how these elements affect the security and reliability of NFC. The approach combines a qualitative literature review and an end-user survey to provide insights into NFC security issues, focusing on data spoofing and access control. The survey gathers primary data on user awareness, perceived security, and trust in NFC technology, along with post-compromise recovery strategies. This integration ensures the study addresses the key issues identified in the literature, strengthening the research's relevance by aligning theory with real-world user experiences.

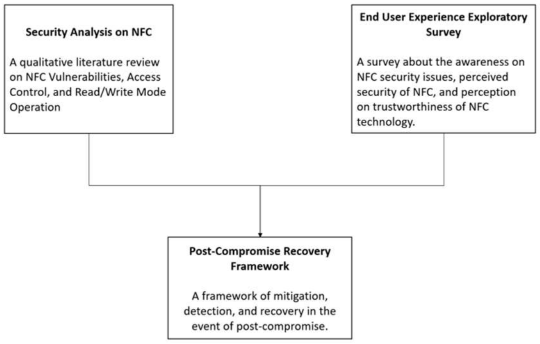

Security Analysis on NFC
A qualitative literature review on NFC Vulnerabilities, Access Control, and Read/Write Mode Operation
End User Experience Exploratory Survey
A survey about the awareness on NFC security issues, perceived security of NFC, and perception on trustworthiness of NFC technology.
Post-Compromise Recovery Framework
A framework of mitigation, detection, and recovery in the event of post-compromise.

Figure 3: Conceptual Framework of the Research Methodology

3.2 STUDY DESIGN

The study employed a mixed-methods approach, combining a literature review and an end-user survey. An exploratory approach was utilized to assess user perceptions of NFC technology awareness, security, and trustworthiness. Thematic synthesis was used to qualitatively analyze and report patterns within the data, offering a comprehensive view of NFC security vulnerabilities by aggregating findings from multiple sources.

This approach facilitated meaningful conclusions and a cohesive narrative to address the research questions. An exploratory method was utilized to assess user perceptions of NFC technology awareness, security, and trustworthiness. Data was collected via an online survey distributed through Google Forms, which allowed for broad and efficient access. This approach enabled the identification of key themes and patterns, providing valuable insights for future, targeted research. The survey included 30 items in a single questionnaire.

The study was conducted in Kuala Lumpur, an urban city with a high density of technology-savvy residents who are likely to use NFC-enabled devices. The urban setting provides a suitable context for examining the use of NFC technology, as residents are more likely to adopt and interact with such technologies in their daily lives. The data was then analyzed using quantitative analysis. Correlation analysis was used to assess the relationships between ordinal variables, such as NFC device usage frequency and security perceptions. Spearman's Rank Correlation was specifically applied to evaluate non-linear relationships between these variables, given that they are ordinal in nature. Appendix C summarizes the result of the hypotheses testing.

4. RESULTS

4.1 RESULTS OF QUALITATIVE LITERATURE REVIEW ON NFC SECURITY AND VULNERABILITIES

The identified themes for types of NFC threats can be summarized into three base themes (i) Communication Channel Vulnerabilities or the infrastructure level, (ii) Device Level Vulnerabilities or the System Level, and (iii) Service Provider Level vulnerabilities. The identified theme for NFC Security is Protective Mechanism which can be refined as Access Control Mechanism in securing the NFC-enabled devices and communication channel. These themes are validated with the findings from the MITRE CVE database. One theme is the result of data synthesis, (i) End User Level and the sub-themes User Interaction and Awareness. These identified themes were referred to as the baseline security issues in the NFC Security Policy development. Table 1 summarizes the result of the Qualitative Literature Review. The results from the scholarly research are validated with the real-life case as recorded in the MITRE CVE database. By organizing these security vulnerabilities into pertinent themes, a more comprehensive view and understanding of the diverse facets of NFC vulnerabilities helped the researcher in the policy development with targeted protective actions.

Table 1: Identified Themes of Key Security Issues in NFC Vulnerabilities

Category of Theme	NFC Security Themes from Literature Review	NFC Security Themes from MITRE CVE Database
Communication Channel Vulnerabilities	Data Spoofing and Data Interception	Denial of Service
	Data Corruption and Data Modification	Information Leak
Device Level Vulnerabilities	Relay Attacks on the Device	Arbitrary Code Execution
	Tag Tampering and Tag Cloning	Unauthorized Memory Write Access
		Stack Overflow

		(impacting Service Availability)
		Uncaught Exceptions (*impacting NFC application availability)*
		Remote Code Execution
		User-After-Free *(Memory Management)*
		Unauthorized Memory Write Access
Service Provider Level	Authentication and Attestation	Improper Authentication – Weak Attestation Protocol
Access Control Mechanism	Cryptographic Techniques	Improper Authentication
	Secure Element (SE)	Uninitialized Value Access
	NFC Communication Protocol	
NFC End User	Awareness of NFC Vulnerabilities	User Interaction and Awareness of Baseline Security

4.2 RESULTS AND INSIGHTS FROM THE END USER NFC AWARENES, EXPERIENCE, AND PERCEPTION SURVEY

a) *Awareness and Usage of NFC Technology*

From the result of the study, the majority of respondents were aware of NFC technology and used it for a variety of activities, including data sharing and mobile payments. Nevertheless, the extent of precise understanding regarding certain security vulnerabilities linked to NFC technology differed and the level of security awareness on the vulnerabilities of NFC is not in-depth. Although a large number of users understood the basic idea of NFC, less were aware of the specific threats and vulnerabilities, like data spoofing and relay attacks. The lack of comprehensive knowledge in this area emphasizes the necessity for focused educational initiatives aimed at improving consumers' comprehension of the security threats associated with NFC. Additionally, the results indicated a positive relationship between users' trust in the technology and how frequently they used NFC devices, indicating that increased familiarity and confidence are gained through continuous use.

This understanding is crucial for legislators and service providers as it emphasizes the need of user education in guaranteeing the secure and efficient use of NFC technology. Stakeholders may greatly improve the security of NFC End Users by creating thorough educating programs that provide detailed information about specific hazards and effective methods to reduce them. Furthermore, recognizing the positive relationship between increased usage and better trust might assist in formulating security awareness campaign to promote more frequent utilization, hence enhancing overall NFC End User assurance in the technology. In the digital economy, this is especially important since NFC transactions' speed and ease facilitate the transition to a cashless world and make daily tasks like shopping, traveling, and using services more efficient and secured.

c. *Perceived Security and Trust in NFC-based Transaction*

User perceptions of security and trust in NFC-based transactions were critical aspects explored in the survey. The findings indicated a moderate positive association between users' confidence in the security of NFC transactions and their trust in the overall security measures used in NFC technology. This suggests that individuals who experience a sense of security during each transaction are more likely to possess a greater level of overall trust in the technology. Nevertheless, it was observed that being knowledgeable about particular security measures, such as the NFC attestation process, did not substantially increase trust. This implies that better communication of the advantages of these measures is necessary to establish NFC End Users' level of confidence. Knowing that confidence in individual transactions might lead to a deeper trust in technology emphasizes the need for focused attention in this important area.

Service providers and developers should prioritize improving the security of individual transactions and effectively conveying these security measures to users. Providing evidence of the efficacy of security mechanisms in daily transactions can greatly enhance general confidence. Moreover, by ensuring that users comprehend the attestation process and its advantages, it is possible to narrow the divide between technical security measures and user perceptions of safety. Service Providers need to consistently inform users with the latest security protocols and enhancements. Frequent communication can help consumers understand the value of security and stay up to date on the newest threats and defense techniques. The continued success and widespread adoption of cashless payment systems rely on the preservation of a strong level of trust in NFC-based transactions within the broader context of the digital economy. In addition to the product specific security awareness, in order to reduce the risks related to NFC vulnerabilities, it is essential to include a Security by Design strategy in the system design. This entails including security safeguards at each phase of the development lifecycle, guaranteeing that security is an intrinsic element rather than an oversight.

d. *Concerns and Awareness on NFC Security Risk*

The survey showed a significant correlation between users' knowledge of NFC security issues and their apprehension regarding particular dangers such as data spoofing. This discovery emphasizes the significance of awareness for improving NFC End Users' perceptions of risk. Users with a higher level of knowledge regarding potential security risks are also more inclined to be worried and implement preventive steps. Nevertheless, the total degree of comprehensive understanding was determined to be insufficient, highlighting a crucial area that requires enhancement. By using focused educational and communication tactics, we may increase awareness and reduce these concerns, leading to better security practices among NFC End Users.

This discovery serves as a strong incentive for stakeholders to create and execute comprehensive teaching programs and campaigns with the goal of increasing End Users' knowledge regarding the security issues associated with NFC. By furnishing consumers with comprehensive information regarding specific hazards and offering practical measures to alleviate them, it is feasible to cultivate a user base that is more vigilant about security. Adopting this proactive strategy can result in improved security practices and a decrease in susceptibility to threats, ultimately strengthening the overall security posture surrounding the usage of NFC technology. For example, NFC End-Users should be aware of the security risks in each type of NFC-enabled devices that they are using such as keyless car entry system, building keyless entry system, smart home keyless door lock system. Not only Service Provider, the reseller of these NFC-enabled devices must hold due diligence to fully explain what are the associated risk of each system and educate NFC End Users of the expected preventive measures that must be performed daily, weekly, or monthly to ensure that the system security is in optimum secured performance.

e. *Familiarity with Post-Compromise Recovery Strategies*

The survey also examined the significance of methods for recovering from post-compromise incidents. The results showed a substantial correlation between NFC End Users' trust in service providers' recovery measures and their confidence in their own abilities to recover from a security compromise related to NFC. This indicates that both institutional and personal variables contribute to determining users' perceptions of the effectiveness of recovery. Nevertheless, there was a large consensus among the respondents regarding the significance of implementing strong post-compromise rehabilitation strategies, emphasizing the requirement for thorough and well-articulated recovery plans. The significant correlation between an individual's self-assurance in their ability to recover and their trust in the tactics employed by service providers indicates that users require a sense of empowerment and knowledge regarding the recovery procedures. Service providers should prioritize educating users about the actions they can take in case of a breach and ensure that recovery plans are clear and easily available. By promoting a cooperative strategy for security that engages both users and service providers, it is feasible to establish a stronger NFC security framework. Communication pertaining to post-compromise recovery strategies must no longer be passive in nature but must be reformed to be dynamic as to allow NFC End Users to have active participation. This is especially crucial in the digital economy, where the speed and efficiency of post-compromise recovery can have a substantial influence on the overall stability of cashless transaction systems and user trust.

f. *Comparative Analysis with Existing Literature*

When the survey results are compared to the existing literature, several similarities and some new insights are revealed. The extensive but superficial comprehension of NFC technology among users is consistent with prior research that has underscored the necessity of enhanced user education regarding security risks [52],[53]. The Protective Motivation Theory, which asserts that perceived vulnerabilities and perceived severity are the elementary conditions that influence NFC End User's coping appraisal. This also supported by the correlation between frequent use and increased trust.

However, the absence of significant differences in awareness based on demographic factors is in contrast to earlier studies that posit that demographic variables can influence the adoption of technology. This discovery implies that NFC technology may have attained a degree of widespread usage that is not as noticeable among various demographic differences. Additionally, the emphasis on post-compromise recovery strategies is in accordance with the most effective cybersecurity practices such as NIST Cybersecurity Framework [54] and Microsoft Zero Tolerance Model [55] which emphasize the necessity of comprehensive incident response plans to effectively manage and mitigate the consequences of security intrusions. [56] In a recent related study, highlight the need for service providers to enhance their authentication mechanism to better protect against cyber threats, particularly to rectify inadequate remediation mechanisms as many service providers incorrectly implement remediation methods, making it difficult to revoke attacker access post-compromise. Appendix C presents the overall result of the Hypothesis Testing.

5.3 PRACTICAL IMPLICATIONS

a) Security by Design

The practical implication of the insights is to inculcate DevOps Security as early as possible. DevOps Security is a philosophy that combines three scopes of disciplines; development, operations, and security [57]. This process includes the prompt identification and resolution of vulnerabilities through the implementation of comprehensive unit and functional testing within continuous integration/continuous delivery pipelines. Developers, End Users, and Stakeholders must participate in consistent technology awareness programs and security training to remain informed about the most recent threats and best practices. These precautions are essential for protecting NFC applications, including smart home access locks, vehicle keyless systems, and access control systems, from potential vulnerabilities. Robust security protocols and user awareness can substantially reduce the risks associated with NFC technology.

4. End-User Level Security Policy for NFC End Users

The NFC End-User Level Security Policy is designed to safeguard end users against NFC-related security threats, including data spoofing, relay attacks, and unauthorized data access. The primary objectives of this policy are to improve security awareness, take proactive steps, and make sure that sufficient post-compromise recovery mechanisms are in place. The policy is in alignment with the Microsoft Zero Trust principles [58], but it is specifically customized to address the distinct issues and vulnerabilities related to NFC technology at the End-User level.

6.0 RECOMMENDATIONS

6.1 NFC SECURITY POLICY FOR NFC END USERS

There is a substantial importance to address the gap in the security chain between the NFC End Users, and the NFC Services. Integrating the key insights derived from the end-user NFC awareness, experience, and trust perception survey, along with the broader thematic analysis conducted in earlier chapters, this policy is hope to complement the existing security policies that are available in the industry. For this study, policy and framework are defined as follows:

a) A policy can be defined as a formal statement of a set of principles that is expected to be observed to by its intended audience. Each policy should address a critical issue that is relevant to the overarching objective [59].

b) A framework can be defined as a collection of rules, concepts, or convictions that are employed to determine or plan an action [60]. In other words, a framework provides a blueprint as how the policy can be implemented.

The target audience of this policy are policymakers at business level or at community level, and NFC End Users

(i) For policymakers, the recommendations focus on creating regulations that emphasize security by design for NFC-enabled devices and services, along with guidelines for continuous monitoring and updating of security measures.

(ii) For end users, the study provides practical advice on secure NFC practices, including regular updates, enabling strong authentication mechanisms, and recognizing potential threats

The Microsoft Zero Trust Policy is primarily intended for enterprise ecosystem, with a specific emphasis on ensuring complete security across several network levels. In complementary, the recommended NFC End-User Level Security Policy is specifically tailored for individual users. The primary distinctions encompass:

(i) The Microsoft Zero Trust Policy covers security at the enterprise level, including networks, apps, and infrastructure. Meanwhile, the NFC End-User Level Security Policy only deals with end-user interactions using NFC technology.
(ii) The NFC Security Policy is focused on User-Centric actions as The NFC policy prioritizes user education, awareness, and practical security actions that individuals may take, which include enabling multi-factor authentication (MFA) for device login, and regularly updating their devices.
(iii) The NFC policy specifically targets dangers related to NFC technology, such as relay attacks and data spoofing. These threats may not be the main concern of the broader Microsoft Zero Trust Policy.

The NFC End-User Level Security Policy serves as a connection between security rules at the enterprise level and the activities of individual users by enhancing Enterprise-level cybersecurity measures. While organizations incorporate the Microsoft Zero Trust principles on a larger scale, the NFC policy ensures that End Users also adhere to secure procedures, thereby establishing a unified security framework. The NFC policy aims to reduce hazards caused by user behavior, which cannot be fully addressed by corporate policies alone, this is achieved by prioritizing user education and awareness. The NFC policy offers relevant instructions for End Users to safeguard their NFC-enabled devices, enhancing the overall security measures implemented by the organization. The NFC Security Policy for NFC End Users are developed using the Microsoft Zero Trust Policy as the reference framework, based on the insights from the survey, and the literature review. Appendix D presents the NFC Security Policy in the policy format and structure accordingly. Policymakers and NFC End Users may refer to this policy as part of the Information Security Assurance and Information Governance campaign.

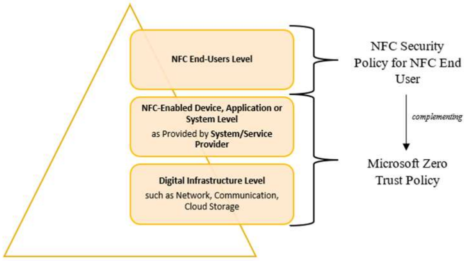

NFC End-Users Level
NFC-Enabled Device, Application or System Level
as Provided by System/Service Provider
Digital Infrastructure Level
such as Network, Communication, Cloud Storage
NFC Security Policy for NFC End User
complementing
Microsoft Zero Trust Policy

Figure 4 The target audience of the NFC Security Policy

Based on Figure 4, the security triad can be classified into three levels:

(i) Digital Infrastructure Level

This is the backbone of all digital technology, encompassing the fundamental hardware and software systems that support NFC technology. In this level, servers, cloud services, and network architecture are integrated to guarantee the uninterrupted operation and security of NFC-based applications. Security at this level necessitates resilient cloud infrastructure, secure server configurations, and robust network security protocols to prevent data breaches and unauthorized access. This is the most effective application of the Microsoft Zero Trust Policy.

(ii) NFC-Enabled Device, Application, or System Level

At this level, the infrastructure is utilized by system or service providers to deliver NFC-based services. Smartphones, point-of-sale terminals, access control systems, and any other devices or applications that utilize NFC technology are included in this category. Application security testing, secure software development practices, and device integrity are the primary security measures at this level. Service providers must guarantee that their systems are resistant to attacks such as spoofing, relay attacks, and unauthorized data access.

(iii) NFC End-Users Level

This level pertains to the usage of NFC-based services by end users. At this stage, the commodity of exchange is the end users' personal information, financial information, and other personal identifier data. At the end-user level, security measures prioritize user education, secure usage practices, and awareness of potential hazards. Users must be informed about the importance of enabling security features on their devices, regularly updating software, and recognizing phishing attempts and other malicious activities.

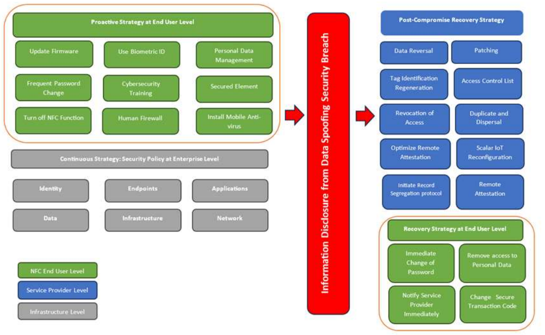

Proactive Strategy at End User Level
Update Firmware
Use Biometric ID
Personal Data Management
Frequent Password Change
Cybersecurity Training
Secured Element
Turn off NFC Function
Human Firewall
Install Mobile Anti-virus
Continuous Strategy: Security Policy at Enterprise Level
Identity
Endpoints
Applications
Data
Infrastructure
Network
NFC End User Level
Service Provider Level
Infrastructure Level
Information Disclosure from Data Spoofing Security Breach
Post-Compromise Recovery Strategy
Data Reversal
Patching
Tag Identification Regeneration
Access Control List
Revocation of Access
Duplicate and Dispersal
Optimize Remote Attestation
Scalar IoT Reconfiguration
Initiate Record Segregation protocol
Remote Attestation
Recovery Strategy at End User Level
Immediate Change of Password
Remove access to Personal Data
Notify Service Provider Immediately
Change Secure Transaction Code

Figure 4 The Proposed NFC Security Framework for NFC End Users

Figure 5 depicts the NFC Post Compromise Security Framework for NFC End Users covers the end-to-end spectrum of security breach, prior and after, providing End users with a concise action to be taken proactively and reactively. There are four scopes of action group (i) proactive action by NFC End Users, (ii) continuous actions at Infrastructure Level, (iii) reactive action at System Level or Service Provider Level, and (iv) reactive action by NFC End-Users. However, the focus area of discussion on this recommended framework is denoted within the box in the Figure 5, as the action items at Infrastructure Level and Service Provider level are covered in depth by Microsoft Zero Trust Policy.

Appendix E summarizes the proactive strategy at NFC End User Level. In an effort to fortify the security of NFC at the end-user level, a variety of proactive strategies are advised. By consistently updating firmware, devices are safeguarded with the most recent security upgrades, which mitigate known vulnerabilities. The security of biometric authentication, such as facial recognition or fingerprint authentication, is superior to that of conventional passwords due to the fact that biometric IDs are specific to each individual. Next, regularly reviewing and adjusting privacy settings is a key component of effective personal data management, as it reduces the risk of data compromise by minimizing information exposure.
Frequent password changes are beneficial in safeguarding accounts from unauthorized access, thereby reducing the likelihood of password compromise over time. Participating in cybersecurity training programs can enhances user awareness and knowledge, thereby allowing them to recognize and circumvent potential security hazards. Secured elements within NFC devices are implemented to ensure that sensitive data is stored in a manner that is both tamper-resistant and robust. Additionally, the functionality of NFC devices must be disabled when they are not in use to prevent fraudulent access. In order to increase user vigilance, or to function as a "human firewall," it is necessary to exercise caution when sharing personal information and to avoid suspicious links or downloads. Finally, malware and other cyber threats are further safeguarded by updating and installing mobile anti-virus software on a regular basis.

Appendix E summarizes the reactive strategy at NFC End User Level. In order to mitigate the consequences of security breaches and guarantee the ongoing protection of personal data and accounts, it is crucial to establish a comprehensive recovery strategy at the End-User level. In the aftermath of a compromise, it is important for NFC End Users to modify their passwords as soon as possible. By preventing unauthorized access to accounts, this ensures that attackers who may have obtained old credentials are unable to use them. Timely password updates act as a first line of defense in securing accounts post-breach. NFC End Users must also revoke access to personal data in conjunction with password management. By removing permissions or access to sensitive information, users can curtail the extent to which an attacker can misuse compromised data. This measure is essential for the protection of privacy and the mitigation of potential harm by preventing the further exploitation of personal information.

Another critical step in the recovery process is promptly notifying the service provider. Once a compromise is identified, NFC End Users must promptly notify their service providers in order to enable them to take the necessary steps to reduce its impact. This may involve the temporary suspension of services to prevent further harm, the issuance of additional security advisories, or the enhancement of monitoring for suspicious activities. Prompt notification enables a coordinated response that can considerably improve security measures and reduce the overall effect of the breach. Furthermore, secure transaction credentials must be updated to ensure the security of financial transactions following a breach. By updating these codes, future financial activities are safeguarded from the possibility of unauthorized transactions being conducted using the compromised codes or device or application. Collectively, these recovery strategies allow NFC end-users to effectively mitigate the consequences of security breaches. In summary, Information Owners can safeguard their personal information and accounts from further unauthorized access by implementing swift and proactive measures, including revoking data access, updating transaction codes, notifying service providers, and changing passwords frequently.

6.2 PROPOSED IMPLEMENTATION STRATEGY

The policy and framework can be implemented and rolled out to the public in general and the NFC End Users in specific through the recommended strategy:

a) Collaborative User Education and Awareness

Improving user awareness is crucial for enhancing the security of NFC-enabled devices and mitigating risks associated with data spoofing and other vulnerabilities. It is essential to create educational materials that are comprehensive. These should encompass FAQs, guides, and tutorials that provide a comprehensive explanation of the potential hazards, applications, and uses of NFC technology. Complex information can be rendered more engaging and comprehensible through the use of visual aide, including infographics and videos. In addition, NFC End Users can identify phishing attempts, comprehend NFC data communication, and adopt secure usage practices by participating in regular security awareness workshops in both online and in-person formats. Establishing partnerships with educational institutions and community centers can expand the scope of these initiatives. By including security education in the onboarding process, it is guaranteed that all new users of NFC services have the opportunity and access to attend accessible training that provide wealth of information about the security of their devices, potential hazards, and NFC functionalities. The education and awareness of NFC End Users can be further enhanced by the development or promotion of mobile applications that offer real-time updates on NFC security threats, suggestions for safe usage, and supplementary learning tools for assessing the level of security of their NFC-enabled device.

b) Frequent Communication and Alerts

Clear communication and timely alerts are essential elements of an effective NFC security policy. Establishing a system for sending regular updates and alerts about the latest NFC security threats and vulnerabilities ensures that users stay informed and vigilant. Reaching a widespread audience can be facilitated by employing a variety of communication channels, including SMS, email, and app notifications. The implementation of interactive user interfaces in NFC-enabled applications that offer clear security-related messages, prompts to update security settings, or notifications during potentially risky situations can increase user awareness and encourage immediate action. Proactive reporting and response are fostered by the provision of user-friendly channels for reporting suspicious activities or security concerns related to NFC usage, such as a dedicated support line or in-app reporting feature. It is essential to maintain transparency in all communications concerning security issues. Trust is fostered and user engagement in security practices is encouraged by demonstrating the measures being taken to address vulnerabilities and the ways in which users can safeguard themselves.

c) Encouraging Personal Cybersecurity Best Practices Through Incentives

User engagement in NFC security measures can be substantially improved by rewarding secure practices. Offering incentives such as subscription discounts, rewards points, or recognition for participants who complete security training modules or demonstrate secure NFC usage practices can motivate users to adopt and maintain safe practices. By integrating assessments, challenges, and leaderboards, gamification can enhance End User engagement in NFC security education programs, rendering the study of NFC security both competitive and enjoyable. Additionally, offering certifications to users who successfully complete advanced security training or consistently exhibit secure NFC practices, and publicly acknowledging these users on company websites or social media platforms, can serve to encourage and recognize secure behavior. A comprehensive approach to NFC security necessitates collaboration with various stakeholders. Working closely with NFC device manufacturers and service providers ensures robust security features and effective communication to end users. By collaborating with cybersecurity experts, research institutions, and communities, it is possible to remain informed about the most recent threats and best practices, and to disseminate this knowledge to NFC End Users through consistent updates. By conducting public awareness campaigns that utilize social media, traditional media, and public events to disseminate information regarding NFC security and best practices, it is possible to further increase user awareness and foster a culture of security.

d) Policy Integration

The NFC Security Policy for NFC End Users should be formally incorporated into the overall Enterprise Security Policy, delineating the duties and responsibilities of a variety of stakeholders, such as service providers, manufacturers, and users. The policy should also establish metrics for evaluating the efficacy of these awareness initiatives, including user engagement rates, the completion of training programs, and feedback from users on their perceived level of security awareness. The policy's objective is to establish a more informed NFC End User base that is capable of identifying and addressing potential security concerns through the implementation of these strategies. This proactive strategy not only can improve the security of NFC transactions but also fosters a culture of responsibility and vigilance among users, thereby decreasing the likelihood of data hijacking and other cyber threats.

7.0 CONCLUSION

This study explored the security vulnerabilities inherent in NFC technology, with a particular focus on NFC End-User risks. Through a comprehensive literature review and an end-user survey, key themes in NFC vulnerabilities were identified, and the effectiveness of various security measures and existing post-compromise recovery strategies was evaluated. The findings highlight the critical need for targeted user education and a tailored security policy that bridges the gap between enterprise-level security frameworks and end-user practices. The proposed NFC End-user security policy, aligned with Microsoft's Zero Trust principles, is designed to create a more secure NFC ecosystem, ultimately enhancing user trust and safeguarding sensitive information in an increasingly interconnected digital landscape of wireless communication and technology.

7.1 CONTRIBUTION OF THE STUDY

This study contributes to the field of NFC security by addressing the critical gap in post-compromise recovery strategy, specifically focusing on end-user vulnerabilities and the development of a comprehensive NFC end-user security policy. While previous research has largely concentrated on preventing breaches and securing enterprise-level systems, this study shifts the focus toward the end-user environment. The study fills a crucial gap where most technical solutions overlook the human element of NFC security.

7.2 LIMITATION OF THE STUDY

The study’s focus on NFC technology awareness and recovery strategies may also vary across different regions, cultures, and technological environments. Findings may not fully generalize to populations with different levels of technology adoption or security awareness. Furthermore, the use of an online survey could exclude certain demographics, such as older adults or individuals with limited internet access, potentially biasing the sample toward those more comfortable with digital platforms. Online surveys often attract self-selected participants, who may have a particular interest in or experience with NFC technology, further skewing results. Additionally, while the study focused on an urban population, its findings may not extend to rural areas or different cultural contexts where NFC adoption and perceptions could differ.

7.3 FUTURE RESEARCH RECOMMENDATION

To enhance generalizability, future research should consider using a larger, more diverse sample and probability sampling methods. Validating the findings across various contexts and populations would ensure broader applicability. Researchers replicating this study might conduct in-depth testing on the demographic target. Additionally, future research could include experimental testing of the policy's effectiveness by simulating relay attacks on NFC-enabled devices within a population exposed to a targeted NFC Security Awareness campaign. This would allow for measuring how effectively end-users manage their NFC-enabled devices post-awareness training.

REFERENCES:

[1] Japertas, S., & Jankūnienė, R. (2020). NFC Vulnerabilities Investigation. In Distributed Computer and Communication Networks: Control, Computation, Communications:23rd International Conference, DCCN 2020, Moscow, Russia, September 14-18, 2020, Revised Selected Papers 23 (pp. 450-463). Springer International Publishing.

[2] Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2010). Practical NFC peer-to-peer relay attack using mobile phones. In Radio Frequency Identification: Security and Privacy Issues: 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010, Revised Selected Papers 6 (pp. 35-49). Springer Berlin Heidelberg.

[3] Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in next generation mobile payment systems: A comprehensive survey. IEEE Access, 9, 115932-115950.

[4] Egan, G. (2023, October 16). 2019 state of the Phish report: Attack rates rise, account compromise soars | Proofpoint US. Proofpoint. https://www.proofpoint.com/us/corporate-blog/post/2019-state-phish-report-attack-rates-rise-account-compromise-soars

[5] Mulliner, C. (2009, March). Vulnerability analysis and attacks on NFC-enabled mobile

phones. In 2009 International Conference on Availability, Reliability and Security (pp. 695-700). IEEE.

[6] Roland, M., Langer, J., & Scharinger, J. (2011, February). Security vulnerabilities of the NDEF signature record type. In 2011 Third International Workshop on Near Field Communication (pp. 65-70). IEEE.

[7] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[8] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11).

[9] Greenberg, A. (2021, June 24). NFC flaws let researchers hack ATMs by waving a phone. WIRED.https://www.wired.com/story/atm-hack-nfc-bugs-point-of-sale/

[10] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[11] MITRE. (2024). Common Vulnerabilities and Exposures. CVE -CVE. https://cve.mitre.org/

[12] Yubico. (2024, January 12). Security advisory YSA-2020-04. https://www.yubico.com/support/security-advisories/ysa-2020-04/

[13] Japertas, S., & Jankūnienė, R. (2020). NFC Vulnerabilities Investigation. In Distributed Computer and Communication Networks: Control, Computation, Communications: 23rd International Conference, DCCN 2020, Moscow, Russia, September 14-18, 2020, Revised Selected Papers 23 (pp. 450-463). Springer International Publishing.

[14] Dictionary of Computer and Internet Terms (2009): Dictionary of computer and internet terms (2009): Internet archive. (2017, January 24). https://archive.org/details/DictionaryOfComputerAndInternetTerms2009_201701

[15] Sethia, D., Gupta, D., & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. IEEE Transactions on Consumer Electronics, 64(4), 470-479.

[16] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[17] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[18] Roland, M., Langer, J., & Scharinger, J. (2011, February). Security vulnerabilities of the NDEF signature record type. In 2011 Third International Workshop on Near Field Communication (pp. 65-70). IEEE.

[19] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[20] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[21] Giwa, O. (2024, July 3). NFC TAG AUTHENTICATION: AN OVERVIEW. ResearchGate. https://www.researchgate.net/profile/Oluwaseyi-Giwa 2/publication/381990857_nfc_tag_authentication_an_overview/links/6689941d0a25e27fbc2f87e1/nfc-tag-authentication-an-overview.pdf

[22] Japertas, S., & Jankūnienė, R. (2020). NFC Vulnerabilities Investigation. In Distributed Computer and Communication Networks: Control, Computation, Communications: 23rd International Conference, DCCN 2020, Moscow, Russia, September 14-18, 2020, Revised Selected Papers 23 (pp. 450-463). Springer International Publishing.

[23] Japertas, S., & Jankūnienė, R. (2020). NFC Vulnerabilities Investigation. In Distributed Computer and Communication Networks: Control, Computation, Communications: 23rd International Conference, DCCN 2020, Moscow, Russia, September 14-18, 2020, Revised Selected Papers 23 (pp. 450-463). Springer International Publishing.

[24] Thammarat, C. (2020). Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol. Symmetry, 12(10), 1649.

[25] Cheng, H. C., Liao, W. W., Chi, T. Y., & Wei, S. Y. (2011, February). A secure and practical key management mechanism for NFC read-write mode. In 13th International Conference on Advanced Communication Technology (ICACT2011) (pp. 1095-1011). IEEE.

[26] Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2010). Practical NFC peer-to-peer relay attack using mobile phones. In Radio Frequency Identification: Security and Privacy Issues: 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9,

2010, Revised Selected Papers 6 (pp. 35-49). Springer Berlin Heidelberg.

[27] Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2010). Practical NFC peer-to-peer relay attack using mobile phones. In Radio Frequency Identification: Security and Privacy Issues: 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010, Revised Selected Papers 6 (pp. 35-49). Springer Berlin Heidelberg.

[28] Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology, 7(4.31), 298-305.

[29] Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology, 7(4.31), 298-305.

[30] Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology, 7(4.31), 298-305.

[31] Rios-Aguilar, S., Beltrán, M., & Rubén, G. C. (2021). Security Threats to Business Information Systems Using NFC Read/Write Mode. Computers, Materials & Continua, 67(3).

[32] Sethia, D., Gupta, D., & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. IEEE Transactions on Consumer Electronics, 64(4), 470- 479.

[33] Sethia, D., Gupta, D., & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. IEEE Transactions on Consumer Electronics, 64(4), 470-479.

[34] Sethia, D., Gupta, D., & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. IEEE Transactions on Consumer Electronics, 64(4), 470- 479.

[35] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[36] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[37] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[38] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[39] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[40] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[41] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11).

[42] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11).

[43] Sethia, D., Gupta, D., & Saran, H. (2018). NFC secure element-based mutual authentication and attestation for IoT access. IEEE Transactions on Consumer Electronics, 64(4), 470-479.

[44] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11).

[45] Yubico. (2024, January 12). Security advisory YSA-2020-04. https://www.yubico.com/support/security-advisories/ysa-2020-04/

[46] Microsoft. (2024). Zero trust model - Modern security architecture | Microsoft security. https://www.microsoft.com/. https://www.microsoft.com/en-my/security/business/zero-trust

[47] Lee, J., Choi, H. K., Yoon, J. H., & Kim, S. (2023). An Empirical Analysis of Incorrect Account Remediation in the Case of Broken Authentication. IEEE Access.

[48] Cremers, C., Horowitz, G., Jacomme, C., & Ronen, E. (2024). Tokenweaver: Privacy preserving and post-compromise secure attestation.

[49] Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. Predicting and changing health behavior: Research and practice with social cognition models, 3, 70-106.

[50] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), 93-114.

[51] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), 93-114.

[52] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). International Journal of Advanced Computer Science and Applications, 11(11).

[53] Cavoukian, A. (2011). Mobile Near Field Communications (NFC):" Tap'n Go": Keep it Secure and Private (pp. 1-19). Information and Privacy Commissioner of Ontario, Canada.

[54] NIST. (2023, September 26). Cybersecurity framework. https://www.nist.gov/cyberframework

[55] Microsoft. (2024). Zero trust model - Modern security architecture | Microsoft security. https://www.microsoft.com/. https://www.microsoft.com/en-my/security/business/zero-trust

[56] Lee, J., Choi, H. K., Yoon, J. H., & Kim, S. (2023). An Empirical Analysis of Incorrect Account Remediation in the Case of Broken Authentication. IEEE Access.

[57] Fortinet. (2024). What is DevOps Security? https://www.fortinet.com/resources/cyberglossary/devops-security

[58] Microsoft. (2024). Zero trust model - Modern security architecture | Microsoft security. https://www.microsoft.com/. https://www.microsoft.com/en-my/security/business/zero-trust

[59] Wrensch, J. (2023, August 23). The difference between a policy, procedure, standard and guideline. Michalsons. https://www.michalsons.com/blog/the-difference-between-a- policy-procedure-standard-and-a-guideline/42265

[60] Cambridge. (2024). Framework. Cambridge Dictionary | English Dictionary, Translations & Thesaurus. https://dictionary.cambridge.org/dictionary/english/framework

APPENDIX A STUDY INSTRUMENTS – QUESTIONNAIRE

Questionnaire Title: Near Field Communication (NFC): User Experience Survey in using NFC-based devices and services.

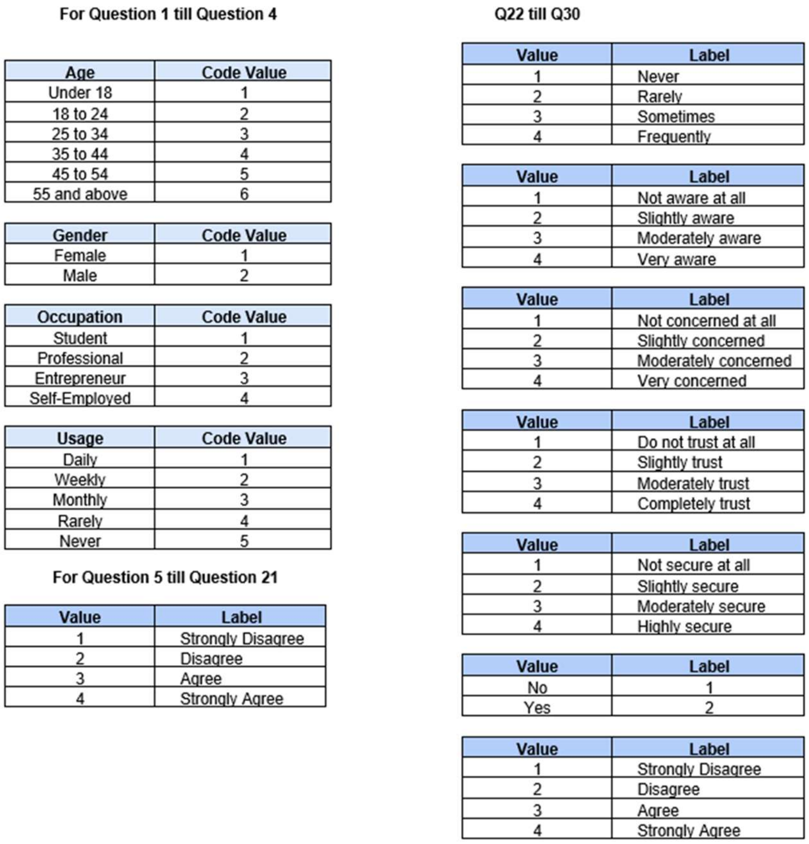
Section	Themes	Survey Items
A	**Demographic Information**	Q1) What is your age group? Q2) What is your gender? Q3) What is your occupation? Q4) Usage of NFC Devices: How often do you use NFC-enabled devices?
B	**NFC Usage and Perception**	Q5) Awareness of NFC Technology: I am familiar with NFC technology. Q6) I frequently use NFC for mobile payments. Q7) I use NFC for data sharing between devices. Q8) I find NFC technology is convenient for every transaction. Q9) I am confident in the security of transaction using NFC-enabled devices. Q10) I am aware of the potential security risks associated with NFC. Q11) I am willing to learn more on ways to improve the security of my NFC-enabled device.
C	**NFC Attestation and Security**	Q12) I am familiar with the NFC Attestation process. Q13) I believe the existing NFC attestation process of my devices is effective in preventing unauthorized access. Q14) I trust the current security measures implemented in NFC technology. Q15) I am concerned about the possibility of data spoofing in NFC-based transaction. Q16) I believe that additional security measures are needed for enhancing the security of NFC-enabled devices and for NFC-based transactions.
D	**Post-Compromise Recovery Strategy**	Q17) I believe having a recovery strategy is important for maintaining the security of NFC transactions. Q18) I am aware of the steps to take if my NFC data/devices is compromised. Q19) I trust that the service providers have adequate recovery strategies in place for NFC security breaches.

		Q20) I feel confident in my ability to recover from an NFC-related security breach. Q21) I believe that the End Users should be educated about NFC security and be well informed of the recovery strategies in the event of NFC attack.
E	**NFC End User Experience**	Q22) How often do you use NFC for mobile payments? (e.g., Google Pay, Apple Pay, NFC-enabled Touch and Go Cards) Q23) **Awareness of NFC Security Risks:** How aware are you of the potential security risks associated with NFC Technology? Q24) **Concern about NFC Security:** How concerned are you about the security of your personal information when using an NFC enabled device? Q25) **Trust in NFC-enabled devices in Mobile Payments:** How much do your trust the security of NFC-enabled devices in performing mobile payments? Q26) **Usage of NFC for Access Control:** How often do you use NFC-enabled devices for access control (e.g., entering office buildings, accessing keyless entry vehicle)? Q27) **Perceived Security of NFC Access Control Systems:** How secure do you believe the NFC access control systems are? Q28) **Actions Taken to Enhance NFC Security:** How often do you take actions to enhance the security of your NFC-enabled devices (e.g., updating software, enabling encryption)? Q29) **Encounter with NFC Security Incidents:** Have you ever encountered any security incidents related to NFC usage (e.g., unauthorized transactions, data breaches)? Q30) **Data Breach Recovery Process:** There are sufficient information and procedures been made available for End Users/Customers/Employees to refer to in the event of NFC attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

APPENDIX B STUDY INSTRUMENTS CODEBOOK

This codebook is referred to during Data Preparation and Data Analysis in IBM SPSS.



For Question 1 till Question 4

Age	Code Value
Under 18	1
18 to 24	2
25 to 34	3
35 to 44	4
45 to 54	5
55 and above	6

Gender	Code Value
Female	1
Male	2

Occupation	Code Value
Student	1
Professional	2
Entrepreneur	3
Self-Employed	4

Usage	Code Value
Daily	1
Weekly	2
Monthly	3
Rarely	4
Never	5

For Question 5 till Question 21

Value	Label
1	Strongly Disagree
2	Disagree
3	Agree
4	Strongly Agree

Q22 till Q30

Value	Label
1	Never
2	Rarely
3	Sometimes
4	Frequently

Value	Label
1	Not aware at all
2	Slightly aware
3	Moderately aware
4	Very aware

Value	Label
1	Not concerned at all
2	Slightly concerned
3	Moderately concerned
4	Very concerned

Value	Label
1	Do not trust at all
2	Slightly trust
3	Moderately trust
4	Completely trust

Value	Label
1	Not secure at all
2	Slightly secure
3	Moderately secure
4	Highly secure

Value	Label
No	1
Yes	2

Value	Label
1	Strongly Disagree
2	Disagree
3	Agree
4	Strongly Agree

APPENDIX C RESULTS OF HYPOTHESES TESTING

Themes	Research Questions (RQ)	Research Hypotheses	Statistical Method	Results	Insights
1. Awareness and Security Perception	RQ1 What is the relationship between demographic factors and NFC awareness?	H0: There is no significant relationship between demographic factors and NFC awareness. H1: There is a significant relationship between demographic factors and NFC awareness.	Chi-square test	Not significant (failed to reject H0)	Demographic factors such as age, gender, and occupation do not significantly influence NFC awareness. Awareness levels are relatively uniform across different demographic groups.
	RQ2 How does the frequency of NFC device usage influence awareness of security risks?	H0: No significant correlation exists between NFC device usage frequency and awareness of security risks. H1: A significant correlation exists between NFC device usage frequency and awareness of security risks.	Spearman's rank correlation	Not significant (failed to reject H0)	No significant correlation was found, suggesting that frequency of NFC device usage does not significantly impact users' awareness of security risks.
	RQ3 Is there a correlation between awareness of NFC security risks and concern about data spoofing?	H0: There is no significant correlation between awareness of NFC security risks and concern about data spoofing. H1: There is a significant correlation between awareness of NFC security risks and concern about data spoofing.	Spearman's rank correlation	Significant (rejected H0) Accept that the sample gives reasonable evidence to support the alternative hypothesis.	A significant correlation exists, indicating that users aware of security risks are also concerned about data spoofing.
2. Awareness on Attestation and Security Measures	RQ4 How does familiarity with the NFC attestation process affect trust in NFC security measures?	H0: There is no significant difference in trust levels between those familiar and not familiar with the NFC attestation process. H1: There is a significant difference in trust levels between those familiar and not familiar with the NFC attestation process.	Spearman's rank correlation	Not significant (failed to reject H0)	Familiarity with the NFC attestation process does not significantly affect trust in NFC security measures.
3. User Perception and Confidence on NFC Security	RQ5 What is the relationship between confidence in NFC security and trust in security measures?	H0: There is no significant correlation between confidence in NFC security and trust in security measures. H1: There is a significant correlation between confidence in NFC security and trust in security measures.	Spearman's rank correlation	Significant (rejected H0) Acknowledge that the alternative hypothesis is supported by reasonable evidence provided by the sample.	A moderate positive correlation exists, indicating that users confident in transaction security also trust the overall security measures.

	RQ6 What is the relationship between confidence in personal recovery ability and trust in service providers' recovery strategies?	H0: There is no significant correlation between confidence in personal recovery ability and trust in service providers' recovery strategies. H1: There is a significant correlation between confidence in personal recovery ability and trust in service providers' recovery strategies.	Spearman's rank correlation	Significant (rejected H0) Acknowledge that the alternative hypothesis is supported by reasonable evidence provided by the sample.	A significant correlation exists, suggesting that both personal and institutional factors shape users' perceptions of recovery effectiveness.
4. Perceived Security of NFC	RQ7 How does the frequency of NFC usage for mobile payments correlate with trust in NFC-enabled devices?	H0: There is no significant correlation between the frequency of NFC usage for mobile payments and trust in NFC-enabled devices. H1: There is a significant correlation between the frequency of NFC usage for mobile payments and trust in NFC-enabled devices.	Spearman's rank correlation	Significant (rejected H0) Acknowledge that the alternative hypothesis is supported by reasonable evidence provided by the sample	A significant correlation exists, indicating that increased usage may lead to greater familiarity and confidence, enhancing trust in NFC-enabled devices.
	RQ8 What is the relationship between actions taken to enhance NFC security and past encounters with NFC security incidents?	H0: There is no significant relationship between actions taken to enhance NFC security and past encounters with NFC security incidents. H1: There is a significant relationship between actions taken to enhance NFC security and past encounters with NFC security incidents.	Chi-square test	Not significant	No significant relationship was found, suggesting that proactive measures are driven by general security awareness rather than past experiences.
	RQ9 How does the adequacy of data breach recovery processes relate to overall trust in NFC technology?	H0: There is no significant correlation between the adequacy of data breach recovery processes and overall trust in NFC technology. H1: There is a significant correlation between the adequacy of data breach recovery processes and overall trust in NFC technology.	Spearman's rank correlation	Not significant	No significant correlation was found, suggesting that trust in NFC technology is not significantly impacted by the perceived adequacy of data breach recovery processes.
5. Confidence in Post-Compromise Strategy	RQ10 How do demographic factors influence the perceived importance of post-compromise recovery strategy?	H0: There is no significant difference in the perceived importance of a post-compromise recovery strategy across different demographic groups. H1: There is a significant difference	Kruskal-Wallis H test	Not significant	No significant differences were found, indicating a general consensus on the importance of post-compromise recovery strategies across demographic groups.

		in the perceived importance of a post-compromise recovery strategy across different demographic groups.			
	RQ11 What is the relationship between the perception of NFC access control security and frequency of use?	H0: There is no significant correlation between the perception of NFC access control security and frequency of use. H1: There is a significant correlation between the perception of NFC access control security and frequency of use.	Spearman's rank correlation	Not significant	No significant correlation was found, suggesting that perception of access control security is not significantly impacted by frequency of NFC usage.

APPENDIX D NFC END USER SECURITY POLICY

NFC SECURITY POLICY FOR NFC END USERS			
Date of Issue:	*DD/MM/YYYY*	**Revision Number:**	*YY - ####*
Document Owner:	*Author's Name*	**Department:**	*Issuing Department*
Policy Overview:	**Target Audience** • Policymakers at Organization typically of the Information Assurance Office and Information Governance Office. • Public NFC End-Users **Purpose** • The NFC End-User Level Security Policy aims to protect end users from NFC-related security risks, such as data spoofing, relay attacks, and unauthorized data access. • This policy focuses on enhancing security awareness, implementing proactive measures, and ensuring robust post-compromise recovery strategies. • The policy is tailored specifically to address the unique challenges and vulnerabilities associated with NFC technology at the End-User level. **Scope** • This policy is applicable to all end users of NFC-enabled devices, such as smartphones, tablets, and other mobile devices. • It encompasses all activities related to NFC transactions, data exchanges, and interactions, ensuring that users are protected from potential security threats and vulnerabilities.		
Policy Statement:	This policy aims to enhance security awareness on NFC vulnerabilities, implement proactive measures in mitigating the security risks, and providing a concise post-compromise recovery action plan.		
Key Principles:	**Principle 1** **Verify Explicitly**	a. **Multi-Factor Authentication (MFA):** End users must adopt MFA for all transactions involving NFC technology to ensure secure authentication. b. **Device Health Checks:** Users should regularly update their devices and install security patches to maintain device integrity. c. **Anomaly Detection:** Utilize mobile security applications that detect and respond to unusual NFC activity patterns.	
	Principle 2 **Use Least Privilege Access**	a. **Just-in-Time (JIT) Access:** NFC functionalities should be enabled only when necessary, reducing the window of opportunity for attacks. Turn off the NFC function when not in used. b. **Data Protection:** Encrypt sensitive data both at rest and in transit to prevent unauthorized access. Ensure the corresponding application or device has incorporated encryption setting.	

	Privilege 3 **Assume Breach**	**a. Segmentation and Isolation:** Ensure to segregate the NFC-enabled device based on purpose-based. Avoid using one device for all transaction/function/use. For sensitive transaction use a dedicated, highly secured NFC device separate from social usage. **b. End-to-End Encryption:** Ensure the device, the application, the communication are encrypted. **c. Continuous Monitoring:** Schedule a regular Device Optimisation scan, Security Scan, Firmware Update, Data Backup, and Password Change to ensure the security of the NFC-enabled device is intact.
Definitions:	NFC: Near Field Communication MFA: Multi-Factor Authentication JIT: Just-in-Time	
Policy Implementation:	**Proactive Measures**	
	Education and Training • Service Providers to regularly educate users about NFC security risks and best practices of their NFC-enabled device. • NFC End Users are encouraged to attend to security podcast, security bulleting, security newsletter with regards to NFC **Software Updates** • NFC End Users are encouraged to keep their devices and applications updated. • Incorporate push notifications or in-mail via message centre. **Security Features** • Encourage the utilization of built-in security features, which includes secure NFC settings and device encryption. • Ensure the NFC-enabled device has obtained industry standard certification or regulatory body inspection.	
	Post-Compromise Recovery Actions	
	Notify Service Provider Immediately • Contact your service or device provider to prevent any unauthorized transactions and to commence a formal investigation. • This enables the provider to take immediate action, such as disabling compromised accounts and providing additional instructions for securing your information. **Immediate Change of Password** • Change all passwords associated with your NFC-enabled services and accounts immediately upon detecting a breach to prevent further unauthorized access. • Ensure that the new passwords are both unique and secure in order to improve security. **Remove access to Linked Folder** • To prevent unauthorized access to sensitive data, disconnect any compromised NFC device from linked folders and cloud storage. • This measure assists in the containment of the intrusion and protects End User information from being accessed or modified by attackers.	

	Change Secure Transaction Code • Replace the secure transaction codes (such as PINs or authentication codes) that are currently in use for NFC-enabled transactions with new, more secure codes. • This action aids in the restoration of security for future transactions and prevents the use of compromised codes by attackers.
	Monitoring
	Device Optimization • Schedule daily Device Optimization to clear cache and thus preventing any rootkit malware that may have been scanned unknowingly. • Ensure the device is power off after two days of consecutive use. This will ensure any background process is terminated. **Periodical Security Scan** • Install mobile device antivirus and run security scan periodically **Push Notification or Alert upon New known Security Risk** • Be alert on any new security risk pertaining to own NFC-enabled device and learn the required mitigation or recovery steps by the service provider or application provider.
References:	Microsoft Zero Trust Policy (Microsoft, 2024) Cybersecurity Malaysia (Cybersecurity Malaysia, 2011)
Revision History:	• *Revision Number – Revision Date – Revision Summary – Updated By*
Approval History:	• *Approver Date – Approver Name – Approver Digital Signature*

APPENDIX E PROACTIVE & REACTIVE STRATEGY AT NFC END USER LEVEL

Phase	Activity Label	Category	Activity Details	Description	Frequency
Prevention	Update Firmware	Device Maintenance	Apply firmware updates	Regularly update firmware to ensure security patches and updates are applied.	As needed
Prevention	Use Biometric ID	Authentication	Enable biometric ID	Use fingerprint or facial recognition for higher security compared to traditional passwords.	Continuous
Prevention	Personal Data Management	Data Protection	Manage personal data	Control access to personal information and adjust privacy settings regularly.	Monthly
Prevention	Frequent Password	Credential Management	Change passwords	Regularly update passwords to protect accounts from unauthorized access. (Depending on the criticality of the data in the apps)	Every 3 months,
Prevention	Cybersecurity Training	User Education	Participate in training	Engage in training programs to stay informed about cybersecurity threats and best practices.	Quarterly
Prevention	Secured Element	Device Security	Use secure element	Utilize dedicated security hardware within NFC devices for storing sensitive data.	Continuous
Prevention	Turn off NFC Func	Risk Reduction	Disable NFC	Turn off NFC when not in use to prevent unauthorized access.	Daily
Prevention	Human Firewall	User Vigilance	Enhance vigilance	Practice caution when sharing information and avoid suspicious links or downloads.	Continuous
Prevention	Install Mobile Antivirus	Device Protection	Use anti-virus software	Install and update anti-virus applications to detect and remove malware.	Run the scan weekly
Recovery	Immediate Change of Password	Password Management	Change Password	Promptly change all passwords to prevent unauthorized access post-compromise.	Immediately after a security breach
Recovery	Remove access to Personal Data	Data Access	Review Personal Data	Revoke any access or permissions to personal data to mitigate further data loss or misuse.	Immediately after a security breach
Recovery	Notify Service Provider Immediately	Service Provider Notification	Inform NFC Service Provision	Inform the service provider about the security breach to take necessary actions on their end.	Immediately after a security breach
Recovery	Change Secure Transaction Code	Transaction Security	Update Secure Access Details	Update secure transaction codes to ensure continued secure transactions, or, Disable the function from the device by deregistering the device from the system.	Immediately after a security breach