*Computers, Materials & Continua*
DOI:10.32604/cmc.2021.014969
***Article***

Tech Science Press

# Security Threats to Business Information Systems Using NFC Read/Write Mode

**Sergio Rios-Aguilar[1,2,*], Marta Beltrán[2] and González-Crespo Rubén[3]**

[1]Department of Organization Engineering, Business Administration and Statistics, ETSI Informáticos, Universidad Politécnica de Madrid (UPM), Boadilla del Monte (Madrid), 28660, Spain
[2]Department of Computing, ETSII, Universidad Rey Juan Carlos, Móstoles (Madrid), 28933, Spain
[3]ESIT, Universidad Internacional de La Rioja (UNIR), Logroño (La Rioja), 26006, Spain
[*]Corresponding Author: Sergio Rios-Aguilar. Email: sergio.rios@upm.es
Received: 29 October 2020; Accepted: 06 December 2020

**Abstract:** Radio Frequency IDentification (RFID) and related technologies such as Near Field Communication (NFC) are becoming essential in industrial contexts thanks to their ability to perform contactless data exchange, either device-to-device or tag-to-device. One of the three main operation modes of NFC, called read/write mode, makes use of the latter type of interaction. It is extensively used in business information systems that make use of NFC tags to provide the end-user with augmented information in one of several available NFC data exchange formats, such as plain text, simple URLs or enriched URLs. Using a wide variety of physical form factors, NFC-compatible tags (wireless transponders) are currently available in many locations with applications going from smart posters, contactless tokens, tap-and-go payments or transport ticketing to automated device configuration, patient identification at hospitals or inventory management within supply chains. Most of these applications handle sensitive processes or data. This paper proposes a complete security threat model for the read/write operation mode of NFC used in Next Generation Industrial IoT (Nx-IIoT) contexts. This model, based on a well-known methodology, STRIDE, allows developers and users to identify NFC applications vulnerabilities or weaknesses, analyze potential threats, propose risk management strategies, and design mitigation mechanisms to mention only some significant examples.

**Keywords:** Near field communications; read/write NFC; security; threat modelling; STRIDE; Nx-IIoT

## 1 Introduction

Near Field Communication (NFC) is a short-range half-duplex wireless communication technology relying on magnetic field induction that allows two or more devices to perform a data exchange when they are located at a maximum of few centimetres from each other [1,2].

The main advantage of NFC over other wireless communication technologies is that NFC has been designed with a focus on the simplicity of operation, offering the user a "touch-and-go" experience. Transactions are initialized automatically, only by bringing an NFC device (for example, an NFC enabled smartphone) close to an NFC compliant transponder (a tag) or other NFC device [3].

NFC technology is based on the contactless smartcard standard ISO/IEC14443 and operates at a universally open and licensed 13.56 MHz frequency. Some NFC devices can also communicate on the same frequency with vicinity RFID transponders based on the more recent ISO/IEC 15693 [4,5]

NFC specifies three different operation modes: reader/writer, card emulation and peer to peer. In the reader/writer operation mode, an NFC device reads data from a tag, and it is also able to perform write operations to the tag, as needed. In the card emulation mode, an NFC enabled smartphone behaves as a smart card (even if the device is switched off if appropriate hardware implementation is available). Finally, the peer to peer operation mode enables a bidirectional connection between two NFC enabled smartphones, for direct in-formation transmission (e.g., image files) [6].

There is extensive literature about the security of the NFC card emulation mode, focusing on mobile payments. However, this area is often considered to be a "closed garden" with a few clearly established intervening stakeholders (mobile operators, banks, payment networks, credit/debit card issuers, etc.) and with little room for innovation in its well-defined transaction flow. Furthermore, entry barriers for developers are high. The peer to peer mode has attracted low research attention as it is now considered just a commodity for wireless information/file sharing between user's smartphones [7].

This paper focuses on the reader/writer mode, as it is present in a huge and increasing number of use cases: Nx-IIoT sensor identification, Nx-IIoT device/machinery pairing, Nx-IIoT real-time operations dashboard access, as well as other use cases outside industrial contexts, such as mobile marketing using smart posters, workforce presence control, location-based services, capacity control in closed spaces following changing health regulations, hospitalized patients ID management, tourist routes, city-wide treasure hunting games, etc. All these application domains show genuine innovation opportunities for developers and users, which inevitably means that security issues have to be taken into consideration in the broadest sense [8–13].

Different research works and security issues observed within real use cases have demonstrated that data modification, insertion or corruption are significant threats that the considered technology poses in the different application domains it is being introduced. The target of known attacks can be the entire NFC application or only a particular NFC component (tag, smartphone/reader or even an existing back-end supporting the business logic of the service). On the other hand, eavesdropping and man-in-the-middle attacks are usually considered in the literature regarding NFC security, given the wireless nature of the standard.

To the best of our knowledge, there is not a thorough threat model of the utilization of NFC technologies in reader/writer mode within a project, regardless of the application domain or the specifics of the project itself. NFC is still an emerging technology with evolving applications, and there is a lack of standard, generalizable and reliable security analysis, based on a well-known and widely-adopted methodology such as STRIDE [14], capable of providing valuable insights useful

when trying to identify and to mitigate existing security threats. The main contributions of this work are:

(a) A new threat model of the NFC reader/writer operation mode regarding security, based on the STRIDE methodology.
(b) An in-depth systematic analysis, using attack trees, of the different attack patterns that an adversary may use to materialize the identified set of threats.
(c) A discussion about mitigation, countermeasures and remediation options capable of avoiding or mitigating impacts of identified threats, working on aspects of both, NFC standardization and implementation.

The rest of this paper is organized as follows. Section 2 provides the background on enabling technologies (NFC) and an overview of the related work. Section 3 introduces a motivating example and discusses the primary motivations for this work. Section 4 describes the proposed threat model, identifying and analyzing security threats. Section 5 details possible mitigation to the identified set of threats and discusses some of the main future challenges regarding NFC security. Finally, Section 6 summarizes our main conclusions and the most interesting lines for future research.

## 2 Background and Related Work

### *2.1 NFC Tags and Contents*

The NFC Forum is an association of industry organizations with interest in NFC, and its members include chip manufacturers, credit card issuers, mobile network operators, mobile handset manufacturers, application developers, financial service companies, among others.

Complementing the ISO/IEC NFC related standards, the NFC Forum creates and drives specifications for data formats, protocols, and reference applications. This association supports a tight certification program that assures interoperability between different products and implementations [15].

The NFC Forum defines the NFC Data Exchange Format (NDEF) as a common format for storing data on NFC tags, and it supports a set of well-known types, from simple data types to complex data structures, depending on the specific use cases [5,16].

For example, the specification includes a simple record format for URIs, that can be used to store website URLs, e-mail addresses, phone numbers and any other data that can be represented by standard URIs. Also, a more complex "Smart Poster" record type defined in NDEF consists of one URI record and, optionally, one or more other records. For example, text records that can be used for describing a URL or the service it provides in multiple languages [17–19].

There are five NFC Forum approved tag types capable of storing NDEF data, with different technical characteristics in terms of storage capacity, data rate, and cost. Tags of type 2 are the most commonly used in Smart poster applications; while type 5 is the most recently approved (2015) and can be read not only by NFC readers at the usual distance of a few centimeters, but also using a vicinity UHF RFID reader, at distances up to 1.5 m (see Tab. 1) [20–25].

### *2.2 Previous Research on NFC Security*

In one of the first and seminal works on NFC security [26], the authors make a complete outline of threats and possible mitigations concerning NFC applications. The authors also put the focus on eavesdropping, data corruption and modification, as well as on man-in-the-middle

attacks along with data insertion. One interesting conclusion of their work is that in practice, it is not feasible to conduct a man-in-the-middle attack under real-world conditions. In any case, it is essential to note that all of the identified threats always refer to NFC's air interface, i.e., all of them refer to HF radio-based attacks.

**Table 1:** NFC Forum tag types and characteristics

| Tag type | Type 1 | Type 2 | Type 3 | Type 4 | Type 5 |
|---|---|---|---|---|---|
| ISO/IEC standards | 14443A | 14443A | 18092 | 14443A/B | 15693 |
| Memory size | 96B-2KB | 48B-2KB | 2KB | 32KB | 64KB |
| Data rate (Kpbs) | 106 | 106 | 212/424 | 106 | 26.5 |
| Cost | * | * | *** | *** | */*** |

A later work stated that both standards ISO14443 and ISO18092 (used in NFC Forum tag of type 3) are open to relay attacks via RF which cannot be recognized by the transponder tag nor by the NFC reader, but those attacks are essentially focused on NFC card emulation operation mode involving payments [27].

Considering the reader or active part of the communications (an NFC-enabled smartphone), and analyzing vulnerabilities and attacks, [28] presented an innovative and widely cited work identifying multiple attacks such as URI spoofing when using smart posters. These attacks involve the use of several techniques that effectively hide the malicious parts of the URI and taking advantage of GUI limitations when displaying contents on the constrained size screen of some smartphones, avoid raising suspicions on the user. Also, the author presented, as a proof of concept, an application capable of intercepting all NDEF messages, performing denial of service attacks based on the storage of intentionally malformed NDEF content in a card. Reference [29] also presented several possible DoS attacks using a malicious application running on specific smartphones.

Reference [3] explored the security of NFC devices as well, identifying several threats. One of them refers to the presence of a unique ID on the NFC tag for collision avoidance before actual data communications as a possible way of conducting denial of service attacks, as well as possible security issues if that ID is copied and used in specific applications [30].

Finally, two other relevant works put the focus on phishing as a social engineering attack after spoofing URIs on a tag, making it easy to deceive end-users into revealing personal information [27,30].

## 3 Motivating Examples and Research Questions

Industry 4.0 relies on different paradigms and technologies trying to add intelligence to production and business operations. NFC is one of these technologies because it can provide new forms of convenient and configurable communication, enabling better human–machine interfaces, easy to build, to maintain and to use and highly customizable.

For example, the NFC reader/writer operation mode enables intelligent access control within factories through NFC-based authorization when controlling the access to installations, warehouses, line plants or machines. The deployment of tap-and-authenticate solutions allows managers to restrict physical or logical access to resources only to authorized or trained employees.

This kind of solutions also allows us to set up different access profiles or preferences, or to grant time-limited access for temporary staff, to mention only some examples.

Another good example is the utilization of smartphones or tablets as extended interfaces for machinery with rudimentary interfaces, sealed or not accessible interfaces or when machines are unpowered, within a context of Nx-IIoT environments.

There is a plethora of use cases that could benefit from NFC within the Industry 4.0. One of the most significant barriers to the adoption of NFC technologies in new smart factories is the perception of their low level of security. This is one of the main reasons why the use cases mentioned as examples, and many others like them are not yet as widespread as expected.

The limitations identified in previous works when focusing on these industrial use cases can be summarized in:

- Previous work has focused on describing and analyzing specific attacks or threats as well as their possible mitigation. However, they do not carry out a systematic analysis, using a recognized and proven methodology, that identifies the complete set of threats that an architecture suffers from the fact of incorporating NFC technology.
- In addition, previous work tends to focus on the air-interface security, rather than full NFC applications
- Finally, when these works analyze "NFC applications," they do so without focusing on a specific mode of operation, such as the reader/writer, which is the most used in industrial environments.

This work aims to overcome these limitations, establishing a model of security threats that any person responsible for designing an industrial environment can use as a guide to understand the risks faced by introducing NFC technology (in the reader/writer mode) in the designed architecture. The following research questions summarize the most important answered in the rest of this paper:

- Is it possible to obtain a threat model of the NFC reader/writer mode for security threats, using a standard methodology such as STRIDE?
- What assumptions about the attackers, the target architecture and trust should be made in order to apply this model within industrial environments?
- What threats arise from the utilization of the NFC reader/writer mode and which specific attack patterns may help an attacker to materialize them?
- Are there mitigations that could avoid these threats within industrial architectures or, at least, reduce their impacts?

## 4 Threat Model

### *4.1 Assumptions and Methodology*

This section presents a standard, generalizable and reliable security threat model of the reader/writer NFC operation mode. This model is standard because it is obtained applying a standard methodologies such as STRIDE [14,31]. It is generalizable because it is not bound to a specific application domain, implementation or product, the aim is to analyze security and privacy issues of the technology and of the standard way of using it, not of specific architectures or projects. Furthermore, it is reliable because it is complete, identifying threats coming from different attackers with different goals, strategies, or capabilities. Some assumptions have been considered to obtain this new model,

- Attacker assumptions:
  - (a) Attackers have unlimited resources to make effective their threats.
  - (b) Attackers may have different goals, strategies and capabilities; as well as different levels of access to different components of the NFC based system (tag, smartphone/reader, back-end) All these access levels will be considered during the modelling process.
- Architectural assumptions:
  - (c) A general architecture for an NFC reader/writer operation mode application is composed of a tag, which is located within a public domain place with some degree of physical security, an NFC capable smartphone running Android or iOS ($\geq$ v11) with a wireless data connection to the Internet, and a web application back-end running the specific service provided to the user (proof of presence, location-based information, etc.).
  - (d) The provided service must be frictionless from the user's point of view. Thus, it must not rely on the previous installation of a mobile app that handles NFC interactions. The system must follow the "Tap and go" spirit of the reader/writer operation mode in NFC, using only the core NFC functionality inherently built into NFC-enabled Android/iOS smartphones, with no additional software required that should be explicitly installed.
  - (e) The operation mode is reader/writer, and the use case is Text/URI/Smart poster (using the appropriate NDEF data formats in the tag, correspondingly).
- Trust assumptions:
  - (f) The legitimate back-end service responsible for the business logic of the general system being analyzed can be trusted, i.e., is adequately built and hardened.

Our intention with these assumptions is to identify security threats that can be attributed to the specific use of NFC, ignoring other well-known and generic threats caused by weak implementations of the overall back-end service, cryptography, etc. (See Tab. 2).

**Table 2:** Security threats and possible attacks to the reader/writer operation mode of NFC

| Stride Treat | Attack |
|---|---|
| Spoofing an external identity | Spoofing URIs (phishing) |
| | Spoofing Wi-Fi connection |
| | Tag replacement and/or destruction of original tag |
| | Tag shielding |
| | Tag spoofing using a rogue app |
| Tampering a data store | Overwrite NDEF contents |
| Information disclosure from data stores | Tag cloning/copying |
| | Restoring erased NDEF data |
| Denial of service flow | Compromising NFC's Air Interface via jamming |
| | Creating repeated interactions |

Regarding our methodology, STRIDE technique has been selected. This technique is a well-known and widely used threat analysis methodology and de-facto standard to systematically analyze architectural security threats by identifying the types of attacks that software systems are exposed to, mainly because of design-level vulnerabilities or weaknesses.

Finally, it has to be pointed out that all performed experiments and tests, necessary to propose and to validate the different strategies that an attacker may use to materialize identified threats, have been performed within a controlled lab reproducing typical Industry 4.0 applications due to ethical and legal reasons.

Different devices relying on different versions of different operating systems (Android and iOS) with different security configurations have been used. Applications have been implemented replicating real ones of different domains such as Business Information Systems using text/URI/Smart poster NDEF data contained into NFC tags to provide the user with several kinds of services (presence, location-based, marketing) with different security and privacy requirements, programmed with different programming languages.

### *4.2 Threats to Security*

#### *4.2.1 Spoofing*

The frictionless operation of NFC, which is excellent in terms of user experience, has some drawbacks in terms of security, being one of the critical threats the potential spoofing of NFC tags: As the typical user will not be able to tell the difference between an authentic tag from a counterfeited one, NFC applications based on NDEF information contained in tags are potentially vulnerable to spoofing [3].

**Attack pattern 1**: Tag replacement. The adversary can physically remove or destroy a tag rendering it unusable, and then place the spoofed one over or behind the original one. The first option, removal, can be easily performed in many cases, by simply detaching or peeling off an NFC sticker. The second one, destruction, can be performed using an "RFID zapper," which is a simple device that destroys the main chip of the tag through the induction of a high voltage at the tag antenna. Another alternative is to make a tiny cut to the antenna itself, rendering it useless (There are a lot of how-to guides over the Internet related to physically disabling contactless payments on debit/credit cards) [15,32].

**Attack pattern 2**: Shielding of a tag. The adversary can perform this attack RF-shielding the original tag with a special metal-coated sticker or metal foil and placing the spoofed tag over the now shielded original tag [15].

**Attack pattern 3**: Spoofing URIs. The adversary can, directly or possibly after performing other types of attacks, store a malicious URI on the tag (in NDEF URI or NDEF Smart poster data formats). Besides the usual phishing objectives such as user names and password stealing, the consequences of following a malicious URI can be extensive: leakage of geo-location information, vibration attacks, client Denial of Service attacks trying to difficult the user interaction through input stealing techniques, or trying to exhaust the mobile browser's space via repeat templates and faulty regular expressions. These kinds of attacks are especially effective when the browser is not updated with recent security patches, and unfortunately, this happens for a wide user base [3].

**Attack pattern 4**: Spoofing a tag with a rogue application on the smartphone. The adversary could use phishing or other social engineering attacks to install a rogue application on the user's smartphone. This application could intercept and modify the contents of the tag before it gets handled by the default Operating System application. The rogue application could then change

contents on the fly, and the user would not be able to tell if those contents are legitimate, except in the case she scans the tag using another "clean" or not "infected" smartphone. Unlike other vector attacks using a previously installed rogue application that tricks the user making her think a new NFC has been read ("phantom read"), this attack benefits from the fact that the user interaction is expected.

**Attack pattern 5**: Spoofing a Wi-Fi connection. Thanks to NFC Forum's Connection Handover specification, it is possible for an NFC-enabled smartphone to tap an NFC tag and get an NDEF message with static handover information, such as Wi-Fi pairing information. After requesting user's approval, the connection to the Wi-Fi Access Point is established. An adversary could take benefit from this functionality to spoof a legitimate wireless network, making all the user's smartphone data traffic route over the adversary's controlled malicious Wi-Fi Access Point. Another variant of this attack involves an adversary hiding tags programmed with Wi-Fi handover data close to common places where smartphones are left (e.g., under a desk) and tricking the user into accepting the connection using hacked SSID names. For example, naming SSID "again" or using other deceptive names, makes the confirmation message to appear to the user as "Connect to the network again?" or "Connect to the network? WhatsApp requests permission" [33,34].

#### *4.2.2 Tampering*

The user usually has no clue about the real contents she is going to get from the tag before making the interaction with her smartphone, and in a significant amount of cases, when the NDEF content of the tag is a URI, the user is neither able to check or verify the validity of the destination. Therefore, an adversary could perform several types of social engineering attacks or phishing through the modification of tag contents.

**Attack pattern 6**: Overwriting NDEF tag content. NFC tags can be deployed in public spaces with no write protection at all. In this case, the adversary can easily overwrite the tag contents, replacing the previous contents with her own NDEF data, and even protect her tampering activities blocking the tag afterwards, enabling the write protection

#### *4.2.3 Repudiation*

This threat defined in STRIDE is not applicable, as there is no logging activity of user's data or identifiable information about her smartphone on the NFC tag side. However, in a strict sense, according to STRIDE, the absence of logging procedures is a threat in itself: "No transaction logs/Insufficient transaction logs". Current versions of the involved NFC-Forum standards do not cover this kind of logging activity.

#### *4.2.4 Information Disclosure*

Some NFC applications involve the reuse of tags, changing their contents when needed (e.g., daily in an attendance control system). Other times, the tags previously used in one application must be reused for another application. This means that an adversary could extract confidential information from a reused tag or could be able to infer new valid content based on the recovered information structure. In other cases, the objective for an adversary could be getting as much information as possible from a tag, in order to create high fidelity copies or perfect clones.

**Attack pattern 7**: Restoring erased NDEF payload data. NFC Forum's NDEF format includes a very light record header that contains, among other important fields, a 3-bit field (the Type Name Format or TNF) used to identify the type of record. One of the possible record type names is the "empty" type. When a smartphone touches a tag with "empty" TNF, it shows the user that

the tag is empty without reading the remaining content of the tag, even though the information in the payload section is still intact. The adversary could "restore" the missing data available on the tag, that could then possibly use for stealing user identities, contact information, Wi-Fi or Bluetooth connection data, for example [5].

**Attack pattern 8**: Copying tag contents or tag cloning. Copying the data of a regular NFC tag can be easily done using one of the many free NFC apps available in the corresponding App Stores. Usually, NFC tags behave just as a simple memory/data store, and when they are read, they return the data written to them. Some more advanced tags include a chip with extra functionality, such as appending their serial number to the NDEF message, but the problem remains intact: the same tag will always return the same NDEF message on every tap. Even if the tag includes an NDEF signed message, proving the identity of the creator, it does not prevent both elements (message plus signature) from being copied to another tag. This attack is an issue when the tag is used to prevent counterfeiting of a valuable item, or generally speaking, when the tag is used for creating trust from the tap [20].

#### *4.2.5 Denial of Service*

**Attack pattern 9**: Data corruption in the NFC air interface. This is a kind of attack inherent to the wireless nature of the communications involved. In this case, the adversary develops a denial of service attack by means of disturbing the communication, not allowing a communicating party to understand the data sent by the other one. This data corruption can be achieved via the transmission of selected frequencies of the spectrum at the correct times [26].

**Attack pattern 10**: Repeated interactions. When an NFC enabled smartphone touches or gets very close to a tag, this action causes a reaction of the handset, regardless of whether the tag has valid contents or is empty. This way, the smartphone keeps occupied. The adversary can use hidden tags in usual places where the users leave their smartphones, for example, under a restaurant table or a library desk [34].

#### *4.2.6 Elevation of Privilege*

This threat defined in STRIDE is not applicable, as there are no root or privileges involved in the data flow between an NFC tag and an NFC-enabled smartphone.

## 5 Discussion, Possible Mitigation and Challenges

In this section, a discussion is provided for each category of the aforementioned security threats along with possible mitigation and related challenges.

### *5.1 Spoofing*

Different countermeasures regarding physical protection are useful when trying to prevent tag replacement. In effect, just mounting the NFC tag behind a barrier of plastic or glass prevents peeling off the tag as well as its physical removal, and makes evident a potential tag replacement to the end-user, as placing the new tag over the barrier would raise suspicions for sure. This also applies if the adversary shields the original tag and overlaps the spoofed one.

Putting metal frames on the backside of the original tag prevents the use of a non-visible spoofed tag after destroying the original one. This implies the use of specific "on-metal" tags because the metal frame behind the tag acts a ground plane, severely reducing the performance of the tag's internal antenna. The disadvantages are that on-metal tags not only are a bit more expensive than the regular ones but also suffer from a performance reduction in terms of reading

distance. This last limitation could be partially compensated by the use of bigger tags (which in turn increases the overall costs).

Concerning countermeasures for the spoofing of URIs, it is essential to keep in mind that NDEF records are usually stored in plain text, and thus a smartphone reading an NFC tag is not able to detect whether the read NDEF message is authentic or fake. So, without some level of integrity protection, an NFC tag containing a spoofed and malicious URL could allow an adversary to launch a phishing attack.

The usual way to prevent this kind of attack was relying on the installation of an antivirus app that provides safe web browsing functionality (using blacklists, whit lists and crowd-sourced website reputation ratings). However, the truth is that there are still many smartphone users without any antivirus app, or a similar security suite installed on their devices.

One clear alternative is signing the NDEF record, allowing the user to identify the signer (if she wishes to do so), and at the same time protecting the integrity of the contents. To address this issue, the NFC Forum developed the Signature Record Type Definition (Signature RTD 2.0), that defines how a digital signature should be appended to an NDEF record. The NDEF record itself is still stored in clear text, therefore making it possible for any NFC tag reader to read the signed data even in the case they cannot verify it [35].

The problem of this approach is that it requires the use of a fully operative trusted PKI, and today, the verification of the signature usually involves the use of a pre-installed dedicated app. This problem will be solved as soon as the signature verification functionality is implemented at OS level in NFC enabled smartphones, perhaps using the services of the NFC Forum approved CAs (it would be even better if those CAs provided the content issuers with an online signature generation service for the sake of a reduced complexity).

So, taking into consideration the previous discussion, one partially effective countermeasure to deal with the URI spoofing threat could be linking to an app developed by the content issuer and made it available to the user on the major App Stores, and making visible the corresponding logos on the NFC smart poster as an indication to the end-user about the expected contents. This could provide the user a mechanism to authenticate contents, but at the cost of sacrificing the "touch and go" experience.

On another front, there exists a vulnerability affecting only Android OS and related to NFC spoofing attacks. This vulnerability, with assigned code CVE-2019-9295 in the Common Vulnerabilities and Exposures list, allows a rogue application to trick the Android OS Tags app (default Tags reader) into thinking a new NFC tag was just read or spoofing a tag that has been read [36]. Google has addressed this vulnerability in Android 10 only, and the fix has not been backported to prior versions of Android. So, the only countermeasure available is updating to Android 10 or later, even though there is a non-negligible base of Android smartphones that will not be able to upgrade due to hardware constraints or vendor-specific Android OS skins not following the official versions upgrade path for older models.

Finally, the spoofing of a Wi-Fi Internet connection via NFC is another version of a common social engineering trick that allows an adversary to eavesdrop the user's traffic using rogue Access Points. The only countermeasure available is the use of a VPN, and this falls into the category of training and awareness-raising for the users about dealing with public Internet connections.

### *5.2 Tampering*

One specific way of protecting NFC cards from overwriting NDEF contents attacks is the use of write protection. All NFC Forum tag types provide the content issuer with soft write protection, which is simply a flag in the tag data memory area whose status can be toggled, indicating that NFC enabled smartphones or other NFC devices must not write data to the card. It is important to note that this flag does not physically prevent write operations, as it depends on applications' compliance with the rule. So, relying on this countermeasure should be avoided.

Fortunately, NFC Forum Types 1 & 2 tags support a usable hard write protection method, using special lock bits that enable a permanent write-protection of the tag. For the rest of the NFC Forum tags, this write protection is not covered by the specification as in the previous case, and the existence of this protection mechanism depends on specific implementations from tag vendors. Then, using NFC Forum Types 1 & 2 tags or selected Type 3, 4 & 5 tags, the content issuer must switch on the permanent physical write protection of the tags before their physical deployment in public places, as a countermeasure to avoid malicious tampering carried out by an adversary.

### *5.3 Repudiation*

Several specific models of NFC tags (e.g., NTAG213, NTAG215 and NTAG216) implement an internal interaction counter, and are even able to reflect its value in the NDEF message area, so that the URL transmitted back to the reader device can include the counter's value as a parameter. This is not standard functionality in an NFC tag, and anyway, the described operation can't be used for logging activity of user's data or identifiable information about her smartphone. A possible mitigation for this threat is not without complexity, and is outside the scope of this work, but it is feasible, and will be the focus of future work.

### *5.4 Information Disclosure*

In those cases when NDEF-written NFC tags are reused by developers or other content issuers before their public deployment, the logical and intuitive countermeasure to prevent potential data restoring by and adversary is to properly erase data from the NFC tag. Usually, this can be easily done using official apps from the tag vendors, which provides the user with a profound or factory-reset erase option that overwrites each and every single memory block of the tag being processed with new data (such as 0xFF).

On another front, an adversary can easily choose from several free applications available in the app stores to fully clone the data of a regular NFC tag, or copy the relevant NDEF contents of a tag. Besides that, there is not even the need to use a specialized app to clone the data, as an adversary could tap the tag using her smartphone, save the returned URL in the browser and reuse it at will. When the HTTP(s) server receives the request, it is completely unable to tell if this request is a consequence of an actual tap on an NFC tag or if it comes from a stored URL.

In order to detect cloned tags, several vendors such as NXP, HID and ST offer special tag chips that are able to transparently append their unique serial number to the URL contained into the NDEF message, as a query string . The utility of this functionality is quite limited for detecting cloned tags, so in some cases, this operation is improved with the additional insertion of a dynamic tap counter in the query string. In the former case, the same tag (or its clone) will return the same URL on very tap, and in the latter case, the URL returned will only differ in the tap counter value (with appropriate server processing, it should be possible to detect cloned

tags) but the URL format is very predictable and could be used by an adversary to trick a server application.

One recent solution is the use of dynamic unclonable tags. Generally speaking, this means that the tag vendor encodes each tag including a unique hidden key, that is used (alone or in combination with other extra data, for example, the tag serial number and the current value of the internal touch counter) to generate a unique code at each tap. This code is appended to the URL in the query string and can be checked at the application server, using the same key (stored in the server itself, or accessing the tag vendor's authentication server) as well as the aforementioned extra data received in the HTTP request as part of the query string.

Since the code is dynamically generated and changes on every tap, it is not possible to copy the data in a way it can be reused without being rejected by the server. So, this functionality allows the application server to tell real taps from fake taps that make use of stored URLs in a browser or shared URLs. This is especially relevant for security applications where it is critical to rely on trusted taps at fixed locations (for example, when logging rounds of security personnel patrolling facilities, coupled with authentication methods, such as simple fingerprint biometrics or combined with other advanced behavior-based biometrics) [37].

Finally, special care should be taken if this functionality is used to provide clients of a company with proof of authenticity of their products, detecting counterfeits. In effect, the described mechanism, using "trusted tags" truly offers proof of authenticity of a specific tag, but the problem is that the end-user usually does not know anything about what web page to expect after the tap (maybe it is the first time she visits the company's web page). So, an adversary could use her own tag in a counterfeited product, claiming its authentic. A more secure solution is to check the validity of the tags using the official app of the company, previously downloaded by the user from the appropriate app store, with the downside of losing the frictionless "touch and go" operation of NFC technology.

### *5.5 Denial of Service*

Jamming NFC RF signals can be as easy as using an "out-of-the-box" broadband jammer usually reserved to security forces (police, army, etc). To disturb the NFC data interchange, it is just necessary to jam the sub-carrier sidebands during transmission (in ISO 14443 that means 13.56 MHz +/− 848 kHz). This can be easily done with standard equipment from a distance of a few meters, but it requires huge power and big antennas to gain more jamming distance.

Conventional RF jamming is the only option when the adversary is not able to get close to the target NFC card, but if physical proximity is feasible, there is another option: reflective jamming using a particular tag. This tag must be placed very close to the target one (ideally hidden and just behind it), and whenever an NFC reader device approaches and initiates a communication with the target card, the jammer card scavenges energy from the ongoing communication, generating a blocking RF signal making the intended communication impossible. This type of jammer cards is readily available on the market, usually as protections against non-authorized credit card wireless data extraction, or even credentials theft.

There are no known countermeasures against jamming, but with an estimation of the expected interactions and a close inspection of the HTTP server logs frequently could reveal lack of operations, resulting in early detection of a jamming attack (or other types of DoS attacks such as removal and destruction) to a specific NFC tag.

Finally, in the less frequent case of suffering the repeated interactions attack, the countermeasures are quite obvious: locating the source of interaction requests (the hidden tags) and removing it, temporarily disable the NFC operation in the smartphone or just moving the smartphone to a safe place where no interaction is requested.

## 6 Conclusion

NFC (Near Field Communication) is a popular short-range wireless communication technology. Its reader/writer mode provides a plethora of useful applications within Industry 4.0 and the Industrial Internet of Things. A barrier of adoption for this technology in these application domains is the security issues that previous research works and real projects have identified.

Beyond the potential benefits and applications of NFC, often discussed and demonstrated so far, practitioners should also be aware of and prepared for security threats that come with the technology. Many of the aforementioned application domains involve mobile devices and NFC tags generating, collecting, storing, or sharing a significant amount of data that may be personal or business-critical.

This paper has proposed a threat model of the NFC reader/writer operation mode. The proposed model is based on building attack trees with the STRIDE methodology for security threats, performing experiments within a controlled lab to verify which attack patterns would allow an adversary to materialize identified threats. Furthermore, to analyze available mitigation strategies and countermeasures.

This model can be a powerful tool to understand the threats that this technology brings to any project that relies on it, to proactively manage the associated risks, to prioritize the deployment of mitigation strategies and to improve the organization security posture by making informed decisions.

We are currently working on validating the model in other application domains, since, although the threats that imply the use of NFC would be the same, it is possible that we may find other attack patterns that would allow an adversary to materialize them. And, in other parallel line of work, we are currently working on a novel logging mechanism in order to address the security threats related to repudiation,

Finally, we are also extending the model to include privacy threats and other technologies or paradigms that often appear in use cases alongside NFC such as a VLC [38].

**Funding Statement:** The author(s) received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] NFC Forum, *Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications*. Wakefield, MA, USA: NFC-Forum, 2017. [Online]. Available: https://members.nfc-forum.org/resources /white_papers/NFC_Smart_Posters_White_Paper.pdf.

[2] G. Proehl, *An Introduction to Near Field Communications*. Amsterdam, The Netherlands: ST-Microelectronics, 2013. [Online]. Available: http://www.st. com/content/st_com/en/applications/connectivity/near-field-communication-nfc.html.

[3] G. Madlmayr, J. Langer, C. Kantner and J. Scharinger, "NFC devices: Security and privacy," in *Proc. of the 2008 Third Int. Conf. on Availability, Reliability and Security*, Barcelona, Spain IEEE, pp. 642–647, 2008.

[4] M. Roland and J. Langer, "Digital signature records for the NFC data exchange format," in *Proc. of the 2010 Second Int. Workshop on Near Field Communication*, Monaco, Principality of Monaco, IEEE, pp. 71–76, 2010.

[5] D. Saeed, R. Iqbal, H. H. R. Sherazi and U. G. Khan, "Evaluating near-field communication tag security for identity theft prevention," *Internet Technology Letters*, vol. 2, no. 5, pp. e123, 2019.

[6] A. Asaduzzaman, S. Mazumder and S. Salinas, "A promising security protocol for protecting near field communication devices from networking attacks," *International Journal of Security and Networks*, vol. 13, no. 2, pp. 98–107, 2018.

[7] D. Giese, K. Liu, M. Sun, T. Syed and L. Zhang, "Security analysis of near-field communication (nfc) payments. arXivpreprint arXiv: 1904106232019, 2019.

[8] H. Abukwaik, C. Groß and M. Aleksy, "NFC-based commissioning of adaptive sensing applications for the 5G IIoT," in *Proc. of the Int. Conf. on Broadband and Wireless Computing, Communication and Applications*, Antwerp, Belgium, Springer, pp. 150–161, 2019.

[9] R. Ramanathan and J. Imtiaz, "NFC in industrial applications for monitoring plant information," in *Proc. of the 2013 Fourth Int. Conf. on Computing, Communications and Networking Technologies*, Tiruchengode, India, IEEE, pp. 1–4, 2013.

[10] A. M. Lesas and S. Miranda, "State-of-the-art of NFC," in *The Art and Science of NFC Programming*, 1st ed., Hoboken, NJ, USA: John Wiley & Sons, 2017.

[11] M. J. L. Fernández, J. G. Fernández, S. Rios-Aguilar, B. S. Selvi and R. G. Crespo, "Control of attendance applied in higher education through mobile nfc technologies," *Expert Systems with Applications*, vol. 40, no. 11, pp. 4478–4489, 2013.

[12] S. Rios-Aguilar, J. Pascual-Espada and R. González-Crespo, "NFC and cloud-based lightweight anonymous assessment mobile intelligent information system for higher education and recruitment competitions," *Mobile Networks and Applications*, vol. 21, no. 2, pp. 327–336, 2016.

[13] C. González García, E. R. Núñez-Valdez, V. García-Díaz, C. Pelayo García-Bustelo and M. Cueva Lovelle, "A review of artificial intelligence in the internet of things," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 4, pp. 9–20, 2019.

[14] A. Shostack, "Finding threats," In: *Threat Modeling: Designing for Security*, 1st ed., Hoboken, NJ, USA: John Wiley & Sons, 2014.

[15] M. Roland, "Near field communication," In: *Security Issues in Mobile NFC Devices*, Heidelberg, Germany: Springer, 2015.

[16] NFC Forum, Data Exchange Format (NDEF) Technical Specification v1.0, Wakefield, MA, USA: NFC Forum, 2006. [Online]. Available: https://nfc-forum.org/product/nfc-data-exchange-format-ndef-technical-specification/.

[17] NFC Forum, Smart Poster Record Type Definition Technical Specification v1.0, Wakefield, MA, USA: NFC Forum, 2006. [Online]. Available: https://nfc-forum.org/product/smart-poster-record-type-definition-technical-specification/.

[18] NFC Forum, URI Record Type Definition Technical Specification v1.0, Wakefield, MA, USA: NFC Forum, 2006. [Online]. Available: https://nfc-forum.org/product/nfc-uri-record-type-definition-technical-specification/.

[19] NFC Forum, Smart Posters. How to Use NFC Tags and Readers to Create Interactive Experiences that Benefit both Consumers and Businesses, Wakefield, MA, USA: NFC Forum, 2011. [Online]. Available: https://members.nfc-forum.org/resources/white_papers/NFC_Smart_Posters_White_Paper.pdf.

[20] HID-Global, The Power of Choice: From Standard NFC to Secure Solutions, Austin, texas, USA: HID Global, 2019. [Online]. Available: https://www.hidglobal.com/sites/default/files/resourcefiles/hid-nfc-tags-and- solutions-wp-en.pdf.

[21] NFC Forum, Type 1 Tag Operation Specification v1.2, Wakefield, MA, USA: NFC Forum, 2014. [Online]. Available: https://nfc-forum.org/product/nfc-forum-type-1-tag-specification-version-1-0/.

[22] NFC Forum, Type 2 Tag Operation Specification v1.2, Wakefield, MA, USA:: NFC Forum, 2014. [Online]. Available: https://nfc-forum.org/product/nfc-forum-type-2-tag-specification-version-1-0/.

[23] NFC Forum, Type 3 Tag Operation Specification v1.2, Wakefield, MA, USA: NFC Forum, 2014. [Online]. Available: https://nfc-forum.org/product/nfc-forum-type-3-tag-specification-version-1-0/.

[24] NFC Forum, Type 4 Tag Operation Specification v3.0, Wakefield, MA, USA: NFC Forum, [Online]. Available:, 2014. [Online]. Available: https://nfc-forum.org/product/nfc-forum-type-4-tag-specification-version-1-1/.

[25] NFC Forum, Type 5 Tag Operation Specification v1.0, Wakefield, MA, USA: NFC Forum, 2015. [Online]. Available: https://nfc-forum.org/product/nfc-forum-type-5-tag-technical-specification-1-1/.

[26] E. Haselsteiner and K. Breitfuß, "Security in near field communication (NFC) - strengths and weaknesses," in *Workshop on RFID Security*, Graz, Austria, pp. 12–14, 2006, http://rfidsec2013.iaik.tugraz.at/RFIDSec06/Program/papers/002.

[27] M. M. Singh, K. A. A. K. Adzman and R. Hassan, "Near field communication (NFC) technology security vulnerabilities and countermeasures," *International Journal of Engineering & Technology*, vol. 7, no. 4.31, pp. 298–305, 2018.

[28] C. Mulliner, "Vulnerability analysis and attacks on nfc-enabled mobile phones," in *Proc. of the 2009 Int. Conf. on Availability, Reliability and Security*, Fukoka, Japan, IEEE, pp. 695–700, 2009.

[29] M. Roland, J. Langer and J. Scharinger, "Security vulnerabilities of the NDEF signature record type," in *Proc. of the 2011 Third Int. Workshop on Near Field Communication*, Hagenberg, Austria, IEEE, pp. 65–70, 2011.

[30] C. H. Chen, I. C. Lin and C. C. Yang, "NFC attacks analysis and survey," in *Proc. of the 2014 Eighth Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing*, Birmingham, UK, IEEE, pp. 458–462, 2014.

[31] A. Shostack, "Experiences threat modeling at Microsoft," in *2008 Workshop on Modeling Security*, Toulouse, France, Microsoft, vol. 2008, 2008.

[32] P. Schoo and M. Paolucci, "Do you talk to each poster? Security and privacy for interactions with web service by means of contact free tag readings," in *Proc. of the 2009 First Int. Workshop on Near Field Communication*, Hagenberg, Austria, IEEE, pp. 81–86, 2009.

[33] NFC Forum, Connection Handover Technical Specification v1.5, Wakefield, MA, USA: NFC Forum, 2019. [Online]. Available: https://nfc-forum.org/product/connection-handover-ch-technical-specification-1-5/.

[34] S. Maruyama, S. Wakabayashi and T. Mori, "Trojan of things: Embedding malicious nfc tags into common objects," *arXiv preprint*, 2017, arXiv:170207124.

[35] NFC-Forum, Signature Record Type Definition Technical Specification v2.0, Wakefield, MA, USA: NFC Forum, 2015. [Online]. Available: https://nfc-forum.org/product/nfc-signature-rtd-certificate-policy/.

[36] National Institute of Standards and Technology, *Common vulnerabilities and exposures (CVE-2019-9295)*. Gaithersburg, MD, USA: NIST, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-9295.

[37] Y. Sun, Q. Gao, X. Du and Z. Gu, "Smartphone user authentication based on holding position and touch-typing biometrics," *Computers Materials & Continua*, vol. 61, no. 3, pp. 1365–1375, 2019.

[38] S. Rios-Aguilar, Í. Sarría Martínez de Mendivil and M. Beltrán Pardo, "NFC and VLC based mobile business information system for registering class attendance," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 6, no. 2, pp. 71–77, 2020.