Quick Response (QR) code security and threats

University of Turku
Department of Computing
Bachelor's Thesis
Information Technology
March 2026
Luca Mäkilä

UNIVERSITY OF TURKU
Department of Computing

Luca Mäkilä: Quick Response (QR) code security and threats

Bachelor's Thesis, 26 p.
Information Technology
March 2026

The use of Quick Response (QR) codes has increased rapidly in consumer use during the last years. The increase has also attracted malicious users who tamper legitimate codes or steal personal ones. Contrary to what one would think, the security measures surrounding QR codes has not been able to keep up as well as it should have. This topic is very important in networking and cyber security as QR codes possess security risks and are not talked about that much. Previous research shows that QR codes can be used in phishing and malware download campaigns. They also show that researchers have come up with numerous own solutions to defend against these attacks. This thesis is a literature review on previous studies that focus on the attacks and security solutions surrounding QR codes. This has been done using the IEEE Xplore and ACM Digital Library databases to find the research material. Key findings of this thesis are that QR codes can be utilized to perform hard to notice attacks, and that the current mainstream applications do not possess high enough security to protect against these attacks.

Keywords: QR codes, security, safety, attacks, threats, phishing, malware, cyber security

Contents

1 Introduction

It is not uncommon today to see data being transferred with Quick Response (QR) codes as they are cheap to make, easy to deploy and can store a large amount of data. QR codes, along with similar Aztec codes and Data matrices, are a subcategory of two-dimensional matrix barcodes (2D matrix barcode). All of them are used to transfer data from the code to the receiver without direct contact. The 2D matrix barcodes are successors to the older one-dimensional barcodes (1D barcode) that can be seen most commonly on store proucts. The main advantages of the 2D matrix barcodes in contrast to the 1D barcodes are the amount of data that can be stored in them, error correction possibilities and their ease of use. Combining the flexibility and extendability of 2D matrix barcodes, they can be brought to areas where 1D barcodes would be too tedious to use. The initial use of 2D matrix barcodes was to enhance the productivity in industrial and manufacturing environments where large amounts of data from numerous products needs to be scanned daily. Later, as mobile devices began to emerge, the potential of 2D matrix barcodes were brought to consumer environments as a fast and reliable way to distribute large amounts of information. [4], [9], [15]

As mentioned, there are several different kinds of 2D matrix barcodes and the most recognizable 2D matrix barcode in consumer use is the QR code, which is the main topic of interest in this thesis. [4] With the extensive use of QR codes today in consumer use, there is a cost: they can be used in malicious cyber activity as easily

as in benign ways. The initial motivations for this thesis was a news article where a customer almost got their credentials stolen through a malicious QR code[1] and the general lack of any discussion regarding QR codes' security. This thesis reviews previous research and aims to identify the common attack types surrounding QR codes in consumer use and review the security solutions researchers have made to the QR code systems. These objectives were used to formulate the following research questions (RQ):

RQ 1: What are the common attacks against QR code systems in consumer use?

RQ 2: What security solutions have researchers made to mitigate the attacks?

This thesis is a systematized literature review which was made by reading relevant research articles. The articles were selected and reviewed by the author of this thesis alone. Two research databases containing computer science related articles were used: IEEE Xplore and ACM Digital Library. The literature was searched from the databases using the following prompts: ""QR Code" AND "Artificial Intelligence" AND "Malicious" AND "Security"", and ""QR code" AND ("Security" OR "Safety") AND ("Malicious" OR "Malware" OR "Phishing")". These prompts were made by thinking of suitable keywords that fit the questions and objectives. Due to time management issues and topic changes in this thesis, "Artificial Intelligence" in the first prompt was later deemed useless but persisted in the prompt. This is taken to account in limitations in Chapter 5: Conclusion.

The initial searches found 319 articles in total. Because ACM Digital Library also lists the journals and books where the articles were published, the search was limited to research articles only. After the initial search, the first filter method was to read the titles and abstracts of the articles to determine whether they were relevant to the topic. This reduced the articles down to 39. After that, the articles were

[1]https://www.iltalehti.fi/digiuutiset/a/47302e94-7f13-4054-8273-e76254f9c3cb (now requires free Alma-credentials)

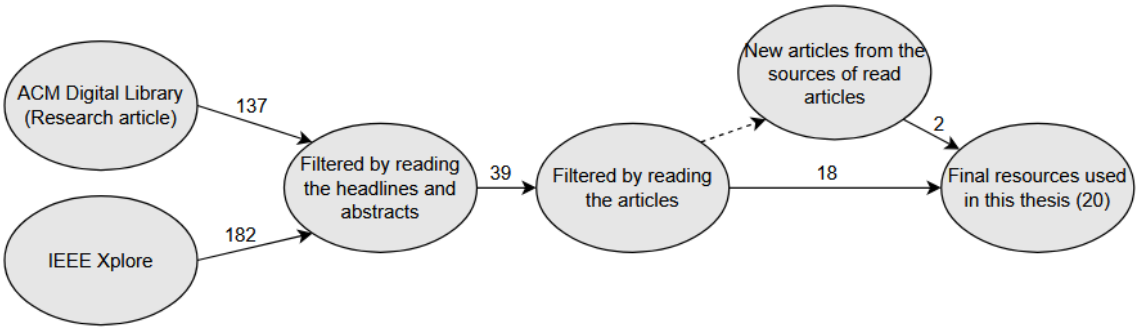

Figure 1.1: Process of gathering literature for this thesis.

fully read to see if they contained suitable research. This reduced the articles down to 18, which were then used as the source material for this thesis. Upon reading the articles, two additional interesting articles, that were not found with the search prompts, were found. These articles were also included in the source material for this thesis. See Figure 1.1 for a detailed literature search process.

This thesis is divided into five chapters, with the first being the introduction to the topic. The second Chapter, "Attacks using QR codes", first presents the structure and intended uses of QR codes leading to the risks of using them followed by addressing the common attack types that are present in QR code environments. The third Chapter, "Current solutions", explains the solutions previous researchers have made in order to mitigate the attacks. The Chapter is divided to scanner applications' and QR codes' security solutions because there were different kinds of solutions to both of these fields. The fourth Chapter, "Discussion", discusses the previous literature, reflects the findings to one another and forms a picture of the current state of QR code safety. The fifth and final Chapter, "Conclusion", summarizes the research answers, discusses limitations and presents further research ideas.

2 Attacks using QR codes

This chapter will first present the intended uses of QR codes before analyzing the different attack types surrounding them. After the attack types, a brief explanation is given about the advantages of the attacker. These are to give an insight on where and how a user can become a victim of QR code based attacks.

2.1 Intended use

QR codes are usually small square-shaped black and white images with the recognizable "finder patterns" in three of its corners. The exact parts of a QR code structure are not crucial to know for this thesis, but for reference see Figure 2.1. QR codes are used in situations where complex or large amounts of data need to be compressed to a small space which also needs to be machine-readable. Situations like these are manufacturing processes, QR encoded Internet links and Paypal payments for example. There are also cases where the QR codes are to be kept private, such as discount coupons, movie or transport tickets and certain payment methods as well. As technology has improved, both public and private QR code uses have risen. [4], [6], [9]

2.2 QR phishing and malware distribution

QR phishing, also known as "QRishing" or "Quishing", is perhaps the most common way a QR code is used maliciously. In phishing, the URL scanned from the QR code redirects the user to a fake copy of the legitimate website in order to steal the users personal information. Usually the legitimate websites are store websites or something similar, to which the users are prompted to enter their personal information such as login details or credit card information. The fake website asks for the information similarly to the legitimate website in order to not raise suspicion. However, the fake website of course gives the information to the attacker who in turn has then succeeded on the attack. [2], [5], [9]

Another notable QR code attack type is malware distribution. In malware distribution attacks, the scanned QR code redirects the users to a malicious website from which the device automatically downloads malware. In some cases the QR code itself is a malware code. In these cases the users do not need to connect to a website to download it, instead the malware executes as soon as the QR code is scanned. If the attack is successful, either the attacker gains access to the device or the device starts to run a malicious script in favor of the attacker. The script then works as any other malware, being able to send itself to saved contacts in order to start a phishing campaign or in a worst case scenario start factory resetting infected devices. [2], [5], [17]

2.3 Code manipulation

As mentioned earlier there are other structurally different 2D matrix barcodes. The most used two of them are Aztec codes and Data matrices, which are relevant to code manipulation attacks. In QR codes the defining characteristic are the square-shaped finder markers in three of its four corners. The rest of the code contains the

encoded data, its metadata and information to the scanner device as to how the code is to be decoded. Aztec codes differ from the traditional QR codes in a way that there is only one square-shaped finder pattern in the middle of the code surrounded by the encoded data. Data matrices do not have a distinct finder pattern feature, instead they have thick surrounding borders on two of its sides and dotted lines on the other two remaining sides, which surrounds the encoded data. [9] See Figure 2.1 for an example of each of the mentioned codes.

Figure 2.1: Examples of a QR code, an Aztec code and a Data matrix [9]. All containing the message "Example Code".

In code manipulation attacks the 2D matrix barcode can have another working 2D matrix barcode code inside of it. A study was made where Aztec codes and Data matrices were tested inside a QR code "host". The study found out that different scanning positions, angles and the addition of whitespace around the inner code made it possible for different scanner applications to read either one code or both of the codes. [4] From a malicious point of view, the attacker could make a legitimate outer host code with a malicious code inside it that leads to a phishing website copy of the legitimate host website.

Another fairly advanced code manipulation technique is to use smart LEDs to make the QR code look different to the scanner than to the human eye. An LED light needs to be positioned so that it points to the targeted QR code and changes the light reflected from the black and white squares. The effect is accomplished by high-frequency flickering with the LED and the combined use of smart lighting and light sensing with the surrounding lights. While not impossible, it requires a very specific setup to accomplish. The QR code must be stationary and large enough to ensure that the LED light is constantly pointed correctly at it. The scanner picks

up the different QR code that the LED light is altering, and the user does not notice any difference. [20]

2.4 Abusing scanned code in applications

Kharraz et al. [8] have well put together three main reasons why the users become more vulnerable to mentioned attacks when using QR codes. The first reason is that because QR codes are not in a human-readable format and the users do not manually enter the URL scanned from the code, they may not find the difference between the benign and malicious URLs. The second reason comes from the limited screen size of mobile devices. Sometimes the URLs can be long enough not to be displayed as a whole on mobile devices' screens. This is an opportunity to make an URL that looks legitimate in the beginning but hides the true domain somewhere far away in the URL. The third reason arises from the fact that URLs can be shortened to an unrecognizable form using certain third-party applications, such as TinyURL[1]. The QR codes made from these shortened URLs do not show the original URL, and rather than directly accessing the original website, the URL redirects the users via the third-party service used to shorted the URL creating obfuscation. [8]

2.5 Advantages of the attacker

In QR phishing and malware distribution the attacker tends to abuse the known weaknesses of the scanner devices and lack of security mechanisms in them. Although the most common scanner devices, smartphones, are relevant in numerous lives today, they are surprisingly prone to cyberattacks, especially malware attacks. Due to Android phones' security system limitations, many Android smartphone antivirus applications do not handle malware and spyware. In addition to poor innate

[1]https://tinyurl.com/

mobile security, a net survey from 2014 concluded that only 14 % of mobile users in the USA had installed an antivirus application, and up to 34 % did not have any antivirus installed. A more recent survey in 2019 shows that the severity of lacking mobile device security has not been taken seriously enough by consumers. The newer survey found out that even among expert mobile users only around 33 % use virus scanners. This lack of security awareness makes mobile devices extremely vulnerable to different types of cyberattacks. [3], [11]

Ironically other relevant mobile security issues are most of the antivirus software. A majority of the software are signature based which means that the software can check potential malicious activity from a database of known attacks. The problem rises with zero-day attacks in which the attacker abuses a newfound weakness in the system not yet detected and patched by the developers. The software does not recognize the attack and it can get through security systems. [11] The attackers are able to bypass the signature based software by generating and distributing same-day QR codes. The lifetime of a same-day QR code is intentionally only a day or two as its purpose is to evade URL detectors and become unusable before the URL is set to the detection database. [11], [17]

The most significant properties of QR codes the attackers can abuse are their easy generation, distribution and opacity. These three make it fairly easy to scatter QR code stickers anywhere. Some of the most common places to use malicious QR codes are busy or information-rich places such as city centers or campus areas. The attacker can introduce an element of social engineering to the attack as well. They can make the malicious QR codes look legitimate by carefully choosing the area and making the surroundings of the QR code look appealing, such as an alleged discount code on a storefront. [8], [17]

3 Current solutions

While the attacks using QR codes are many and diverse, so are the security solutions. The solutions can be brought to different interfaces when working with QR codes, for example modifying the code or increasing scanner security measures. From the sources found, two distinct themes emerged: Scanner application security and security implemented to the code's structure. Scanner application solutions were quite similar to one another so they can be covered in one section. However, solutions to code-level security were more diverse, which is why the themes are segmented to three smaller sub-themes: authentication, encryption and other solutions. Table 3.1 displays which articles are reviewed under which themes.

3.1 Scanner application security

When people think of security in scanning and opening links using their mobile devices, the first thing to come to mind is probably the security solutions of the application. This section covers the scanner security solutions that have been made in order to enhance security when scanning and opening QR codes.

In their research article, Rafsanjani et al. [15] propose a comprehensive secure QR scanner application called QsecR. It is built upon a three-part framework consisting of URL redirection, feature extraction and classification, and malicious URL detection phases. The first phase, URL redirection, aims to notice the different ways cybercriminals have obfuscated URLs. The detector checks the scanned QR

code specifically of any URLs. If an URL is found, it is sent to phase two of the validation process. If the URL is shortened, the detector uses Android WebView to find the original URL using repetitive redirection process called "URL loading override". Any other forms of data are considered benign and are not checked any further. [15]

Table 3.1: Different security measure approaches divided into themes

Article & year	Main topic of the article	Scanner application security solutions	Authentication solutions	Encryption solutions	Other
Rafsanjani et al. (2023) [15]	Legitimate QR code filtering with a classification framework	x			
Krombholz et al. (2015) [10]	Scanner applications' features and flaws, and what could be enhanced on security	x			
Sabri et al. (2023) [16]	QR code link comparison to known malicious domains	x			
Bani-Hani et al. (2014) [1]	Embed QR code generator IDs to the code to ensure integrity		x		
Garnaik et al. (2022) [6]	Use private QR code rotation angles on the device to implement a two factor authentication		x		
Xue et al. (2022) [19]	QR code authentication using device-specific pulse width modification		x		
Song et al. (2018) [18]	Using the imperfections of 3D printed QR codes as an authentication method		x		
Goel et al. (2017) [7]	Transfer AES encrypted data in QR codes			x	
Mittal et al. (2021) [12]	Embed QR codes in cover images to hide larger QR codes			x	
Pan et al. (2019) [14]	Hide QR codes in a Moiré pattern and reveal them in specific angles				x

The second phase of the QsecR framework is feature extraction and classification which is made to extract most relevant and crucial information from the URL to detect malicious links (see Figure 3.1). The parsed URL is then compared to a dataset in a series of classes to determine its legitimacy. There are four main features through which different parts of the URL are sent. The blacklist class checks databases of known malicious links. The lexical class checks the whole URL, its host name, path and top level domain. The host based class extracts information about the host and web rank, the more known website, the less likely it is a malicious one. Lastly the content class extracts the website's content to identify any malicious code. Each of the mentioned extraction classes are done with small enough data sets for near perfect accuracy results. The research paper mentions that although more classes are undeniably better for detection, it becomes overwhelming to process and costly to response time which in turn is a cost on user experience. [15]

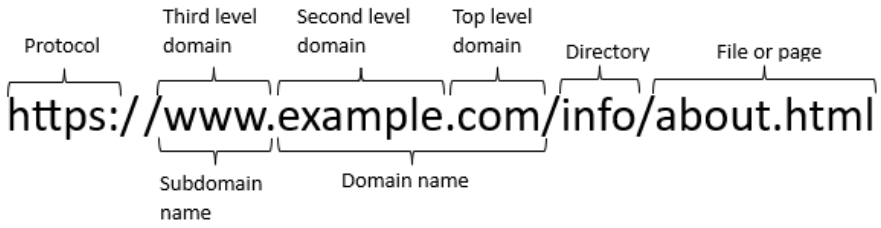

Figure 3.1: Structure of an URL. Reconstructed from [13]

QsecR's third phase is malicious URL detection. A value from 1 to 5 from the second phase's average estimation is given to the third phase's equations to process. With high enough value, the system sends a notification to the user's device informing that the scanned code was in some way malicious and they should proceed with care or drop the process altogether. The researchers behind QsecR deduce that the most crucial parts of a secure QR scanner are URL redirection and careful feature classification processes. [15]

In a different article, Krombholz et al. [10] surveyed 12 of the most common mobile QR code scanner applications and did a security evaluation on the results. The observed application security features were URL modification detection, automatic website analysis and URI display (see Table 3.2). They also examined possible privacy violations of the applications, which were unauthorized external communication, user tracking and location data (see Table 3.3). The results show that the majority of the scanner applications violate user privacy with external communication and user tracking. None of them alerted the user of modified QR codes and none, but one application, did a website analysis when the code was scanned. Only half of the applications even displayed the URL to the user before accessing it. [10]

Writers of the article conclude that applications' security could be enhanced by embedding a malicious URL detection framework and using Google Safe Browsing, to which Google provides a public API for. They also claim content displaying and verification to be useful enhancements to QR applications in general, as the user can decide whether or not to trust the content. [10]

Table 3.2: Security measures of different scanner applications. Reconstructed from [10]

Security measures using different scanner applications			
App	Modification detection	Website analysis	URI display
Scan	No	No	No
Barcode Scanner	No	No	Yes
RedLaser	No	No	Yes
Bakodo	No	No	Yes
QR Droid	No	No	Yes
Quick Scan	No	No	Yes
ShopSavvy	No	No	No
QR Code Reader	No	No	No
Qrafter	No	Yes	Yes
ScanLife	No	No	No
i-nigma	No	No	Yes
AT&T Code Scanner	No	No	No

Table 3.3: Privacy violations of different scanner applications. Reconstructed from [10]

Privacy violations using different scanner applications			
App	External communication	User tracking	Location data
Scan	Yes	Yes	No
Barcode Scanner	No	No	No
RedLaser	Yes	Yes	Yes
Bakodo	Yes	Yes	Yes
QR Droid	Yes	Yes	No
Quick Scan	Yes	No	No
ShopSavvy	Yes	Yes	Yes
QR Code Reader	No	No	No
Qrafter	Yes	No	No
ScanLife	Yes	Yes	Yes
i-nigma	Yes	Yes	No
AT&T Code Scanner	Yes	Yes	Yes

An article by Sabri et al. [16] propose their own secure QR scanner application. Their solution in addition to checking the validity of a code is to save them to an online database which can be accessed every time a QR code is scanned. [16] Taken to account how many QR codes there are out in the world, checking a code from a database every time it is scanned may be too slow for the intended speed and ease of use of QR codes. If we also take to account the fast production of malicious same-day codes, this solution can be efficient targeting them, although resource heavy on the database side. If the same-day codes are similar to one another, not only do they excessively use the database's search feature, but they also clutter the database with unusable codes after a while.

3.2 QR code safety and Authentication

This section covers the security solutions proposed to QR codes themselves and how to uphold their authenticity against malicious codes. In contrast to scanner applications, there were a lot more variety among code safety.

The following solutions have a common theme around authenticating the access to the code in one way or another. These authentications span from more traditional authentication keys to some unusual solutions such as 3D printing the QR codes and using the imperfections as an authentication method. Authentications ensure that the data is from a trusted source, or the owner of the data is who they claim to be.

Secure QR code system. Bani-Hani et al. [1] propose a secure QR code system, which uses a technology resembling asymmetric cryptography. In asymmetric cryptography the encoder, sender of the data, encrypts the data with a private key, and the decoder, receiver of the data, decrypts it with a public key[1]. In their solution, rather than encrypting the data stored in the QR code, the key pair functions only as a password or authenticator technology. The QR code itself contains an ID of the generator, which is then used to fetch the public key. When the QR code is scanned, the application sends a public key request to a trusted third party platform. If the platform contains a match for the generator's ID, it sends the public key to the application, which then accesses the QR code by automatically unlocking the password. This verifies that the QR code is indeed owned by a trusted generator and is safe to use. If the ID match is not found, the application warns the user of a possible malicious QR code. In addition to the authentication technology, they implement a URL checking system similar to what QsecR provided. To reduce the impact if an attacker accesses the phone via the application, they have implemented application isolation in the smart phone environment so that it has little to no access to the phone's resources. [1]

SQR: Secure QR Transaction with Randomized Rotation. Garnaik et al. [6] implement a time-based one-time password (TOTP) to QR code scanning, making it resemble a two-factor authentication. This method is used in digital

[1]RFC 4949: Internet security glossary, version 2, pages 21-22, year 2007

private and personal QR codes, such as in payment or discount codes. [6] This kind of technology is already in use with a more known platform: Google Authenticator.

Google Authenticator works by generating a new 6-digit code every 30 seconds. The code can be used as an authentication method to an online service: when the code is entered to the service input, it is compared to a 6-digit code on an authenticator server. If the codes are identical, the authentication process allows access to the service.[2]

The TOTP works slightly differently on the QR code security method. Instead of reading 6-digit codes and inserting them to an input, the QR code changes its rotation on the phone screen. When the scanner reads the QR code, the code's rotational angle is the TOTP. The rotational angle is sent to an authentication server, as well as the angle the scanner reads. If the angles match, the authentication process allows the action to continue. This is a very useful security method especially to counter scenarios where the attacker tries to steal the QR code by taking a picture of it and intending to use it as their own. If the attacker were to take a picture of this implementation, the stolen QR code on the picture is most likely on a different angle than it should be relative to the screen, which fails the authentication process. [6]

SCREEN ID. Xue et al. [19] propose an authentication solution to QR codes that utilizes the brightness of the screen it is showed from. There are two functionally different forms of adjusting screen brightness: analog dimming and pulse width modulation (PWM). Analog dimming regulates the direct current to adjust the brightness, whereas PWM refreshes the screen using square waves carrying full-amplitude current. Their research focused on the screens with PWM dimming feature as it functions ideally how the research wants, has several advantages over analog dimming and is rapidly gaining popularity among mobile devices with LCD or OLED

[2]https://github.com/google/google-authenticator

screens. Using a light sensor they analyzed the PWMs of 50 phone screens, as well as retrieved data from 300 different screens for the research. They found out that the PWM frequency could be used as a screen identification feature differentiating 99.3 % of tested screens with 0.1 Hz frequency resolution. [19]

Their solution for the QR code authentication is to embed the device screen's PWM frequency and PWM latency between two rows of the square wave to the QR code. When the QR code is then read from the screen, the reader uses the embedded data in tandem with the screen the QR code is showed from to complete the authentication process. This also requires the readers to support this authentication solution. According to them, embedding a rolling shutter interval to the reader is enough to estimate the screen's PWM frequency. If the frequency does not match the calculated estimate, the QR code will not be accepted. This ultimately prevents an attack where the attacker has taken a photo of the QR code, as the screen the attacker shows it from most likely does not match the PWM frequency and latency embedded in the code. [19]

My Smartphone Recognizes Genuine QR Codes! Practical Unclonable QR Code via 3D Printing. Song et al. [18] present an end-to-end QR code verification framework for 3D printed QR codes. The goal of their framework is to provide means to uphold 3D printed products' authenticity to reduce the spread of unauthorized or otherwise fraudulent 3D printed products. The framework they present consists of product-embedded 3D printed QR codes and a database of authenticated QR codes. Their reasoning for this approach is to utilize the inevitable "micro-faults" as fingerprints that occur when manufacturing with 3D printers. The fingerprints depend on multiple factors, some of which are present on almost every 3D printer, such as the stepper motor, hot-end and transmission systems. However, these fingerprints are never perfectly identical to each other thus being great authentication features. When authorized manufacturers print their products, they

embed an identifier QR code to it and upload the finished products' QR codes' fingerprints to a database of authenticated fingerprints. When the QR code is scanned, the reader sends a request to the database to check whether the QR code and the fingerprint are authenticated or not. Their test results for system accuracy for inter- and intra-printer verification performance, and performance with alien and increasing QR codes showed over 95 % success rate on almost every field of accuracy which makes this solution viable for manufacturers. This solution mitigates the manufacturing of fraudulent 3D items in the industry, as the fingerprints on 3D printed QR codes are unique enough to uphold authenticity. It also requires time and resources from the attacker if they were to manufacture fraudulent items with 3D printed QR codes, as a single QR code in on itself took about two hours to print. [18]

3.3 Encryption

This subsection covers the articles that share a theme with encrypting the QR code or its contents as a safety measure. Encryptions ensure that the content is secured during transmission and can not be accessed by outsiders.

A way to secure a QR code: SQR. Goel et al. [7] propose a common encryption solution to QR codes: the Advanced Encryption Standard (AES[3]). Rather than transporting plaintext in QR codes, their solution first encrypts the data to be stored with a key generated from a password. When the QR code is scanned, the user is prompted with a password input to decrypt the data stored. [7] This is a strong solution to attacks targeting the transmission areas of data traffic, as AES encryption very difficult to crack. While it was briefly mentioned in the article, it should be emphasized that AES encryption is a symmetric encryption type where both the sender and the receiver needs to know the passwords to generate the keys, so for example a library extension for known keys is not suitable for this solution.

[3]RFC 4949: Internet security glossary, version 2, pages 15-16, year 2007

Achieving Privacy and Security Using QR-Code through Homomorphic Encryption and Steganography. Mittal et al. [12] propose homomorphic NTRU encryption and steganography solutions to QR codes used in banking environments. Homomorphic encryption allows sensitive encrypted data to be used as a parameter to functions as if it were in plaintext. The output of said functions still remain encrypted and can then be decrypted using correct keys. This technique ensures that personal and/or sensitive information, such as banking credentials, stay encrypted.[4] N-th degree Truncated polynomial Ring Units (NTRU) is an encryption algorithm that the National Institute of Standards and Technology (NIST) has issued to be the best post-quantum cryptography standardization, meaning it can withstand a cyberattack done by a quantum computer.[5] Steganography's basic premise is to encrypt data into another piece of data known as a cover image to simultaneously hide it in plain sight and to uphold secrecy. This article aims to use all three mentioned techniques to enhance the security of banking and online transactions. Similar to the article by Goel et al. [7] the sensitive data is first encrypted with homomorphic NTRU encryption after which a QR code is made from it, which is then embedded into a cover image to hide it. All of this is to ensure maximum security which is also quantum-proof. [12] Unlike other solutions, this may be the only solution that is possible solely in digital form, as the data hidden with steganography relies on the cover image's metadata, which is difficult to extract from printed images.

3.4 Other

While the authentication and encryption solutions are the common policies for security, it does not need to be limited just to them. In this subsection is presented an

[4]https://www.ibm.com/think/topics/homomorphic-encryption

[5]https://ntru.org/

uncommon solution to security that does not quite align with either authentication nor encryption.

mQRCode: Secure QR Code Using Nonlinearity of Spatial Frequency in Light. Pan et al. [14] propose an unusual approach to QR code security. Their solution uses the nonlinearities in the spatial frequency of light to camouflage QR codes. Spatial frequency is a characteristic of a structure that is periodic across its position in space, such as an infinite continuous straight black lines on a white surface with a fixed distance between two lines. Nonlinearity of spatial frequency occurs when two spatial patterns overlap with different angles. The generated pattern is referred to as a Moiré pattern (see Figure 3.2). When using cameras to take pictures of spatial patterns, they are susceptible to Moiré patterns because of the design of the camera's color filter array (CFA). Thus, when taking a picture of a display with a camera, the display's pixels form a spatial pattern, and the camera's CFA forms another layer. These two layers then overlap and form a nonlinear optical interaction (see Figure 3.3). The interaction of the two layers is then exploited in this article to manufacture the mQRCode system. [14]

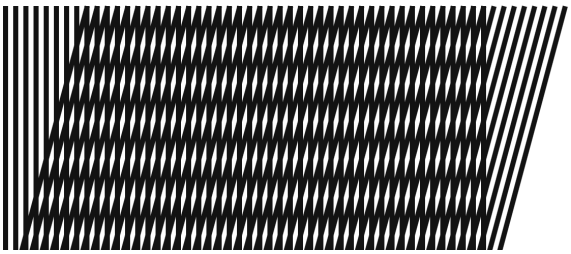

Figure 3.2: Moiré pattern of two spatial frequencies (different angled black lines at 0° and 15°). Reconstructed from [14].

In the mQRCode system the generated QR code is encrypted with a color filter array model, phase modulation, frequency modulation and phase discontinuity. The color filter array makes it difficult for human eyes to distinguish the QR code, and presents the requirement to hold the scanner at a specified position. Phase modulation enlarges the contrast of the Moiré pattern, and frequency modulation makes

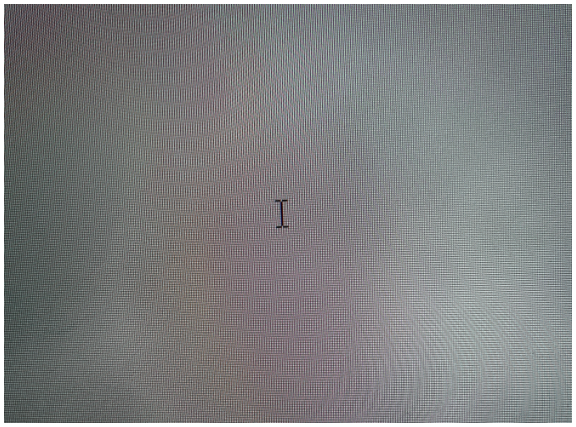

Figure 3.3: Moiré pattern formed by taking a picture of a display. Reconstructed from [14]. The image brightness and resolution have been altered to better see the pattern.

it possible to scan the code from different distances. Finally, phase discontinuity removes any observable horizontal and vertical lines which could give the structure of the code away. This is done by introducing noise to the encryption camouflage. When scanning the code, the scanner must be held at a specified position in order for the scanner's CFA and the code's Moiré encryption to match, which reveals the code to the scanner. The article presents two decryption schemes for the mQRCode system: multi-frame decryption and fast frame decryption. In the multi-frame decryption the scanner takes multiple pictures of the encrypted QR code and runs them through a seven phase decryption process to construct the original QR code. In the fast encryption scheme the display with the QR code flashes between the Moiré pattern and the encrypted code. The scanner takes an image of them both and decrypts the mQRCode with the Moiré pattern. In contrast to the multi-frame decryption, the fast decryption process is faster and requires only two frames for decryption, but is more prone to errors if the scanner, or code, is not held stationary in place. [14]

4 Discussion

Previous research [2], [5], [9], [17] discuss that QR code attacks which have either phishing or malware download as their main objective aim to deceive the victims similarly to malicious emails and text messages. These attack objectives therefore do not differ that much from more traditional phishing and malware attacks – the QR codes are used as entry points to the main attack in the same manner malicious links are used in phishing and malware emails and messages. The attackers have some advantage using QR codes as the attacks are made easier to accomplish due to QR codes' obfuscated data and the lack of security and advanced functionality in scanner applications as Krombholz [10] listed.

The other more unique attack type that previous research [6], [14], [19] presented is the QR code stealing attack. In the physical world, this attack type could be contrasted to as digital theft or illegal replication of personal possession or in the worst case even identity theft. It is apparent that in order for this attack to succeed the attacker requires a clear line of sight to the QR code in order to take a picture of it. This implies that users falling for this attack are not as protective of their QR codes as they should be. The reason behind this is the same feature what makes QR codes practical in the first place: the data in a compact and non-human readable form. It is not that uncommon to see users trust a visibly unreadable data format because if they cannot read it on the go, surely no one else can. This careless mindset is a key component in QR code stealing attacks.

The previous research do not give that many numbers on how common QR code based attacks are. The only numbers previous research provide are from Kharraz [8] and Krombholz [10] which show that only 145 of the 94770 QR codes crawled from 14.7 million unique web pages contain at least some signs of malicious intent [8], and that 24 out of 83 people scan QR codes very often, with 36 out of the same 83 people do not think much of QR codes or do not consider them to be malicious [10]. These research are over ten years old which almost certainly show numbers that are way lower than they are today. In addition to this, Kharraz's research only reviewed QR codes online and not those in emails, text messages or even in the wild which could yield a much larger percentage of malicious QR codes.

Figures 4.1 and 4.2 show what means the attackers use to trick users into scanning malicious codes, and what the consequences of QR code stealing are. Based on previous research and the nature of QR codes, the attacks have a common factor between them which the attackers abuse to achieve their goals. The attackers target the weakest link in the system which is the users' trust in it. The users trust that the encrypted and obfuscated QR codes are benign to scan and are secure enough

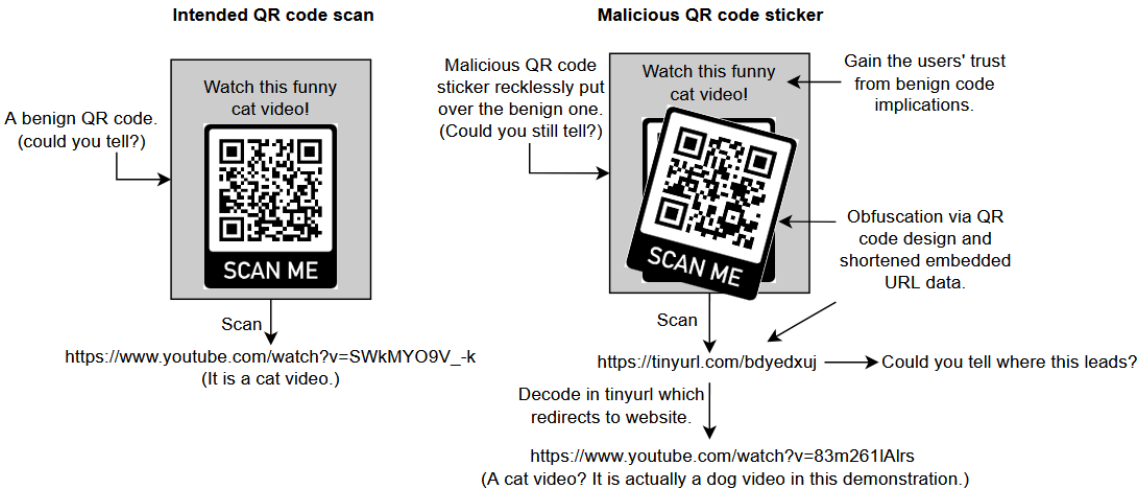

Figure 4.1: An example of how the attacker can trick the users to scan a malicious code. Both QR codes are benign in this example.

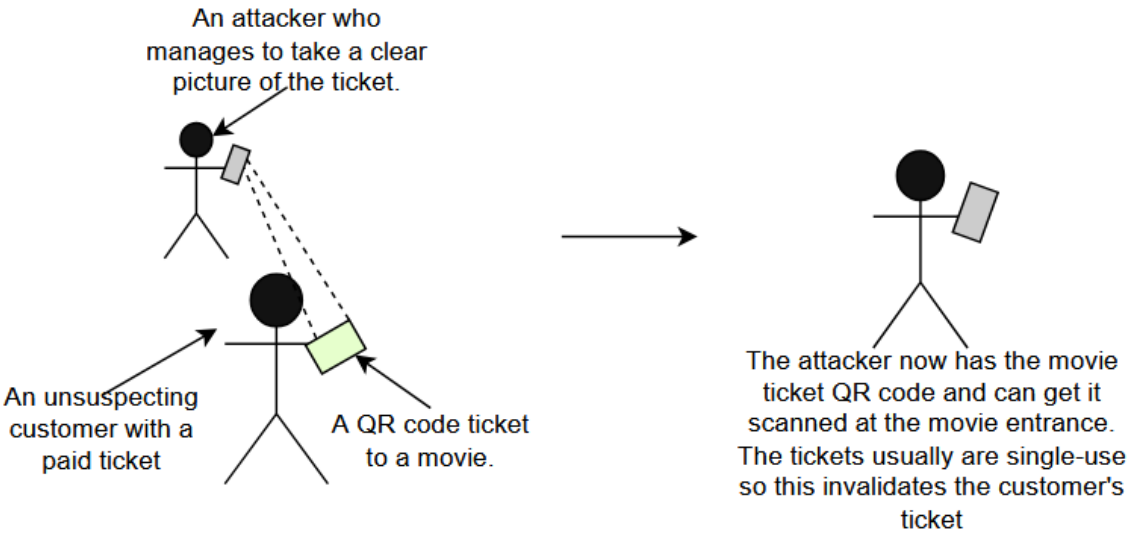

Figure 4.2: An example of how an attacker can steal a personal QR code to use as their own.

to not be concealed because they are, well, encrypted and obfuscated and do not show imminent danger around them.

The other topic from the previous research is the QR code system's security solutions. Krombholz's [10] previous research about the scanner applications available for mobile devices had lacking security features which made the users trust the system unnecessarily blindly. The solutions invented in scanner security solution research share themes in their functionality, but no two identical solutions were made between them. This distribution in security solutions and the lack of identicalness in them inherently show that there are no standards or regulations regarding the security in the QR code system. The invented solutions to QR codes and scanner applications focus on authentication and verification methods which reduces the weigh of trust based merely on the fact that the codes are obfuscated, and assure the user whether the QR code contents are to be trusted. Many modern day mobile devices' camera applications do have a QR code decoder in them which show what is encrypted in the code, however they lack any deeper security solutions, such as website content validation.

The solutions from previous research directly secure the vulnerable trust based component the attackers aim to abuse. Combining the solutions of code authentication, content verification and proper encryption could make for a great whole scanner application which leaves no blind spots for the user. A core component that was not discussed in previous research was the education that should be given to users when working with QR codes. Although proper security measures are always important everywhere, the users should also know what to expect and what can go wrong. Figure 4.3 shows the common attack types QR code users face and what the best practices are to defend against them.

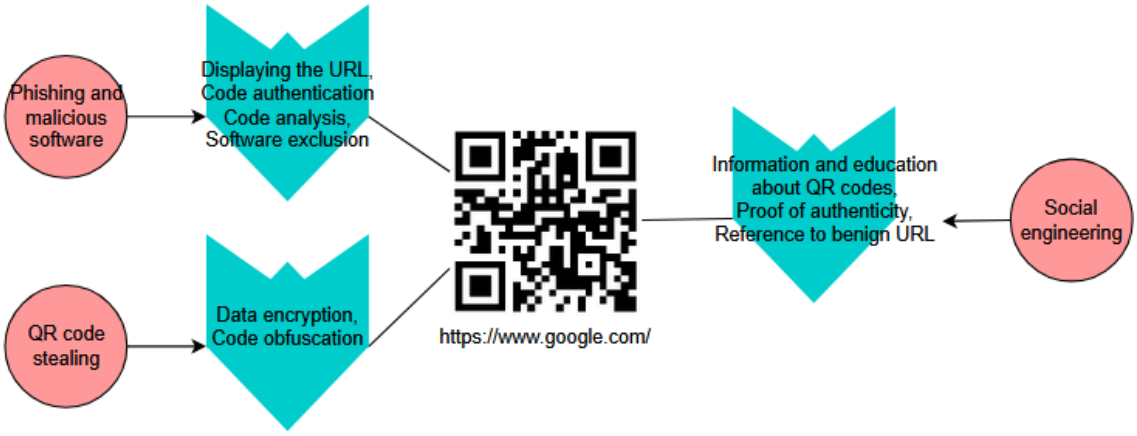

Figure 4.3: Visualization of the attacks and prevention methods surrounding QR codes, based on the previous studies.

From the previous research it can be seen that the environment of QR codes is still a vast landscape for potential threats, the greatest of which is targeting the users' trust. Even though the attacks are not that sophisticated from more traditional phishing, malware downloading and stealing, the QR code system does need proper security solutions to protect against them. The previous research have made effective solutions for these, but the fractured entirety that could be constructed from them is missing. It is clear that attacks utilizing QR codes are still prevalent and can occur to anyone, emphasizing that all QR code users should be wary and double check everything they scan with their devices.

5 Conclusion

As QR codes rise in popularity and usage, their need for security solutions grows in tandem. This thesis has taken a look at the most common attacks utilizing QR code systems and the suggested solutions previous researchers have made to mitigate them. During the writing process, a handful of news articles discussing malicious QR codes, usually with a presented attack, have appeared. This strengthens the fact that QR codes are still used maliciously. The aim of this thesis is to answer the research questions presented in the introduction section through the found source material. The research questions and answers are as follows:

RQ1: The literature reviewed presented many attack types surrounding QR codes. The most common attack vectors, which open possibilities to more advanced attacks, are the use of malicious QR codes and personal QR code stealing. These vectors then make it possible to execute the advanced attacks which are phishing credentials, malware downloads and using others' personal QR codes as the attacker's own.

RQ2: Previous research propose numerous different security solutions to both QR codes and scanner applications. On the QR code level, the security solutions focus on either data encryption or authentication solutions. On the scanner application level, most of the solutions had a common theme of using online databases for URL checking.

Despite answering both research questions, this thesis faces some notable limitations. A good portion of the source material used are not that up to date. The source material is at least two years old with the mean being a little over seven years and the median being seven years old. During the writing process no new source material were searched past the September of 2025 as the previously found source material were deemed to be worthy enough. Initially this thesis was supposed to include the aspect of artificial intelligence in the QR code systems but was discarded later in the writing process. This discard could have limited the sources found as the search prompts still mention artificial intelligence.

Based on the limitations, some great further research are to see if new literature has been made regarding the safety or attacks surrounding QR codes, and whether artificial intelligence has had an impact on QR code safety. As this thesis focused on the user devices used and attacked against, other good further research ideas are to see if similar attacks could be possible in scanner devices used in manufacturing supply lines and in stores and what their effects could be. Another great field research idea is to go out, map and scan QR codes in the wild and see how likely it is to fall victim to QR code attacks. Proper equipment is recommended to do this as possible malware downloads are pests in your personal device.

References

[1] R. M. Bani-Hani, Y. A. Wahsheh, and M. B. Al-Sarhan, "Secure qr code system", in *2014 10th International Conference on Innovations in Information Technology (IIT)*, IEEE, 2014, pp. 1–6.

[2] V. S. Bhamidipati and R. S. Wvs, "A novel approach to ensure security and privacy while using qr code scanning in business applications", in *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)*, IEEE, 2022, pp. 198–203.

[3] F. Breitinger, R. Tully-Doyle, and C. Hassenfeldt, "A survey on smartphone user's security choices, awareness and education", *Computers & Security*, vol. 88, p. 101 647, 2020.

[4] A. Dabrowski, K. Krombholz, J. Ullrich, and E. R. Weippl, "Qr inception: Barcode-in-barcode attacks", in *Proceedings of the 4th ACM workshop on security and privacy in smartphones & mobile devices*, 2014, pp. 3–10.

[5] R. Focardi, F. L. Luccio, and H. A. Wahsheh, "Usable cryptographic qr codes", in *2018 IEEE International Conference on Industrial Technology (ICIT)*, IEEE, 2018, pp. 1664–1669.

[6] S. S. Garnaik, Y. Kim, and J. Ryoo, "Sqr: Secure qr transaction with randomized rotation", in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, IEEE, 2022, pp. 1697–1702.

[7] N. Goel, A. Sharma, and S. Goswami, "A way to secure a qr code: Sqr", in *2017 international conference on computing, communication and automation (ICCCA)*, IEEE, 2017, pp. 494–497.

[8] A. Kharraz, E. Kirda, W. Robertson, D. Balzarotti, and A. Francillon, "Optical delusions: A study of malicious qr codes in the wild", in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, IEEE, 2014, pp. 192–203.

[9] P. Kieseberg et al., "Qr code security", in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430–435.

[10] K. Krombholz, P. Frühwirt, T. Rieder, I. Kapsalis, J. Ullrich, and E. Weippl, "Qr code security–how secure and usable apps can protect users against malicious qr codes", in *2015 10th International Conference on Availability, Reliability and Security*, IEEE, 2015, pp. 230–237.

[11] V. Mavroeidis and M. Nicho, "Quick response code secure: A cryptographically secure anti-phishing tool for qr code attacks", in *Computer Network Security: 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2017, Warsaw, Poland, August 28-30, 2017, Proceedings 7*, Springer, 2017, pp. 313–324.

[12] S. Mittal, P. Kaur, and K. Ramkumar, "Achieving privacy and security using qr-code through homomorphic encryption and steganography", in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, IEEE, 2021, pp. 1–6.

[13] A. Nandu, J. Sosa, Y. Pant, Y. Panchal, and S. Sayyad, "Malicious url detection using machine learning", in *2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, IEEE, 2024, pp. 1–6.

[14] H. Pan, Y.-C. Chen, L. Yang, G. Xue, C.-W. You, and X. Ji, "Mqrcode: Secure qr code using nonlinearity of spatial frequency in light", in *The 25th Annual International Conference on Mobile Computing and Networking*, 2019, pp. 1–18.

[15] A. S. Rafsanjani, N. B. Kamaruddin, H. M. Rusli, and M. Dabbagh, "Qsecr: Secure qr code scanner according to a novel malicious url detection framework", *IEEE Access*, vol. 11, pp. 92 523–92 539, 2023.

[16] N. S. A. M. Sabri, N. M. Noor, and Z. Kasiran, "Secured qr scanner (sqr) based on query method", in *2023 IEEE 8th International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, IEEE, 2023, pp. 1–6.

[17] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Phishing with malicious qr codes", in *Proceedings of the 2022 European Symposium on Usable Security*, 2022, pp. 160–171.

[18] C. Song, Z. Li, W. Xu, C. Zhou, Z. Jin, and K. Ren, "My smartphone recognizes genuine qr codes! practical unclonable qr code via 3d printing", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 2, pp. 1–20, 2018.

[19] G. Xue et al., "Screenid: Enhancing qrcode security by utilizing screen dimming feature", *IEEE/ACM Transactions on Networking*, vol. 31, no. 2, pp. 862–876, 2022.

[20] A. Zhou, G. Su, S. Zhu, and H. Ma, "Invisible qr code hijacking using smart led", *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 3, pp. 1–23, 2019.