QR CODE SECURITY: ATTACKS AND COUNTERMEASURES

[1]MERT OGÜN BİLİR, [2]ESMA ERGÜNER ÖZKOÇ, [3] GİZEM ÖĞÜTÇÜ

[1,2,3]Management Information Systems Department, Başkent University
E-mail: [1]mertogunbilir@gmail.com, [2]eeozkoc@baskent.edu.tr, [3]ogutcu@baskent.edu.tr

Abstract - The QR codes (Quick Response Code), which were first used in the production area in 1994, have spread to many areas of life (marketing, advertising, object identification, product tracking, etc.) with the use of mobile devices as QR code readers. Despite the increasing popularity of QR codes, (i) does not create any perceptions of vulnerabilities among users and on the contrary, arouses curiosity (ii) the amount of data in the QR code is considerable (sufficient to execute attacks), making the QR code a target for attacks. There are many security issues and risks such as malicious code execution, redirection to unsafe web addresses and violation of user privacy. In this study, attacks on QR code and countermeasures are presented

Keywords - QR Codes, Security, Malware, Phishing attacks, Mobile device.

I. INTRODUCTION

QR Code (Quick Response) is a square barcode arranged from black shapes and motifs on a white background. Compared to conventional 1-dimensional barcodes, 2-dimensional data matrix can transmit and store more information[1].

Developed by Denso in 1994 for use in the automobile industry, the QR code became popular due to its easy production and distribution, storage capacity and fast readability.

Today, QR codes are often used to direct users to websites based on their interests, which may provide more information or services. In addition, QR codes are used in many different applications. One of these is to solve the problems in image processing by adding QR code to the plates against the errors encountered in reading the numbers and letters on the plate in the automatic plate recognition system [2].

In another application, in order to ensure the safety of work equipment varying according to sectors, to reduce the number of occupational accidents and to ensure sustainable safety importance; suspended scaffolding, hoist, crane etc. QR codes are placed on the machines, providing easy access and ease of use to the documents belonging to the employees and the machines [1]. In the marketing industry, QR codes are used as a complementary way of advertising. An ad can take the customer to a web page with additional information about the product. For example, the chain supermarket Tesco has used QR codes to increase online shopping and further penetrate the South Korean market.Some companies accept “one-click” payments through the QR code.

In order to purchase the product, the customer is directed to the payment page or the company web page by reading the QR code on the mobile phone. Paypal, one of the largest payment companies, has started to use this payment method in some countries [3]. Object identification for the visually impaired [4] is another area where QR code is used.

Although there are many advantages of using QR code in a wide range of daily life, it also brings security problems. The main reason for this is that people cannot read the codes with the naked eye. To read QR code, people use a special device or smartphone. By reading the QR code, users can easily be redirected to a malicious website, such as a phishing website or a malware distributor. This is because users do not know the information encoded in the QR code before scanning.For such different reasons, attackers use QR codes for various types of attacks [5]. In addition, attackers can access, save, and modify private data stored on the device where the QR code is read. For this reason, various measures should be taken in order to increase the security level of smart phones, protect the privacy of the user and increase the user awareness.In a study of perceived QR code security risk and how to mitigate it [6], an online survey was conducted to measure users' awareness of QR code security risks and to determine how users respond to alerts of malicious QR codes.

Survey results have shown that users with more experience in computer and technology are more likely to ignore warning messages, and that most users have low awareness of QR code risks.

When people questioned why they read a QR code they didn't know the source of, it was revealed that the main reason was curiosity. Besides, from a technical point of view; The maximum amount of binary data a QR code (version 40) can contain is 2,953 bytes, while the smallest malware (crash. Pentium Trojan) is 4 bytes and the SQL Slammer worm is 376 bytes. In this case, a QR code is tempting enough for both malicious and technically abusive people who want to attack. The fact that no QR code has been developed to destroy the entire system has yet to be read does not change the fact that the QR code is a potential threat.These risks require further research on new information coding technology. For this reason, in this study, the attacks that can be done with QR code are investigated and the precautions that can be taken against these attacks are explained. In the second part of the study, the structure of the QR code, the attacks that can be done

with the QR code in the third part, and the measures and solutions that can be taken against these attacks are given.

II. QR CODE STRUCTURE

Data stored and encoded by the QR code can be viewed in one of four standardized modes;

- Numeric: Up to 7,089 characters (0,1,2,3,4,5,6,7,8,9)
- Alpha numeric: Up to 4,296 characters (0-9, A-Z [upper case only], space, $,%, *, +, -,., /, :)
- Binary / Byte: Up to 2,953 characters (8-bit bytes)
- Kanji: Up to 1,871 characters

The amount of data that can be stored in the QR code varies depending on the mode, version and error correction level. There are 40 different versions of QR code starting from version 1 (1,2,3, ..., 40) (Kieseberg et al., 2010: 2). Error correction level of QR code; Low (7%), Medium (15%), Quality (25%), High (30%). (Sharma, 2012: 1)

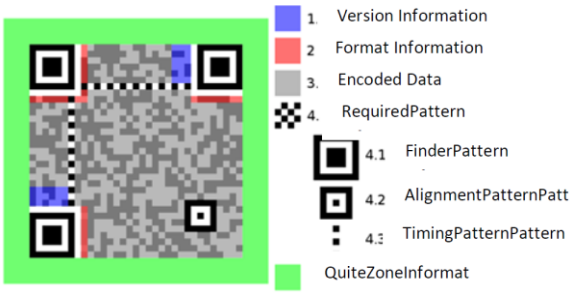


Fig.1.: QR code structure [7]

1. Version Information: Defines the version of the QR code. The storage capacity of each code is different. As the data they store increases, so does their version. In addition, the error correction levels of the codes are different.
2. Format Information: The Format Information section consists of 15 bits next to the separators and contains information about the error correction level of the QR Code and the selected masking pattern.
3. Encoded Data: The data of the QR code is stored in this field. The data is stored by converting binary numbers '0' and '1' into black and white cells.
4. Required Pattern

4.1. Finder Pattern: Consists of three identical frames in all corners of the QR code, with the exception of the lower right corner only. Each pattern is based on a 3x3 matrix. This section enables the reader software to recognize and correctly orient the QR code. Surrounded by white Seperators with a pixel width, it is easy to recognize and easily distinguish from real data. Any changes made in these ways may prevent decoders from reading the code.

4.2 Aligment patterns: This pattern ensures that the QR reader is not distorted and corrected when the code is bent or curved. Supports decoder software to prevent moderate image distortion. QR code did not have alignment patterns in version 1, while version 2 included more alignment patterns with QR code size.

4.3. Timing Pattern: The alternative black and white modules in the timing pattern allow the software to determine the width of a single module. When the symbol is distorted or there is an error for the cell spacing, it is arranged both vertically and horizontally to correct the central coordinate of the data cell [8].

5. Quiet Zone: Free space around the QR code without data. Nothing is written and printed in this field. It must be at least 4 modules wide (each point is 1 module) wide. With this free space, the code is read without error [7].

III. ATTACKS AND COUNTERMEASURES

QR codes can be used to attack both human interaction and automated systems. The attacks that can be arranged in this part of the study and the measures that can be taken against these attacks are given.

3.1. ATTACKS

SQL and Command Injection can be easily injected into automated systems by hackers. Assume that QR decoding software is a scenario that connects to a database and uses QR code information to execute a query in the back database. In such a scenario, if the QR code contains a query such as “1 'OR' 1 '=' 1 (without the quotation marks), the reader may run the query without verifying whether it comes from an authenticated source and may cause this information to be shown to a potential hacker designed for an authorized user.However, QR codes have not yet been used to provide database queries, but if this happens in the future, QR codes can be used to attack such systems. Google has attempted to use a QR code to log in to a Google account [9].

In the command injection method, an attacker could inject HTML code that modifies content of the web page. Whenever the user visits the changed page, the web browser interprets the code, causing malicious commands to be executed on the device (mostly smartphone or tablet) where the user is reading the QR code [10]. In other words, the data from the QR code is used as the input command line parameter. In such a case, an attacker could easily exploit this by changing the QR code and thus executing random commands on the system. In this way, an attacker can initiate rootkits, spywares, DoS attacks or connect to a remote computer and access the system's resources. [9]. Different implementations of the reader software on computers or smartphones may be attacked by command injection or traditional buffer overflows if the command injection is not cleared. An attacker could have control over the user's contact information

or all of their smartphone, including contact content such as email, SMS [11].

Social engineering is the art of manipulating unauthorized people to access confidential information. It is used to steal information or forcibly log into a system that someone is not authorized to access. One of the most popular applications in social engineering is Phishing. Phishing is the practice of redirecting users to fake websites by masking legitimate websites intended to steal sensitive personal information, such as user names, passwords, or credit card information. One of the main applications in phishing attacks is phishing e-mails and QR Codes that contain links to fake websites or websites that contain malware. The main reason why the QR code can easily be used in this attack is that the code cannot be read by the human being. When the user reads the QR code with the reader, they can only see which URL they are redirected to. After redirecting to fake websites, when the user unwittingly enters his / her information, the confidential information of the user (such as user name and password, or even credit card information) is passed into the hands of fraudsters [3]. In a study [12], it was seen that 225 people visited the websites when posters containing QR codes were distributed to 139 different places for phishing during four weeks. It has been observed that 85% of the people who scan the QR code, visited the relevant URL. According to the survey, curiosity is the biggest motivating factor for scanning QR codes. 75% of users scanned the QR code for curiosity or entertainment. The rest of the users scanned forget more information.

QR Codes are used in advertisements to direct the audience to special offers or additional information about specific products. An attacker can replace QR codes, and when the user scans the QR code, the user may be unknowingly redirected to a fake web site[9].

An attacker could encode a URL into the QR code so that when the code was read, it would be redirected to a page where malware would be automatically downloaded. In this way, an attacker could spread the virus, spyware, Trojan horse, or software that contains worms that do great harm to the user and the system. In September-October 2011, Kaspersky Labs identified aTrojan horse that could send short messages in QR codes for mobile applications on a website [8].

A QR code can also be used to execute browser-based attacks and cross-site scripting attacks (XSS). A QR code can contain an encrypted URL. In the scenario where the encrypted URL contains a warning message in the browser, when the user accesses the URL, the malicious software in the warning message can be run and damage the user device, including the web browser [9].

In addition, QR code can be used to make changes in automation systems for fraud. For example, it can be used to trick the system into replacing the code of the more expensive product with the code of an inexpensive product and passing it through the reader [11]. Fake bank ads in social media accountusers can be fooledsuch as, click on the link to win the right to participate in the lottery, if you log into the mobile branch you win bonuses or prizes. After clicking to link, the fraudster can make transactions in the bank with the information entered by the user. Although the bank has sent a password to the user for security, the user only receives the error message after entering the password on the fake website (when the password is received by malicious people). However, because malicious people have access to personal information and password, they can capture the QR code with that password and make transactions without any user card from the ATM they want. The attacker can use these methods only by reading the QR code on his mobile phone, emptying his bank accounts, making money transfers, or even withdrawing credits on behalf of the user[13]. The Central Bank of the People's Republic of China has decided to suspend payments made through the QR-Code as QR-code payment systems are used to money launderingand fraud within China [14].

In addition to the aforementioned attacks, the easiest way to attack an existing QR code is to generate a sticker containing a new QR code, along with the QR code manipulated in the same manner as the original QR code. This misleading QR code is to overwrite the existing original code. There are two different attack methods. The first is the change of both colors. An attacker can change any module from black to white or white to black by inverting any module. In a single color change, an attacker can change a single color. It can convert white modules to black only. You can instantly change a single poster using just one pen.

3.2. Countermeasures

One of the measures that can be taken against the attacks mentioned in the previous section is that people who are the weakest link of the security chain are more careful about social engineering attacks and do not read QR codes of unknown origin. The user has difficulties in the decision-making process regarding the reliability of a QR code. Since QR codes cannot be read by people, content can be displayed to inform the user in advance [15]. Furthermore, the reliability of the QR code being read can be tested using secure QR code readers developed specifically for QR code reading. In a secure QR code system, (i) there must be an authentication mechanism in the QR code generating software, ensure data integrity, (ii) verify online content, and (iii) isolate potentially harmful content in the QR code [16].

(i) Verification of the generator of the QR code and testing of data integrity will prevent possible Fraud, SQL Injection, Command Injection attacks. It is important to standardize and integrateQR code standardization of digital signatures to verify the

creator of the code and thus check whether the QR code has been changed. The digital signature significantly complicates QR code-based attacks, as the attacker needs to make checksum and change the verification process accordingly. However, the increase in the amount of data to be encoded reduces the area encoding the actual data. In addition, QR code readers need to be adapted to validate digital signatures and to indicate whether authentication is successful, similar to SSL [15]. In addition to digital signature algorithms, encryption and hash algorithms are used to verify the generator of the QR code and to test the data integrity.

(ii) the result of redirecting to an untrusted URL, the most frequent attack covered by QR codes; phishing, malware (virus, worm, trojan horse) attacks against the spread of online content needs to be tested for reliability. The QR code reader application must be able to distinguish between fake and real URLs. Many applications have been proposed to determine if the QR code contains malicious URLs. For example, the QRphish API implementation is known to have a detection mechanism that is better than the public blacklist, such as Phistank[17] with an accuracy of 93.34%, and is capable of detecting URLs with a detection mechanism of 82.9% [18].

iii) The QR code content must be isolated to prevent executable codes or commands from reaching the resources of the device where the QR code is being read. By isolating the content, violations of confidentiality, access to personal information, and the use of the reader device as a tool for attacks such as DDOS and Bot net can be prevented. The simplest method is to prevent applications, including the QR code reader application, from accessing the resources (camera, phonebook, photos, location information, etc.) of the QR code reader device (smartphone, tablet). Reader application permissions can also be used to initiate various attacks, such as buffer overrun, Command and SQL injection.

In addition, masking method or visual QR codeswill be prevent the attack of manipulation of the QR code the; The distribution of black and white modules in a QR code that conforms to the specifications follows a particular model. This pattern is determined by the mask used to specify whether to change the colour of the module being considered. The higher the deviation from the equal distribution of black and white modules, the more likely the QR code is to be changed. To use masking methods to secure the reader application, a detailed analysis of the variation between error rate and security should be performed [15]. In addition, in recent years, researchers have tried to equip the QR code with aesthetic elements and formulated codes that are acceptable to decode to minimize visual perception distortion by visualizing the beautification. For this purpose, the shape and colour of the modules in the code can be changed or a picture can be embedded in the QR code (Fig1, Fig2) [19]. This method significantly supports the user in detecting modified QR codes. The more complex the theme, the more difficult it is for an attacker to change QR codes unobtrusively [15].



Fig 2. Changing the color and shape of the modules



Fig 3. Embedding a Picture [19].

IV. CONCLUSIONS

With the rapid spread of QR codes, internet and smart phones, it has started to take place in every area of our life. Banking applications, advertisements, business cards, product tracking are just a few of them. The wide application area, the people being unaware of the attacks against the QR code, the inability to see the data in the QR code from the human eye, sufficient data storage capacity, the QR code has become the focus of the attacks.

Attacks that can be blocked with QR code; SQL and Command Injection, Phishing, Fraud / Fraud, the spread of malware (viruses, worms, spyware, Trojans, etc.). These attacks can result in substantial material and moral losses, such as access to personal data from users, unauthorized use or disuse of the resources of QR code reader devices, and mediation of other attacks by users without realizing it.

The first thing to prevent these attacks is to increase the awareness of the users.For example, when the QR code directs the user to fill out a form, he or she should know that if the form requires personal information, it should not fill out the form, because legal and original codes do not require personal information. Secondly, users should choose applications with sufficient security requirements to read the QR code. These requirements can be listed as having an authentication mechanism in the software that generates the QR code, ensuring data integrity, verifying online content, and isolating potentially harmful content in the QR code.

In conclusion, in this study; It is shown that QR code scanning that do not know the source of it, have serious consequences. In addition, the attacks that may be encountered in order to increase the awareness of the users on this subject and the measures that can be taken against these attacks are also included.

REFERENCES

[1] Elçi, A. (2014). A System Proposal for Security Monitoring in Work Equipment “DataMatrix Barcode Application”. (Unpublished master's thesis) New Century Istanbul

University Institute of Health Sciences, Istanbul, Turkey. 10-40.,
[2] Moharil, B., Ghadge, V., Gokhale, C., ve Tambvekar, P. (2012). An Efficient Approach for Automatic Number Plate Recognition System Using Quick Response Codes. (IJCSIT) International Journal of Computer Science and Information Technologies, 3 (5), 5108.
[3] Kapsalis, I. (2013). Security of QR Codes. Norwegian University of Science and Technology Department of Telematics. 8-10.
[4] Al-Khalifa, H. S. (2008). Utilizing QR Code and mobile phones for blinds and visually impaired people, K. Miesenberger et al. (Eds.): ICCHP 2008, LNCS 5105, pp. 1065–1069.
[5] Shin, D. Ve Yao, H. (2013). A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 4(4), 49-50.
[6] Yin, L. R., ZHang, Z. ve Baldwin, N. (2014). Perceived Security Risks of Using Quick Response (QR) Codes in Mobile Computing with Smart Phones.
[7] Polat, Z. A. (2014). Thoughts on the Possible Uses of DataMatrix Technology in Our Profession. Remote Sensing and Geographical Information Systems Symposium (Uzal-GIS 2014), 3.
[8] Wane, A.R. ve Jamankar, S. P. (2013). An Effective Mechanism For Ensuring Security Of Qr Code. International Journal of Advanced Research in Computer Science. 4 (6), 176-179.
[9] Sharma, V. (2012). A Study Malicious QR Codes. International Journal of Computational Intelligence and Information Security, 3(5). 1-5.
[10] Ahuja, S. (2014). QR Codes And Security Concerns. (IJCSIT) International Journal of Computer Science and Information Technologies, 5 (3),3878.
[11] 11.Kieseberg, P., Leithner, M., Mulazzani, L., Schrittwieser, S., Sinha, M., Ve Weippl, E. (2010). QR Code Security. 5-6. DOI: 10.1145/1971519.1971593.
[12] Vidas, T. Owusu, E. Wang, S. Zeng, C. Cranor, L. F. ve Christin, N. (2013). QRishing: The Susceptibility Of Smartphone Users To Qr Code Phishing Attacks. 1-15. DOI: 10.1007/978-3-642-41320-9_4
[13] Koygun, P. O. was obtained from the New Method QR Code, 10/02/2019
[14] https://www.cnnturk.com/video/turkiye/dolandiricilikta-yeni-yontem-qr-kod address fraud.
[15] Erdal, E., China Stops QR Code Payments to Prevent Fraud, 10/02/2018
[16] https://www.webtekno.com/cin-dolandiriciligi-onlemek-icin-qr-kod-odememes-durduruyor-h38598.html.
[17] Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Ve Weippl, E. (2014). QR Code Security: A Survey of Attacks And Challenges For Usable Security. 7-8.
[18] Bani-Hani, R. M. Wahsheh, Y. A. Al-Sarhan, M. B. (2014). Secure QR Code System. 10th International Conference on Innovations in Information Technology (IIT). 2. DOI:10.1109/INNOVATIONS.2014.6985772
[19] David Ulevitch, Phistank (OpenDNS), 02/02/2019
[20] Alnajjar, A. Y. Anbar, M. Manickam, S. Elejla, O. Ve El-Taj, H. (2016). QRphish: An Automated QR Code Phishing Detection Approach. Journal Of Engineering And Applied Sciences 11(3). 553-560. DOI: 10.3923/jeasci.2016.553.560
[21] https://www.phishtank.com/, .
[22] Lin, S. S., Hu, M. C., Lee, C. H., ve Lee, T. Y. (2015). Efficient QR Code Beautification With High Quality Visual Content. IEEE TRANSACTIONS ON MULTIMEDIA, 17,(9). 1515.

★★★