International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Quick Response Code and Securities

Prathamesh A. Wakde[1], Zahir Mulani[2]

Bharati Vidyapeeth's Institute of Management & Information Technology CBD Belapur, Navi Mumbai

Abstract: ***The QR code is a 2D code which has the ability to store different type's information. Any device having a camera can read the QR code. The information present in the QR code in not in the human readable format hence a person cannot check whether the information in the QR code is valid or malicious. QR code can be used for hacking the interaction of humans and automated systems. The paper discusses the QR code and different attacks on it.***

Keywords: QR code, Smartphones and automated systems

1. Introduction

The QR code was invented in Japan in 1994 by a company named Densowave. The QR code is in the matrix format. The information stored in stored in QR code is in both horizontal and vertical directions thus storing more data than the bar code. The QR code can be scanned or accessed through a phone having a camera. The QR code reader application is required in the phone to access the QR code.

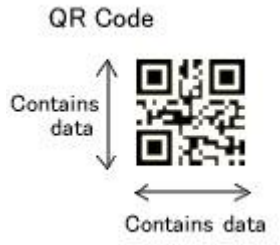

Figure 1: QR code

There are 40 different versions of Quick Response code each with different data storage capacities. The version 1 of QR code comprises of 441 modules from which 133 modules can be used to store the data. The version 40 of QR code has 23,648 modules to store the data. QR code can store different types of data like numeric, alphanumeric, binary and control codes. The QR code can be scanned even if it partially damaged. This is due to the error correction technique in QR code. The error correction technique is based on Reed Salomon codes. There are four levels of error corrections: Low(L), Medium(M), Quartile(Q), High(H).

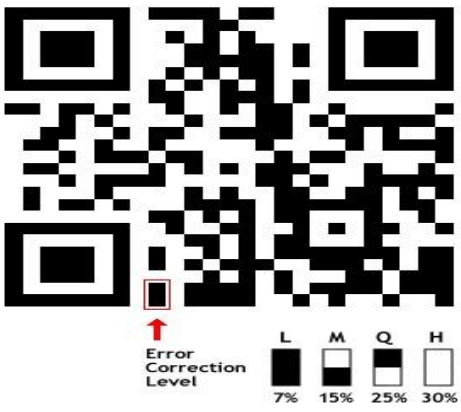

Figure 2: Error Correction level of QR Code

The Low (L) level of error correction can permit up to 7% damage. The Medium (M) level of error correction can permit up to 15% damage. The Quartile (Q) level of error correction can permit up to 25% damage. The High (H) level of error correction can permit up to 30% damage. The Low (L) level of error correction is preferred the most due to its high level of error correction therefore decreasing the amount of data that can stored in the code.

2. QR Code Structure

The QR code has different areas reserved for specific purpose. There are 8 different sections in QR code. In the fig. 3, we refer QR code version 2.

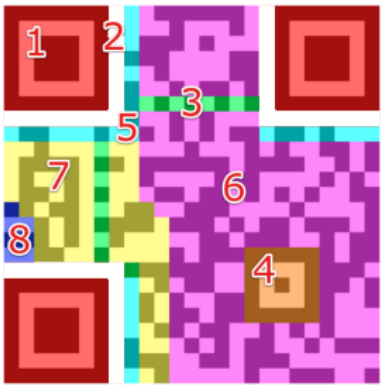

Figure 3: QR code Section

1) Pattern finder: The pattern finder consists of three identical structures which is located at three different corners. It helps the software to determine the version of QR code.
2) Separators: The separators are in white colour and have a width of one pixel. It helps to improve the recognisability of the pattern finder and helps them to separate them from actual data.
3) Time Pattern: The Time pattern is the alternate black and white modules which enables the software to determine the width of a single module.
4) Alignment Pattern: The alignment pattern helps the software in compensating for image distortion.
5) Format information: The format information contains the 15 bits next to the separators and it stores the information related to the error correction level of the QR code.
6) Data: The data is stored in the data section. The data in converted into the bit stream and then stored in the 8 bit

parts in the data section. This is also known as codewords.

7) Error Correction: Error correction is similar to the data section. The error correction codes are stored in 8 bit long codewords in the error correction sections.
8) Remainder bits: The remainder bit contains the empty bits, if data and error correction bits cannot be divided into 8 bits without remainder, the remainder bits are used.

The entire QR code in then covered with a quiet zone, an area which is similar to the white modules. It helps to improve the code recognition by the software.

3. QR Code and its Security Concerns

Phishing is fraudulent activity which procures user's credentials by deception. For example, a user might be cheated by an email that spoofs the identity of a website on which user already has an account and after clicking on the link, user is redirected to a phishing website which is similar looking to the original one but is a fake website. If the user enters his credentials, this data will be sent to the scammers. The same scenario takes place if in case a user clicks on a fake online advertisement. This happens because the user doesn't pays attention to the URL in the address bar. Phishing is a phenomenon with a handsome profit for the attackers. Phishing can be done in multiple ways and it is not just restricted to e-mails, Trojans or viruses. Also QR Codes are an easy way for targeting innocent users so the scammers take an undue advantage of this fact and choose traffic heavy public places for deploying phishing or any other variant of social engineering. QR code phishing or QRishing introduced in a term used for phishing attacks that are initiated by scanning of the QR codes. This paper addresses various strategies that can be followed by an attacker, how this does affects the back end system, the consequences faced by the innocent user who have scanned malicious codes through QR code, and also encryption and obscurity of data using QR codes.

4. QR Codes as Vector Attack

QR Codes can be used for attacking both the human - interaction and the automated systems. The automated systems are vulnerable to SQL injection and command injections. In the SQL injection method the SQL commands are injected in the SQL statement by a malevolent hacker. Hence the security of a web application can be compromised and alteration in SQL statements takes place by injecting SQL commands. While in the Command injection method the hacker injects an HTML code in an input mechanism that lacks validation constraints thus altering the dynamically generated content on a page. Whenever the user will visit the affected page, browser will interpret the code, which causes the execution of malicious commands on user's computer. Moreover the humans may fall for various phishing attacks wherein the attacker procures user's credentials by deception, frauds wherein the QR codes are manipulated so that they redirect the users to cloned webpage. Another type of attack includes attacking reader software, with the use of command injections, different implementations of QR code reader software can be attacked. With this the attacker gains full control over the information in the Smartphone like contacts, Emails, messages etc. So just in case anyone scans a random QR code, created by an attacker, using any of the attack methods then the innocent user who is unaware about the situation will generate the attacks on the behalf of the attacker .The attack targets the user's device through which the QR code was being scanned. The attack is deployed with the help of a marker which changes the white modules to black modules. The altered QR code contains URL of phishing web page that is quiet similar to the original one. QR code can be altered and use as a tool for performing phishing attacks. Another security concern is that these codes can be used as a mode of payment. Attacker can use a name quiet similar to that of the legitimate name and by doing so the attacker redirects the payments to his accounts.

5. Security Approach

There are various methods to tackle various security issues related to Quick Response codes. The user should manually check the URL before opening that particular link. Moreover if a website does not has a valid certificate or tries to establish insecure connection then the QR code reader must alert the user. Digital signatures can be included inside the QR code .Most important thing is to educate the users to always check the link before opening that link. If any QR code exists randomly and no information is present with it, then the user need to be more cautious that the QR code might lead to a malicious website. Not many applications give us the provision to perform these operations concurrently. Also Quick Response code reader's application can be developed in such a way that they are able to read encrypted as well as obscured data.

6. Conclusion

This paper shows various attacks using QR code. As each technology have its own benefits and limitations, so does the QR codes. As QR codes are gaining popularity, their misuse is also increasing day by day. QR codes are commonly used in advertising and making payments. So along with this usage, security issues also arise. Various approaches exist to tackle various security issues related to QR codes.

References

[1] Jean-Pierre Lacroix, Shikatani Lacroix. QR Codes whitepaper, 2011.[Available]: www.sldesignlounge.com/wpcontent/.../QR-Code-White-Paper.pdf
[2] QR Code Security, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl, SBA Research
[3] QR Codes and Security Solutions, A. Sankara Narayanan Department of Information Technology, Salalah College of Technology, Sultanate of Oman
[4] Security of QR Codes. Ioannis Kapsalis, Norwegian University of Science and Technology.
[5] Denso Wave. To two-dimensional code from the bar code. [Available]: http://www.qrcode.com/aboutqr.html

[6] DENSO Wave Incorporated. What is a QR Code?, 2013. http://www.qrcode. com/en/.
[7] http://searchsoftwarequality.techtarget.com/definition/commandinjection
[8] http://www.w3schools.com/sql/sql_injection.asp
[9] https://www.securelist.com/en/threats/spam?chapter=85
[10] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. Cranor. QRishing: The susceptibility of smartphone users to QR code phishing attacks. In CMU-CyLab-12 (2012), pp. 1–12.
[11] QRStuff. QR Code Error Correction, 2011. QRStuff blog: http://www.qrstuff. com/blog/2011/12/14/qr-code-error-correction.