ISSN:0975-9646

QR Codes and Security Concerns

Shruti Ahuja

CBS Group Of Institutions, Jhajjar
Maharshi Dayanand University*, Rohtak,India*

Abstract: It is important to differentiate between various objects and places in the real world. Any Smartphone equipped with a camera can read the content of QR code directly. QR codes being a two dimensional codes are useful in storing the information .This information isn't present in human readable form hence an individual cannot anticipate whether this is a valid information or a maliciously manipulated code. QR Codes can be used for attacking both the human interaction and the automated systems. While the humans may fall for various phishing attacks, the automated systems are vulnerable to command injections and SQL injection. This paper examines the QR codes different attacks. Though it is easy to modify the information stored in the QR code but one must make sure that the identifier written in the QR code is issued by an authorized organization.

Keywords– QR Codes, Smartphone and Automated Systems.

1. WHAT ARE QR CODES

QR codes are appearing at more and more places in urban environment due to their increasing popularity. These QR codes are similar to physical hyperlinks as they give the user the ability to scan the QR Code and take them to a particular website.

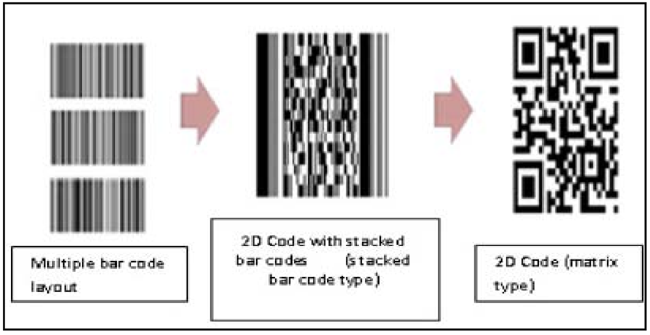

Fig. 1: Multiple bar code to 2D code [5]

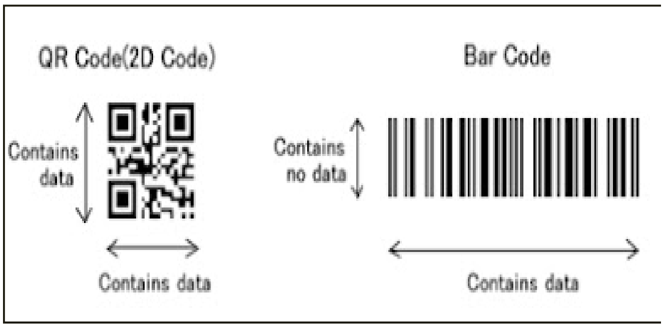

Fig. 2: QR Code and Bar Code (Contains Data) [5]

Bar codes have widespread use because of their accuracy, reading speed etc., but the major limitation was the storing capacity and the character type. Hence 2-Dimensional codes emerged as a solution to all these limitations of 1-Dimensional codes. QR codes are capable of encoding the data both in horizontal and vertical direction, thus able to encode several times more data than the barcodes. The black and white modules of the QR codes comprise of the encoded data. Smart phones having built-in camera, capture the image of the encoded QR Code and then with the help of any Quick response code reader software decode the QR code.

Masking is an additional feature of QR codes .It increases the contrast of the image and helps the QR code reader software in decoding the code. With the use of masking, the generated QR codes has an equal distribution between white and black modules.

There are almost 40 versions of the QR codes each with different data capacities. Version 1 comprises of 21 X 21 modules out of which 133 modules can be used to store the encoded data while Version 40 comprises of 23,648 modules which can be used to store the data.

Any Smartphone equipped with a camera can read the content of QR code directly. This information isn't present in human readable form hence an individual cannot anticipate whether this is a valid information or a maliciously manipulated code. QR Codes can be used for attacking both the human interaction and the automated systems.

QR codes are capable of encoding different types of data like binary, numeric, alphanumeric, Kanji and control codes. The technology of QR codes has proved out to be successful even if the code is partially damaged or dirty [7]. This is feasible due to the error correction in QR codes, which is based on the Reed-Salomon Codes [1].There are four levels of error correction; Low (L) which can tolerate up to 7% damage, Medium (M) can tolerate up to 15% damage, Quartile (Q) can tolerate up to 25% damage and High (H) can tolerate up to 30% damage [6].

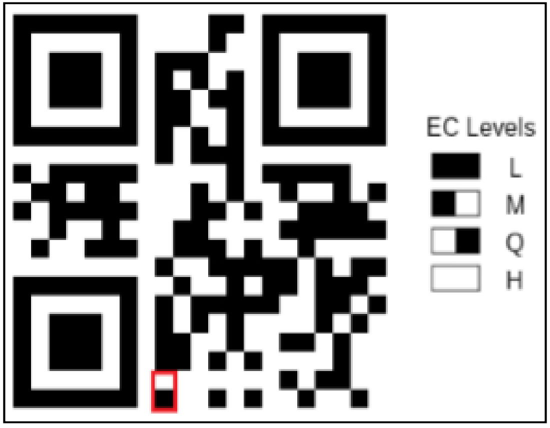

Fig. 3: Error correction level of QR Code[4]

The reason why the Low (L) error correction level is preferred is that the High error correction levels raise the percentage of codeword used in error correction thereby decreasing the amount of data that can be stored in the code.

2. QR Codes And 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 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 [9] is 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 does this affects the back end system, the consequences faced by the innocent user who have scanned malicious codes, and simultaneous encryption and obscurity of data using QR codes.

3. QR Codes As Attack Vectors

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.

4. Security Approaches

There are approaches to tackle various security issues related to QR 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. Also simultaneous encryption and obscurity of data using QR codes can be done. Not many applications give us the provision to perform these operations concurrently. Furthermore QR code readers can be created in such a way that they are able to read encrypted as well as non – encrypted, obscured data.

5. Conclusion

This paper outlines 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. Also simultaneous encryption and obscurity of data using QR codes can be done

References

[1] Huffman, W., and Pless, V. Fundamentals of Error-Correcting Codes. Cambridge, Ma University Press, 2003.

[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] QRStuff. QR Code Error Correction, 2011. QRStuff blog: http://www.qrstuff. com/blog/2011/12/14/qr-code-error-correction.

[7] DENSO Wave Incorporated. What is a QR Code?, 2013. http://www.qrcode. com/en/.

[8] https://www.securelist.com/en/threats/spam?chapter=85

[9] 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.

[10] http://www.w3schools.com/sql/sql_injection.asp

[11] http://searchsoftwarequality.techtarget.com/definition/ command-injection