Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 5, Issue 5; July-September, 2018, pp. 372-374

http://www.krishisanskriti.org/Publication.html

Quick Response (QR) Codes and its Security Best Practices

Aquil Ahmad Khan[1] and Mayank Jain[2]

[1,2]ICERT, New Delhi
E-mail: [1]akhan2786@gmail.com, [2]engineermayankjain@gmail.com

Abstract—*A new method to embed QR Code(or Quick Response code) is used to authenticate and check the originality of the document. It can produce QR Code without using any encryption algorithm which could be created and will be ready to print. QR code is a matrix bar code which can be read by an imaging device (camera) and then processed to read its data. The QR code is simply an array of bits to be identified by a scanner. Bits are reserved for the scanner to be able to identify and orient the image, as well as for version and format information. QR codes are really useful and help us to complete tasks faster in smartphones. You can quickly open a website just by scanning a QR code and you do not need to manually type the URL in your smartphone. QR Code generation system will be utilized in universities, schools, faculties to modify the distribution of digitally verifiable mark sheets of scholars. The project aims at developing a QR Code digital system which can be used in global payments industry to automate the digitally verifiable payments result shard money and their profile information. Because it is easy to generate a QR code, the system offers convenience to businesses and consumers. Authenticity of the document can also be verified easily by online method. The Quality of the developed QR Code is also verified. The QR Code is the best way to compose the identical information of any entity to quickly figure out the originality.*

Keywords*: Digital, QR Code, URL, 2-D BAR Code Matrix, Mark Sheet.*

1. INTRODUCTION

In the digital world, preference is to look at visuals, videos, games and to scan shorter text instead of totally browse longer version. With the increase in usage of QR codes in the general public, it is necessary to ensure that the data conveyed through the QR code is not harmful to the user. There are currently two major attack vectors for potential vulnerabilities: attacks on human interactions and automated attacks. QR code has been successfully implemented in the global payments industry, as well. Because it is easy to generate a QR code, the system offers convenience to businesses and consumers, alike. It can be printed on business cards, points of sale, and product labels which customers can simply scan to pay for a product or service. The QR Code is a recent involvement of digital technology with global payments industry. The Format of QR code looks like a 2-Dimesional Matrix Bar code. Today, the Mobile Codes available are in 2-Dimesional and 1-Dimesional bar codes which work under the internet on Mobiles. Mobile phones today with proper configuration added Camera make it possible to read Mobile Codes as Code Scanner or Reader due to recent advancements in imaging technology. It combines both hardware modeling and image processing techniques.

QR Code invented by Denso Wave in 1994. It uses as a registered trademark by Denso Wave for tracking product. Denso Wave promoted the widespread use of QR codes, by providing QR code tutorial at www.qrcode.com. QR codes are quick, easy method to tracking their vehicles and auto parts. Since the early 1990s, QR codes have been used on large scale in marketing campaigns to create an interaction with a consumer. Denso Wave made an extensive use of this technology because of their potential in the auto industry. The QR code first came into the market as a commercial product in 2011 when the telecommunications industry was on a hike. Today QR Code has become popular due to new technology with Smart phones, because of

- QR codes have a hundred times more storage capacity than the BAR code.
- It stores information on both axes as horizontal and vertical.
- The BAR code is only 1-Dimesional, But QR Codes has two-dimensional matrixes also.
- QR Code has error correction capability, but Bar Code doesn't have.
- Standard linear bar codes can only hold up to 20 alphanumeric digits, but QR codes can hold up to 7,089 numeric characters and up to 4,296 alphanumeric characters value of data
- QR Code is standardized based on respective national standards or international standards. It was approved as an international standard in June 2000.

Attacks on human interactions

Attacks on human interactions rely on the fact that humans by themselves are unable to interpret what information is encoded

in QR codes, and thus rely on QR code readers to decode the information. Since the information in the QR code is completely obfuscated, it is possible to trick and attack users via phishing, pharming, and other social engineering attacks by putting up fake QR codes. It is also possible to attack users by manipulating and exploiting existing QR code readers that users use via command injection or buffer overflows.

Phishing

Phishing is the main security issue involved with QR codes. It is also described as QRishing. QR codes are generally scanned by a smartphone camera to visit a website. Now, many website advertisements put QR code along with a URL so users can quickly scan QR code to visit the website. Hackers or scammers try to change the QR code added in the poster. They can also print the similar kind of fake posters and put in public places. Innocent customers will scan these fake QR codes to visit the websites but they will be redirected to phishing websites. In mobile devices, it is hard to check the full address in the browsers. Due to limited space, browsers did not displayed the full address in the URL field and most people never try to check the full address, which makes them more vulnerable. When they use this phishing page to login, their credentials are compromised.

In the same way, attackers can use QR codes to point to malicious websites to distribute malware via drive by download attack. Drive by download attacks are attacks in which a website forcefully download the software in your device when you visit the website.

Automated attacks

Automated attacks often result from the assumption that the encoded information in QR codes is sanitized. However, it is known that QR codes themselves can easily be manipulated in order to change encoded information, potentially producing attacks on backend software. Without QR code input sanitation, it is possible to produce attacks such as SQL injection, command injection, and fraud.

Best Practices for users

QRishing & Drive by download attacks can be prevented by using the following measures:

Observe before use: If you find a QR code in any banner advertisement in a public place, look at it closely. Most of the times, hackers stick their fake QR code above the legitimate QR code in a legitimate poster. So try to see if it is real or not. One can check by touching the poster. If it does not look like it's actually printed on the poster, do not use it. If you are not sure, never scan that QR code.

Be suspicious and never giver personal or login info: Always be suspicious of the page you land on via QR code. Never share your personal information on these pages. Only do this if the QR code is from a very trusted source. To login any website, always enter the URL manually on the browser's address bar.

Best practices for merchants

- Include signage telling the user what the code does. Otherwise the user has no way of knowing if the code should point to a URL, phone number, or SMS.
- Print the URL near to the code so that if the code is hijacked and pointed to http://evilwebsite.com/ , the user can see that they are not visiting to original website.
- Include https in the URL. Get users used to checking for https before they interact with you.
- Every time you find a QR code in a public area, you should know its originality. If a code is on a billboard, on a storefront, or anywhere else it can be accessed by the public, it could be at risk.
- Distinctive, branded QR codes with special colours or other design features are far more likely to get attention, and it will help people to know that they are dealing with a legitimate link to your brand and not a counterfeit code. It will be much more difficult for a hacker to simulate a highly designed and colourful code than a plain one.

2. CONCLUSION

From the above, it is clear that authenticity and security of a document is provided without using any encryption algorithm. This authenticity is providing by using QR Code mechanism. This is very simple and innovative method to digitize the documents in the digital era. The keen advantages of Digital Education System are the transparency of records, round the clock availability, eliability and easy to access. Since QR Codes gains more popularity by using it for marketing purposes. We expect that attacks to avoid misuse of these QR codes will require more and more attention by the hacking community in the future.

This paper will present some security conscious of the mobile phones users. In general, we believe that QR codes have great potential in business media. Some possibilities are discussed in this paper and there are many creative ideas waiting for us to explore. Also, this paper can be served as the first step for the readers to investigate this exciting topic of mobile learning.

REFERENCES

[1] http://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/#gref
[2] https://courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf
[3] Jean-Pierre Lacroix, Shikatani Lacroix. QR Codes whitepaper, 2011.[Available]: www.sldesignlounge.com/wpcontent/.../QR-Code-White-Paper.pdf
[4] QR Codes: How To Integrate A QR Code Into Marketing Campaigns, 2010.

http://www.crwgraphics.com/qr-codes-how-to-integrate-qrcode-into-marketing-campaign.htm

[5] Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko. A Novel Secret Sharing Technique Using QR Code, International Journal of Image Processing (IJIP), Volume (4) : Issue (5), pp.468-475, 2010.

[6] Charlotte Gray. New technology security risks: QR codes and near filed communication, http://www.qwiktag.com/index.php/knowledge-base/150-technology-security-risks-qr-codes

[7] Educause.edu/eli. 7 things you should know about QR codes, 2009 http://net.educause.edu/ir/library/pdf/ELI7046.pdf

[8] Michael Dye, Cameron Marshall, and Blayne Sharpe. NearField Communication: The New E-Commerce, 2007. http://faculty.uca.edu/ronmc/INFO3321/Summer_2007/ET1/ET%20Topic%20Overview.htm

[9] Mwg Shannon. How QR codes hide privacy, security risks, 2011. http://www.msnbc.msn.com/id/45729377/ns/technology_and_science-security/t/how-qr-codes-hide-privacy-securityrisks/#.T8OqibAweFk

[10] Michael Protos.Why you should be wary of QR codes, 2011. http://gcn.com/articles/2011/09/13/qr-codevulnerabilities.aspx

[11] Ernst Haselsteiner, Klemens Breitfuß, Security in Near Field Communication (NFC). http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf