Security of Quick Response Code

K.Ravikumar[1*], R.Geetha[2]

[1,2]Department of Computer Science, Tamil University, Thanjavur, Tamil Nadu, India

Abstract- QR (Quick Response) Codes and the way they will be wont to attack each human interaction and automatic systems. Because the encoded data is meant to be code solely, some individuals cannot distinguish between a legitimate and a maliciously manipulated QR code. Whereas humans may fall for phishing attacks, automatic readers square measure possibly susceptible to SQL injections and command injections. Our contribution consists of Associate in Nursing Associate in Nursing lysis of the QR Code as an attack vector, showing totally different attack methods from the attackers purpose of read and exploring their potential consequences.

I. INTRODUCTION

Quick Response codes are 2-dimensional barcodes that visually write bits of data described as black sq. dots placed on a white sq. grid. as a result of QR codes are how to transmit info, this paper examines QR codes for security flaws that would cause a danger to the common user and presents potential fixes to those security flaws. we tend to propose new security protocols for QR code creation that involve coding bits that are encrypted or digitally signed via ancient security protocols. we tend to then decide to compare the effectuality of QR code phishing tries to it of short computer address phishing tries employing a social experiment. Finally, we tend to perform a bug search on 2 existing QR code applications, the popular ASCII text file QR code scanner ZXing associate degreed an ASCII text file QR code payments library known as SPayD. we tend to with success applied security standards to QR codes and made numerous types of secure QR codes. However, every comes at a value of either house or computation time, and so ought to be used only if required. The social experiment was inconclusive as a result of not enough folks followed either the QR code or the shortened computer address. Lastly, the bug search showed that each scanners had vulnerabilities involving code injection, unauthorized actions, and knowledge unseaworthy.

1.1.Working Principles of QR Code

Quick response code (QR code) has been popular due to its easy generation and distribution, large storage capacity, and fast readability [1]. According to a recent survey, 75% of retailers use QR codes to interact with and track potential buyers [2]. Generally, QR codes are used to direct users to the websites of their interest, which can provide further information or services. By scanning a QR code, however, users can be easily taken to a malicious website, for instance, a phishing website or one distributing malware. This is because users usually do not know the information encoded in the QR code until they scan it. Hence, attackers can exploit this and use QR codes for various types of attacks. In this paper, we are mainly interested in phishing and malware attacks based on QR codes. Phishing attacks trick users to divulge their sensitive information by masquerading as a trustworthy entity [3, 4]. For instance, a QR code can redirect users to a fake bank website that looks exactly like the real bank website. A normal user will not be able to see the differences and thus type in her credential information that will be handed to the attackers [5, 6, 7]. On the other hand, a malicious QR code can also be used to redirect users to a URL distributing malware [8]. An early example of malware attacks through QR codes was that people were fooled into scanning a QR code and downloaded a malicious application, which sent off multiple text messages to a number that charged users $5 per SMS message [9]. There are other types of attacks such as social engineering and cross-site attacks.

1.2.QR Code Storege

Code and process it with a QR code reader. The QR code itself is just Associate in Nursing array of bits to be fast Response codes, usually abbreviated as QR codes, started as Associate in Nursing extension of the quality UPC barcode usually utilized in retail and production. in contrast to a 1-D barcode, a QR code could be a 2-D matrix code that conveys data by the arrangement of its dark and lightweight parts in columns and rows [1]. the info in an exceedingly QR code will be accessed by taking an image of the QR known by a scanner. Bits area unit reserved for the scanner to be ready to determine and orient the image, moreover as for version and format data (Figure 1). The remaining bits area unit

accustomed write the message, and also the certain quantity of accessible area leftover depends on the version of the QR code, that indicates the quantity of bits per row/column, and also the level of error correction, that introduces redundancy. the foremost data dense QR codes used nowadays will store just below three,000 bytes of information [2].

Capable of secret writing constant quantity of information in concerning simple fraction the house of ancient 1-D barcodes, QR codes gift a {way a far} a lot of space-efficient way of presenting scan-able knowledge. ab initio fictional to be used in automotive factories in Japan, QR codes were accustomed programmatically determine and track automotive elements quickly so as to hurry up production. However, they before long began to check a lot of widespread use as convenient ways of sharing and sending knowledge. in style business uses of QR codes currently embody uniform resource locator redirection, payment info exchange, and electronic flight tickets.

1.3. Security Encode
Background a QR code is just a string of bits visually encoded as black and white squares on a grid. In most uses of QR codes wherever the intent is to possess most accessibility, like the common uniform resource locator redirection, there aren't any security standards. Therefore, anybody will browse or write QR code messages with exemption. However, bound applications could need restricted access or verification of QR codes, and so there's a desire to style QR codes that meet varied security specifications. during this section of the paper, we have a tendency to shall discuss the implementation of a couple of security standards for QR codes, their prices, and a few samples of use cases for every. the primary could be a normal that enables the creator of a QR code to write in code the message for a selected reader. The second could be a normal that enables the reader to verify the origin of the QR code. Lastly, we have a tendency to shall discuss a couple of alternative makes an attempt we have a tendency to create at security protocols, wherever they let down, and what future work can be created in those areas.

II. ENCRYPTION

Encryption the primary security customary for QR codes is Encrypted QR codes, or EQRs. we are going to propose 2 forms of EQRs: cruciform EQRs (SEQR) and Public Key EQRs (PKEQR). In SEQRs we tend to use a cruciform secret writing theme wherever each the reader and therefore the author of the EQR share a secret key. The secret writing theme is extraordinarily straightforward: write in code the bits of the message victimization AES block cipher with the shared secret key. In PKEQRs we tend to use the RSA public key secret writing theme combined with AES, employing a public RSA key to write in code the AES key and as well as the encrypted key within the message. the sole

factor to notice with these 2 strategies is that the error correction bits ought to correct errors on the encrypted message, not the message itself, so as to avoid unseaworthy data of the initial message.

2.1.Data Encryption Standard
URLs embedded in QR codes, especially phishing and malware attacks [12]. In the study, 31 QR code scanners available at the Google Play were analyzed in terms of their security features and security warning capabilities, and two top-rated QR code scanners, Norton Snap and QR Pal, were selected and tested against phishing attacks exploiting malicious URLs embedded in QR codes. The test results ware quite alarming with Norton Snap being able to detect only 28.0% (112/400, 95% Confidence, CI-4.25%) of phishing URLs and QR Pal only 27.75% (111/400, 95% Confidence, CI-4.24%). In our previous study, a secure QR code scanner solution called SafeQR was proposed to better detect phishing and malware attacks based on malicious embedded URLs.

SafeQR utilized two well-known security APIs, Google Safe Browsing API and Phish tank API, in order to improve the detection rate for the attacks. In this companion paper, we discuss in detail the design of a user study to test a set of hypotheses on user awareness of QR code based threats, effectiveness of QR code based attacks, helpfulness of visuals security warnings, and habituation effect. Specifically, we first discuss how we designed the security warnings of SafeQR using Microsoft's (Neat, Explained, Actionable, Tested) and SPRUCE (Source, Process, Risk, Unique, Choices and Evidence), and then how we designed and conducted our user study to test their effectiveness. The result of our user study is promising, showing that SafeQR enables better user perception of imminent security threats, compared to other QR code scanners.

III. QR CODE SECURITY PROTOCOLS

This study introduces Associate in Nursing advance technique on removing scratch or injury that exists on QR-code [4]. The R-code decryption formula is unable to decrypt if the scratch that applies on the QR-code is quite Error Correcting Level threshold of current QR-code or the injury applies on some curtain space, that think about as info space of the QR code. The scratch removal technique consists of many processes. so as to extract scratch from injury QR-code, simulate HSV (Hue, Saturation and Value) is applied and scratch on injury QR-code becomes additional distinctive. Next, Morphological Image process technique is apply by begin with Dilation method that modification the image structure and permit scratch become even additional obvious. At now scratch ought to be obvious enough and able to take away. to extend potency of decryption, Median filter is applied by remodel image to Binary image to removing noise.

As the results of their experiment, image that been optimizing with the image process technique is in a position to be decipher with primary cell phone QR code computer code with none data lost. The image process technique and procedure is potency enough to be used as Pre-processing of QR code. However, if the scratch color intercity is on the point of black or strength isn't well adjusted; the numerous price can be increase.
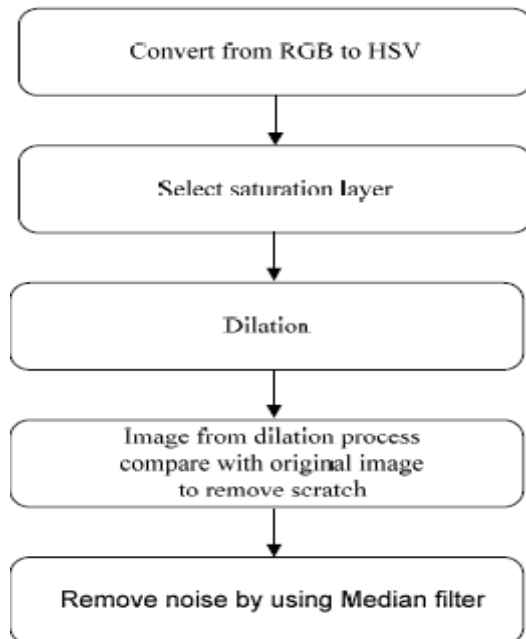

Fig. 1

IV. ENCODING QR CODE PROTOCOLS

We dedicated quite little bit of time wondering different security protocols for QR codes that utilize the character of the QR code itself rather than playacting encoding operations on the bits. The schemes higher than square measure a lot of viable just because the algorithms concerned square measure better-known, evidenced to figure, and are optimized over a few years. However, our different efforts square measure, still value noting just in case future researchers would like to analyze any. One try created was for a "proof of work" QR code. during this theme, that takes its plan from Bitcoin, a QR code contains a message, a series of random bits, and therefore the hash of the concatenation of these 2. The catch is that the bits containing the hash square measure placed in regions typically reserved for fastened orientation patterns, particularly the squares at the corners of the QR code. If the hash doesn't kind the right orientation patterns, the code are

undecipherable. very like however Bitcoin miners should reckon for a protracted time to provide a hash ending in multiple 0's, creators of the "proof of work" QR code should reckon for a protracted time to provide a hash that is each valid for the encoded message and contains the right orientation bits.

Apart from Steganography, Cryptography and Visual Cryptography techniques QR codes might even be used for secured digital communication. QR codes ar generated by the combining visual cryptography and steganography. These QR codes ar used for form of applications like Secret communication, Copyright protection, Marketing, Business, and Education etc. Ching-yin Law & Simon therefore illustrate the usage of QR codes in education.

V. CONCLUSION

QR code's use in numerous areas that's however to be explored. The technology includes a firm ground for analysis aspects. a lot of and a lot of experiments area unit through with QR codes in numerous aspects like enhancing the protection, higher recognition, reducing redundancy so as to save lots of house, chance of cryptography totally different quite information like audio, etc. As QR code provides the structural flexibility, it unveils the large platform for researchers to explore the probabilities to boost the performance of QR code or to merge QR code with totally different technologies.

REFERENCES

[1] A. Lewko, A. Sahai, B. Waters, "Revocation Systems with Very Small Private Keys" , Proc. IEEE Symposium on Security and Privacy 2010, pp. 273–285, **2017.**
[2] A. Boldyreva, V.Goyal, V. Kumar, "Identity-Based Encryption with Efficient Revocation" Proc. ACM Conference on Computer and Communications Security 2008, pp. 417–426, **2017.**
[3]   International standard ISO/IEC 18004, "Information technology Automatic identification and data capture techniques Bar code symbology QR Code‖", Reference number - ISO/IEC 18004:2000(E), First edition 2000-06-15.
[4] HenrykBlasinski, "Per-colorant- channel color barcodes for mobile applications an interference cancellation framework", IEEE Transactions on Image Processing, vol. 22, no. 4, April **2013.**
[5] A. Sankara Narayanan, "QR codes and security solutions‖, International Journal of Computer Science and Telecommunication" , Volume **3**, Issue **7**, July **2012.**
[6] KamonHomkajorn, MahasakKetcham, and SartidVongpradhip, "A technique to remove scratches from QR code images" , International Conference on Computer and Communication Technologies (ICCCT'2012), May 26-27, **2012.**
[7] Kuan-Chieh Liao, "A novel user authentication scheme based on QR-code" , Journal of networks, vol. **5**, no. 8, August **2010.**