International Journal of Information Movement *Vol.2 Issue III* *(July 2017)*
Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 172-178**

SECURING QR CODES WITH ENCRYPTION SCHEMES: A SURVEY

Kanchan
M.Tech. Scholar, Deptt. of ECE
Galaxy Global Group of Institutions, Haryana, India
Email:- gatherkanchan@gmail.com
,
Saranjeet Singh
Faculty, Deptt. of ECE
Galaxy Global Group of Institutions, Haryana, India
Email: mail2saranjeet@gmail.com

Abstract: – QR code (abbreviated from Quick Response code) matrix barcode (or two-dimensional code) first designed for the automotive industry is a trademark. Recently, the system standard UPC barcode from its fast readability and large storage capacity than the industry has become popular outside. Code black modules (square dots) are arranged in a square pattern on a white background. Information encoded data (numeric, alphanumeric, byte / binary, Kanji), or through supported extensions, virtually any type of data, four standardized types ("modes") can be made. QR code on the Internet, with the rapid development of the transmission required, for the protection of digital information against illegal use becomes more and more important. QR code to get this paper proposes a chaotic scheme, massive data capacity and high correlation between pixels in QR codes as files, traditional techniques are not suitable for encryption QR code. (Such as AES and DES) as compared with conventional methods, chaos-based encryption schemes QR code has done well.

Keywords: Security: QR Codes, Chaotic Encryption.

1.0 Introduction

QR codes were invented in Japan by Toyota subsidiary Denso Wave in 1994 to track vehicles during the manufacturing process, and the basic components to be scanned at high speed, was designed to allow. Since the two-dimensional barcode has become one of the most popular types. Unlike the old one-dimensional barcode that can be scanned by a narrow beam mechanically was designed to [1].

QR Code standard UPC barcode system than its fast readability and greater storage capacity outside of the automotive industry has become popular. Applications product tracking, item identification, time tracking, document management, and includes general marketing [2].

A QR code black modules (square dots) arranged in a square grid on a white background, which (like a camera, scanner, etc.) can be read by an imaging device and Reed-Solomon error correction until are processed using the picture can be properly interpreted. If necessary, the data patterns that are present in the image of both horizontal and vertical components are extracted [3].

2.0 Uses of QR Codes

QR codes to track automotive parts manufacturing plant has been invented more than urban spaces and have found their way into mobile devices.

2.1 Advertising: Advertising is the most common use case in the URL or contact information, geo-locations and text encoding to make them immediately available to the user. Billboard ads with QR codes can be found in most urban spaces to inform potential future customers to manually type in the URL of a webpage eliminates the need to travel. According to the supermarket chain Tesco have used QR codes to promote online shopping and to penetrate further into the South Korean market. Another innovative and cost-effective marketing campaign QR code by

cutting the hair style was started by a shampoo company. People with these haircuts their \ Child Tattoo "after scanning the company's Web site redirected to the ad worked as shampoo.

2.2 Mobile Payments: QR code and mobile payment process by scanning a QR code to purchase a product or service are used to provide the opportunity. After scanning the QR code, users pay an intermediate agent or the company's web page is redirected to payment gateway. PayPal, which is one of the largest payments companies, already pay some countries this practice is adopted.

2.3 Access Control: According to the QR code in combination with other methods to enhance security are used for physical access control. Cao et al. QR code and One-Time Password (OTP) by combining techniques offer a secure authentication system [4]. The user's information is a main server, the user's information, a mobile application that generates QR code, and scan the QR code with a camera is stored in the client PC holds. In order to authenticate the user encoded an encrypted password, which is then scanned with a QR code from the client PC generates.

2.4 Augmented Reality and Navigation: QR codes are also used in digital government services effectively to deliver valuable information to the public. According to the QR code to increase citizen participation and park trails and museums are used to navigate through them. In addition to the education and supplementary material are used within the game. QR codes are also people who take part in a social event or to support the learning process in order to share information are used to share information between. In addition, QR codes are presented in interesting and creative use and a surface on which the QR code is deployed as an augmented reality application, and as a result are used, impressive 3D virtual objects are produced and displayed to the user.

3.0 QR Codes as Attack Vectors

In this section we describe different attack scenarios based on QR codes. In the media, the most frequently reported attack scenario is social engineering. In Information Technology (IT) security, social engineering refers to the art of manipulating people to reveal confidential information to the social engineer and it is mainly used to steal data. One of the most popular practices in social engineering is phishing. Attackers use malicious QR codes to direct users to fraudulent web sites, which masquerade as legitimate web sites aiming to steal sensitive personal information such as usernames, passwords or credit card information. There are two main attack vectors to exploit QR codes:

3.1 The attacker replaces the entire QR code. This attack is simple yet effective. An attacker creates a new QR code with a malicious link encoded and pastes it over an already existing one on e.g. a billboard advertisement.

Fig. 3.1: The modification attack

3.2 The attacker modifies individual modules of a QR code. The main idea of this modification is that the encoded content is modified solely by changing the color of specific modules of the QR Code to which the user will be directed after scanning the code as proposed in.

4.0 Security issues of QR Codes ?

We need to focus on the security implications of the case where a QR code as a means of payment is used. In previous section we discussed earlier how the QR code on the PayPal online store is built. Especially payment via PayPal only payments will usually require the user to enter the name. May be similar to ours is an implementation of

a potential attack, the attacker changes the QR code is changed in a way that includes the recipient's name. A valid user name very easy to use a closer view without offending clients to redirect their account will have to pay. Similarly, the payment system of the Bank has introduced some risk to the same kind of attacks shows. More specifically, the system "scan and pay" donations such campaigns or competitions where some posters to advertise the event is used as is used in public campaigns, to be deployed in a phishing attack is. A malicious attacker could change poster located on the QR code, and in the same way as we mentioned earlier, donations may be sent to his account. This system STUZZA, among which is the largest Austrian banks was proposed by an existing collaboration platform, is on its way to becoming a European standard. However, we strongly believe that the security implications of such standardization has to be taken into account before.

There are also security implications, while our analysis of the survey results are generated. All four cities that we surveyed, 57% of the participants (157) and an Android device and 31% of participants (85) was an Apple iOS device. Another 8% of the participants (22) were holding Windows Phone devices (the remaining 4% was a mixture of BlackBerry and Symbian devices). For both Android and iOS devices, the majority of the Web kit based browsers. At that time we did our research, there are known vulnerabilities and exploits that mobile browser or material handlers were the target public. Researchers have found that some of the famous exploits of Web kit browsers are listed. These vulnerabilities that an attacker "trick" a user could be exploited by a malicious web page is. As a medium to attract users to the QR code may be, in this case is a very convenient tool. When a user ID such as a webpage, your browser is a malicious webpage and insecurity in the attack will manage to successfully complete browser based on the material will execute.

Browse resources that even a successful attack, the attacker can use to be. There are many types of attacks that steal such cookies, session hijacking, or even cross-site scripting (XSS) to gain control of the device which can be positioned in such a way as can be. However, we conclude that most of the users of Android (85) Appliances mobile browser, which is protected against many of these attacks were using the latest version must mention. Apple iOS device users when we saw a wide variety of versions of the web browser and the latest version of Safari was just 19. Another side attack scenario is based on the adventures. In this case, the attack is targeting the operating system-related exploits. In our study, we have 10 different versions of the Android operating system and Apple iOS versions in 10 different. The majority of Android users (45) Version 4.1.2 is the latest version of which were using. Accordingly, the 46 participants of the Apple devices to the latest version 6.1.x. One of the participants was using the devices at the same time that there is an operating system those more than two years old and had used the key security issues. There are known root exploits observed in our study that many of the operating system is a short list of some of the impact.

5.0 Related Work

Lorenzi D. et al., (2012) Digital government is universally gaining acceptance as the public becomes more technologically advanced. The government must embrace new technology to minimize costs and maximize utility of services to the taxpayer. While administrative services have been easily ported to the digital world, there are still many important citizen-centric services that have not yet been effectively migrated. Quick Response codes (QR codes) provide a means to effectively distribute many different varieties of information to the public. We propose a QR code system and a corresponding Smartphone application for the U. S. National Park Service (NPS) with the goal of providing a new level of interactivity for the public. The focus is on developing a QR code waypoint system for park navigation, as well as incentivizing park use through gamification of site attractions. The system provides increased safety for park goers, disseminates information more effectively and accurately, and improves feedback between the NPS and the public [5].

Kapsalis I., (2013), the 2-dimensional barcodes known as QR (Quick Response) Codes are increasing their popularity as they appear in more places in the urban environment. QR Codes can be considered as physical hyper-links that give the ability to users to access, through their mobile devices that are able to scan QR Codes, additional information located in a web-page. Apart from marketing, QR Codes have been also adopted indifferent areas such as the on-line payments. This development along with the trend that some of the users may follow which indicates to scan unauthenticated data, such as QR Codes located in public places, motivated us to investigate how QR Codes can be used as an attack vector. We first developed an implementation which attempts to brute-force QR Codes by attacking directly the modules, aiming to retrieve an alternated URL upon scanning the QR Code and after having applied the module changes. Our implementation showed us that such an attack is unfeasible in a real attack scenario. However, the second approach that we followed, in which we attacked the binary representation of the

encoded string, we managed to produce the desired result. Furthermore, we conducted an empirical study aiming to identify the user's level of security awareness concerning the security issues related to QR Codes. The on-line survey that was accessible through our QR Code stickers was our mean of interaction with the users.

We deployed our stickers in 4European cities (Vienna, Helsinki, Athens and Paris) and we managed to attract 273 individuals that scanned and visited our web pages. Out of these visitors, 83 participants completed our online survey. The results collected indicate that users are motivated mainly by their curiosity and they have serious lack of knowledge on the potential threats and the ways to protect them [6].Vidas T. et al.,(2013) The matrix barcodes known as Quick Response (QR) codes are rapidly becoming pervasive in urban environments around the world. QR codes are used to represent data, such as a web address, in a compact form that can be scanned readily and parsed by consumer mobile devices. They are popular with marketers because of their ease in deployment and use. However, this technology encourages mobile users to scan unauthenticated data from posters, billboards, stickers, and more, providing a new attack vector for miscreants. By positioning QR codes under false pretenses, attackers can entice users to scan the codes and subsequently visit malicious websites, install codes, or any other action the mobile device supports. We investigated the viability of QR code- initiated phishing attacks, or QR is hing, by conducting two experiments. In one experiment we visually monitored user interactions with QR codes; primarily to observe the proportion of users who scan a QR code but elect not to visit the associated website. In a second experiment, we distributed posters containing QR codes across 139 different locations to observe the broader application of QR codes for phishing. Over our four-week study, our disingenuous flyers were scanned by 225 individuals who subsequently visited the associated websites. Our survey results suggest that curiosity is the largest motivating factor for scanning QR codes. In our small surveillance experiment, we observed that 85% of those who scanned a QR code subsequently visited the associated URL [7**]**. Kim S. H. et al.,(2013) Internet phishing attacks have been evolving along with the growth of online transactions on the Internet. MITM (Man-In-The-Middle) phishing is an attack that manipulates authentication and transaction information when an attacker is located in between a web server and a user. The possibility of this sort of phishing attack has been posed for a long time, but the menace was mostly ignored. Since Bruce Schneier introduced the concept of emasculating two-factor authentication in 2005, Leung and Jakobsson proposed Control Relay-MITM and doppelganger phishing attacks, respectively. We introduce ART (Active Real-Time) MITM phishing attack as an enhanced phishing attack against above ones.

While providing same UX (User experience) of real web server to a user, ART-MITM makes all security solutions that are installed on the user's computer useless and runs automated attack processes. To defeat against ART-MITM phishing attack, we propose a geo-location based QR-code authentication scheme using mobile phone. The proposed scheme provides convenience, mobility, and security for the user; as a result, the scheme can be seen as a realistic solution to such enhanced phishing attacks [8]. Krombholz K. et al., (2014) QR (Quick Response) codes are two-dimensional barcodes with the ability to encode different types of information. Because of their high information density and robustness, QR codes have gained popularity in various fields of application. Even though they offer a broad range of advantages, QR codes pose significant security risks. Attackers can encode malicious links that lead e.g. to phishing sites. Such malicious QR codes can be printed on small stickers and replace benign ones on billboard advertisements. Although many real world examples of QR code based attacks have been reported in the media, only little research has been conducted in this field and almost no attention has been paid on the interplay of security and human-computer interaction. In this work, we describe the manifold use cases of QR codes. Furthermore, we analyze the most significant attack scenarios with respect to the specific use cases. Additionally, we systemize the research that has already been conducted and identified usable security and security awareness as the main research challenges.

Finally we propose design requirements with respect to the QR code itself, the reader application and usability aspects in order to support further research into to making QR code processing both secure and usable [9]. Chen J.H. et al., (2014) In recent years there has been increasing attention towards digital rights. Therefore, this paper proposes a matrix barcode to verify image copyrights. The copyright text, Quick Response code (QR code), and watermarking techniques are used to achieve a hidden identification scheme implementing Direct Sequence Spread Spectrum (DSSS) and modulation of The Modified Code Division Multiple Access (MCDMA) to hide the QR code data. DSSS and MCDMA hash the data and QR code has a robust feature to prevent external attacks and destruction of

the cover image. The QR codes information can be easily extracted by mobile devices. Even if the barcode suffers external damage, a copy of the barcode can be hidden within the image to easily recover the barcode data. Compare to the other scheme, our method has two advantages: 1) the QR code has universal, rapid identification and fault tolerance features, so it is suitable for copyright protection; and 2) using DSSS and MCDMA methods to hide information can provide more security and fault-tolerant features [10]. Muthaiah R. M. et al., (2014) A highly efficient technique for hiding data behind images or any other digital media and to make them more secure from the intruders is proposed. There are concepts like digital watermarking, image steganography, fingerprinting that are intended for the same purpose but with slight variations. In this context, cryptography can also be used to ensure security of data but the difference between the former ones and the latter, to be told in a nut shell, is the concept of steganography keenly focuses on keeping the existence of a message secret whereas the cryptographic techniques revolves around keeping the contents of the message secret and safe from the intruder. There are security threats when the above said techniques are used individually to protect and keep information secret. Hence we propose a technique where we hide the data behind any digital media, here behind an image and to have its existence secretive, we put the image with hidden data into a QR code and use a powerful encryption algorithm [11]. Dobrescu A. et al., (2015) Now Web technologies and tools have seen an accelerated progress in the last years bringing added value to the marketing activity carried out at company level. They have always sought to facilitate production, distribution and communication processes. Moreover, the applications developed online have enabled the communication with the consumers and facilitated the fast sending of the information regarding the goods commercialized. The emergence and development of QR codes on the market enabled the marketing specialists to communicate easier with their target public as these codes help them send a range of information on the products /services commercialized, promotions, competitions, events held, etc. This paper looks at the way the QR codes were used in time in the marketing activities carried out by enterprises working in various business areas. Research of secondary sources was carried out in the period from 5.04.2015 – 3.05.2015, in Bucharest [12].

6.0 QR Code Encryption

With the rapid growth of the requirement of QR Code transmission on Internet, protection of digital information against illegal usage becomes more and more important. Due to bulky data capacity and high correlation among pixels in QR Code files, traditional techniques are not suitable for QR Code encryption. Compared with traditional methods, chaos-based QR Code encryption schemes have shown superior performance

The chaos streams are generated by using various chaotic maps. Among the various maps, four maps are investigated and their characteristics are analyzed.

6.1 Map:

A simple and well-studied example of a 1D map that exhibits complicated behavior is the logistic map from the interval {0,1} in to {0,1}, parameterized by μ:

$$G\mu(x) = \mu * (x) \tag{6.1}$$

The state evolution is described by x(n+1)=μ*x(n)*(1-x(n))

where $0 \leq \mu \leq 4$. This map constitutes a discrete-time dynamical system in the sense that the map g_μ :{ 0, 1}→ {0, 1} generates a semi-group through the operation of composition of functions. In the logistic map, as μ is varied from 0 to 4, a period-doubling bifurcation occurs [13].

6.2 Tent Map:

In mathematics, the tent map is an iterated function, in the shape of a tent, forming a discrete-time dynamical system. It takes a point x_n on the real line and maps it to another point:

$$x_{n+1} = \begin{cases} \mu x_n & for\ x_n < \frac{1}{2} \\ \mu(1-x_n & for\ \frac{1}{2} \leq x_n \end{cases} \tag{6.2}$$

Where μ is a positive real constant

Depending on the value of μ, the tent map demonstrates a range of dynamical behavior ranging from predictable to chaotic [14].

6.3 Quadratic Map

More complicated analytic quadratic map is

$$x_{n+1} = f_c\ (x_n) = x_n^2 + c \quad (6.3)$$

For an analytic map points where f '(x_c) = 0 are called critical points. Quadratic map has the only critical point x_c = 0.So a fixed point is stable (attracting), super stable, repelling, indifferent (neutral) according as its multiplier satisfies |m| < 1, |m| = 0, |m| > 1 or |m| = 1. The second fixed point is always repelling. For |x| > x_2 iterations go to infinity. For |x| < x_2 they go to the attracting fixed point x_1. This interval is the basis of attraction of the point [15].

6.4 Bernoulli Map

Bernoulli map or the 2x mod. 1 map defined as

$$F(x) = \begin{cases} 2x, 0 \le x < 0.5 \\ 2x - 1\ 0.5 \le x < 1 \end{cases} \quad (6.4)$$

A Bernoulli process is a discrete time stochastic process consisting of a finite or infinite sequence of independent random variable X1, X2, X3,..., such that for each i, the value of X_i is either 0 or 1 for all values of i, the probability that X_i = 1 is the same number p. From any given time, future trials are also a Bernoulli process independent of the past trials [16].

6.5 Conclusion

QR code, abbreviated from Quick Reply code, is a two-dimensional barcode. A QR code is able to store and communicate data encompassing web link URLs (Uniform Resource Locators), plain text, email addresses, link data and so on. It was primarily projected for intention of pursuing vehicle portions across produce in industry procedure. Though afterward QR code aroused the public's attention and came to be personal- and publicizing vector cheers to its versatility and ease of use. Each person is able to gain his/her own QR code across bestowing data that is going to be encoded into the code, whichever via a little sorts of multimedia or web sites. After on the finish of code creation, data stored in this code can be removed via so-called decoder or scanner - a request or a mechanism to be utilized for decoding the QR code and obtaining the stored data. Over the last decades, due to the characteristics of high speed and paralleling, optical picture encryption methods have been consenting attention to QR codes. Though, these methods involve a convoluted cipher image that is not extremely convenient for optical encryption because spatial light modulators are not able to adjust the amplitude and the period simultaneously. In future works, a novel QR image encryption algorithm based on chaos map will be proposed. Widely used in basic one-dimensional chaotic system plugged, our proposed scheme with large key space offers good encryption system. We will prove that the new algorithm, the key space is large enough, thus making brute force attacks infeasible security analysis.

7.0 References

[1] Rouillard J. and Laroussi M., "Perzoovasive: Contextual Pervasive QR Codes As Tool To Provide An Adaptive Learning Support", Proceedings of the 5th international conference on Soft computing as trans-disciplinary science and technology, Association for Computing Machinery, pp. 542-548, 2008.

[2] Ceipidor C. B., Medaglia C. M., Perrone A., Marsico M.D. and Romano G. D.. "A Museum Mobile Game For Children Using QR-Codes", Proceedings of the 8th International Conference on Interaction Design and Children, Association for Computing Machinery, pp. 282-283, 2009.

[3] Wang J., Shyi C. N., Hou T. W. and Fong. C. P., "Design And Implementation Of Augmented Reality System Collaborating With QR Code.", Computer Symposium (ICS), IEEE, pp. 414-418, 2010.

[4] Kieseberg P., Leithner M., Mulazzani M., Munroe L., Schrittwieser S., Sinha M. and Weippl E., "QR Code Security", Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, Association for Computing Machinery, pp. 430-435, 2010.

[5] Lorenzi D., Shafiq B., Vaidya J., Nabi G., Chun S. and Atluri V., "Using QR Codes For Enhancing The Scope Of Digital Government Services", Proceedings of the 13th Annual International Conference on Digital Government Research, Association for Computing Machinery, pp. 21-29, 2012.

[6] Kapsalis I., "Security Of QR Codes", Norwegian University of Science and Technology, 2013.

[7] Vidas T., Owusu E., Wang S., Zeng C., Cranor L. F. and Christin N., "QRishing: The Susceptibility Of Smartphone Users To QR Code Phishing Attacks." International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, pp. 52-69, 2013..

[8] Kim S. H., Choi D., Jin S. H. and Lee S. H., "Geo-Location Based QR-Code Authentication Scheme To Defeat Active Real-Time Phishing Attack." Proceedings of the 2013 ACM workshop on Digital identity management, Association for Computing Machinery, pp. 51-62, 2013.

[9] Krombholz K., Frühwirt P., Kieseberg P., Kapsalis I., Huber M. and Weippl E., "QR Code Security: A Survey Of Attacks And Challenges For Usable Security." Human Aspects of Information Security, Privacy and Trust, Springer International Publishing, pp. 79-90, 2014.

[10] Chen J. H., Chen W. Y. and Chen C. H., "Identification Recovery Scheme Using Quick Response (QR) Code And Watermarking Technique." Applied Mathematics & Information Sciences 8, No. 2, pp. 585-596, 2014

[11] Muthaiah R. M. and Krishnamoorthy N., "An Efficient Technique For Data Hiding With Use Of QR Codes-Overcoming The Pros And Cons Of Cryptography And Steganography To Keep The Hidden Data Secretive." International Journal of Computer Applications, Vol. 100(14), pp.1-5, 2014.

[12] Dobrescu A., "Implications Of QR Codes For The Business Environment." Calitatea 16, No. S3:166, 2015.

[13] Lasota A. and Mackey M. C., “Chaos, fractals, and noise: stochastic aspects of dynamics”, Vol. 97, Springer Science & Business Media, 2013.

[14] Liang S., Hao Q., Jun L. and Zhi-quan W., “Chaotic optimization algorithm based on Tent map,” Control and Decision, Vol. 20(2), pp. 179-182, 2005.

[15] Elhadj Z. and Sprott J. C., “A Minimal 2-D Quadratic Map With Quasi-Periodic Route To Chaos,” International Journal of Bifurcation and chaos, Vol. 18(05), pp. 1567-1577, 2008.

[16] Sang T., Wang R. and Yan Y, “Generating binary Bernoulli sequences based on a class of even-symmetric chaotic maps,” IEEE Transactions on Communications, Vol. 49(4), pp. 620-623, 2001.