IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-4, Issue-7 E-ISSN: 2347-2693

SECURING QR CODES WITH ENCRYPTION SCHEMES: A SURVEY

TARUNIKA[†] and ANITA SAHOO[††]

[†,††] Department of Computer Science and Engineering,
Jss academy of technical education, Noida, India

Available online at: www.ijcseonline.org

Received:18/Jun/2016 Revised:26/Jun/2016 Accepted:16/Jul/2016 Published:31/Jul/2016

***Abstract*- QR code (shortened from Quick Response code) matrix barcode (or two-dimensional code) initially intended for the car business is a trademark. QR code on the Internet, with the quick advancement of the transmission required, for the security of computerized data against unlawful use turns out to be increasingly imperative. To overcome basic restrictions in the one-dimensional disorganized framework,, our proposed scheme presents good encryption system with large key space. Due to bulky data capacity and very high relationship among pixels in QR Code documents, customary methods are not appropriate for QR Code encryption. QR code to get this paper proposes a chaotic scheme, enormous information limit and high relationship between's pixels in QR codes as documents, conventional systems are not reasonable for encryption QR code. (For example, AES and DES) as contrasted and chaos-based encryption schemes QR code has done well.**

***Keywords*: Security, QR Codes, Chaotic Encryption.**

I. INTRODUCTION

QR codes were developed in Japan by Toyota backup Denso Wave in 1994 to track vehicles amid the assembling procedure, and the fundamental parts to be checked at high speed, was intended to permit. Since the two-dimensional barcode has become one of amongst the most mainstream sorts. Dissimilar to the old one-dimensional standardized by a narrow beam mechanically was designed to [1]
QR Code standard UPC standardized tag framework than its quick readability and more storage limit outside of the car business has become popular. Applications item tracking, thing distinguishing proof, time following, record administration, and incorporates general promoting. [2]

A QR code dark modules (square dabs) arranged in a square framework on a white foundation, which (like a camera, scanner, and so forth.) can be perused by an imaging gadget and Reed-Solomon error correction until are handled utilizing the photo can be legitimately deciphered. On the off chance that essential, the information patterns that are present in the image of both horizontal and vertical components are extracted. [3]

II. 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.

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.

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. This "one-click" pay-as-known. the respective After scanning the QR code, users pay an intermediate agent or the company's web page is redirected to. PayPal, which is one of the largest payments companies, already pay some countries this practice is adopted.

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 by combining techniques offer a secure authentication system (OTP [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.

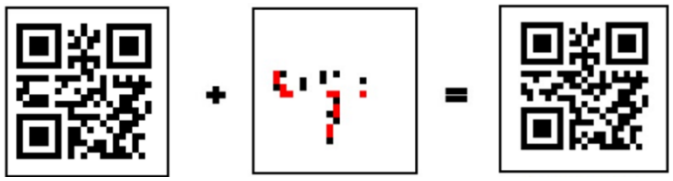
Augmented Reality and Navigation: QR codes are also used in digital government services effectively to deliver valuable information to the public. According to the QR code to increase citizen participation and park trails and museums are used to navigate through them. In addition to the education and 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 showed to the user.

III. QR CODES AS ATTACK VECTORS

In this section we explain 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 known practices in social engineering is phishing. Attackers use malicious QR codes to direct users to fraudulent web sites, which masquerade as changed/similar web sites aiming to steal sensitive personal information such as user id, passwords or credit card information. There are two main attack vectors to exploit QR codes:

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

The attacker changed the individual modules of a QR code. The main purpose 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.



http://gbay.com

Fig. 1. The modification attack

IV. 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 Section 2.2 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 WebKit 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 Webkit 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 were using the devices at the same time that there is an operating system that 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.

V. RELATED WORK

David Lorenziet al., (2012) In this paper Digital government is generally picking up acknowledgment as people in general turns out to be all the more innovatively progressed. The administration must grasp new innovation to minimize costs and amplify utility of administrations to the citizen. While regulatory administrations have been effortlessly ported to the computerized world, there are still numerous imperative subject driven administrations that have not yet been successfully moved. Snappy Response codes (QR codes) give a way to adequately circulate various assortments of data to people in general. We propose a QR code framework and a comparing Smartphone application for the U. S. National Park Service (NPS) with the objective of giving another level of intuitiveness for people in general. The emphasis is on building up a QR code waypoint framework for park route, and additionally incentivizing park use through gamification of site attractions. The framework gives expanded wellbeing to stop goers, disperses data all the more adequately and precisely, and enhances input between the NPS and general society.

IoannisKapsaliset al.,(2013) In this paper The 2-dimensional standardized identifications known as QR (Quick Response) Codes are expanding their ubiquity as they show up in more places in the urban environment. QR Codes can be considered as physical hyper-joins that give the capacity to clients to access, through their cell phones that can examine QR Codes, extra data situated in a site page. Aside from advertising, QR Codes have been additionally embraced apathetic regions, for example, the on-line installments. This advancement alongside the pattern that a portion of the clients may take after which shows to examine unauthenticated information, for example, QR Codes situated in broad daylight places, propelled us to research how QR Codes can be utilized as an assault vector. We initially built up an execution which endeavors to savage power QR Codes by assaulting straightforwardly the modules, intending to recover an exchanged URL after checking the QR Code and in the wake of having connected the module changes. Our usage demonstrated to us that such an assault is unfeasible in a genuine assault situation. Notwithstanding, the second approach that we took after, in which we assaulted the paired representation of the encoded string, we figured out how to create the wanted result. Moreover, we directed an exact study intending to recognize the client's level of security mindfulness concerning the security issues identified with QR Codes. The on-line overview that was available through our QR Code stickers was our mean of collaboration with the clients. We sent our stickers in 4European urban areas (Vienna, Helsinki, Athens and Paris) and we figured out how to draw in 273 people that checked and went by our website pages. Out of these guests, 83 members finished our online overview. The outcomes gathered show that clients are propelled for the most part by their interest and they have genuine absence of information on the potential dangers and the approaches to ensure them.

Timothy Vidaset al.,(2013) In this paper The network standardized identifications known as Quick Response (QR) codes are quickly getting to be pervasive in urban situations around the globe. QR codes are utilized to speak to information, for example, a web address, in a conservative frame that can be filtered promptly and parsed by customer cell phones. They are famous with advertisers in view of their simplicity in sending and utilize. In any case, this innovation urges versatile clients to check unauthenticated information from blurbs, announcements, stickers, and that's just the beginning, giving another assault vector to scalawags. By situating QR codes under false affectations, assailants can allure clients to examine the codes and accordingly visit pernicious sites, introduce codes, or some other activity the cell phone underpins. We examined the reasonability of QR code-started phishing assaults, or QR is hing, by leading two tests. In one test we outwardly checked client collaborations with QR codes; principally to watch the extent of clients who examine a QR code however choose not to visit the related site. In a brief moment test, we appropriated notices containing QR codes crosswise over 139 unique areas to watch the more extensive use of QR codes for phishing. Over our four-week examine, our guileful flyers were checked by 225 people who along these lines went to the related sites. Our review results propose that interest is the biggest persuading element for checking QR codes. In our little observation test, we watched that 85% of the individuals who examined a QR code therefore went to the related URL.

Seung-Hyun Kimet al.,(2013) In this paper Internet phishing assaults have been developing alongside the development of online exchanges on the Internet. MITM (Man-In-The-Middle) phishing is an assault that controls verification and exchange data when an aggressor is situated in the middle of a web server and a client. The likelihood of this kind of phishing assault has been postured for quite a while, yet the danger was for the most part overlooked. Since Bruce Schneier presented the idea of castrating two-element validation in 2005, Leung and Jakobsson proposed Control Relay-MITM and doppelganger phishing assaults, separately. In this paper, we present ART (Active Real-Time) MITM phishing assault as an upgraded phishing assault against above ones. While giving same UX (User experience) of genuine web server to a client, ART-MITM makes all security arrangements that are introduced on the client's PC pointless and runs computerized assault forms. To crush against ART-MITM phishing assault, we propose a geo-area based QR-code verification plan utilizing cellular telephone. The proposed plan gives accommodation, versatility, and security for the client; thus, the plan can be seen as a sensible answer for such improved phishing assaults.

Katharina Krombholzet al., (2014) In this paper QR (Quick Response) codes are two-dimensional standardized tags with the capacity to encode distinctive sorts of data. Due to their high data thickness and heartiness, QR codes have picked up fame in different fields of utilization. Despite the fact that they offer an expansive scope of points of interest, QR codes posture noteworthy security dangers. Aggressors can encode vindictive connections that lead e.g. to phishing destinations. Such malignant QR codes can be imprinted on little stickers and supplant generous ones on announcement commercials. Albeit numerous true case of QR code based assaults have been accounted for in the media, just little research has been led in this field and no consideration has been paid on the transaction of security and human-PC association. In this work, we depict the complex use instances of QR codes. Moreover, we examine the most noteworthy assault situations as for the particular use cases. Furthermore, we systemize the exploration that has as of now been directed and recognized usable security and security mindfulness as the principle research challenges. At long last we propose outline prerequisites as for the QR code itself, the peruser application and ease of use perspectives so as to backing further research into to making QR code preparing both secure and usable.

Ji-Hong Chen et al., (2014) In this paper lately there has been expanding consideration towards computerized rights. In this way, this paper proposes a network standardized tag to confirm picture copyrights. The copyright content, Quick Response code (QR code), and watermarking methods are utilized to accomplish a shrouded recognizable proof plan executing direct succession spread range (DSSS) and regulation of the adjusted code division numerous entrance (MCDMA) to conceal the QR code information. DSSS and MCDMA hash the information and QR code has a vigorous element to forestall outer assaults and devastation of the spread picture. The QR codes data can be effortlessly separated by cell phones. Regardless of the fact that the scanner tag endures outside harm, a duplicate of the standardized tag can be covered up inside the picture to

effortlessly recoup the scanner tag information. Contrast with the other plan, our technique has two points of interest: 1) the QR code has general, fast recognizable proof and adaptation to internal failure highlights, so it is appropriate for copyright insurance; and 2) utilizing DSSS and MCDMA strategies to shroud data can give more security and issue tolerant elements.

R. M. Muthaiahet al., (2014) In this paper A very proficient procedure for concealing information behind pictures or whatever other computerized media and to make them more secure from the interlopers is proposed. There are ideas like advanced watermarking, picture steganography, fingerprinting that are planned for the same reason yet with slight varieties. In this setting, cryptography can likewise be utilized to guarantee security of information yet the distinction between the previous ones and the last mentioned, to be told more or less, is the idea of steganography definitely concentrates on keeping the presence of a message mystery while the cryptographic methods rotates around keeping the substance of the message mystery and safe from the gatecrasher. There are security dangers when the above said procedures are utilized exclusively to ensure and keep data mystery. Thus we propose a strategy where we conceal the information behind any advanced media, here behind a picture and to have its presence shrouded, we put the picture with concealed information into a QR code and utilize an intense encryption calculation.

AndraDobrescu et al., (2015) In this paperWeb advancements and apparatuses have seen a quickened improvement in the most recent years conveying increased the value of the advertising action did at organization level. They have constantly tried to encourage generation, appropriation and correspondence forms. Also, the applications created online have empowered the correspondence with the buyers and encouraged the quick sending of the data in regards to the products marketed. The rise and improvement of QR codes available empowered the advertising pros to discuss simpler with their objective open as these codes help them send a scope of data on the items/administrations popularized, advancements, rivalries, occasions held, and so on. This paper takes a gander at the way the QR codes were utilized as a part of time in the advertising exercises did by endeavors working in different business territories. Examination of optional sources was done in the period from 5.04.2015 – 3.05.2015, in Bucharest.

VI. CONCLUSION AND FUTURE WORK

QR code, truncated from Quick Reply code, is a two-dimensional standardized identification. A QR code can store and impart information including web join URLs (Uniform Resource Locators), plain content, email addresses, join information end so on. It was essentially anticipated for expectation of seeking after vehicle parts crosswise over produce in industry procedure. In spite of the fact that a short time later QR code stimulated people in general's consideration and came to be personal and publicizing vector cheers to its flexibility and convenience. Every individual can pick up his/her own particular QR code crosswise over giving information that will be encoded into the code, whichever by means of a little sorts of sight and sound or sites. After on the completion of code creation, information put away in this code can be removed through supposed decoder or scanner - a request or a component to be used for deciphering the QR code and getting the put away information. In the course of the most recent decades, because of the qualities of fast and paralleling, optical picture encryption techniques have been consenting thoughtfulness regarding QR codes. However, these techniques include a convoluted cipher picture that is not to a great degree helpful for optical encryption on the grounds that spatial light modulators are not ready to modify the amplitude and the period all the while. In future works, a novel QR picture encryption algorithm based on chaos map will be proposed. Generally utilized as a part of essential one-dimensional disorganized framework stopped, our proposed plan with large key space offers great encryption framework. We will demonstrate that the new calculation, the key space is sufficiently large, consequently making brute force attacks infeasible security analysis.

REFERENCES

[1]. Rouillard J.and Laroussi M."PerZoovasive: contextual pervasive QR codes as tool to provide an adaptive learning support." *ACM* ,In Proceedings of the 5th *international conference on Soft computing as transdisciplinary science and technology*, pp. 542-548., 2008.

[2]. Ceipidor U.-B., Medaglia C-M., Amedeo Perrone, Marsico M-D., and Romano G-D. "A museum mobile

game for children using QR-codes." In Proceedings of the *8th International Conference on Interaction Design and Children*, pp. 282-283. ACM, 2009.

[3]. Wang J.-T., Chia-NianShyi, T-W. Hou, and C. P. Fong. "Design and implementation of augmented reality system collaborating with QR code." *IEEE Trans. In Computer Symposium (ICS), 2010 International*, pp. 414-418., 2010.

[4]. Kieseberg P.,Leithner M.,Mulazzani M.,Munroe L., Schrittwieser S.,Sinha M., and Weippl E.. "QR code security." In Proceedings of the *8th International Conference on Advances in Mobile Computing and Multimedia*, pp. 430-435. ACM, 2010.

[5]. Lorenzi D., BasitShafiq, Vaidya J.,Nabi G.,Chun S., and Atluri VL. "Using QR codes for enhancing the scope of digital government services." In Proceedings of the *13th Annual International Conference on Digital Government Research*, pp. 21-29. ACM, 2012.

[6]. IoannisKapsalis, "security of QR codes." (2013).

[7]. Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, and Nicolas Christin. "QRishing: The susceptibility of smartphone users to QR code phishing attacks*." In Financial Cryptography and Data Security*, pp. 52-69. *Springer Berlin Heidelberg*, 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*." In Proceedings of the 2013 ACM workshop on Digital identity management*, pp. 51-62. ACM, 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*." In Human Aspects of Information Security, Privacy, and Trust*, pp. 79-90. *Springer International Publishing*, 2014.

[10]. Chen J-H.,Chen W-Y., andChen C-H. "Identification recovery scheme using quick response (QR) code and watermarking technique." *Applied Mathematics & Information Sciences* 8, no. 2 (2014): 585.

[11]. R. M. Muthaiah, and N. Krishnamoorthy. "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* 100, no. 14 (2014).

[12]. Andra Dobrescu "Implications of QR Codes for the Business Environment." *Calitatea* 16, no. S3 (2015): 166.

