ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

# An Effective mechanism for Ensuring Security of QR Code

Ashish R. Wane
Information Technology
Jawaharlal Darda Institute of Engg. & Tech
Yavatmal(M.S),India
Ashish.wane@gmail.com

Siddharth P. Jamankar
Information Technology
Jawaharlal Darda Institute of Engg. & Tech
Yavatmal(M.S),India
jamankarsiddharth@gmail.com

Onkar V. Chandure
Information Technology
Jawaharlal Darda Institute of Engg. & Tech
Yavatmal(M.S),India
onkar_chandure@yahoo.co.in

***Abstract:*** Identification of objects and places in the real world is important, and 2-D printing code is useful to store identifiers of them. Any camera mobile device with capture function can read content from a barcode tag directly. When a barcode contains important data or privacy information, the risk of security becomes an important problem. Because QR codes simply feature a square barcode with a unique pattern, people have no idea whether the code will take them to reputable information or a site loaded with malware. In this paper, discusses QR codes different data types, attack via QR codes and security solutions. However, since it is easy to modify the content stored in the 2-D code, we must verify whether the identifier written in the 2-D code is indeed issued by the authorized organization.This paper gives information about the security of qr codes and solution.

***Keywords:*** QR Codes, Barcode, Security and Smartphone

## I. INTRODUCTION

QR-code stand for Quick Response Code, which is well known 2 dimensional barcode industrial as it, have high efficiency in accuracy and reading speed. QR-code is continuously developed by Denso Wave company [1], as development today its able to store more information. QR code is able to store up to 7089 numeric. It also able to store in different type of format such as Numeric Characters, Alphabetic Characters, Kanji Characters, Symbols, Binary and Control Code.

The security of one dimensional (1D) barcodes is lower than 2D barcodes. 1D barcodes are very easy to read by scanning the lines and the spaces. However, 2D barcodes are not easy to read a symbol pattern by human eyes. With regard to readability, 1D barcodes must scan along a single directional. If the angle of a scan line does not fit within a range, the data would not be read correctly. However, 2D barcodes get wide ranges of angles for scanning. Thus, 2D barcodes are readability [2]. The key difference between the two is the amount of data they can hold or share. Bar codes are linear one-dimensional codes and can only hold up to 20 numerical digits, whereas QR codes are two-dimensional (2D) matrix barcodes that can hold 7,089 numeric characters and 4,296 alphanumeric characters, and 1,817 kanji characters of information [2]. Their ability to hold more information and their ease of use makes them practical for small businesses.

QR Codes can be used in a variety of ways to market a business, to provide further information on a product or service by encoding general text, URL, phone number, business card and even provide Wi-Fi access. A recent implementation of QR codes is India's 'Aadhar' project that
gives a unique identification number to the citizens of India much like the Social Security Number (SSN) in USA .Another first in Indian aviation (Jet Airways) uses QR codes in their products and services.

## II. LITERATURE REVIEW

QR Codes have already overtaken the conventional bar codes because of the main fact that the capacity of data that can be stored by a conventional bar code is very much less when compared to the data that can be stored by a 2-D barcode, the QR Code. QR Code contains data both in horizontal and vertical positions. QR Codes have already overtaken the classical barcode in popularity in some areas. This stems in many cases from the fact that a typical barcode can only hold a maximum of 20 digits, whereas as QR Code can hold up to 7,089 characters [3]. QR Codes are capable of encoding the same amount of data in approximately one tenth the space of a traditional bar code. A great feature of QR Codes is that they do not need to be scanned from one particular angle, as QR Codes can be read regardless of their positioning. QR Codes can be easily decoded with a mobile phone with appropriate software (Kaywa Reader) [4]. Secure communication can also be established using QR Encoding techniques [5].



CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

## III. QR CODE

The QR code is a kind of matrix symbol, which was developed by the Japanese company Denson-Wave in 1994. Figure 1 shows the basic structure of QR code. They are quiet zone, position detection patterns, separators for position detection patterns, timing patterns, alignment patterns, format information, version information, data, and error correction codewords. They are shown in Figure 1. Details of QR code can be refereed to [6].

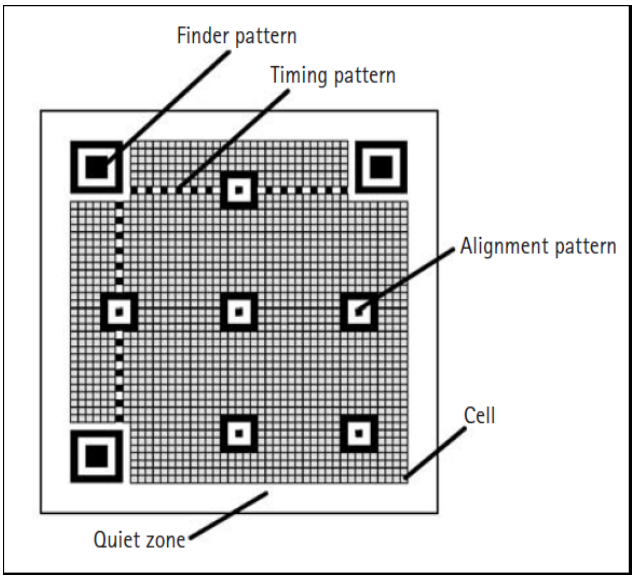


Figure: 1

### *A. Finder Pattern:*

A pattern for detecting the position of the QR Code. By arranging this pattern at the three corners of a symbol, the position, the size, and the angle of the symbol can be detected. This finder pattern consists of a structure which can be detected in all directions (360°).

### *B. Alignment Pattern:*

A pattern for correcting the distortion of the QR Code. It is highly effective for correcting nonlinear distortions. The central coordinate of the alignment pattern will be identified to correct the distortion of the symbol. For this purpose, a black isolated cell is placed in the alignment pattern to make it easier to detect the central coordinate of the alignment pattern.

### *C. Timing Pattern:*

A pattern for identifying the central coordinate of each cell in the QR Code with black and white patterns arranged alternately. It is used for correcting the central coordinate of the data cell when the symbol is distorted or when there is an error for the cell pitch. It is arranged in both vertical and horizontal directions.

### *D. Quiet Zone:*

A margin space necessary for reading the QR Code. This quiet zone makes it easier to have the symbol detected from among the image read by the CCD sensor. Four or more cells are necessary for the quiet zone.

### *E. Data Area:*

The QR Code data will be stored (encoded) into the data area. The grey part in Figure 11 represents the data area. The data will be encoded into the binary numbers of '0' and '1' based on the encoding rule. The binary numbers of '0' and '1' will be converted into black and white cells and then will be arranged. The data area will have Reed-Solomon codes incorporated for the stored data and the error correction functionality.

## IV. SECURITY OF QR CODES

### *A. Threat Model:*

One can distinguish two different threat models for manipulating QR Codes. First, an attacker may invert any module, changing it either from black to white or the other way round. Second, a more restricted attacker can only change white modules to black and not vice versa.

#### *a) mixing of two color:*

The easiest approach for attacking an existing QR Code is by generating a sticker containing a QR Code with the manipulated QR Code in the same style as the original QR Code and position it over the code on the advertisement. Of course this would either require some preparation or a mobile printer and design applications for a mobile device. At least when attacking on a large scale against one chosen target, the time needed for preparation should not pose a serious limitation. Since this attack is trivial, we have decided to exclude it from the scope of this paper. However, we believe that using this method in an attack against a real-world advertisement is a viable option for large-scale attacks.

#### *b) one color:*

In this case we restrict ourselves to the modification of a single color only. The background for this restriction lies in the scenario of an attacker seeking to modify a single poster on the y just by using a pen (thereby reducing the possible modifications to changing white modules to black). This restriction is the basis for the attacks further outlined throughout this paper.

### *B. Attacking different modules:*

Since QR Codes contain a lot of different information, including meta information on version, masking and source encoding, several different regions exist that can be targeted either individually or in combination.0

#### *a) The masks:*

Masks are used to generate QR Codes with a good distribution of black and white modules (close to 50:50 and distributed well over the whole code). This increases the contrast of the picture and thus helps devices to decode it. According to the standard, when generating a QR Code, every mask of the 8 specified ones is applied and each result is rated. The mask that results in the best distribution according to the rating is chosen (the select of using correct masks can be seen in

Figure 4. The bar before shows the number of white and black elements before any masking was applied, after the numbers after the best masking was used). There is always only one mask in use in a given QR Code, it is encoded together with the version in a separate block of the code using strong BCH encoding. In the conditions in Table 2, it refers to the row position of the module and j to its column position. The mask is black for every module the condition is valid for and white for the rest. Targeting the mask can change quite a lot in the whole data and error correction parts, still, this can be a useful basis for additionally applying other methods. A problem when changing the masking is that it is encoded separately, utilizing a strong error correction algorithm.

***b) encoding the character:***

There are several different source encodings specified for the information contained in the code, thereby maximizing the capacity in exchange for increased complexity:

(a). Numeric mode (just encoding digits, thus being able to pack a lot of data in one picture),
(b). Alphanumeric mode (a set of characters containing upper case letters and several additional characters like $ or whitespace),
(c). 8-bit mode (able to encode the JIS 8-bit character set (Latin and Kana) in accordance with JIS X 0201) or
(d). Kanji characters (Shift JIS character set in accordance with JIS X 0208 Annex 1 Shift Coded Representation)

***c) Character reckon Indicator:***

Right after the mode indicator, the next bits indicate the character count of the data that follows. The actual size of the character count indicator largely depends on the mode in use and the version of the QR Code (higher versions contain more data, thus the character count indicator is longer). See the table below for lengths for the most popular modes

| Version | Numeric | Alphanumeric | 8-bit | Kanji |
|---|---|---|---|---|
| 1-9 | 10 | 9 | 8 | 8 |
| 10-26 | 12 | 11 | 16 | 10 |
| 27-40 | 14 | 13 | 16 | 12 |

***(a). Buffer underflow:***

We change the character count indicator to resemble a lower number than in the original QR Code. Thus, a decoding device should only decode the first few letters as message, leaving out the rest. This is especially useful in case the original link that was encoded contained suffxies. Since the size of the data part is fixed, everything after the anticipated number of bytes is either seen as a new segment (see mixed modes), or (in case of a terminator mode indicator) as filler. Since this is only a minor change in the data part (only the length is changed), this should in turn result in only a minor change in the error correction values and might still be decodable. Special attention should also be paid to a possible combination of this attack with other targets in case mixed modes are used.

***(b). Buffer overflow:***

We change the character counter indicatorto a higher number, so the decoding device tries to decode parts of the filler as data (if we can even change the filler we gain valuable space for including additional data). Again, one of the drawbacks of this method lies in the error correcting (and especially error detecting) abilities of the Reed-Solomon-Code. It would be especially interesting to try to launch a code injection attack using this method

## V. QR CODES AS ATTACK VECTORS

We believe that manipulated QR Codes can be used for a plethora of attacks. Depending on whether the reader is a human or an automated program (e.g., in logistics), different scenarios are possible and outlined in this section.

***A. Attacking Automated Processes:***

As QR Codes are a standardized way of encoding information we strongly believe that the majority of software developers do not treat the encoded information as possibly insecure input. As described in detail in the previous section, different parts of the QR Code could be manipulated in order to change the encoded information. Depending on the programs that process the encoded information, whether this would be in logistics, public transportation or in a fully automated assembly line, attacks on the reader software as well as the backend are theoretically possible. Without proper sanitation this could by used by an adversary for the following, non-exhaustive list of attacks. Similar attacks using RFID chips and SQL injections have been shown to be very effective [7], as input sanitation was not employed in these examples.

***a. SQL injection:***

We believe that many automated systems store and process the encoded information in a relational database. By appending a semicolon followed by a SQL query like ;drop table <tablename> to the encoded information, manipulations to the backend database are possible (provided the DBMS allows for multiple queries in a single line). This would delete the table specified in the command, resulting in a denial-of-service attack. More specified attacks may include adding a user, executing system commands (e.g., by using the stored procedure xp-cmd-shell on Microsoft SQL Server), or altering data such as prices or passwords within the database.

***b. Command injection:***

If the encoded information is used as a command line parameter without being sanitized, this could be easily exploited to run arbitrary commands on behalf of the attacker, which may have disastrous consequences for the security of the operating system e.g., installing rootkits, DoS, or connecting a shell to a remote computer under the control of the attacker.

***c. Fraud:***

Changes to the automated system can be used to commit fraud, by tricking the system e.g., into believing that it



CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

processes a cheap product A while processingthe more expensive product B.

## VI. ATTACK BY QR CODES

In September 2011, Kaspersky Lab detected a first-of-its-kind malicious QR code. The attack method used in the QR code was that when a user scans the code he is directed towards a website and then a malicious file downloads in the user's device without the knowledge of the user. Till now, this is the only method of attack known about malicious QR codes. They detected several malicious websites containing QR codes for mobile apps (e.g. Jimm and Opera Mini) which included a Trojan capable of sending text messages to premium-rate short numbers [8].

## VII. SECURITY SOLUTIONS

a. QR codes are tricky because you cannot weed out the bad from the good by simply looking at the code. Because the vulnerability is practically part of the design, consider downloading an app on your phone which provides a preview to each code before it opens a webpage (eg: Inigma) reader. This way, you will have right to refuse the QR code is corrupted.
b. Scan a code and get directed to a login form, always remember never to fill it in for it may be a trap used by criminals to get access to personal information. Legitimate QR codes never ask for personal info.
c. 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.
d. Print the URL near to the code. This way if the code is hijacked and pointed to http://evilsite.xxx/ the user can see they're not visiting the correct site.
e. Include https in the URL. Get users used to checking for https before they interact with you.
f. If possible, use a short domain. Not only will it reduce the size of the QR code, it will give your users confidence if they can see the full domain in their phone's URL bar.
g. Don't ask a user to get their credit card out on a busy street. Use a mobile payment solution which charges to the user's phone bill or deducts it from their credit.

## VIII. QR CODES DATA TYPES

QR codes can contain many different types of information. Different app readers on smart phone are able to act and read this data. Think of it as an alternative way of getting data into your phone (as opposed to typing it in manually). Here are some of the possibilities[9].

***a) Contact information:***

QR codes can contain contact information so someone can easily scan a QR code, view your contact details, and add you on their phone. You can input your name, phone number, e-mail, address,website, memo, and more.

***b) Calendar event*** :

If you have an event you want to promote, you can create a QR code containing info for that event. QR codes containing event info can contain event title, start and end date/time, time zone, location, and description. This could work well on an event flyer or possibly even on a website promoting.

***c) E-mail address:***

A QR code can contain your e-mail address so someone can scan the code, see your e-mail, and then open an e-mail on their phones. If your call to action is mostly to have someone e-mail you, this would be great.

***d) Phone number:***

Maybe e-mail isn't immediate enough and you want someone to call. Link them up to a phone number.

***e) SMS*** :

QR codes can populate a text message with a number and message. You can have your QR code send you a text saying "Tell me more about XYZ," for instance.

## IX. CONCLUSION

In this paper we outlined the dangers of possible attacks utilizing manipulated QR Codes. Since QR Codes gain increasing popularity through their use for marketing purposes, we expect that this kind of attack will receive more and more attention by the hacking community in the future. Furthermore, many mobile devices (e.g., smartphones) at present are able to decode QR Codes and access the URLs contained in them. This adds a new dimension to the topic of trust, especially since most users are not security-conscious enough when using their mobile phones (which also enables the use of novel phishing techniques). In addition to phishing, a multitude of other attack methods, both against humansand automated systems, might be performed using QR.

## X. REFERENCES

[1]. "Denso wave incorporated," http://www.denso-wave.com/qrcode/indexe.html.

[2]. 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.

[3]. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar WeipplT. J., "QR Code Security"

[4]. Tasos Falas, Hossein Kashani, "Two-Dimensional Bar-code Decoding with Camera-Equipped Mobile Phones", Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops(PerComW'07) 0-7695-2788-4/07 $20.00 © 2007

[5]. William Claycomb, Dongwan Shin, "Using A Two Dimensional Colorized Barcode Solution for Authentication in Pervasive Computing", 1-4244-0237-9/06/$20.00 ©2006 IEEE

[6]. ISO/IEC18004, "*Information technology-automatic identification and data capture techniques*". Bar Code Symbology - QR Code.

[7]. M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Is your cat infected with a computer virus? In PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications, pages 169{179, Washington, DC,\ USA, 2006. IEEE Computer Society.

[8]. Vishrut Sharma. A STUDY OF MALICIOUS QR CODES, International Journal of Computational Intelligence and Information Security, May 2012 Vol. 3, No. 5, ISSN: 1837-7823.

[9]. Denso Wave. To two-dimensional code from the bar code.[Available]: http://www.qrcode.com/aboutqr.html