Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

QR CODE HACKING

QR CODE A REAL TREAT OR NOT

6 WAYS TO PROTECT YOURSELF FROM QR CODE HACKING

HACKING, CRACKING AND OTHER SECURITY CONSIDERATIONS

Vol.8 No.07
Issue 07/2013(67) ISSN: 1733-7186

PLUS

INTERVIEW WITH ANTONIO IERANÒ AND NICK LYNCH

Joe Security LLC
Automated Malware Analysis

Next Generation Sandbox System

Joe Sandbox is an automated, highly configurable and scalable malware analysis system that provides extensive in-depth analysis reports to customers worldwide.

Technology Leader

Introducing **Hybrid Code Analysis**, Joe Security has developed a unique algorithm that combines dynamic and static code analysis in an intelligent way.

Cross Platform

Joe Sandbox is the only fully-automated Sandbox System to support **Windows XP, Vista, W7, W7 x64 and Android** platforms.

Quality Support and Consulting

With direct access to the developer team, Joe Security provides excellent technical support and custom code to his customers.

JoeSecurity
www.joesecurity.org

Joe Security LLC
Hochbergerstrasse 60C
4057 Basel, Switzerland

swiss made software

Joe Security LLC
Automated Malware Analysis

Introducing Joe Sandbox Mobile!

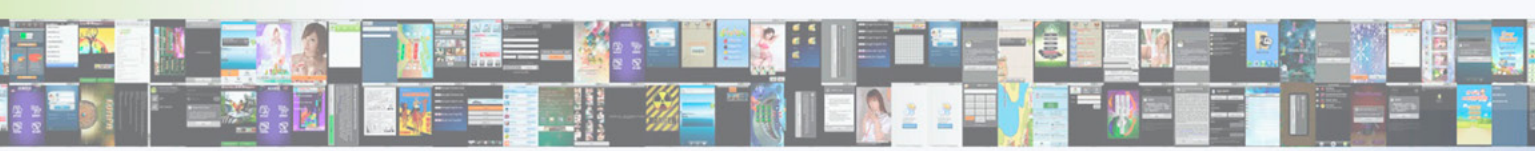
The new solution for in-depth malware analysis on Android based systems.
Using **Hybrid Code Analysis**, static and dynamic analysis is combined in a clever way.

Powerful Instrumentation Engine

The highly-configurable, generic Instrumentation Engine not only analyzes **System API calls**, but any function matching specified signatures up to parameter level.

Generic Behavior Signatures

Providing an open interface and a solid initial set of generic behavior signatures, application activity is abstracted into well-formatted report data.



Free Services Available Online

All of Joe Security's Sandbox Systems are available as free web services at
apk-analyzer.net, file-analyzer.net, url-analyzer.net and document-analyzer.net

JoeSecurity
www.joesecurity.org

Joe Security LLC
Hochbergerstrasse 60C
4057 Basel, Switzerland

swiss made software

Hakin9 team

Editor in Chief:
Magdalena Gierwatowska
magdalena.gierwatowska@hakin9.org

Editorial Advisory Board: Peter Harmsen, Dan Smith, Hans van Beek, Leighton Johnson, Gareth Watters, Sushil Verma, Jose Ruiz, Casey Parman, Wendy Bennington, Liew Edwin.

Proofreaders: Magdalena Gierwatowska, Krzysztof Samborski

Special thanks to our Beta testers and Proofreaders who helped us with this issue. Our magazine would not exist without your assistance and expertise.

Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@hakin9.org

Product Manager:
Krzysztof Samborski
krzysztof.samborski@hakin9.org

Production Director:
Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director:
Radoslaw Sawicki
radoslaw.sawicki@hakin9.org

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl
DTP: Ireneusz Pogroszewski

Publisher: Hakin9 Media sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
www.hakin9.org

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

I'm pleased to welcome you at the end of the summer period with a brand new issue. The issue that is supposed to be just a start in the area of QR code research. This is still a new topic and many people wouldn't like to share their research and discoveries on QR hacking as it is still a pretty new marketing tool and there is not much that can be done to secure people from those attacks apart from their awareness. We could mainly advise you to be protective and reasonable while scanning some QR codes, think about the source of it, where they have been placed etc.

We hope that these issue will convince you to interact a little bit more in the area of mobile security or moreover QR code hacking, as the mobile security is not being so fragile.

We are coming with the new edition of Hakin9 Magazine so you can access it through your computers, tablets, smartphones and e-book readers.

Just want to say that it wouldn't be possible without the support we receive from our authors, Hakin9 Team Members and betatesters involved in the creation of this Magazine.

What are we going to offer you this time? Take a look at a quick overview below.

David Nordell is going to take a look at the possibilities of financial crimes made by hidden pieces of malware. We are going go through disadvantages and advantages of QR code use with Carlos Rodriguez Perez. The main factors of QR treat will be showed by Antonio Ierano.

David Allen is going to show you that most QR code disasters are self-imposed by the users and implementers. V. Michael Balas is going in depth with the topic but we won't tell you the approach, it is must read.

We hope the effort of Hakin9 Team was worthwhile and the QR Code Hacking issue will appeal to you. Enjoy the magazine!

Magdalena Gierwatowska
Editor of Hakin9

and the Hakin9 Team

BASICS

THE TECHNIQUES

INTERVIEW

Hacking QR Codes A Case of Curiosity and Pattern Fallacies

Summary: "A curious user, putting incredible amount of trust, scans the machine only readable QR code, the code redirects him to a site or provides certain information or can trigger several attacks and fraud the users"

Quick Response codes aka QR Codes have been in use since 1994 courtesy of DENSO WAVE. These are 2D barcodes encoded both vertically and horizontally thereby multiplying the capacity of holding data than the traditional 1D bar codes (7089 digits in comparison to 20). Hidden in those pixelated lines is embedded code which is only machine readable that points the user to a new location on the web or processes particular information. In the last few years QR Codes have seen widespread popularity in usage like never before due to the increase in QR Code scanners, which are typically smart phones enabled with mobile internet. This led manufactures and advertisers to incorporate QR codes on their banners and making the most of it. Now, QR Codes are everywhere, on bus stops, pubs, railway stations, street light poles and recently on English football club's jersey to direct you to a WAP site. Popularly QR Codes have found their application in encoding URLs, visiting cards, addresses, and various forms of advertisement data on posters. Along with its great uses, QR codes have also many potential risks due to the vulnerabilities around its design and hence prying threat vectors would always be after exploiting those vulnerabilities. Hence not making a very sweeping statement, but funnily enough every kid on the block has a QR Code scanner and is a potential victim of being hacked. Recently, the much awaited Google Glass was a victim to the magnitude of exploitation it could be subject to by QR Codes as founded by researchers from Lookout Mobile. The researchers reverse engineered QR Codes turning them malicious and once scanned by the Google Glass it would reconfigure the device and overturn the control to the hacker making him aware of all the information linked to the same.

Here in this article I will try to analyse those possible structural risks of the QR codes and the attack vectors which affect both humans and automated information processing systems.

Anatomy of QR Codes – dissect the devil

As devil lies in the detail therefore, to begin with, it is important to understand how QR Codes work and how they're designed. This will help us understand the loopholes in their overall structure and usage, exposing them to various risks.

The QR Codes as shown in Figure 1 are made up of inner structure which is built from contrasted

(black and white) squares with an overall base of a matrix like structure. Around the QR code there is a white margin (cannot be seen in figure) also called as "Quiet Zone" and is 4 times wider than the inner square of the overall structure. Inside the inner square, the following critical patterns or components exist which form what we call as the quick response code. Any manipulation to the components shown in (Figure 1) can lead to information which is unwarranted and often incorrect.

Finder Pattern
The finder pattern is a concentric square made up of 3x3 black module-white module-7X7 black module which is located on the three corners of the QR code except the bottom right one. These are identical structures which enables the decoder software for correct orientation.

Alignment Pattern
Alignment pattern also forms a part of the crucial structure of the QR code as it allows the decoding software to scan an inverted image and convert it into a matrix of black and white structural modules which forms the overall encoded information. It's also like a finder pattern's structure which is basically a concentric square.

Separators
These are 1 pixel sized blocks of white spaces separating the finder pattern to the rest of the data and allow the decoder to distinguish between the timing pattern, finder pattern, and the format pattern.

Timing Pattern
As seen in the Figure 1, there is an alternating stripe of black and white blocks, just under the two tops most finder patterns, going horizontally and other pattern going vertically downwards along the top left and lower left finder pattern. This structural pattern is important for the decoding software, by enabling it to determine the width of each module.

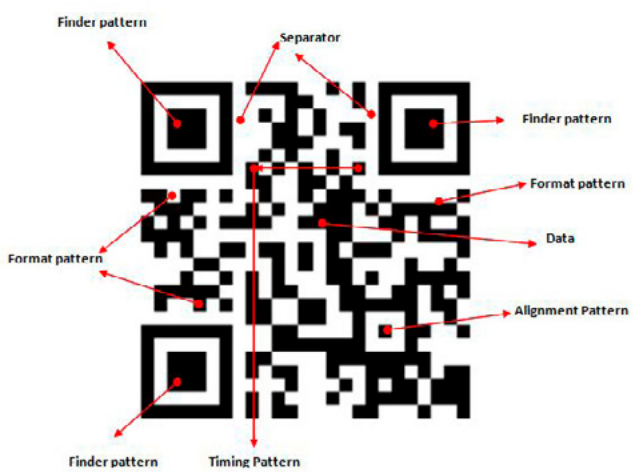


Figure 1. *QR Code Anatomy*

Format data
This is the 15 bits of data which is just next to the separators and provides information on the masking rule used in QR codes and the error correction level. Masking a QR codes pertains to the inversion of colored and colorless modules crucial to decoding software.

Data
Apart from the structural format as explained above the data occupies most of the middle space. These are blocks of 8 bits of encoded words (blacks and whites). The capacity of data to be held in a QR Code entirely depends on the error correction level.

Error correction level
In QR Codes, the basis of error correction is the Reed Solomon codes, which forms different levels of error correction (Low=7%, Medium=15%, Quartile=25%, High=30%), this percentage shows the value of recovery of symbol codes. Choosing a higher value means accommodating less data but at the same time including chunk of error correcting code.

The above knowledge on structure of QR Codes is necessary to understand the anatomical components in order to estimate and analyse the risks around them and then figure out the ways they can be exploited.

Vulnerabilities embedded in QR Codes – Structural and Usage

Structural Manipulation-the case fallacies
A QR code can either be manipulated with fallacy of the structure as the components we discussed above can easily be manipulated by techniques discussed in this section. Furthermore the possible threats multiply as the code is not human readable, easily accessible and threat agents are prone to social engineering along with the increased popularity and visibility.

Let's first have a look at the ways in which the structural components of an existing QR Code can be manipulated by an adversary.

Distorting the encoded information by masking, characters and count indicators
Masking in QR codes refers to overlapping of several layers of distributions of black and white pixels or modules leading to the final picture of a QR

code which has the best distribution (1:1) of black and white modules. This inherent property of QR code is vulnerable to physical manipulation of the masks rendering the encoded information useless as the code now read by the scanner would not direct the user to its actual content. Hence, manipulating the pixel distribution on the final mask, changes the data content and the error correction code. This can further be substituted by manipulating the structural pattern of the actual QR code and changing their count indicators and the encoded characters. To implement this, it is required to skew the pixels in the data part of the QR code, which can be done by layering the code with a sticker covering the modules to be skewed. In certain cases where the error correction algorithm (Reed Solomon Code) is incorporated to rectify high level (30%) of the incorrect codes, this vulnerability may be contained to an extent.

Hazards in usage- the case of curiosity and trust

With its growing visibility and ease of production, the usage of QR codes make the users curious to scan whatever comes there way. There's no way for you to know what lies behind until you scan it. For this reason, the inquisitiveness behind the usage of these codes is a vulnerability itself which can be fairly exploited by adversaries. Malware peddlers are on rise for most operating systems used in mobile phones such as Android, Windows Mobile, iOS. Therefore attackers can easily stick maliciously encoded QR Codes anywhere in a prominent area and just wait until someone scans it and hence gets caught in the rain. In the following section we discuss, how these vulnerabilities can be exploited making QR codes as potential attack vectors.

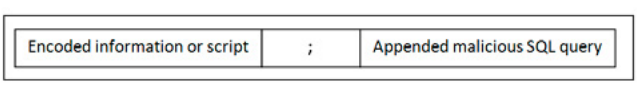
QR Codes – agent of exploitation for humans and information processing systems

In the earlier parts we discussed the vulnerabilities in the design of QR Codes and the way they can be manipulated due to inherent properties of the codes which are inconceivable to a naïve user. We also touched upon the vulnerability of the same by the increasing popularity and ease of access, making it more prone to be used as an attack vector. In this section, the discussion is based on using QR codes as an agent or means to implement commonly known exploitation techniques affecting both humans and information processing systems.

In manufacturing and automobile industries QR Codes are popularly used to track products by automated processing units. These units are easily vulnerable to be exploited by a malicious QR Code by various ways, as discussed below:

SQL injection by query stacking

Many automated information processing system which use QR-Codes as an input for a task to be completed can be targeted by manipulated QR Codes if the input processed through the encoded information is stored in a SQL server based relational database. For Instance, if an information processing system integrated with an assembly line used QR codes to input the product name and number and hence storing them in a relational database, then an adversary can place a maliciously encoded QR code which includes a query string with the input variable appended with a malicious SQL script to drop the whole table. This QR Code as soon as scanned by the information processing system would treat it as an input to the SQL server affecting the relational database and delete the whole table. The Figure 2 illustrates the same.



Stacked QR Code: Sample encoded information ; Drop <table name>

Figure 2. *Illustration of SQL Injection by query stacking in QR Codes*

Similar misuse of this vulnerability can be done command line injections which inputs relays of shell scripts being scanned by a QR code and fed into a processing unit. A Shell command injection can encoded into a QR code and made to be processed leading to exploitation of the OS and the server in their core directories.

Launching XSS (Cross Site Scripting)

Most of the websites which are static in nature, built using HTML (Hyper Text Mark-Up Language) which is a tag based language for static website development. HTML combined with scripting languages like Javascript and PHP provides a mechanism for building websites dynamically. Hence, using these languages, most of the websites built today are dynamic. These languages allow the web-server (place where data is stored) to send executable code to the client. A web server is connected to the HTML front end by using a protocol called HTTP (Hyper Text Transfer Protocol) that is used for transfer data. HTTP is a stateless protocol that does not store details about the users who have sent requests to the web-server (Higure 3).

Cross-site scripting takes advantage of the stateless nature of HTTP. This can be further used by

used by an attacker to encode a script of an URL in a QR Code redirecting the browser to a web-server generating a page with scripts embedded by the hacker. These scripts (usually JavaScript) enables the hackers to retrieve all the information from the user's mobile phone browser and hence render it exploited.

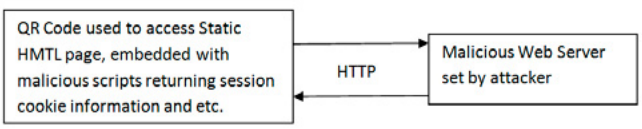


Figure 3. *XSS scenario with QR Code as entry point*

Reflected CSRF

CSRF is another type of malicious attack on websites and web applications also known as one click attack, side jacking or session ridding. There are many who refer CSRF as a version of XSS, but technically both are different. CSRF exploits the privileges of authenticated users for performing undesired functions on the user's behalf. It is interesting to note that a QR Code can easily be an attack vector for such exploit. For instance a user attempts to scan a QR code with his smart tabloid in a parking lot which promises him to get a discount, if he logins to his eBay account and scans the code. Now as soon he logins and scans the code the malicious script encoded in the QR code extracts his login information and initiates an automated PayPal payment through his eBay account. Hence, exploiting his browser by CSRF, the attacker uses an external system to expose the victim to a link or content.

Redirecting to Trojan horses/Malware

Trojan horses are standalone malicious programs which are designed specially in such a manner that the host system on which it is installed doesn't even get to know the real intention behind the program. Hackers usually disguise Trojan horses in forms of PDF files, mp3 files, ZIP files and other forms of utility programs. A QR code can easily be used to redirect a naïve user to website promising him free music or special Apps but actually installing a Trojan as soon as he begins the download. The downloaded Trojan installs itself on the root directory of the host smartphone, PDA or tabloid and can prove to be lethal for the system. It may initiate sending automated SMS on a premium number, costing the user money or maybe even worse by sending illicit SMS or emails to all contacts in the phone directory. If a QR Code injects a malware into a phone then it also have the capability to access Facebook, Twitter and other social networking sites and post without prior knowledge of the user.

Conclusion

QR Codes as we discussed above a ways to input information into a processing unit with a decoding facility and performs certain actions. As these codes cannot be decoded with human eyes therefore they're vulnerable to exploited and pose a serious threat to the users. Blindly, scanning a QR code which proves to be malicious can have grave consequences on the device. These codes can easily be used as attack vectors to launch exploits such as SQL injections, XSS, CSRF, and also to download Trojan horses. The QR codes ones scanned acts as an input to triggering the mentioned exploits without the knowledge of the user.

One of the ways this can be dealt this is, using scanners which preview the URLs before opening it in the browser and hence is the user deems it be suspicious they can reject it. Most times, advertisers ask users to enter their personal information on scanning QR code and setup a honey trap to steal that information and use it for illicit purposes. QR Codes can further be standardised using only HTTPS to establish communication with the web servers along with the URL printed on the stickers so that the users can have a degree of trust in the same.

Finally, along with the great potential of the various applications of QR Codes, its exploitation is imminent due to the inherent structure it is made up of and largely because it is not human readable and thus can act as an agent to prompt various hacking attacks.

RISHABH RASTOGI

Rishabh Rastogi is an information security, risk and governance minded professional who thrives on evaluating technologies and business processes from a critical perspective. When he isn't thinking risks, or trying to review an audit programme, he can often be found cooking, exploring new music, building terrariums, aquariums and evolving new hobbies.

QR Codes

Probably someone thinks that the QR code is just something random, that doesn't make sense, only a heap of stripes and points. Nothing is further from the true. The QR code is a "new" and simple way to share our ideas and our knowledge.

First, I should introduce to you the history of the QR codes, how they were born, who created them and why. Also I will include some graphics on the increase of his use in the last years.

Later I will talk about the uses we can give them and how use it in our benefit, also I will mention the current uses. I will show you how since his growth has been increased from his creation.

After I'm going to show you his involvement in the world of the hacker, here I will talk to you a bit on the mobile malware.

And finally I will do a reflection on the mentioned previously.

History of the QR Code

The QR Code (quick response code) born in Japan in 1994, created by Denso Wave Company, it was made as a new way of transmitting information quickly, it is characterized by the three squares that we can see, now take a look this image:

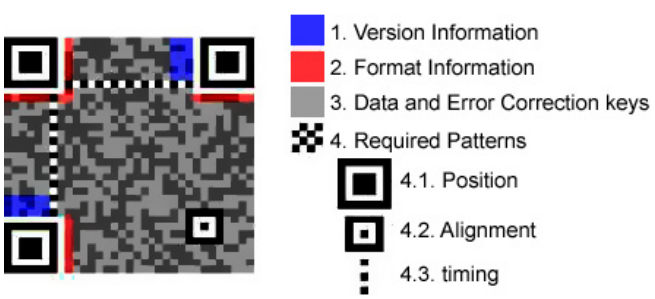


Figure 1. *QR code structure*

This is how it works, as you see in the image the blue part corresponds to the version of the QR Code, the red part indicates the format of the file that we want to share, I mean it is an image, url, etc.. I hope that you have realized that the QR Codes aren't random.

Now, to finish this part of the article, I will analyze the use of QR Codes since its popularity has increased. Look the graphic.

As you can see in the image (sorry if it's a bit small) the use of the QR Codes has increased in a 157% since from the first quarter of 2009, if we

observe the graph strikes us the strong trend that from January, 2010 is taking place worldwide.

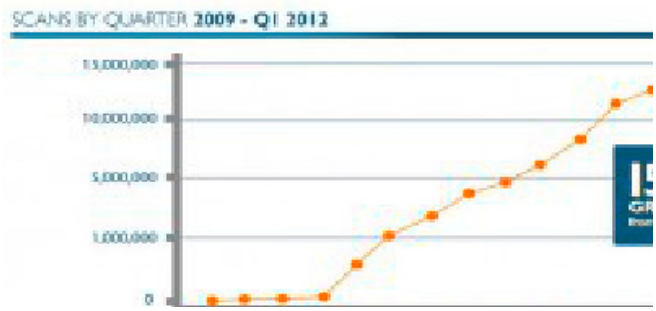


Figure 2. *Growth of QR code scans*

Also it is necessary to say, that the actual use of these codes is low, because few users who take the time to scan the codes with their smartphones. You will probably wonder, Who uses these codes? Well, these codes are used principally in companies that want to give a modern aspect to their products.

Utilities And Current Uses

I will start by naming some advantages and disadvantages of the QR Codes.

Advantages:

- Easy and quickly way to share our information.
- Free and compatible with all our smartphones, tablets, and computers, universal format.
- In a QR Code you can store even 7.089 numerical characters or 4.296 alphanumerical characters.
- The code has the aptitude to correct mistakes, the information can be restored if part of the code is damaged.
- The QR can be read in any position, vertical, horizontal...

Disadvantages

- We need to download an application in our smartphone, tablet or computer to read these codes, While the mobile operating systems do not include the reader the cost of seeking and lowering an application can be a lag and impedes the general adoption of the tool.
- Low use. Few people know them and those who know them find little real value to use them.

As you can see, the QR Codes need to attract more people, and be more accessible, because though it is true that many companies use them, still they need to catch the great public.

The users tend to use these codes to take part in contests or promotions, in addition to access multimedia content, but as I said before, normal users don't tend to use these codes.

Now, we are going to talk about the alternatives to the QR Codes, I will do a brief revision on more acquaintances.

Bidi Codes

This code has been created by Movistar Company, this code is private, and no open source, and therefore they are not free, since they are orientated to commercial ends, also we need specifics applications to read these codes. In conclusion, I think that the QR is a better choice, not only because is open source, but also because they are totally compatible with our smartphone, tablet or computer.

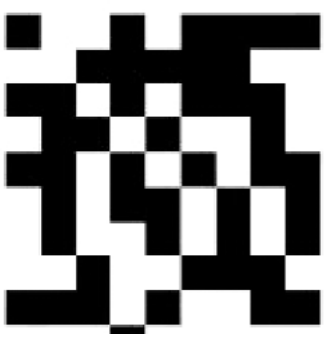


Figure 3. *The look of Bidi Codes*

Datamatrix Codes

Datamatrix, another ''friend'' of the QR, well, this code has more similarities to the QR, for example, this one yes is open source like QR, one of the advantages of these codes is that the minimal size is minor that in the QR, nevertheless, this advantage can suppose a misadventure, since it enters conflict with the chambers of the mobiles, because being so small, the cameras have problems to focus on it.

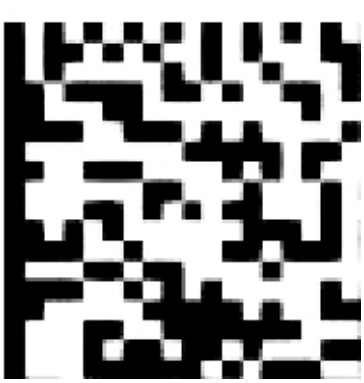


Figure 4. *The look of Datamatrix Codes*

Now, I'm going to show you some applications to create or read our codes.

```
Create your own QR Code online -> QR Code Generator
Read QR Codes in your smartphone/Tablet -> QR Code Reader
Read QR Codes in your computer -> QR Code Reader PC
```

QR Code In The Hacker World

Ok, this is the interesting part of the article, here, I will speak also a bit of the Mobile Malware, and some techniques to avoid it. So, without further ado let's begin.

Surely some he wonders how the QR can influence in the Hacker World, or in the Malware World, well, there is no better way of explaining it that with an example:

> *Imagine you're a malware developer, and you are looking for new techniques to spread your malware, you're tired of thinking and suddenly you have an idea, Why not include my trojan in a QR Code?*

This is the question that many cyber delinquents ask to themselves, is very easy to pass a trojan by an application for our smartphone, for example an X-Ray Reader (fake of course), once we have read the fraudulent code, the malware disburdens himself and attack, usually the attack consists in a malware that is installed in our smartphone, once installed is dedicated to illegal activities, such as sending SMS to a payment service that takes advantages of the attacker. The social networks or the publicity are the main vehicles to make these codes to the users. But, How can we protect ourselves from this? Below I'm going to give you some tips to protect ourselves from this.

What to do

- Always download apps only from the Play store (Android), AppStore (Mac), Market (Windows Phone). The apps that you can find here are revised.
- Use an Antivirus System, Avira or Avast! For example, the two are totally free.
- Keep your device updated.
- See the rights of the applications, I mean, if you see an app with full rights I recommend you not to install it unless you know well what it is.

To complete this section I'm going to talk about the mobile malware, just a few clarifications about this.

The Mobile Malware

Well, this one is a wide enough topic, before I mention some techniques to protect myour devices, and now I'll talk a bit more on this topic.

Figure 5. *The Mobile Malware*

In the last years the mobile malware has increased, just as the use of the mobile phones or smartphones has increased.

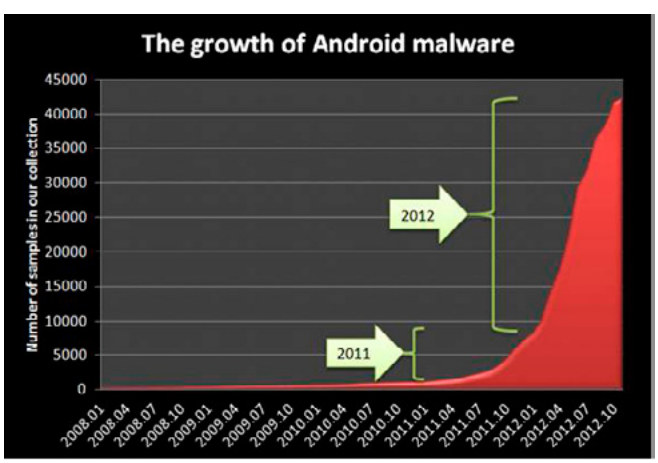


Figure 6. *The growth of Android malware*

As you can see there has been a sharp increase since 2012, I think that this is normal, since we all have a smartphone, and this implies a business for the cyber delinquents, because they have the possibility to earn money with our smartphones, and this is a very lucrative business. We've talking about Android, but, what about the other Operating Systems like IOS or Windows Phone?. Let's take a look.

IOS

Well, we're talking about a very exclusive system, I mean that is hard to install apps out of the AppStore or iTunes, but there are other ways to install apps, in iOS, for example, we are able to apply Jailbreak in our device, And what is Jailbreak? Well, is the process of removing the limitations on Apple devices, in other words, we are superusers. The jailbreak allow us to install apps, themes, extensions... out of the AppStore, through Cydia, this is like the Appstore for the rooted devices, although it's true that in the last versions this isn't available

but there are still a lot of vulnerable devices, And how can Hackers infect by Cydia? Very easy, the apps from Cydia are installed by repositories, and they are not revised, so, for it there would be necessary to upload the app of the Trojan to Cydia and convince the user to install it, for example, saying that is a game.

Figure 7. *Cydia Apps*

Windows Phone

There is not much to say about this system, is very new but, however recently it has been discovered vulnerabilities in the Wi-Fi system that can allow Hackers to gain access to users encrypted domain credentials, but there isn't still specific malware to this system.

Figure 8. *Windows Phone logo*

To finish the article, I'll do a reflection on what has been said above.

Reflection

In this article we have learned many things about the QR Codes, what are, and what they're used for, we've seen their different uses, and his dangers, but the most important question that we have to do to ourselves is; What benefit do I get by scanning a code? Or What benefit do it's supposed for my company or business? Well, these questions haven't a clear answer, because many users don't know them or don't know what they're used for.

The utilities that have the QR Codes are great, and we haven't yet reached to know all them, we are sure to expect great surprises from these codes, but nowadays the QR haven't big success between the normal users.

CARLOS RODRIGUEZ PEREZ

Hijacking QR Codes©

I am a joint US/UK national living just outside London. Do I know much about QR codes? Well, more than most, but I am not a programmer. That being said, I hold my own on the technical side of the understanding. I'm the one that did all the QR codes for the London 2012 Olympics, contracting directly with LOCOG (the London organising committee for the Olympic Games).

We're at the heart of the first "Mobile Olympics" as they were called. We had just over 80 QR Codes in use dealing with everything from ticketing, brochures, and codes on all the mascots around London. By far, our most used code was the one that took you to install the "Real Time Results" app, of which there were over 40M downloads. This app for all major phone O/S's gave you every result in every sport within 2 seconds of when it finished, gave you information about the competitors, and a lot of other informative facts. It is by far the single most downloaded and effective application for any single event use, ever.

Background

The QR code system was invented in 1994 by Toyota's subsidiary, Denso Wave. Its purpose was to track vehicles during manufacturing; it was designed to allow high-speed component scanning. It has since become one of the most popular types of two-dimensional barcodes. Originally designed for industrial uses, QR codes have become common in consumer advertising. Typically, a smartphone is used as a QR-code scanner, displaying the code and converting it to some useful form (such as a standard URL for a website, thereby obviating the need for a user to type it manually into a web browser). Today there are three types of codes in use:

Direct codes
Performing a point-to-point movement of data, for instance a code is embedded with the site information like that of *www.guinness.com*, which when scanned takes you directly to the Guinness web site.

Indirect codes
Taking you to a server that then takes the user to a site that then takes them to another site base on the criteria within the packets of the data transfer. So, for instance Barclays Bank might offer personal banking and publish a code in a daily newspaper. That code would be scanned by lots of different people. Apple users want to be taken to the server that gives them Apple software, and the Android users to Android software, etc.

Partial Indirect Codes
These are a highbred of the two allowing for very fast throughput of the data for consumer applications (Figure 1).

Real use today, Mobile Engagement

Today in Japan they are used much more than anywhere else in the world, and mostly in industrial applications. It is a technology that clearly came out of the industrial sector to be used in commercial applications. As such its primary ap-

plication has become connecting consumers with brands via advertising and marketing campaigns. Connecting technologies primarily in use now are QR codes, mobile sites, mobile apps, and augmented reality…

Why is the growth in this technology so slow?

- Since the invention of the codes was for industrial purposes, 99% of them are plain black and white. They are boring and do not fit into modern media. For most, they are not easily changed…
- To use one you have to have a scanner, which you have to download from any of the app stores. Easy and simple to get, but requires personal intervention on the smartphone. In some small countries you might have one included on your phone, but not often…
- More than 90% of QR codes, even today, take you to a company's normal web site that would be viewed by a normal computer screen. These are unreadable on a smartphone. If the site is not "mobile optimised" people just don't go to it.
- Two companies are choking the market with their artificial hold on the growth of the market. In 1996 Denso made the technology "open source" to all. Two US firms, Scanbuy and NeoMedia have succeeded in patenting in the US market various bits of the "open source" technology and now charge extortionate fees for anyone who uses them. Most particularly, NeoMedia makes almost all its revenues by exploiting its stranglehold on the intellectual property. Both firms only control this intellectual property in the USA, but the USA is the marketing capital of the world… Scanbuy and NeoMedia each have revenues of approximately $3.5M USD, so not really very much. The total value of all the companies doing all the work (outside Japan) is not $25M/ year globally. As such, a very tiny drop in the world's marketing budgets… (Figure 2)

Figure 1. *A real use of QR codes*

Is anyone doing it right?

Ironically, we have only found one company, Azon Mobile (*www.azonmobile.com*) that offers easy to build customer and colour QR codes and hooks them up with real Mobile Web Sites for a very fair price. You can change the codes and combine pic-

Figure 2. *The future of QR codes*

tures, logos and a myriad of other special effects right from their site (Figure 3).

Where does it go wrong?

Most of the disasters with QR codes are self-imposed by the users and implementers

- If you use a direct code and *miss-spell the name of the web site*, like "Love Film" did when they launched in the UK market 2 years ago. A scan of the QR code in their brochures took you to *http://http://lovefilm.com*. Try it yourself; you go to a page with an "error404" message. That did nothing but anger the people who went to the app store, downloaded a QR code scanner, and then scanned the code all for nothing… Not something you want to do to consumers, word travels fast… We've seen dozens of examples of this.
- *Bad presentation* as noted in point #3 above.
- The technology of QR *is impossible to really secure*, due to the fact that it is in the public domain and it is being read by a smartphone.
- Smartphones are owned by consumers who *insert SIM Cards* into those phones, many of which come from a lot of dubious places that routinely hack malicious code into them. Unwitting consumers insert them into the phones and get lots of results they hadn't intended.
- *Malicious QR codes* are ones deliberately made to look legitimate, but when combined with a permissive reader can put a phone's contents and user's privacy at risk. Pulling down a major brand from the internet and putting a code with it is easy. This practice is known as "attagging", a slang form of "attack tagging". They are easily created and can also be affixed over legitimate QR codes. Recently the new "Google Glass" glasses were found to be easily subject to malicious codes and took a pair down with little effort.
- *Diversion tagging*. On a smartphone, the reader's permissions may allow use of the camera, full Internet access, read/write contact data, GPS, read browser history, read/write local storage, and global system changes. Diversions of indirect code servers can steer a code to the wrong place.
- *Greed tagging*. Presenting an offer to consumers that is too good to be true. A scan of a QR code takes you to a site which draws down a lot of information about the phone and user. As with any normal computer virus it can link to dangerous web sites with browser exploits, enabling the microphone/camera/GPS, and then streaming those feeds to a remote server, analysis of sensitive data (passwords, files, contacts, transactions), and sending email/SMS/IM messages. Or DDOS packets as part of a botnet, corrupting privacy settings, stealing identity, and even containing malicious logic themselves such as JavaScript or a virus. These actions could occur in the background while the user is only seeing the reader opening a seemingly harmless web page. In Russia, a malicious QR code caused phones that scanned it to send premium texts at a fee of US$6 each
- *Image translation*. With a bit of reading of the original Denso spec, you can see where each part of the data in QR code resides. Any first year graphics student can use Photoshop to insert data in the code to change the data in the code and send the user to a malicious site. Then you get all the results in point #5-7 above…
- *Curiosity Tagging*: or as I call it, stupidity tagging… If you scan a code for no other reason than the curiosity factor, then you get what you get. The biggest risk is that people cannot control their curiosity, and end up facing severe consequences. Just a few months ago a pro-American hacker, Jester, was banking on this when he decided to change his Twitter avatar to a QR code to craft an attack.

Figure 3. *Example of a QR Code*

In his blog, he said anyone who scanned the QR code on his Twitter page was redirected to a jolly little greeting via their default web brows-

er on their mobile device on some free web hosting. The greeting on the page featured the word 'Boo!' directly below it. He claimed that he has exploited the open source Webkit built into the device's default browser. This is the same vulnerability which was exploited in "Mobile Rat, turning Android mobile into ultimate spy tool," as was demonstrated at the RSA conference. This curiosity spawned the cat thing which went on for five days without being noticed. During these five days, the QR code was scanned nearly over 1,200 times and over 500 devices reverse shelled back to the server on listening mode. Tom Teller, a security evangelist at Checkpoint, said "It is a drive-by download attack, where a user scans a bar code and is redirected to an unknown website. Once the website is visited, the modified exploits will affect the system software and additional malware will get deployed, such as keyloggers." If you think this is the end, you are wrong. Attackers have gone ahead with exploiting vulnerabilities on mobile platform by misusing the various protocols and invoking service set commands on the mobile device. This approach is called a 'Telpic attack.' Telpic attack applies a similar technique, using a QR code as an attack vector. As described in Tech Experiments, "it is a malicious way of tricking an Android user into reading a QR code through a mobile camera redirecting it to malicious URL." This technique is not just limited to malicious URLs, but also executing USSD or the 'Unstructured Supplementary Service Data, 'which is a vendor-specific command.

So where does it all lead???

The possibilities are endless… There are tons of service list commands, starting from displaying the IMEI number to executing a factory reset command. Google it and you will find plenty of service list commands for various platforms and various models. These service list commands are executed by exploiting the vulnerability of the 'tel 'protocol available on mobile platforms. You must have seen various mobile websites offering call button option, and when you click on one of those, you are redirected to the dialler of your phone. Here is where the tel protocol is used to call the number from the mobile phone's dialler. If an attacker generates a QR code, embedding this protocol with a factory reset service command; imagine what havoc it may cause. As soon as the victim scans the QR code, the tel protocol will be invoked, followed by the service command to reset the mobile phone, and thus you're entire settings and data from your device will be wiped in a matter of seconds. Detailed instruction about restoring deleted objects can be found in the mobile forensics course offered by the InfoSec institute. These kinds of malicious codes can spread though scanning a QR code, a catchy URL, near-field communication (NFC) sharing, etc. There are plenty of vulnerable devices; you just need to find one.

Conclusions

- QR codes were designed primarily for industrial use
- Growth of the use of QR which was only ever a very small market, has primarily been constrained by poor implementation and in the US, the two firms choking the market by protecting their intellectual property as they see it…
- A QR code as such, is a one dimensional flat image that is not by itself hack able, but there are many points of contact around it where it is easily compromised
- There is still a very bright future for QR codes if made graphically appealing and implemented properly

DAVID ALLEN

David is a joint UK/US citizen with a global career in the IT business spanning over 30 years in all phases of the business from the birth of the PC right through to the most sophisticated mobile apps of today. His most fun experience was heading up the QR deployment for the mobile app experiences at the London 2012 Olympics. Over 80 codes were deployed in every venue and for every sport in the games. It set the standard for all "mobile enabled" games in the future.

dra01@btconnect.com
@mobileengage
www.mobileengage.co.uk

Qrcode a Real Threat or Not?

Qrcode has been around since a quite long time and, from time to time, they comes out as a vector of threats.
A QR ("quick response") code is a two dimensional barcode invented by the Japanese corporation Denso Wave in 1994. Information is encoded in both the vertical and horizontal direction, thus holding up to several hundred times more data than a traditional bar code in a singular QRcode it is possible to store up to 7.089 number or 4.296 characters, binary (8 bit): up to 2.953 byte and Kanji/Kana up to 1.817 characters.

Data is accessed by capturing a photograph of the code using a camera or a scanner (e.g. built into a smartphone) and processing the image with a QR reader software.

The Qrcode has been developed in several section where can be found data, sync pattern and so on. Generally speaking it can be divided into:

- Finder Pattern: The finder pattern consists of three identical structures that are located in all corners of the QR Code except the bottom right one. Each pattern is based on a 3x3 matrix of black modules surrounded by white modules that are again surrounded by black modules. The Finder Patterns enable the decoder software to recognize the QR Code and determine the correct orientation.
- Separators: The white separators have a width of one pixel and improve the recognisability of the Finder Patters as they separate them from the actual data.
- Timing Pattern: Alternating black and white modules in the Timing Pattern enable the decoder software to determine the width of a single module.
- Alignment Patterns (4): Alignment Patterns support the decoder software in compensating for moderate image distortions. Version 1 QR Codes do not have Alignment Patterns. With growing size of the code, more Alignment Patterns are added.
- Format Information (5): The Formation Information section consists of 15 bits next to the separators and stores information about the error correction level of the QR Code and the chosen masking pattern.
- Data: Data is converted into a bit stream and then stored in 8 bit parts (called codewords) in the data section.

Figure 1. *QRCode I Use in my business-cards*

- Error Correction: Similar to the data section, error correction codes are stored in 8 bit long codewords in the error correction section.
- Remainder Bits: This section consists of empty bits of data and error correction bits cannot be divided into 8 bit codewords without remainder (Figure 2).

Now the immediate threat of a QR code is related to 3 main factors:

- The Qrcode itself is not readable in Human terms and need to be "translated" by an application.

Figure 2. *QRCode cannot be read by human but need a device able to capture a picture and a software to decode it in order to read the data*

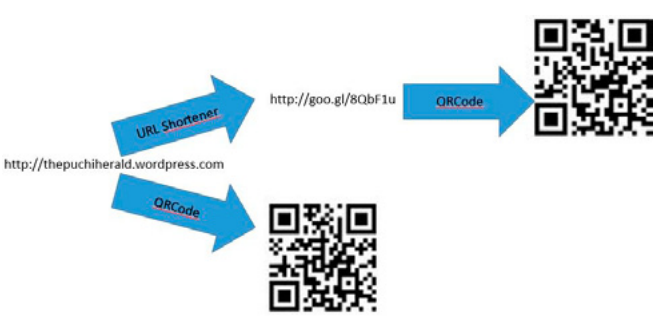


Figure 3. *Qrcode can be generated from an URL or the shorter version. When using a URL Shortener service we loose readibility of the URL address thous is easier to be redirected to a fake site*

This way the user has not Idea about the real Qrcode content, but has to rely on the application that read the code. In most of the case, think of a URL as an example, the application can redirect directly the browser without any warning or prompt, this way the user can be directed towards some malware site.

- The Qrcode can be found not only on electronic form (Webpage, PDF document and so on) but also on posters, newspaper and magazine and any kind of advertisement, that make its exposure wider that usual infections vector, and make easier to be tampered or modified.
- The Qrcode readers usually do not include security features, besides the great number of freeware Qrcode readers and generators available on the internet made quite easy to avoid controls.

A concerning point is it's easy to understand that the way Qrcode transport data allows it to easily hide any kind of info.

For example, we could easily create a related to a malware infection, convert this URL through a shortened URL service, associate it to a common logo and embed this info in a QRCode (Figure 3).

A normal User would check the code through its application and would find a familiar logo to click on; although he would check the URL he would probably see the short version that is anyway not readable. Unless the user is using on its smartphone or tablet a security suite could be easily fooled and redirected anywhere.

Point two is a sneaky point, since for its nature QRcode are quite easy to be modified. Reason for that is Qrcode has embedded Reed-Solomon error correction code. So even if tampered or partially damaged the Qrcode reader is able to read the modified Qrcode. The reason behind this behaviour is simple, a printed code can lose colour,

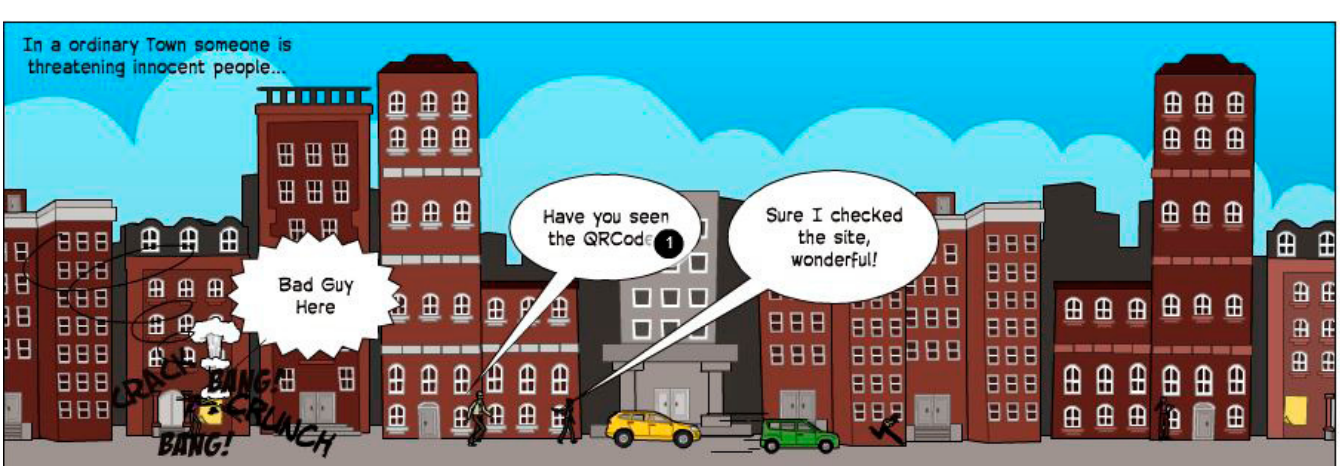


Figure 4. *A QRCode can be on a Advertisement in a crowded city street and watched by anyone with a smartphone*

not be in the perfect shape or position to be scanned, have dirty on the surface and the systems should be able to detect anyway data. That makes it possible so modify the data area of the Qrcode and fool the reader to deliver different data than the original ones. If you think that those codes can be printed on paper, posters and even T-Shirt is quite easy to imagine how many ways to change the info exists (Figure 4 and Figure 5). You do not need to change any QRCode, just think to be able to modify an advertisement on a poster in a highly visible area, as an airport, and you could attack a lot of users. And believe me is not easy to see the difference between the original one and the modified one not using a proper reading tool. Human eye is not the best tool to detect those modifications.

What can a Qrcode attack lead to?

Taking into consideration the things discussed in the previous chapter is now easy to imagine how a Qrcode can be used as an attacking vector.

I can divide the attack into 3 main areas:

- Third part hacking
- Device\user hacking
- User hacking

The first case is quite simple, we can assume that the attacker does not want to hit the user who's reading the QR code but want, instead, attack a third part. Would be easy, as an example; insert a SQL code into the URL data in order to perform an attack on the destination site. We can imagine performing SQL, Ddos and other kind of attack this way, may be using a vulnerability of the qrcode reader. On the other hand, as for point 3, the reader itself can be a part of the attack itself, so, for example, it can use URL found on the QRCode to start a SQL injection and so on (Figure 6).

The second case means that the target of the attack is the user device itself, to be able to monitor, download malware or change configuration of the device. We can again consider the risk related to vulnerability that can be exploited or worse the reader as a co component of the infection. This way could be easy to think Qrcode as one of the main vector used to spread a botnet. We can think of SQL injection, Command injections and so on.

The third case is the most commonly used, and the modified Qrcode lead the user to a fake site or info, the best vehicle for phishing, pharming, fraud or, generally speaking, social engineer attacks.

The 3 areas are, as often happen in security, mixed together in more sophisticated blended attack that can leverage one or more techniques.

A real threat or not?

All the things that have been discussed before just showed us that Qrcode can be an efficient and effective vector of attack that it is quite easy to put in place. Now the question is if the danger is real and how much we should worry about.

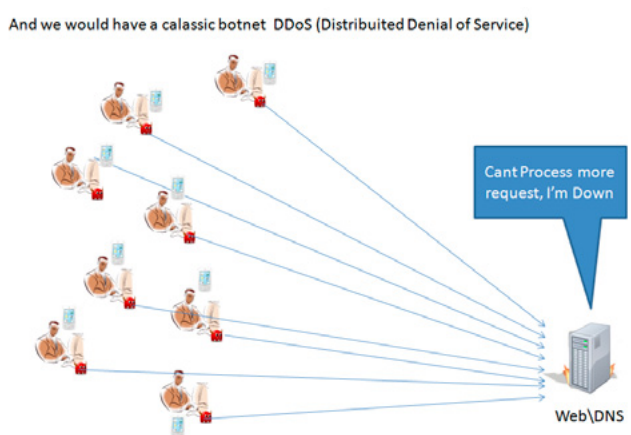


Figure 6. *QRcode could simply make users to send request to a site even if the user does not this. if the users are enought we could have even a DDOS effect (theoretically)*

Figure 5. *An attacker can simply "change" the qrcode or cover the poster with a modified one*

It's hard to give an answer at the moment, since analysis by security vendors start reporting the threat, so it is still not clear the actual extension of the problem. For sure users should pay attention on what kind of Qrcode readers are using, trying to use software coming by trusted source. The rest of the issues are common to the ones related to the browsing activities, so the usual antimalware and web security options should be effective. QRCode are still far to be widely appealing as other infecting vectors are more immediate, so it's hard to see a quick expansion, we should also consider that not all geographic areas are so QrC-addicted. QRCodes were born in Japan QRCode found a great diffusion in Japan, Korea and closest areas. Widely used in Europe as well are less commonly used in USA.

Protecting tips

QRcode are a smart and efficient way to transport information, and can be really useful to make easy to people to reach website, promotions and so on. Marketing is the perfect user for this technology. But how we can protect ourselves? It's quite simple:

End-User

- Use a QRC Reader coming from a trusted source
- Verify if the QRC reader has a minimum set of security issues as the possibility to check the URL before running.
- Use a security tool in your smartphone-tablet-computer to protect you from unwanted and malicious activities.
- …

Publisher

- Use a trusted QRC generator
- When possible suggest a trusted QRC reader
- Check the result both online and printed to see if everything work fine before wide spreading it.
- …

What next?

Meanwhile something is moving on the market, it starts to appear the so called Secure QR Code or SQRC.

Figure 7. *Security QR Code*

SQRC is Denso's variation of QR Code technology that allows users to encode both public and private data where security and confidentiality is an absolute requirement. While a SQRC Code looks just like any other QR Code, SQRC codes contain two additional data components. The first is the private data which is protected by the second component which is a password (Figure 7).

Only a specific scanner, which is with the same setting of the encryption key that is set with the SQRC is made can read SQRC. The SQRC consists of mixed public data and private data (data encryption key). Scanner that supports the SQRC is able to read both the *public data* (e.g. person's name) and *private data* (person's age, health details and identification number). The security QR code has the same figure as normal QR Code and only the public data can be read as QR Code by a general scanner.

Remarks

SQRC Encryption Key is of 8 bytes in size. The generator (software) will specify a unique encryption key for each set of SQRC is generated, while the scanner is able to specify max. 8 SQRC read-only encryption key.

Table 1. *QR Code v.s. SQRC*

Features	QR Code	SQRC
Code Type		
ISO Standardization	Yes (ISO/IEC 180004)	No
Security Function	No	Yes
Data Capacity	Numeric: 7,089 characters Alpha numeral: 4,296 characters Binary (8 bit): 2,953 characters	→
Readabliity	Yes	→
Durability	Yes (Max. 30%)	→

ANTONIO IERANÒ

Antonio Ieranò is an IT professional, marketing specialist, and tech evangelist with over 16 years of experience serving as a community liaison, subject matter expert, and high-profile trainer for key technologies and solutions. Mr Ieranò's experience includes acting as the public face of Cisco security technologies; leading pan-European technical teams in development of new Cisco security products; and serving as a key public speaker and trainer on behalf of new high-tech products. His expertise spans IT development and implementation, marketing strategy, legal issues, and budget / financial management.

QR Codes: Convenience or Minefield?

Imagine that you are walking in the street in the town where you live. You need to find a new place to live, and don't really want to use an estate agent, because they usually lie about the places they have available, and charge a commission too. But you pass a tree with a sheet of paper stapled to the bark, reading "beautiful two-room apartment, lots of light, modern kitchen and bathroom … no agents."

In the past, that home-made ad would probably have had a telephone number for you to call. But this one continues "scan QR code for details." So you scan the code, and hope that your smartphone will immediately show you a web page with photos, details, and a contact telephone number or e-mail. What you had expected was something like this:

Figure 1. *Real QR code*

which when decoded by the QRcode app on your phone translates to *http://www.greatapartments.com/london* (for the sake of argument), and you see what you were expecting.

But what if the code were actually this one, without you realizing it?:

Figure 2. *Fake QR code*

This translates into an SMS message 'go daily quiz' that your phone will send to the local cellphone number 050-999-9999. But the number may easily be a premium-rate SMS or phone service, and you end up being defrauded through a bloated cellphone bill. And of course, if there really is a phone quiz that sends you new questions every day, you may end up being tempted to spend even more money trying to win some non-existent prize.

Worse still, what if the code is this ones:

Figure 3. *Fake QR code – hacking the data*

This sends your cellphone's browser to the address *http://hackmylaptop.com*, where the web page looks like a real advertisement for an apartment for rent. But the photos of the living room and kitchen have been doctored to hide a piece of malware that is automatically downloaded into the phone's memory when you open the page; and next time you synchronise the phone with your computer to download photos you have taken, that malware transfers itself to the computer alongside the legitimate content, and then 'calls home' to a control site, in order to download additional malware that hacks into your bank account, or steals your credit card details, or turns your computer into part of a botnet that ends up being used for DDOS attacks. Or, for that matter, the drive-by malware that you unknowingly downloaded inside the photo turns out to download additional man-in-the-middle malware that steals money from your bank account every time you log on to carry out legitimate transactions. And if the phone is synchronized to a corporate network, which is more and more common, then the entire network can be compromised by an unsuspecting employee trying to use a QR code to get access to what he or she things is a perfectly innocent web page.

These are only two types of potential scenarios for a security issue that is becoming steadily more common with the spread of QR codes across almost every type of printed media, and even the Internet. There is no question that these codes – an extension of the much older barcodes – are useful to anyone, whether individual or business, who wants to attract web traffic or just make it easier for others to make contact. More and more business cards have a QR code printed on them so that you can just scan them instead of typing the contact details into your phone's contact list. Newspaper advertisements include QR codes so that you can go straight to the right information page without having

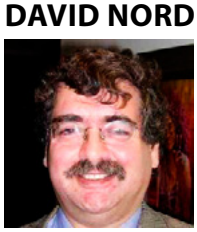
to type the URL on a small and fiddly keyboard. A QR code can point to an instant download of an audio or video clip or full-length recording. Even exclusive banking services, such as Switzerland's UBS private banking, have QR codes on their newspaper and magazine advertising, both to make it easier for potential clients to access their web pages and to show that they, too, are part of the modern high-tech world. In short, almost every kind of information that marketers want to get in front of their public is becoming accessible through QR codes.

But this convenience carries risk. Part is because of the inherent opacity of QR codes – you don't know what information is actually hidden behind the code, whether a URL for a normal web site, or one hiding drive-by malware, or one that looks like your real bank's site but is really a replica designed to make you input your account number and password so that a fraudster can steal your money; whether a legitimate telephone or SMS number, or one for premium services that defraud you, at least until you get a nasty surprise in your next bill. This inherent opacity also means that fraudsters can take advantage of legitimate QR codes printed, for example, on advertising posters for concerts, shops and restaurants at bus stops or railway stations: it takes very little work for criminals to print stick-on labels with QR codes that direct the public's cellphones to completely different 'services,' and stick them on top of the original code. You wanted to book tickets for a rock concert? What you got instead was a piece of malware that will empty your bank account, and you only find out when it's too late that the QR code that even has the rock group's logo designed into it actually directed you to *www.evilwebsite.xxx*.

This risk is made worse by the nature of smart phones and their operating systems, and it doesn't really matter whether they are iPhones, Androids, Blackberries or anything else, although most security experts regard the Android as the least secure system. Part of the problem is that the size and resolution of smart phone screens make it more difficult to see if the web page you landed on after scanning the QR code is actually the one you expected. Another part is that, unlike Internet-linked computers, cell phones can connect directly to premium services, whether you expected it or not. Most importantly, the level of security against malware of every kind is much lower than on laptop or desktop computers, even though most modern smart phones are really miniature computers in their own right with far more processing power and memory than PCs had only a couple of years ago. Most PC owners realize that they need to install at least some anti-virus software, even though that is only a partial security solution. By contrast, far fewer smart phone owners understand that they also need to install security software; and even then, there is a smaller selection of security software for all the different operating systems. Only a very few, more sophisticated, users realise that carefully-written malware can instruct Android phones to open up root access, which essentially allows hackers to get remote control of the phone. Even fewer users know that malware is available to enable hackers to use smart phones as bugs to listen in remotely to conversations: this is one of the reasons why many government offices insist that both visitors and staff leave their cellphones at a security checkpoint (the other risks, of course, include people photographing sensitive documents, whether or not they then send the photos immediately or just use them after leaving). And although some apps do exist that will show you all the tasks running on your smartphone, which could be a clue that something unwanted is hiding in memory, they are less easily available than Windows Task Manager on PCs.

So are there solutions? The most important is simply education: the technology journalists reviewing new smart phones, apps and services also have a duty to remind the public that all the cool new technology carries risks, and that there are ways to protect against them. In particular, every smart phone user needs to install security apps that protect against malware, and of course keep them updated. Network operators should also play a role in educating their users about the risks, and should be obliged by communications regulators to block access to premium phone and SMS services as a default setting. But the programmers and software companies that publish QR code apps can also play a very important role: instead of giving instant access to whatever service the QR code conceals, they should automatically pop up a screen that asks the user to confirm access to that service: if you think that you're just saving time by scanning the code for *www.realbank.com*, and the QR app asks you "do you really want to access *www.fakebank.com*?," then you are much less likely to end up with an empty bank account and a lot of headaches.

DAVID NORDELL



David Nordell is CEO of New Global Markets, a start-up developing solutions for financial crime intelligence and compliance, and a consultant on cyber security.

Dr.WEB®
20 years

Dr.Web SpIDer is 8-legged!

New Version 8.0

Security Space and Dr.Web Antivirus for Windows

Get your free 60-day license under https://www.drweb.com/press/
to protect your PC and your smartphone with Dr.Web!
Your promo code: ***Hakin9***

Protect your mobile device free of charge!
https://support.drweb.com/free_mobile/

Doctor Web is a Russian anti-virus vendor with a software development record dating back to 1992.
www.drweb.com

QR Codes – Hacking, Cracking and Other Security Considerations

Fear and uncertainty are running deep in the QR Code® space regarding the possibilities of data hijacking, hardware manipulation or other malicious attacks on mobile devices delivered by way of QR Codes. Can a QR Code really be "cracked" or "hacked" in such a way as to do this kind of damage? Let's talk...

The popularity of QR Codes in North America continues to grow at an incredible rate as these 2D bar codes become increasingly more popular with marketers, advertising agencies and name brand companies, all of whom want to deliver revenue generating data into the hand held and mobile spaces. According to ScanLife (*http://www.scanlife.com/blog/2013/02/qr-code-adoption-2013-trends-and-statistics/*) 1 in 5 Americans have scanned a QR Code in 2013. This figure is actually a drop in the proverbial bucket considering that America is still just over 50% saturation with smart phone or tablet devices. There is no doubt the use of QR Codes will continue grow dramatically over the next several years and this one fact is the key ingredient to similar growth of malicious attacks delivered through QR Codes.

Ignorance of the problem

On March 6th of 1992, the world waited for the Michaelangelo Computer Virus (*http://abcnews.go.com/Archives/video/march-1992-computer-virus-scare-13056853*) to strike hundreds of thousands of computers across the planet. The threat was so great this one computer event received massive and widespread media attention in virtually every industrialized country. Ultimately, the virus did little actual damage but its media coverage frightened the world into a more pro-active position regarding protection from such attacks. The antivirus software industry now had its first truly legitimate example of the need for antivirus software. John McAfee was well on his way to making millions.

No such awareness exists in the mobile and hand held spaces, making these hardware environments ripe for the picking by those that wish to inflict harm, steal data or attack a device for some other malicious purpose. People simply don't have the same awareness of the potential of attacks on these devices as they do with their personal computers and the bad guys are exploiting that to their own advantage.

We don't see this kind of media coverage anymore when it comes to malicious computer hacks. They just aren't news worthy. Everyone is too busy downloading apps, email and other instant gratification events onto their mobile devices without giving a second thought to the potential risks. For the moment, at least, no one has really been bitten by a truly malicious attack in the mobile space. That reality has lured us into a sense of complacency where we think it will never happen to us, but we do believe that if it does happen, it will happen to some one else. This ignorance of the problem is further exacerbated by the fact there are only a hand full of operating systems running on these devices. A crafty hacker only needs to write one

set of code to cause a widespread problem. Delivering a virus to a mobile device through email isn't a big problem, just at the moment, because antiviral apps for these devices are becoming more available. This is not to diminish the possibility of emails delivering a virus or Trojan horse. It's just to say that this hasn't been a critical issue until now. That will change. QR Codes however, have direct access to the hardware on these devices, thereby making QR Codes exponentially more dangerous as a potential delivery vehicle for a malicious attack. It's exactly like leaving your personal computer, turned on and logged in, on a busy street corner. Having direct access to the hardware is indeed the key issue. This can not be overstated, QR Codes have direct access to the hardware and this is a HUGE problem.

Hacking the Hardware

Standard UPC codes are based on a table of data which provides some form of unique identification. These codes describe something but they don't necessarily cause an action to be taken by the hardware unless that specific functionality is already built into the hardware. The hardware does something specific because that specific action is programmed into the hardware. The code itself is not necessarily the trigger of that action.

QR Codes are very different in that they do indeed trigger specific hardware and software actions on a mobile device. Scan a code and get a browser to launch and populate the URL address. Scan a code and get vCard data for your address book. Scan a code for a map and see that location on your screen. All of these actions are actually triggered by the code itself making QR Codes the key to the door for those wishing to steal data, inflict harm or damage a device.

One such example targeted the much sought after Google Glass technology in July of this year. According to an article in Forbes Magazine (*http://www.forbes.com/sites/andygreenberg/2013/07/17/google-glass-hacked-with-qr-code-photobombs/*) researchers at the security firm of Lookout Mobile were able to create a QR Code that actually reprogrammed the Google Glass hardware itself! This was accomplished by exploiting the method that Google Glass used to captured an image of a QR Code. One small loophole and the hackers jumped right through it.

DENSO Wave Inc. of Japan also uses the same approach to program its huge variety of bar code scanning devices. In the box with your DENSO scanner is an instruction book that contains dozens of QR Codes that are used to program specific functionality directly into the hardware of the scanner. Keep in mind DENSO is the inventor of QR Code technology so it makes perfect sense for them to directly incorporate hardware access with QR Codes. In DENSO's case, its a feature and not an exploit of a weakness in the hardware or OS of a particular device, as was the case in the Google Glass issue.

You must keep in mind there are three absolute conditions in the world of QR Codes that you simply can not control or impact in any way whatsoever. You can't control the device being used to scan your code, the OS on that device or which reader app is being used. All three of these individual conditions have their own unique behavioral characteristics. These three conditions, as variables, yield millions of possible conditional opportunities that can indeed be exploited to do harm in the mobile space. OS updates will happen much more often in the future specifically to prevent these exploits. As an example; scan this code on this device running this OS and using this particular app and you will get result A. Scan the same code on the same device but with another reader app and you will get result B. By simply changing a function in the OS and this problems goes away. Again, the potential combinations of exploits are virtually limitless. They are simply waiting to be discovered by smart people that want your information.

And therein lies the true nature of the problem. A smart hacker can create a QR Code that exploits a specific weakness in the OS running on the hardware. Such exploits could include things like surrendering access of your contact database to a hidden URL, invisibly tracking your movements through on board GPS, keystroke duplication, installing a Trojan, phishing or even grabbing up your financial and credit card information. The sky is the limit!

It isn't a question of will it happen, it's a question of when. With more and more internet bandwidth being consumed by mobile devices it is simply a matter of time before the first real and dangerous hacks will appear through QR Codes that cause widespread damage.

The Anatomy of a QR Code

Let me cut right to the chase. A printed QR Code is "virtually" impossible to "hack", at least in the sense of taking an existing QR Code and moving it's modules around to get the code to behave in a way not originally intended. To the best of my knowledge, there is no scanning app that will tell you which modules in a specific code are respon-

sible for any one character. The thought being that a hacker would want to "re-arrange" the modules of a deployed QR Code to their own specific requirements. Keep in mind that QR Codes are basically ink on a substrate so "hacking" or "cracking" them on a wide spread scale isn't a practical consideration. The only efficient and effective way to alter an existing, printed QR Code is to cover it with another QR Code that has alternate intent. This would be impossible to do in any wide spread print distribution like magazines, news papers or direct mail pieces. That being said, some of these codes are still vulnerable to being "re-routed" because of the URL shortening engine that was used to embedded a web destination into the QR Code. More on short URL's in a moment.

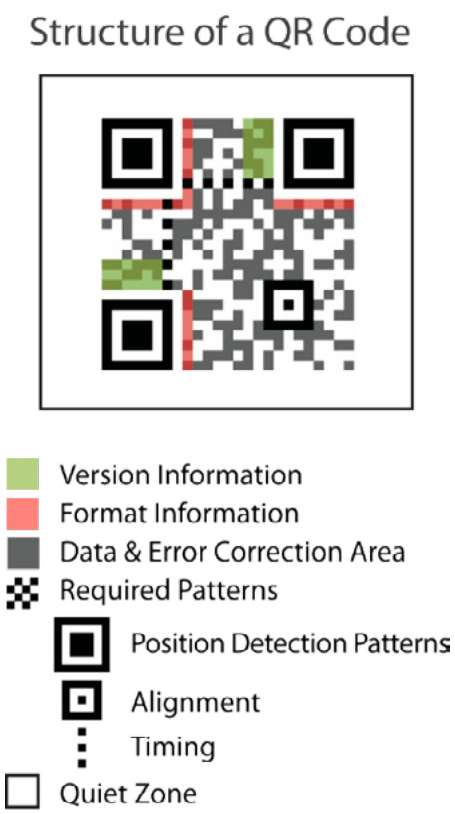


Figure 1. *Anatomy of a QR Code Courtesy DENSO Wave, Inc.*

Once printed, how does one change a specific module from black to white or white to black? It's simply not a practical consideration so I believe that we really don't need to worry about our QR Codes getting "hacked" or "cracked". I believe that we absolutely must worry about "hijacking" of QR Codes where a malicious code replaces a good one. Where "hijacking" means fraudulent data base manipulation of the short URL. Where "hijacking" means taking a branded QR Code, by its nature believed to be safe, and replacing it with another similarly branded QR Code with malicious intent.

Three Elements of "Hijacking" – Part One – Covering a code

Again, once printed, changing the operation of a QR Code by manipulating modules within the printed code is nearly impossible and not at all an efficient option for hackers. The only way to have a direct effect would be to completely replace the valid QR Code with an invalid code through the use of a sticker! This would be very impractical from a hacker's perspective because of the sheer volume of single codes that would need to be replaced. I therefore submit that a QR Code in a magazine advertisement, when connected to a name brand that is accountable, is most likely very safe to scan. I would say the same for newspapers, direct mail and other mass distribution systems. The only exception here is that I personally would not scan any QR Code in the personals section of any magazine or newspaper or a QR Code that is printed in some other format that is singular in it's nature. For example, a QR Code in the personals section, a one off code in the income opportunities advertisements or anywhere else that the code is not backed up with name brand recognition and direct accountability.

All of that being said, what are the conditions under which a QR Code can be easily "replaced"? Here are some examples. Movie posters with QR Codes are commonly distributed. I personally wouldn't scan one unless it's in the window of the theater and behind glass. The vast majority of QR Codes at bus stops are perfectly legitimate but I wouldn't scan one unless I could run my fingers over it to be sure there isn't some sort of sticker in place. I think you see where I am going with this. Any QR Code in a public space, at eye level can easily be covered with a malicious QR Code. If the code is not under a cover of some sort and can clearly be identified as an integrated part of the total distribution, I just won't scan it. Keep in mind however, that I am enlightened. The same cannot be said for the vast majority of QR Code consumers and that is where bad people have a wide open target.

Hijacking Part Two – URL Shorteners and Redirection

This is the one that frightens me the most and that is having the URL encoded into the QR Code highjacked to resolve to a different destination. In terms of URL access there are two different types of QR Codes, direct and indirect. Direct QR Codes aren't a potential problem because the absolute final destination URL is in the code itself. If you are in con-

trol of the domain, then you are in complete control of the URL you put into your QR Codes making hijacking of the URL impossible. That is both good and bad. It's good because you are in direct control of the URL embedded in the QR Code. It's bad if the URL is very long which would yield a larger and more dense QR Code. The greater the density (more modules) of your QR Codes the greater the likelihood of a failed scan. This goes back to the three conditions in the QR Code reality you can't control. It's a best practice to have the lowest possible density in a QR Code for the greatest likelihood of a successful scan on the widest possible variety of devices.

Indirect QR Codes have their advantages and their potential issues. An indirect QR Code will contain a short URL so that there will be less data to be embedded into the QR Code and therefore, you will have a much lower density QR Code. Low density is a lowest common denominator consideration for insuring that QR Codes are successfully scanned as often as possible.

Short URL's point to a database that contains the long URL. For example, *http://goo.gl/AbC123* (not a real URL) might redirect, through that database, to a URL that would be much longer, like *http://myfantasticwebsite.com/firstdirectoy/seconddirectory*. Obviously this second URL example would require a much more dense QR Code, reducing the likelihood of that code to be successfully scanned.

Another advantage of short URL's is the opportunity to have a QR Code run through an analytics engine that ultimately redirects to the client's desired final destination. These engines can deliver exceptionally robust information about the scanning performance of the code. Things like GPS based, opt-in location services, mobile page drill down, accurate measurement of the performance of conversion pages and many other important measurements. The mobile space is an entirely new reality with it's own amazing and unique statistical opportunities. Many of these dedicated QR Code analytics engines are incredibly sophisticated, most are very much misunderstood and they deliver analytic results that far exceed the capabilities of other, more traditional analytics solutions.

So here is the definition of URL shortening issues as they relate to QR Codes. Virtually every publicly accessible URL shortening service on the web came to exist as a result of the needs of social media. If Twitter limits Tweets to 140 characters, wouldn't it be nice to have a short URL deliver to a longer URL, leaving you more characters to personally address in your Tweet? Short URL's in social media are a standard and virtually all the existing URL shorteners came to exist strictly because of the specific social media needs and requirements. None of these engines have contractual agreements for data privacy, none of them guarantee their uptime, and not a one of them can absolutely keep your private information concealed from the public at large.

On top of that, many of these URL shortening systems are hosted through off shore servers that are under the control of foreign governments. One of the most popular URL shortening services in North America is hosted in the .LY Top Level Domain (TLD). The .LY domain is the exclusive property of, and is under the complete control of the Government of Libya! Would any self respecting entity in the free world want their data passing through and residing on servers that are in the hands of the Government of Libya? Other URL shortening services are based in TLD's owned by Greenland, Turks and Caicos, Montenegro and other countries, some of which may not have the best relationship with the government of the United States. Americans are up in arms over the *National Security Administration* (NSA) possible reading their emails or listening to their phone calls. Yet many of these same Americans are using off-shore URL shorteners, allowing their data to pass through the hands of foreigners, and they do so out of ignorance and without giving it a second thought.

Using these off shore URL shortening services is a substantial potential breach of security of truly epic proportion. Your audit trail is gone, there is no chain of custody that can be documented and you are complete exposed to the wishes and desires of others. Here is a potential scenario. You are a manufacturer of a nationally distributed, prepackaged food product. Your marketing team decides to put one QR Code on the spine of 70 million boxes of your product that will be deployed on grocery store shelves across the country. That marketing department doesn't investigate QR Codes deeply enough and they elect to use one of these offshore URL shortening services. Because there are now 70 million iterations of a single QR Code, an enterprising hacker now is very interested in having some fun and he cracks the database of the URL shortening service. Suddenly, this one QR Codes is redirected to a porn site or, worse yet, the new destination eats your phone for lunch. All that remains is to hire a lawyer because someone is going to sue you, count on it.

Here are some tips regarding URL shortening engines and how they relate to QR Codes.

- Don't use any URL shortener that is free and open to the public. You don't have a contract with them, you have no idea who they are and their existing Privacy Policies and Statements will not say a single thing about keeping your specific information out of prying eyes.
- Don't use a URL shortener that is hosted through an off shore Top Level Domain. If you do, you deserve whatever happens to you.
- If you can't get a contract that defines security with them, don't use them.
- Only use short URL's that are created for you by the company that is generating your QR Codes. Even then, make sure their shortening engine lives on the same servers as their analytics tool and their QR Code generator.
- Don't want to work with any one company to get your QR Codes? That's fine. There are many URL shortening scripts out there for you to download and run on your own server where you are in control of security.

Hijacking Part Three – Branded, QR Codes are Not What You Might Think

Branded QR Codes, codes with logo artwork as part of the code, have long been thought of as a way to transmit a sense of security and comfort to the person about to scan the code. Many organizations have deployed such codes in an attempt to link a code to a particular brand with the intent to imply value, integrity and security.

Figure 2. *A Legitimate QR Code with Unique Branding Identity*

Here is an example of a "branded" QR Code. Yes, it's from my company but I am only using this as an example to help make the point. The method I will describe here is used all too frequently and is a wide open invitation to hackers and scam artists. Branding a QR Code in the following way is not a good idea, it doesn't achieve any degree of security and it's a giant greeting card inviting hackers to attack an entity and it's precious brand.

Figure 2 is a typical sample of a "branded" QR Code. The method used to include branding artwork here is a method that exploits the native Error Correction Code (ECC) of QR Code technology. ECC is a technology that allows physically damaged QR Codes to remain viable regardless of the actual amount of damage to the code. ECC is a native feature of QR, it's can't be turned off and it does allow for up to 4 different user defined levels of damage protection. The 4 levels of ECC are "L" for Low, where up to 7% of the code space can be damaged and the code will still scan, Level "M" for medium, which corrects for up to 15% damage, Level "Q" for Quartile, up to 25% damage and finally, Level "H" for high that can recover a QR Code with up to 30% damage. Level L is the default for all codes and the other levels are user facilitated in the QR Code creation engine.

Figure 3. *A "Counterfeit" QR Code with Unique Branding Identity*

Now that you have a basic understanding of ECC it's easy to conceive a process to brand a QR Code. Simply ratchet up your selected ECC to Level H and put in your logo making sure that you don't obscure or "damage" more than 30% of the entire code space and you are in business.

Here is the problem with this approach. People scan branded QR Codes because they perceive some sense of comfort in doing that. A bad guy can create his own QR Code, drop your logo into it and have the code resolve to a destination of his own choice. That "counterfeit" code transmits the same perception of safety, in that the QR Code appears to be created by a responsible entity. These counterfeit codes extend the same invitation to scan the code. Figure 3 is an example of such a counterfeit QR Code. At first blush it's difficult to see any difference at all between the legit code and this one. There simply is no visual indication this is a code you shouldn't scan. Quite the opposite actually happens, especially if your logo is a highly recognized name brand. Scan both codes shown here and see what happens. I promise, this is only a demonstration and nothing will happen to your data or your device.

Figure 4. *A Branded QR Code Using DENSO Wave's LogoQ*

There is a solution to this problem that is very unique. In the above samples the logo obscured or replaced a set of modules in the code. This is only possible because of ECC technology, anyone with a copy of Photoshop can make this happen. Figure 4 shows a branded QR Code that was generated through DENSO Wave software called LogoQ. Using LogoQ, the logo doesn't obscure any portion of the code at all. In fact, the logo is now an integrated part of the code itself, making these types of QR Codes exceptionally difficult to counterfeit.

ISO:18004 Compliance – A Legally Defensible Position

LogoQ isn't the only software out there that can do this with a logo. It is, however, the only software out there that can do this and produce a QR Code that is fully compliant to the ISO:18004 specification which governs QR Codes. So what does ISO compliance have to do with malicious QR Codes? It's about the law.

Many years ago McDonald's never envisioned getting sued over a cup of hot coffee spilled in the lap, but it happened and McDonald's paid up. There are countless examples of how people are suing for unbelievable reasons because America is a very litigious society. If your QR Code is intended to point to a product mobile page but it ultimately points to a porn site, guess what, call a lawyer, you are going to need one. Some might say that this belief is paranoid. I prefer to believe it is professionally responsible, especially when dealing with name brand clients.

Being able to prove that a particular QR Code did not come from you might be an important thing if you get sued. DENSO software applications are the only apps that have a direct and undisputed link to the ISO specifications. This isn't a sales pitch, it's a fact. ISO compliance is a topic worthy of it's own article so I will just say that if you are about to deploy a "mission critical" QR Code campaign, this is something you might want to think about.

The Bottom Line – To hack or not to hack isn't the question

There is no doubt that consumers are going to have to deal with potentially dangerous attacks through QR Codes. Marketers, agencies, corporations or any other entity that deploys a QR Code for the general public to use has a responsibility to do everything they can to insure the safest possible scanning experience. They also have to cover their own back sides as well. This problem certainly shows all the signs of getting much worse before it gets better. So, what can be done to help reduce the risk and not become a victim of a malicious QR Code? Here are my top 10 tips, tricks and best practices to consider.

- Never scan a QR Code if its surrounding content even remotely appears to be questionable or otherwise suspect. Avoid codes in personal advertising, codes in public places that appear to be one-off deployments or any other situation that makes you think twice. Never scan a code because it's "just there".

- The reader app on the device is the door and the QR Code is the key that opens that door. NEVER use a reader app that automatically executes without user feedback. For example, if the reader app immediately opens the browser and connects to a URL upon successfully scanning a QR Code, without a confirmation click from the user, don't use that app! Anything automatic is a disaster waiting to happen.
- Don't install the first reader app you find that is free. Do some comparison shopping, read customer reviews and check out their web sites. The more you know about the app the less likely your are to become a victim. Additionally, carefully check all the default setting of the reader app immediately upon installing it. If you are installing a reader app that requires you agree to its licensing terms, as a general rule, don't install it. Unless of course you are willing to take the time to fully read and understand the license agreement. If you just accept the agreement and continue with the installation, you will have no idea of what you have agreed to and this could be dangerous. You could be giving permission to background processes initiated by the reader app that you might regret.
- If an OS update becomes available for your device, install it.
- Do some research to find out if your QR Code provider uses short URL's. If they do, question them and make sure they aren't using one of the free shortening services.
- There is no such thing as a free QR Code that has a URL redirect associated with it. Providers of analytics services rely on redirects but that would be a service you pay for. If you create a QR code at one of the free sites, and that code has a URL that is just the first hop in a redirect, DON'T USE IT!
- You might think that branding your code by exploiting ECC is a good idea. Please trust me on this, it isn't. I absolutely recommend branded QR Codes, just find those professional that can help you execute correctly.
- Again, as a general rule, I recommend that you should not let your reader app send "push" notifications to your device. The same can be said for web sites that are delivered to your device through QR Codes. Due diligence is expected here.
- You should activate and use all the security features available on your specific device, especially any security feature that is unique within any app you have installed on your device. Many of these features can help keep your data secure.
- For the moment the QR Code industry doesn't have a unified trade association so there isn't a single source to contact for information. If you do indeed come across or scan a malicious QR Code, please report it to someone! You can do this through various QR Code groups on LinkedIn or through QR Code providers on FaceBook. You can even send an email to an existing QR Code provider in the hope they will bring this to the attention of their peers.

Is the potential of a bad QR Code a deal breaker? For some it might be, but I wouldn't look at it that way. Arguably, there is no such thing as a perfectly secure web site or an online database, an email address can easily be spoofed, and, with a little practice, I can open an automatic garage door without knowing the code. In this digital world there will always be dangerous vulnerabilities and those that wish to exploit them for their own benefit. QR Codes are no exception. If you deploy QR Codes do your homework. Be prepared to deliver a valuable and positive experience as well as learning how to protect yourself from frivolous litigation. If you are a rabid scanner of QR Codes you shouldn't scan every code you see just because "it's there". From any perspective it's like everything else in life, a little common sense goes a long way.

V. MICHAEL BALAS

Michael has worked with consumer electronics and personal computers since he was old enough to understand that putting a key into an electrical outlet was a bad thing to do. He spent more than 25 years in the personal computer industry, culminating with a long stretch with Apple Computer as a Business Development Executive based in the American midwest. After leaving Apple in 2002, Michael started an entrepreneurial career and has founded three successful companies. Two of which are in the video production industry and his third, VitreoQR, LLC, is rapidly achieving leadership recognition in QR Code knowledge and expertise. In early 2011, VitreoQR was the very first company to be awarded a sales and support contract (http://www.businesswire.com/news/home/20110224005472/en/DENSO-Appoints-VitreoQR-Sales-Support-Partner-QR) in the QR space from DENSO Wave, the inventors of QR Code technology. In June of 2013 the contract was extended for another three years. The new contract also includes a licensing agreement that gives VitreoQR unprecedented access to a very a substantial library of DENSO's QR Code patents and technologies, making VitreoQR an exceptionally unique company in the global QR Code space.

6 Ways To Protect Yourself From QR Code Hacking

In today's fast moving times, getting information and content instantly at our figure tips has become an increasing necessity. Because of this, Quick Response (QR) codes continue to be the biggest driver of print to mobile activations. When scanned, the codes often contain web links that automatically take a user to a website.

Over the last few years, the practice of placing this type of matrix barcode on billboards, posters, clothing tags, concert tickets, business cards, TV ads and magazines has become common practice. According to ClickZ.com, QR scans saw an increase of 400% between June 2011 and June 2012. But while advertisers have seen this as a great opportunity to provide information and content about their services and products, cybercriminals see this as an opportunity to exploit an unsuspecting and uninformed mobile user base.

In order to utilize QR codes, all you need is a smartphone with a camera and a QR reader application to scan the code. When the code is scanned, you are redirect to wherever the QR code creator has designated. This is obviously a convenient way to get people engaged with content. However, the huge downside is that you never know where you will be redirected until after you scan the code. Just as users must be careful as to not open emails from an unknown sender, users must also be careful when scanning QR codes.

Over the last few years, there have been hundreds of reports regarding cyber attacks due to QR codes leading users to websites that automatically download malicious software and various types of malware. Downloading these applications has allowed these cybercriminals to steal your calendar, contacts, credit card, Facebook and GPS information as well send SMS messages to premium/paid numbers. These kinds of attacks are just the beginning of more sophisticated and problematic ways attackers can infiltrate your mobile device.

In late July, there were reports of Google Glass being hacked. Many functions on Google Glass are actually activated by reading QR codes. Marc Rogers, Principal Researcher at the Lookout Mobile Security, discovered the vulnerability. He noticed that the camera automatically identifies QR codes and uses them to trigger WiFi connections

Figure 1. *Be careful what you scan. Source: http://www.goegi.org/goegi-web-design/mobile-web-design/the-need-for-qr-codes/*

and other background operations. By hiding malicious QR codes in images, Rogers was able to get Glass to connect to a compromised network, show details of all network traffic from Glass, and even take full remote control of the wearable device.

Luckily, there are simple (and free!) things that you can do that can help you prevent your device from being hijacked (Figure 1).

Ignorance Is NOT Bliss

Not all QR codes are built with the best intentions. Understand that there are risks to scanning a QR code. Just because you have a phone running iOS doesn't mean you are invincible. Know the risks. Knowledge is power! (Figure 2)

Watch Where You Are Going

If I haven't scared you away from scanning QR codes, then make sure you are using a QR scan-

Figure 2. *Suspicious QR codes. Source: http://barnettmurphydirectmarketing.com/qr-codes.php*

Figure 3. *Installation of proactive software on your mobile device. mSource: http://www.qrcodepress.com/nfc-technology-adds-requirement-for-virtual-credentials-for-identity-management/853265/*

ner that that previews URLs. Avoid scanning suspicious codes and links that don't seem to match the ads they're incorporated in; also avoid shortened links (Figure 3).

Protect Yourself

Just like the days of getting an anti-virus program for your desktop computer, the usual suspects have built proactive software to help you protect your mobile device. Scanning a QR code with Norton Snap will check the link, and then provide you with a clear safety rating. If you want to continue loading the link, you simply tap on the full link address.

McAfee also provides mobile security software that can be used to protect you from viruses, worms, Trojans, spyware and other malware that can be transmitted via QR codes (Figure 4).

Figure 4. *Open source materials. Source: http://www.xatakandroid.com/sistema-operativo/google-prepara-caracteristica-de-eliminacion-de-datos-selectiva-en-android-para-potenciar-byod*

Figure 5. *Be reasonable. Source: http://yoplayhouse.blogspot.com/2009/01/boy-licks-frozen-light-pole-gets-stuck.html*

Figure 6. *Unsafe sources. Source: http://www.fangdigital.com/54-does-not-constitute-most-and-other-cautionary-tales/*

Sometimes Open Source Isn't The Best Source

Even though Google's intentions were good when making Android an open source operating system, its open source-ness can be used for evil as well. Open source materials allow cyber attackers to examine its source code for easily exploited weaknesses. This is why most QR related malware is target to Android based smartphones. Stay up to date with the latest app and OS updates to ensure current security settings (Figure 5).

Use Common Sense

Though the use of QR codes is new, the end tactics are still the same. If you go to a website from a QR code that asks for your personal information, logins, or passwords don't give it. I have heard a great quote about phishing scams –"If there's doubt, don't fill it out!" (Figure 6)

Think About The Source

Much of the QR phishing scams can be attributed to stickers with codes covering legitimate QR codes. So if you see a magazine ad, a poster, a CD, or any other material that has a QR code sticker on it, chances are, its a scammer. If the QR code looks more like a scratch and sniff sticker and less like a part of the original print, be very suspicious because something doesn't smell right.

NICK LYNCH

Nick is the Co-Founder of OakReach, a native ad and content marketing platform. With over a decade of ad tech experience, Nick is a product developer and operational leader with a strong professional track record in digital media and technology. His opinions and thought leadership have been featured in such industry publications as TechCrunch, Mediapost and ClickZ. Former companies include Adconion, Fox Interactive Media, and Spot Runner.

UPDATE NOW WITH STIG AUDITING

"IN SOME CASES **nipper studio** HAS VIRTUALLY **REMOVED** the NEED FOR a **MANUAL AUDIT**"

CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

2012 Computing Security Awards WINNER Enterprise Security Solution of the Year

Security Products' GOVIES 2013 Government Security Awards

2012 Computing Security Awards WINNER Network Security Solution of the Year

www.titania.com

Interview with Nick Lynch

Nick is the Co-Founder of OakReach, a native ad and content marketing platform. With over a decade of ad tech experience, Nick is a product developer and operational leader with a strong professional track record in digital media and technology. His opinions and thought leadership have been featured in such industry publications as TechCrunch, Mediapost and ClickZ. Former companies include Adconion, Fox Interactive Media, and Spot Runner.

Could you please introduce yourself briefly?

My name is Nick Lynch, Co-Founder & VP of Sales & Marketing for OakReach. I have worked in the AdTech space since 2005 and have worn many different hats: Product development, marketing, sales, and business development.

What is your company responsible for?

OakReach is a content marketing and native ad platform. We provide tools for publishers to create and manage native ad units (sponsored articles, images, and videos) and activate their created content for brand sponsorships and monetization. We also provide content distribution and content sponsorship opportunities to brands, advertisers, and agencies.

What is your area of interest?

I have always been interested in disruptive technology. Anything that upsets the status quo and innovates business models peaks my interest.

Anytime you see Elon Musk or Jeff Bezos in the news, rest assured I am watching!

How long are you in business?

OakReach has been in development since early this year but our official release was in May. Our platform is in beta now and we look to be about 45 days out from a public release.

Did you always know what you want to do in the future?

We are consistently looking forward to what's next and always looking at ways to innovate. In Ad Tech, you always have to stay nimble and flexible to be able to meet new demands and constant change in the marketplace. We feel well positioned as an early mover in the space to be able to adapt quickly to dynamic market demands.

What sort of clients have you got?

We work with both advertisers and publishers (website owners). Our goal is to become THE neutral, third party marketplace for content and native ad distribution.

Have you ever used QR codes in business?

Yes! QR codes have been a great way to activate customers looking for product related content. In previous roles, I have used QR codes for contests, content distribution, as well as lead generation.

Do you think they are a good marketing tool?

When you used in the right environment, they are extremely effective. When used in conjunction with content or when consumers are already engaged tends to yield the most results. But to utilize QR codes in a passive environment where there is no real connection with what a person is doing, leads to poor performance.

Are you involved in some extra project that you would like to share with our readers?

I have a passion for advising and working with other start ups. I advisor for a couple different companies in the space: a hyper local mobile advertising platform called Pagewoo and a recently acquired supply side platform named Adaptive Media (Mimvi acquired Adaptive back in July).

by Magdalena Gierwatowska

Interview with Antonio Ieranò

Antonio is an IT professional, marketing specialist, and tech evangelist with over 16 years of experience serving as a community liaison, subject matter expert, and high-profile trainer for key technologies and solutions. Mr Ieranò's experience includes acting as the public face of Cisco security technologies; leading pan-European technical teams in development of new Cisco security products; and serving as a key public speaker and trainer on behalf of new high-tech products. His expertise spans IT development and implementation, marketing strategy, legal issues, and budget / financial management.

Specialties and Executive Expertise

IT Strategy, Technical Audits, Enterprise Architecture & Applications, Systems Integration, Technical Sales Liaison, Solution Architecture, Network Design, Architecture, & Security, Vulnerability Assessment & Management, Systems Engineering, TCP / IP, Data Privacy, Cisco Technologies, Cloud Computing, IT Audits, Marketing Strategy, Budget Management, Consultative Sales, Social Media Marketing, High-Impact Presentations, Project Management.

You have a very wide experience. Could you please tell us a little bit about your career development?

Well I started as many of us as a developer, may be someone remember PDP-11 and ADA, but I turn soon to be a trainer and a system engineer, I never liked to double-check the code mostly if you remember how was done those years….

I worked for several years as a consultant: project management, problem setting and problem solving in the IT field working with token-ring and other old network structure. Wireless is so distant from thick Ethernet I've used in the past (ok now I'm feeling very old).

I saw internet growing from BBS and Fido-net to the modern connections exploring quite everything.

Did you always know what is you plan for the future?

Absolutely not, planning the future is an odd exercise, I just did what I was likening and what was worth to me. I love technology and IT is still an amazing field to work.

What would you like to specialize in?

Hard to say, but I still think that security is the most entertaining field, even if I usually have a non-product approach to security, I always seen it as a process where products are just a tiny components. I dogged deeper on forensic recently but from a process and investigation perspective.

You currently run your own blog? Am I right?

Yes actually I run more than one, when I have time of course. One dedicated to my non IT thoughts, one dedicated to the tech news I find interesting, another that is a technical one in English, one dedicated to Italian technical news (just a little empty those last months), one on Italian politics news and finally one with my 10 years old daughter.

What is your main area of expertise?

I would say technology and security, but I developed experience also in communication and marketing.

What do you think about using QR codes for marketing purposes?

QRCode is a great instrument mostly because allow content publisher to break the traditional barriers between paper and computer. This way it is possible to add to a static media as magazines and posters dynamic contents. I think it will break some other barriers in advertising in the future.

What are you planning to achieve in the nearest future?

Well I'm looking for something new to explore or something old to develop. I've been a developer, a trainer, a system engineer, a product manager, a speaker, a marketing manager now I would like to be …. I'll tell you as soon as I find a new career.

Did you writ articles for Hakin9 in the past?

As a matter of fact I did, a really pleasant and interesting experience.

What do you think about our Magazine?

Hakin9 is a reference for the IT, great articles coming from real experts and a strong focus on what really matter, I do not think we can ask more to a magazine.

What is your hobby?

When younger I used to play guitars but nowadays I become lazy, I think my hobby is my daughter and my family. But I seldom enjoy wrestling, I've been an ICW wrestler, and sooner or later I'll enjoy my bike.

Have you got enough time for you passions? Or you are too busy?

Luckily I always did works that were aligned with my passions: share knowledge, Technology so hard to say. For sure I would like to have more time to share ideas and exchange experiences.

by Magdalena Gierwatowska

Creating Innovative and Unique QR Code® Solutions

is our only job and its what we do better than anyone else.

It isn't about the code, its about what the code can do for you, *and it goes so much further than just a marketing idea.* VitreoQR has a complete array of world class solutions, from marketing to management, that can help you measure and grow your business. Whatever your challenge might be, inventory control, counterfeit prevention, access control systems, supply chain management or any one of countless other business conditions, VitreoQR can develop a QR Code driven solution to meet your specific needs. As a licensee of DENSO Wave QR Code patents, we have all the necessary tools to make your business more efficient and more profitable through new ideas in 2D barcoding systems.

WARNING: If you don't want to learn more, don't scan this code!

No one understands QR Codes like we do.

Explore the possibilities that QR Code technologies offer as real world solutions to even the most difficult problems. Convey information, manage issues, reach new markets and move more people into your perspective as you have never been able to do before. There simply isn't another technology that can do as much for you, at the same value proposition, as a QR Code. VitreoQR deploys genuine, DENSO Wave QR Codes that are absolutely guaranteed to be fully compliant with the ISO:18004:2006 specification, delivering to you security and peace of mind.

QRCode QRPhoto QRLogo QRMotion QRAnalytics QRCustom SQRC

VitreoQR, LLC
12801 Berea Road, Suite F
Cleveland, Ohio 44111 U.S.A.
P. 440.941.2320
E. info@vitreoqr.com
W. http://vitreoqr.com

In Partnership With DENSO ADC INVENTOR OF THE QR CODE®

A BZ Media Event

Big Data gets real at Big Data TechCon!

Discover how to master Big Data from real-world practitioners – instructors who work in the trenches and can teach you from real-world experience!

Come to Big Data TechCon to learn the best ways to:

- Collect, sort and store massive quantities of structured and unstructured data
- Process real-time data pouring into your organization
- Master Big Data tools and technologies like Hadoop, Map/Reduce, NoSQL databases, and more

Over 60 how-to practical classes and tutorials to choose from!

- Learn HOW TO integrate data-collection technologies with analysis and business-analysis tools to produce the kind of workable information and reports your organization needs
- Understand HOW TO leverage Big Data to help your organization today

"Big Data TechCon is loaded with great networking opportunities and has a good mix of classes with technical depth, as well as overviews. It's a good, technically-focused conference for developers."
—Kim Palko, Principal Product Manager, Red Hat

"Big Data TechCon is great for beginners as well as advanced Big Data practitioners. It's a great conference!"
—Ryan Wood, Software Systems Analyst, Government of Canada

"If you're in or about to get into Big Data, this is the conference to go to."
—Jimmy Chung, Manager, Reports Development, Avectra

BigData TECHCON

San Francisco

October 15-17, 2013

www.BigDataTechCon.com

The HOW-TO conference for Big Data and IT professionals