QR Code Security: A Survey of Attacks and Challenges for Usable Security

Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, Edgar Weippl
[1stletterfirstname][lastname]@sba-research.org

SBA Research, Vienna

Abstract. QR (Quick Response) codes are two-dimensional barcodes with the ability to encode different types of information. Because of their high information density and robustness, QR codes have gained popularity in various fields of application. Even though they offer a broad range of advantages, QR codes pose significant security risks. Attackers can encode malicious links that lead e.g. to phishing sites. Such malicious QR codes can be printed on small stickers and replace benign ones on billboard advertisements. Although many real world examples of QR code based attacks have been reported in the media, only little research has been conducted in this field and almost no attention has been paid on the interplay of security and human-computer interaction. In this work, we describe the manifold use cases of QR codes. Furthermore, we analyze the most significant attack scenarios with respect to the specific use cases. Additionally, we systemize the research that has already been conducted and identified usable security and security awareness as the main research challenges. Finally we propose design requirements with respect to the QR code itself, the reader application and usability aspects in order to support further research into to making QR code processing both secure and usable.

Keywords: qr codes, security, hci, usability

1 Introduction

QR (Quick Response) codes are two-dimensional matrix barcodes that are used to encode information. In recent years, they have more and more found their way into our everyday lives. They were initially invented to track automotive parts during the production process. Nowadays, they have been adapted for a variety of use cases. QR codes are cheap to produce and easy to deploy. Therefore, they became the medium of choice in billboard advertising to access potential customers. One of the most commonly found use case is URL encoding to make information instantly available. Besides a broad range of advantages, QR codes have been misused as attack vector for social engineers. Attackers encode malicious links that lead e.g. to phishing sites or to execute fraudulent code. These malicious QR codes can be printed on small stickers and pasted over already

existing QR codes. Furthermore, attackers can modify selected modules from white to black and vice-versa in order to override the originally encoded content as proposed in [22]. Even though many real world examples have been reported in the media [24], there has been little research conducted on human-computer interaction and security aspects of QR code based attacks. In this work, we provide a comprehensive overview of the most relevant use cases of QR codes and the associated attack vector with an emphasis on phishing. To do so, we conducted a comprehensive literature survey to determine the state of the art regarding user studies and exemplary attacks. Additionally we identified the major research challenges to improve the security of QR codes and contribute questions and directions toward secure and usable QR code processing. The main contributions of this paper are as follows:

- We provide a comprehensive overview on the most relevant use cases and identify associated attack vectors.
- We systemize the state of the art in the research community.
- We identify the major research challenges to improve QR code security with an emphasis on usability and security aspects.

The remainder of this paper is structured as follows: In Section 2 we provide an introduction to the QR code standard and an overview of the use cases. In Section 3 we systemize attack scenarios with QR codes as attack vector and discuss related user studies. In Section 4 we describe reported real world examples and Section 5 discusses related user studies.In Section 6, we identify open research challenges with respect to security and usability aspects. Section 7 concludes our work.

2 The QR Code Standard

In this section, we provide a brief introduction to the QR standard as well as an overview of the manifold use cases of QR codes. QR (Quick Response) codes are two-dimensional bar codes that encode information in both vertical and horizontal direction. To access the encoded data from a QR code, a built-in smartphone camera captures an image of the QR code and then decodes it using QR code reader software. There are 40 different versions of QR codes with different data capacities. Version 1 consists of 21 X 21 modules from which 133 can be used for storing the encoded data. Version 40, which produces the largest QR code, has 23,648, hence 4296 alphanumeric characters [32], [37] can be encoded. Figure 1 shows an example of a version 2 QR code, which is the most commonly used one [27], [34], [40], [15]. In addition to alphanumeric characters, QR codes can encode binaries, Kanjis[1] or control codes. Furthermore, QR codes are readable from different angles and the data can be decoded successfully even if the code is partially covered or damaged [12]. This is because of robust error correction that is based on Reed-Solomon Codes [19]. There are four different error correction

[1] Japanese characters of Chinese origin

levels namely L(Low 7%), M(Medium 15%), Q(Quartile 25%) and H(High 30%) Error correction level L tolerates up to 7% unreadable modules respectively [31]. Higher error correction levels increases the area, which is reserved for error correction codewords and decreases the area reserved for the actual data. Therefore, error correction level L is usually preferred. An additional feature to stabilize the decoding process is masking. Masking ensures an equal distribution between black and white modules. The appropriate mask is automatically chosen by the encoding software when the code is created.

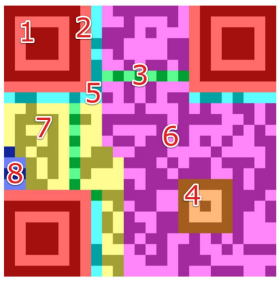

Fig. 1. Example QR Code Version 2 [27]

2.1 Uses of QR Codes

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

Advertising. The most common use case in advertising is encoding URLs or contact information, geo-locations and text to make them instantly available to the user [7]. Billboard advertisements with QR codes can be found in most urban spaces [25] to deliver information to potential future customers, obviating the need to type in the URL manually to visit a webpage. According to [16], the chain supermarket *Tesco* used QR codes to boost online shopping and to penetrate further into the South Korean market. Another innovative and cost efficient marketing campaign was launched by a shampoo company by cutting QR codes into hairstyles [23]. People with these haircuts acted as moving advertisement for shampoo since their "hair tattoos" redirected to the company's web site after scanning.

Mobile Payments. QR codes are also used to process mobile payments and provide opportunities to purchase a product or a service by solely scanning a QR code. This is referred to as "one-click" payment [30], [26], [20]. After scanning the

respective QR code, the user is redirected to an intermediate payment agent or the company's web page. PayPal, which is one of the biggest payment companies has already adopted this payment practice in some countries [11].

Access Control. According to [44], QR codes are used for physical access control in combination with other security enhancing methods. Kao et al. [44] proposed a safe authentication system by combining QR codes and the One Time Password technique (OTP [28]). The user information is stored at a main server, which holds the user information, a mobile application that generates QR codes, and a client PC with a camera to scan the QR code. In order to authenticate, the user generates a QR code with an encrypted password encoded, which is then scanned by the client PC.

Augmented Reality and Navigation. QR codes are also used in digital government services to effectively distribute valuable information to the public. According to [9], QR codes are used to increase citizen participation and to navigate users through park trails and museums [33], [41]. Furthermore they are used as supplementary material for education and within games. QR codes are also used to share information between people who participate in the same social event [10] or to share information in order to support the learning process. Furthermore, interesting and creative uses of QR codes are presented in [2] and [21] where QR Codes are used as a surface on which an augmented reality application is deployed and as a result, impressive 3D virtual objects are produced and displayed to the user.

3 QR Codes as Attack Vectors

In this section we describe different attack scenarios based on QR codes. In the media, the most frequently reported attack scenario is social engineering [24]. In Information Technology (IT) security, social engineering refers to the art of manipulating people to reveal confidential information to the social engineer and it is mainly used to steal data. One of the most popular practices in social engineering is phishing. Attackers use malicious QR codes to direct users to fraudulent web sites, which masquerade as legitimate web sites aiming to steal sensitive personal information such as usernames, passwords or credit card information. There are two main attack vectors to exploit QR codes:

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

The attacker modifies individual modules of a QR code. The main idea of this modification is that the encoded content is modified solely by changing the color of specific modules of the QR Code to which the user will be directed after scanning the code as proposed in [27].

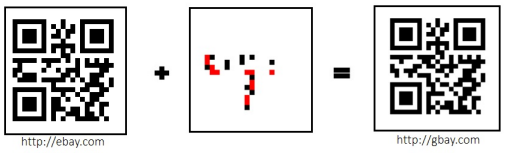

Fig. 2. The modification attack as proposed by Kieseberg et al. [27]

4 Real World Examples

In 2012 security expert Ravi Borgaonkar demonstrated how Man-Machine-Interface (MMI) codes can be used to run different attacks against Samsung devices [6], e.g. by making the phone dial the MMI code **2767*3855#* to wipe the phone. Attackers encoded this MMI code into a QR code with the prefix *tel:* to trigger the execution of the MMI code which erases all data from the mobile device. Sharma et al. [36] outlined different attacks against the automated processes of the scanning library or the scanning software. If a scanning application uses a database to store scanned entires, it is possible to execute a sql injection by scanning values such as *1' OR 1=1* – in order to circumvent authentication mechanisms. Furthermore, he outlined the threat of browser-based exploits, XSS attacks and command injections via QR codes. Jester et al. [29] changed his profile picture on his twitter account to a QR code with a shortened URL encoded. The QR Code directed victims to a webpage, which hosted hidden code exploiting a known browser vulnerability on iOS and Android. Apart from the WebKit [1] secondary exploits exposed the device to the attacker. The attacker claims that he successfully trapped 500 victims that executed the OS-specific payload. Even though researchers and security specialists are questioning the success of this attack, they confirm that this kind of attack is feasible. In [39] Moore and Edelman present a method to identify typosquatting. Typosquatting is the intentional registration of misspellings of popular website addresses. In 2010, it was estimated that there are at least 938,000 typosquatting domains targeting the top 3,264 ".com" sites, and most of these sites supported the pay-per-click ads. This information is fundamental proof that attacking a QR code in order to produce a misspelled and misleading domain name is an effective phishing attack.

5 Related User Studies

The importance of human-computer interaction aspects in QR code security has been acknowledged by the research of Seeburger et al. [35] and Vidas et al. [42]. Seeburger et al. [35] investigated how users interact with QR code stickers in urban spaces with so called *PlaceTagz*. These *PlaceTagz* were deployed in different locations in Melbourne such as cafeterias, libraries and public toilets. When a dweller scans a *PlaceTag*, he is taken to a dialog box where he can read comments

from previous visitors but also leave his own comments. Their results suggest that curiosity is the main motive for a user to scan non-contextual QR codes. With curiosity being the main motivation to interact with an unknown source, users are ignoring the security threats associated with QR codes from unverified sources or are unaware of them. Vidas et al. [42] described QR code-initiated phishing attacks by conducting two experiments in the city of Pittsburgh, a *surveillance* and a *QRishing* experiment. Within their surveillance experiment, they observed how users interacted with the code and if they scanned the codes or not. Furthermore, they observed the proportion of users who scanned the code but refused to visit the encoded URL by visually monitoring user interactions with QR codes. To do so, they deployed a poster with a QR code and a camera to record the user interactions. In the *QRishing* experiment, they deployed QR codes on three different types of posters and flyers to assess the susceptibility of such a phishing attack. In their deployed QR codes, a link to a survey was encoded. This survey contained a set of questions to identify the initiatives and the behavior of the people that scanned the QR codes. Similar to Seeburger et al. [35], Vidas et al. [42] found that curiosity is the main motivation for smartphone users to scan a code. Their findings highlight the need for further research on adequate tools to support the user in detecting potential threats as they are mostly scanning unverified codes because of their curiosity. Their research also highlights that most QR code readers do not provide feasible tools to automatically detect attacks and to minimize the impact on the user's privacy and security.

6 Open Research Challenges

Despite the fact that the use of QR codes is gaining popularity, many users are still not able to distinguish between QR codes from trusted and untrusted sources. As the results by Seeburger et al. [35] and Vidas et al. [42] suggest, scanning a QR code is not a safe practice. One of the main reasons for this is that users need to decode the QR code at first in order to decide whether the content is trusted because they are not human-readable. Even after decoding, users find it difficult to judge the trustworthiness of an encoded URL. Therefore we identify the major research challenges with respect to usability and security with QR codes and describe them in this section.

6.1 Security Awareness Challenges

Bellman et al. [4] determined that there are significant differences in how Internet users perceive privacy challenges and security vulnerabilities. Their findings alongside with the differences in consumer acceptance of QR codes amongst different nationalities suggest that people have different concerns regarding security vulnerabilities when interacting with QR codes. Based on the studies by Seeburger et al. [35] and Vidas et al. [42], another important challenge is to investigate intercultural differences in security awareness. To do so, the deployment

of stickers with QR codes (similar to *PlaceTagz* [35]) in public places like university cafeterias, bus stops and public toilets would be beneficial to investigate the differences between European and Asian users. A detailed understanding of the intercultural differences would significantly contribute to the scientific community in order to enhance awareness raising tools and support the adoption of successful security enhancements worldwide.

6.2 Usable Security Design Guidelines

Yao et al. [45] analyzed the most frequently downloaded QR code readers for Android and found that most of the readers are not able to successfully detect phishing attacks. However, a more detailed analysis on security, privacy and usability factors is necessary in order to design software that supports the user's decision making process about the trustworthiness of a URL. To support the development of a secure and usable multi-layer framework for QR code processing another important challenge is to develop design guidelines. These design guidelines should be developed in a way to harden the QR code itself, the reader software and to furthermore support the user to detect potential threats. In this section, we propose a set of requirements to support research in the areas of security and human-computer interaction with respect to the attack scenarios described in 3. We suggest to distribute the requirements in the following three categories: *(1) Secure QR Code Requirements*, *(2) Service Layer Requirements* and *(3) Usability Requirements*.

QR Code Requirements. In this section, we identify security requirements to secure the QR coding scheme. We consider coding scheme improvements as invariant to the QR code reader application.

Visual QR Codes. In case of an attack scenario (as described in Section 3) visual QR codes significantly support the user in detecting modified or replaced QR codes in urban spaces. The more complex the theme, the harder it becomes for an attacker to modify QR codes in an unobtrusive way. To make it more expensive for an attacker to replace the original QR code (e.g. in billboard advertising), we suggest to investigate the impact of complex color schemes embedded into the color scheme of the whole advertisement on the user's ability to detect malicious modifications.

Digital Signatures. In other domains, digital signatures have proven to be an effective means to improve security as shown in [17]. Therefore, we recommend to place emphasis on the integration of digital signatures in the QR code standardization to verify the originator of the code and to thereby check if the QR code has been modified. A digital signature significantly complicates QR code based attacks as the attacker needs to modify the checksum and the verification process accordingly. However, the increased amount of data to encode reduces the area to encode actual data. Furthermore, QR code readers have to be adapted

in a way to verify the digital signatures and to indicate whether the verification was successful, similar to SSL. We suggest to develop the integration of digital signatures in order to propose a specification update.

Service Layer Requirements. The challenges highlighted in this section place emphasis on securing the QR code reader application and are intended to harden secure QR codes. The overall purpose of service layer improvements is to enrich the security features embedded in the QR codes themselves and to determine whether the user's decision is necessary to obviate a malicious code.

Masking. The distribution of black and white modules in a specification-compliant QR code follows a specific pattern. This pattern is determined by the mask that is used to specify whether or not to change the color of the considered module. Due to its robustness provided by the error-correcting Reed-Solomon codes, a certain degree of corrupt pixels does not have a negative impact on decoding the QR code. The higher the deviation from an even distribution of black and white modules is, the higher the probability that the QR code is modified. A detailed analysis on the trade-off between error rate and security would be beneficial in order to use masking aspects to secure reader software.

Malicious URL Detection. In general, there are different approaches to successfully distinguish potentially malicious URLs from benign ones. However, shortened URLs can be used by an attacker to obfuscate malicious URLs. The trustworthiness of an URL can be determined by metrics as proposed by Choi et al. [8]. Furthermore, URL black- or whitelists can be used to verify the originator of encoded URLs.

Usability Requirements. In this section, we describe research challenges with respect to the user's decision making process on the trustworthiness of a QR code.

Content Display. As QR codes are non human-readable, content display is essential to inform the user about the actually encoded content. We suggest to use the findings of [13, 14] as a starting point for further research on the usability of this feature.

Content Preprocessing. In case of shortened URLs or redirects, simply displaying the encoded content does not provide enough information for the user to determine whether the encoded content is malicious or benign (as shown in [13, 14]). Therefore we emphasize the need for usable content preprocessing tools. Shortened URLs e.g. could be executed in the background in order to display the final URL to the user.

Anti-Phishing Tools. As discussed in Section 3, one of the major problems of manipulated QR codes is phishing. Zhang et al. [46] evaluated different Anti-Phishing solutions that can be further used in QR code reader software. In context of usability it is important that the verification process is transparent to the user. However similar to SSL [5, 38, 43] the main challenge is to properly inform the user about an incident [18].

Content Verification. In addition to content preprocessing before display, verification tools should be emphasized such as e.g. blacklists as proposed in [45]. As the results from [14] and [3] suggest, warnings are in many cases not effective to inform the user about possible threats and the implications of the actions they will perform. These findings highlight the need for further research regarding usable tools to indicate verified and unverified content.

7 Conclusion

In this paper, we provided a comprehensive overview of the state of the art research regarding QR code security and usability. We identified the most significant use cases and the attack vectors associated with them. To do so, we conducted an extensive literature survey. In the media, the most commonly reported fraud conducted with QR codes as attack vector is social engineering and phishing in particular. QR codes have found their way from automotive manufacturing plants into our everyday smartphone usage. They are used in advertising, authentication and even for monetary transactions where sensitive data is transferred. However, very little research has been conducted in this field. Therefore, the major goal of this work was to identify and systemize the major research challenges in the area of security and human-computer-interaction. Based on our systematization, we defined specific requirements to develop multi-layer guidelines as a first step toward the development of a secure QR code processing environment.

Acknowledgements

The research was funded by COMET K1, FFG - Austrian Research Promotion Agency and by the Josef Ressel Center for User-Friendly Secure Mobile Environments (Usmile).

References

1. The WebKit Open Source Project, 2013. available online: http://www.webkit.org/. last accessed on 02/07/2014.
2. G. M. Agusta, K. Hulliyah, R. B. Bahaweres, et al. Qr code augmented reality tracking with merging on conventional marker based backpropagation neural network. In *Advanced Computer Science and Information Systems (ICACSIS), 2012 International Conference on*, pages 245–248. IEEE, 2012.

3. D. Akhawe and A. P. Felt. Alice in Warningland: A Large-scale Field Study of Browser Security Warning Effectiveness. In *Proceedings of the 22Nd USENIX Conference on Security (SEC'13)*, pages 257–272, 2013.
4. S. Bellman, E. J. Johnson, S. J. Kobrin, and G. L. Lohse. International differences in information privacy concerns: A global survey of consumers. 20(5):313–324, 2004.
5. R. Biddle, P. C. van Oorschot, A. S. Patrick, J. Sobey, and T. Whalen. Browser interfaces and extended validation ssl certificates: an empirical study. In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 19–30. ACM, 2009.
6. R. Borgaonkar. Dirty use of ussd codes in cellular network, 2012. available online: http://www.youtube.com/watch?v=Q2-0B04HPhs. last accessed on 02/07/2014.
7. C. Dow, Y. Lee, H. Yang, W. Koo, J. Liao . A location-based mobile advertisement publishing system for vendors. In *Eighth International Conference on Information Technology: New Generations*, pages 24–29, 2011.
8. H. Choi, B. B. Zhu, and H. Lee. Detecting Malicious Web Links and Identifying Their Attack Types. In *Proceedings of the 2Nd USENIX Conference on Web Application Development (WebApps'11)*, pages 11–11, Berkeley, CA, USA, 2011. USENIX Association.
9. D. Lorenzi, B Shafiq, J. Vaidya, G. Nabi, S. Chun, V. Atluri. Using QR codes for enhancing the scope of digital government services. In *Proceedings of the 13th Annual International Conference on Digital Government Research*, pages 21–29, 2012.
10. D. Pirrone, S. Andolina, A. Santangelo, A. Gentile, M. Takizava. Platforms for human-human interaction in large social events. In *Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*, pages 545–551, 2012.
11. David Moth. PayPal trials QR code shop in Singapore subway, 2012. available online: http://econsultancy.com/at/blog/8983-paypal-trials-qr-code-shop-in-singapore-subway. last accessed on 02/07/2014.
12. DENSO Wave Incorporated. What is a QR Code?, 2013. available online: http://www.qrcode.com/en/. last accessed on 02/07/2014.
13. J. S. Downs, M. Holbrook, and L. F. Cranor. Behavioral Response to Phishing Risk. In *Proceedings of the Anti-phishing Working Groups 2Nd Annual eCrime Researchers Summit (eCrime'07)*, pages 37–44, New York, NY, USA, 2007. ACM.
14. S. Egelman, L. F. Cranor, and J. Hong. You'Ve Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the 2008 SIGCHI Conference on Human Factors in Computing Systems (CHI'08)*, pages 1065–1074, 2008.
15. Esponce. Innovative QR Code campaigns (About QR codes), 2013. available online: http://www.esponce.com/about-qr-codes. last accessed on 02/07/2014.
16. Esponce. Innovative QR Code campaigns (Real world case studies), 2013. available online: http://www.esponce.com/case-studies. last accessed on 02/07/2014.
17. C. Hanser and D. Slamanig. Blank digital signatures. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 95–106, New York, NY, USA, 2013. ACM.
18. M. Harbach, S. Fahl, T. Muders, and M. Smith. Towards measuring warning readability. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 989–991. ACM, 2012.
19. I. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. 8(2):300–304, 1960.

20. J. Gao, V. Kulkarni, H. Ranavat, Lee Chang Hsing Mei. A 2D barcode-based mobile payment system. In *Third International Conference on Multimedia and Ubiquitous Engineering*, pages 320–329, 2009.
21. J. Wang, C. Shyi, T.-W. Hou, C.P. Fong. Design and implementation of augmented reality system collaborating with QR code. In *International Computer Symposium (ICS)*, pages 414–418, 2010.
22. P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl. Qr code security. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, pages 430–435. ACM, 2010.
23. J. Korkidis. The world's first qr-code hair cut. available online: http://www.complex.com/art-design/2011/11/the-worlds-first-qr-code-hair-cut, last accessed 04/02/2014.
24. J. Leyden. That square QR barcode on the poster? Check it's not a sticker.
25. M. Ebling, R. Caceres. Bar Codes Everywhere You Look. 9(2):4–5, 2010.
26. Matthew Talbot. QR Codes: Scanning For Loyalty And Payment, 2013. available online: http://blogs.sap.com/innovation/industries/qr-codes-scanning-for-loyalty-and-payment-3-025064. last accessed on 02/07/2014.
27. P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, E. Weippl. Qr code security. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, MoMM '10*, pages 430–435, 2010.
28. K. G. Paterson and D. Stebila. One-time-password-authenticated key exchange. In *Proceedings of the 15th Australasian Conference on Information Security and Privacy*, ACISP'10, pages 264–281, Berlin, Heidelberg, 2010. Springer-Verlag.
29. Paul Wagenseil. Anti-Anonymous hacker threatens to expose them, 2012. http://www.nbcnews.com/id/46716942/ns/technology_and_science-security/. Accessed 02/07/2014.
30. Q. Pay. Qr pay - scan, pay, done. available online: http://www.qrpay.com/. last accessed on 02/07/2014.
31. QRStuff. QR Code Error Correction, 2011. available online: http://www.qrstuff.com/blog/2011/12/14/qr-code-error-correction. last accessed on 02/07/2014.
32. QRStuff. What's a QR Code?, 2011. available online: http://www.qrstuff.com/qr_codes.html. last accessed on 02/07/2014.
33. J. Rouillard and M. Laroussi. Perzoovasive: contextual pervasive qr codes as tool to provide an adaptive learning support. In *Proceedings of the 5th international conference on Soft computing as transdisciplinary science and technology*, pages 542–548. ACM, 2008.
34. Russ Cox. QArt Codes, 2012. available online: http://research.swtch.com/qart. last accessed on 02/07/2014.
35. J. Seeburger. No cure for curiosity: linking physical and digital urban layers. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, pages 247–256. ACM, 2012.
36. V. Sharma. A study of malicious qr codes. 3(3), May 2012.
37. J. Steeman. QR code data capacity, 2004. available online: http://blog.qr4.nl/page/QR-Code-Data-Capacity.aspx. last accessed on 02/07/2014.
38. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of ssl warning effectiveness. pages 399–416, 2009.
39. T. Moore, B. Edelman. Measuring the perpetrators and funders of typosquatting. In *Proceedings of the 14th international conference on Financial Cryptography and Data Security, FC'10*, pages 175–191, 2010.

40. Thonky.com. QR Code Tutorial, 2012. available online: http://www.thonky.com/qr-code-tutorial/. last accessed on 02/07/2014.
41. Ugo B. Ceipidor, Carlo M. Medaglia, A. Perrone, M. De Marsico, G. Di Romano. A museum mobile game for children using QR-codes. In *Proceedings of the 8th International Conference on Interaction Design and Children, IDC '09*, pages 282–283, 2009.
42. T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *Proceedings of the 2013 Workshop on Usable Security (USEC'13)*, 2013.
43. N. Vratonjic, J. Freudiger, V. Bindschaedler, and J.-P. Hubaux. The Inconvenient Truth about Web Certificates. pages 79–117, 2013.
44. Y. Kao, G. Luo, H. Lin, Y. Huang, S. Yuani. Physical access control based on QR code. In *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pages 285–288, 2011.
45. H. Yao and D. Shin. Towards preventing qr code based attacks on android phone using security warnings. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*, pages 341–346. ACM, 2013.
46. Y. Zhang, S. Egelman, L. Cranor, and J. Hong. Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)*, 2007.