

PAPER • OPEN ACCESS

Design of Secure Enhanced Privacy Protection Electronic Hotel-card Based on QR Code

To cite this article: Eryang Chen *et al* 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* **565** 012006

View the [article online](#) for updates and enhancements.



IOP | ebooks™

Bringing you innovative digital publishing with leading voices to create your essential collection of books in STEM research.

Start exploring the collection - download the first chapter of every title for free.

Design of Secure Enhanced Privacy Protection Electronic Hotel-card Based on QR Code

Eryang Chen, Ansheng Ye*, Fang Miao, Wenjie Fan and Yi Jiang

School of Information Science and Engineering, Chengdu University, Sichuan province, China

*Email: cey@cdu.edu.cn

Abstract. The development of the Internet and economy urges researchers to look for a safe and more economical way to secure online hotel-users' private information. This study is rooted in online-hotel user personal privacy and some information protection. The traditional RFID hotel-room card was replaced by the proposed QR e-ID, which combines cryptography, verification code, passwords and multi-directional identity authentication module. All of the privacy information should be registered in the data register center (DRC) with encrypted mode. In order to ensure safety in case if the QR e-ID is used by unknown person it needs a password. The main goal of this study is to investigate how the co-use of computers and mobile devices protect online hotel-users' private information, in addition, reduce the hotel operating costs effectively. The results of the study also provide guidelines to IT developers for future directions in virtual assets protection.

Key words: Personal Privacy, QR e-ID, Multi-directional Identity Authentication, Virtual Assets Protection

1. Introduction

With the development of the Internet, 4G/5G technology and economy, for one thing, smartphone has become an impartible part of life for many people, for another, more and more people choose to visit other places during holidays, booking hotels online. It provides utility by assisting front office process before checking in, however, it has a underlying risk because personal privacy and some information may be exposed in public [1]. Because the information privacy and security issues have not attracted sufficient attention from individual uses, or hotel backstage database may be attacked by hackers [2]. Although personal privacy and some information protection has been discussed on media for quite a long time [3].

For example, credit reporting firm Equifax (US) suffered one of the worst security breaches in history when it announced that sensitive data--including Social Security numbers and driver's license numbers of more than 147 million consumers were exposed to hackers from mid-May to July 2018 [4]. Both The New York Times and Observer broke the news that 50 million profiles of Facebook users were "harvested" without their consent to a consulting firm, Cambridge Analytica in March 2018 [5]. In August 28th 2018, the Internet broke the news that the users data of HuaHua Groups chain hotel were suspected to have leaked. About 500 million information leaks cover all personal information, and the data include Hanting Hotel, Mercure, Xiyu, Wanxin, Novotel, Mercure, CitiGo, Orange, Season, Star Trek, Ibis, Elite, Haiyou and other hotels [6].



To provide an alternative of authentication for online accounts, QR code (Quick Response Codes) is introduced. QR codes were initially used in Marketing for advertising purpose for its strong ability to store identification information of the advertiser and its convenience to use [7]. For example, the only way to log in WeChat in PC is to scan the QR code by a mobile phone or a pad. This study would help practitioners understand how QR codes mitigate online users' fears of threats to their privacy and security.

2. Literature review

QR code was initially invented for the automotive industry in Japan in the early 1990s. Similar to bar codes, QR codes technically are machine-readable optical labels using two-dimensional barcode to store information of the item to which it is attached or associated. A QR code uses four standardized encoding modes such as numeric, alphanumeric, byte/binary, and kanji (the subset of Chinese characters used in the Japanese language) to store data efficiently [8]. Graphically, a QR code consists of black squares arranged in a square grid on a white background, including five areas: finder pattern, alignment pattern, timing pattern, quiet zone, and data area, and each area has its unique functionality [9].

The QR code became popular outside the automotive industry due to its fast readability and greater storage capacity compared to standard UPC barcodes. The symbol versions of the QR Code range from Version 1 to Version 40 [10]. Each version has a different module configuration, which refers to the number of modules contained in a symbol, commencing with Version 1 (21×21 modules) up to Version 40 (177×177 modules). Each QR Code symbol version has the maximum data capacity, according to the amount of data, character type and error correction level.

Today, marketers are creating exciting, new cross media strategies by including digital QR codes on printed pieces across the marketing mix; from collateral to bill statements to signage and product placement, the applications are endless. In other words, QR Codes are called the link between the Electronic and Paper Worlds.

G.PRABAKARAN [11] proposed the authentication system based privacy protection QR-code, that allows the user to safely enter credentials and information to transfer money after launching LIVE-CD on stand alone in place and avoiding the possibility of entering credit card details (send or receive money without using of credit cards). The entered information is encrypted by common key crypto system and stored in a QR (quick response) code. YAN Wen-bo [12] proposed a privacy-preserving scheme for logistics systems based on 2D code and information hiding.

3. Research models

3.1. DRC

Whether information security or network space security, data is the most core security goal. Especially in the open environment, the safety of data and the safe application of data face great challenges. The data is encrypted and stored in the data registration center (DRC), and the system can only be used legally after authorization. This approach makes sense for data security and data security applications [13].

3.2. QR e-ID

A QR e-ID will be automatically generated for the current user after the order is completed. The QR e-ID contains the basic information of the guest room and the identity information of the guest. Therefore, the security of the QR e-ID is an important issue. The DRC plays an important role in improving the QR e-ID safety. Figure 1 shows Mutual information between the database and the QR e-ID.

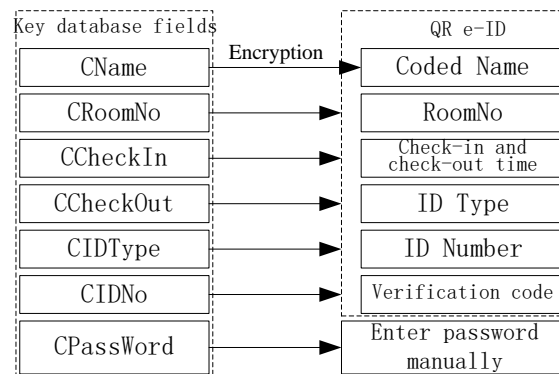


Figure 1. Mutual information between the database and the QR e-ID

In order to improve the security of the QR e-ID as much as possible, the security measures are as follows:

- (1) The security of background data is ensured by the DRC.
- (2) The customer's name is coded as a combination of letters. If the tenant's name is in Chinese, the initials of the Chinese phonetic alphabet will be extracted; If the tenant's name is in English, the initial combination of English letters will be extracted. So that, even if the QR e-code was stolen, it is difficult to obtain the customer's real information directly.
- (3) A set of verification codes is coded according to the guest and booking information. Even if the basic information of the customer and reservation is compromised, the correct verification code cannot be generated, which can avoid the forgery of the QR e-code.
- (4) Each QR e-code requires the user to set up a set of personal passwords, whose length is no less than 6.

3.3. Illegal user identification

According to relevant national laws and regulations, guests must provide their ID card to verify their real information when they check-in for the first time. IT combines cryptography, verification code, and passwords. And this is called the multi-directional identity authentication module shown in Figure 2.

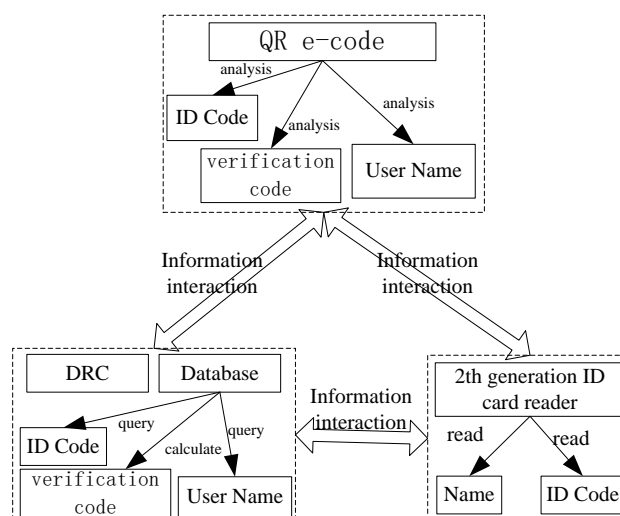


Figure 2. The multi-directional identity authentication module

The name and the ID code read by the 2th generation ID card reader is marked as Name_A and ID code_A; the name, the ID code and the verification code read from the QR code is marked as Name_B,

ID code_B and verification code_B; With ID code_A as the query keyword, DRC and database are queried. The results are marked as Name_C and ID code_C, and verification code_C is calculated.

When customers check in, the verification process is as the follows:

- (1) Only when Name_C or ID code_C is not NULL, then real name authentication passed.
- (2) Only then Name_B = Name_C, ID code_B = ID code_C and verification code_B = verification code_C, then the QR e-code is not a fake.
- (3) When the password entered by the user matches the system successfully, the guest room will open automatically.
- (4) A set of passwords (the password length is not less than 6) is set by the user. After being encrypted by MD5, the password exists in the database as ciphertext, and the tenant enters the password to verify the system.

3.4. Calculation mode of the verification code

The ID number in mainland China is 18 in length, and the bit 18 is a number or a letter "X". Bit 4 to bit 10 is hidden when the QR is coded. And bit 11 to bit 18, check-in time, check-out time and the length of passwords combines to a set of number, according to which the verification code is coded. From beginning to end, each two-digit number is coded as a letter. And the mapping rules $f(m)$ are as follows:

$$\left\{ \begin{array}{l} 01 \rightarrow 'A' \\ 02 \rightarrow 'B' \\ \dots \\ 26 \rightarrow 'Z' \end{array} \right. \quad (1)$$

Take the two-digit number n_1n_2 as an example, the code result α can be expressed as:

$$\alpha = \left\{ \begin{array}{ll} \text{Null}, & n_1n_2 = 00; \\ f(n_1n_2), & 01 \leq n_1n_2 \leq 26; \\ f(n_1)f(n_2), & n_1n_2 \geq 26; \end{array} \right. \quad (2)$$

4. Experiment

4.1. Example

This section shows the actual effects of a QR e-id card, illustrated with the data of a virtual customer. Customer information and room reservation information are as follows:

Name: MaJianlong; RoomNo:303; Check-in Time: May 1, 2018; Check-out Time: May 3, 2018; Certificate type: ID Card; Certificate No:510123199606270066. The user's personal password is 0123456abc. Based on the above information system, the verification code can be calculated as :FBGBHFFTREATRECJ.

The QR e-card is shown in Figure 3.



Figure 3. The QR e-card

The information contained in QR is: CName:MJL; CRoomNo:303; CCheckIn:20180501; CCheckOut:20180503; CIDType:001; CIDNo:510*****06272866; Parameter_VerificationCode:FBGBHFFTREATRECJ.

During the valid time of booking, the customer can check in after entering the personal password “0123456abc” as prompted by the system.

4.2. Security evaluation

The evaluation of the security is shown in Figure 4.

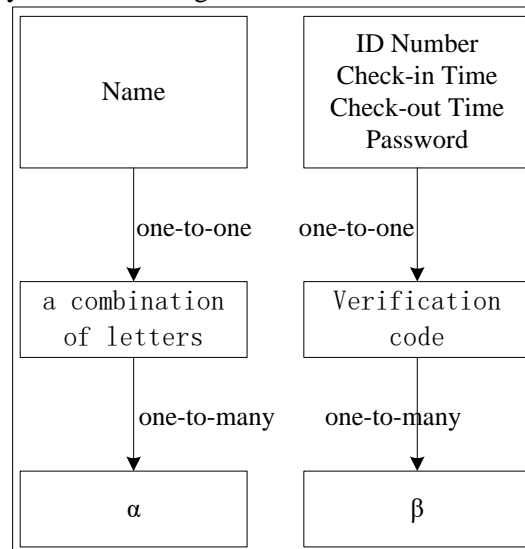


Figure 4. The evaluation of the security

The security of the system can be illustrated by the example in section 4.1.

According to the homophone characteristics of Chinese characters, α . Bit 11 to bit 18 of the ID Number, check-in time, check-out time and the length of passwords combines to a set of number ‘06272866201805012018050310’. And there are at least 2 scenarios for β . In addition, the password whose length is 10 consists of capital letters, small letters, and Numbers. Therefore, the number of passwords can be expressed as (3):

$$f(\gamma) = (26 + 26 + 10)^{10} \approx 3.0331e+17 \quad (3)$$

Based on the above description, there are more than $3 \times 2 \times f(\gamma)$ possibilities for one QR e-code card. The system has high security.

5. Conclusion & future enhancement

This paper presents an alternative method for authentication in hotel room management. Basically this method involves the Check-in process by keeping the QR-CODE at the core part. Here we have made a progress in the user perspective of implementation of the technology. Use of the traditional RFID hotel-room card by using the QR e-code card, which co-use computers and mobile devices to protect online hotel-users’ private information, in addition, reduce the hotel operating costs effectively.

The whole process is carried out by encrypting the data of hotel-users’ private information and generating the QR e-code. This project can be further improved by increasing its application areas by implementing it in virtual assets protection, in addition to the electronic hotel-card.

Acknowledgments

The work is supported by National Key Research and Development Program under Grant 2016YFB0800600, Opening Fund of Geomathematics Key Laboratory of Sichuan Province (csxdz201710), Key Laboratory of Pattern Recognition and Intelligent Information Processing, Institutions of Higher Education of Sichuan Province, Chengdu University, Funding MSSB-2018-0. Sichuan support Plan(No.2016FZ0112).

References

- [1] Crossler, R.E., et al., Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap, in *Journal of Information Systems*. 2014, American Accounting Association. p. 209-226.
- [2] Meso, P., Y. Ding, and S. Xu. Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information Privacy & Security*, 2013. 9(1): p. 47-67.
- [3] Tank A H, Unde M M, Patel B J, et al. Storage and transmission of information using grey level QR (quick-response) code structure[C]// *Advances in Signal Processing*. IEEE, 2016:402-405.
- [4] Credit firm Equifax says 143m Americans' social security numbers exposed in hack, <https://www.theguardian.com/us-news/2017/sep/07/equifax-credit-breach-hack-social-security>.
- [5] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- [7] Wang J S, Zhang J N. Design and Realization of Hotel Management System[J]. *Computer Engineering & Design*, 2011, 2(1):1173-1176.
- [6] Hotel group probes private info leak of 130 million clients, <http://www.globaltimes.cn/content/1117459.shtml>.
- [8] Kroenke, D., *Experiencing MIS*, in 5/E. 2014, Prentice Hall. p. 696.
- [9] Kan, T.-W., C.-H. Teng, and M.Y. Chen, QR Code Based Augmented Reality Applications, in *Handbook of Augmented Reality*, B. Furht, Editor. 2011, Springer: New York. p. 339-354.
- [10] QR Code Tutorial, <http://www.thonky.com/qr-code-tutorial/>
- [11] Prabakaran G, Bhakkiyalakshmi R, "Transmission of Data Using Arm Based Privacy Protection QR-code", *International Journal of Engineering Development and Research (IJEDR)*, ISSN:2321-9939, Vol.2, Issue 2, pp.1458-1461, June 2014.
- [12] YAN Wen-bo, YAO Yuan-zhi, et al. Privacy-preserving scheme for logistics systems based on 2D code and information hiding[J]. *Chinese Journal of Network and Information Security*, 2017, 3(11):22-28.
- [13] MIAO Fang. Data Oriented Security Architecture[J]. *ZTE Technology Journal*, 2016(1):19-22.