The Security Threat and Precautionary Measures of QR Code of Internet of Things Technology

Xinyu Niu[1], Jiandao Zhao[2], Bo Tian[2]

[1]Beijing Research Institute of Automation For Machinery Industry, Beijing 100120, China

[2]RIAMB (Beijing) Technology Development Co., Ltd. Beijing 100120, China

Abstract. The Internet of Things (IoT) is the expansion and extension of the traditional network. It is a network that connects goods and objects, which has been widely used in today's social development process. It occupies an important position in various industries. The emergence of the Internet of Things has greatly improved the refinement level of human management. The QR code (Quick Response Code) is a part of the perception layer of the IoT, which belongs to the perception and recognition technology of the IoT. The QR code not only brings convenience to users but also becomes the carrier and disseminator of malware, phishing, and other attacks. Therefore, it is of great significance for the security of the IoT to understand the potential threats of the QR code, analyze its potential attack methods, and put forward defense plans. This paper briefly introduces the basic characteristics of the QR code, as well as some attack methods and potential threats against the QR code, and put forward some preventive measures from both technical and non-technical aspects. The technical aspect includes the combination of cryptography and the introduction of third-party management. The non-technical aspects are discussed at the national and individual user levels.

Keywords: QR code, Internet of Things, security.

1. Introduction

The IoT is the expansion and extension of the traditional network. It has been widely used in today's social development process and occupies an important position in various industries. Whether it is daily household, buildings, roads, oil and gas pipeline design and other large-scale facilities, as long as these areas are equipped with intelligent cameras and various sensors, they can be intelligently identified and managed. To some extent, the emergence of the IoT has greatly improved the refinement level of human management. The IoT is a network where goods and objects are connected. Its basic features can be summarized as comprehensive perception, reliable transmission, and intelligent processing. The QR code is a part of the perception layer of the IoT and belongs to one of the perception and recognition technologies of the IoT. Like the human sensory system, the perception layer of the IoT is the interface for the internal core of the IoT to collect external data [1].

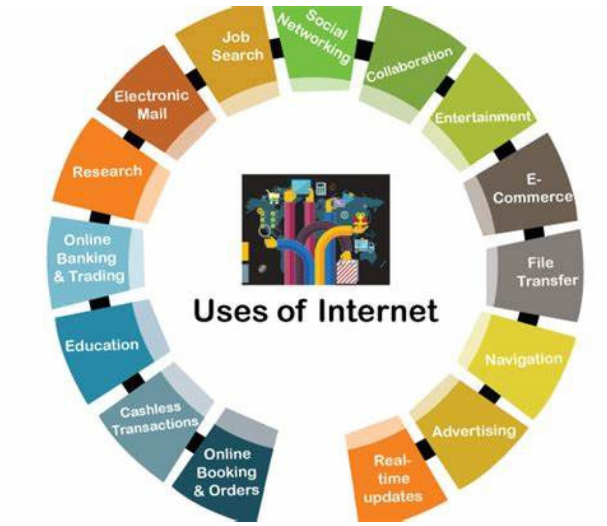

Fig. 1. Uses of Internet

The identification, perception, processing, and information transmission linkages are the four links that make up the Internet of Things. The key technologies span wireless communication, computer technology, automatic control, information sensing, information recognition, and other fields. Among them, QR code, as one of the key technologies in the field of information identification, has been formally introduced into China's mobile communication value-added services since 2006. With mobile terminals and the mobile Internet as the channels for the storage, interpretation, processing, and dissemination of QR code, various QR code mobile value-added services have emerged in various forms. After several years of market turmoil, the applications that meet the needs of the Chinese market are gradually clear, and the relevant industrial chain is also close to maturity. RFID, as another key technology in the field of information identification, has its own advantages and limitations and different applications from QR code. This paper summarizes the attack methods of QR code and some potential security threats and puts forward some preventive measures.

Fig. 2. QR code application scenario.

2. Basic concept of QR code&development status

The QR code is a coding method. It records information through the black and white images formed by the regular distribution of specific geometric shapes on the two-dimensional plane. After the images are read, the corresponding rules of these shapes and binary systems are used to realize the automatic recognition of data symbols. The QR code is a more advanced format than the one-dimensional barcode: one-dimensional barcodes can only record information in one direction, while the QR code can record information in both horizontal and vertical directions. One-dimensional barcodes can only be composed of numbers and letters, while two-dimensional codes like QR can store information such as Chinese characters, numbers, and pictures. In general, the QR code has characteristics such as large data storage, high confidentiality, high traceability, strong damage resistance, large backups, low cost, strong interaction, and good experience, which can be better combined with mobile terminals such as smartphones.

The application of QR code developed earlier. As early as the 1980s, fast food restaurants and convenience stores in Japan and South Korea used QR codes on leaflets and coupons. Later, they gradually developed to use QR codes as admission tickets for movies and performances. The audience only needs to scan the codes on specific equipment to enter. Currently, relevant applications such as registration and payment by scanning encrypted QR codes have become very popular. After the 2008 Beijing Olympic Games, QR codes began to be popularized in China, including film tickets, boarding passes, train tickets, etc. Especially with the popularity of Alipay and WeChat payment, scanning code for payment has become a part of daily life. At present, QR code will be or is being widely used in customs/tax collection and management, document and book circulation management (China's State Council is promoting official document management, and QR code technology has become popular); vehicle management, bill management (almost covering all industries), payment applications (e.g. electronic receipt), asset management, and industrial production process management.

3. QR Code Attacks and Security Threats

The security protection of two-dimensional code has always been a research hotspot. Insufficient unified management specifications can lead to security risks like information disclosure and alteration via QR codes, as the data content and production source are hard to monitor, the coding and decoding process is entirely open, and the quality of the reading software varies[3].

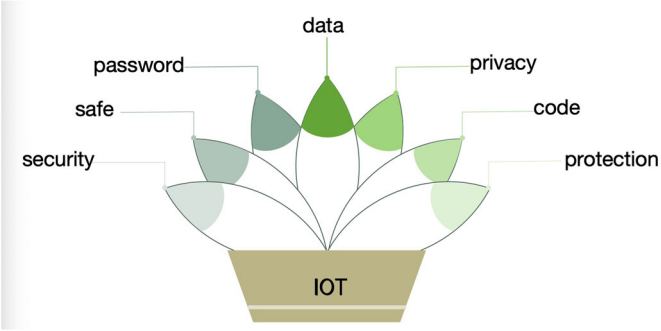

Fig.3. Security of Iinternet of Things.

Attacks against QR code show a variety of characteristics, mainly including the following four categories.

Induce the user to log in to the malicious website: A. Attackers only need to create QR codes for links to malicious websites such as forgery, fraud, or phishing, inducing users to scan and log in to the website to obtain sensitive personal information and financial accounts entered of the user.

Trojan horse implantation: The attacker compiles the command of automatically downloading malware into QR codes. When users scan such QR codes without protective measures, the user's system will be quietly implanted with Trojan horses, worms, or hidden software. Attackers can wantonly destroy user files, steal user information, and even remotely control users, sending charging SMS messages in groups, etc., in the backstage.

Information hijacking: Information theft: In order to make it easier for customers to pay, a lot of companies offer online payment options like scan-to-pay. The online payment platforms create two-dimensional codes based on user orders. Attackers will directly harm users and businesses financially if they manage to obtain user and company communication information and maliciously alter orders.

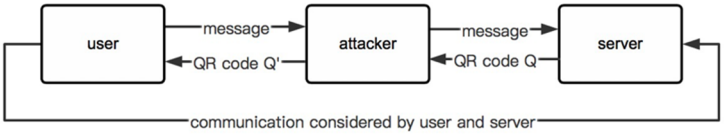

Fig. 4. Flow Chart of Message Hijacking.

Web attack: With the maturity of mobile browser functions, users can enter website domain names or submit Web forms through mobile phones. The attacker takes advantage of the vulnerability of the Web page to encode illegal SQL statements into the QR code. When the user logs in to the Web page using the QR code scanned by the mobile phone, the malicious SQL statement will be automatically executed (SQL injection). If the database prevention mechanism is fragile, the database will be invaded, which will lead to more serious harm.

4. Some Preventive measures

4.1 Technical aspects

4.1.1 Combined Cryptography Method

For the problem of QR code forgery, Common encryption methods and message authentication codes can be used to add encryption and decryption links to the original QR code encoding and decoding. Taking asymmetric encryption as an example, suppose that the original information is M0,

the private key of the issuer is Kr, and the public key is KU, then M'=EKr(M). The M' information is encoded with a QR encoder, and the generated QR code and public key are published on the printed matter. The user enters the public key KU when scanning the QR code. If the correct and readable information can be decoded, the scanned QR code is reliable. The asymmetric encryption method cannot only resist the attacks of above application scenarios, but also resist the tampering behavior of most QR code information.

Including an encrypted hash value module in the QR code is another way to make things simpler. Figure 6 illustrates how the decoder decrypts the hash value during decoding and compares it to the original QR code data. Two-dimensional code leakage can be prevented by using the symmetric encryption approach. Only the key holder can decode the encrypted two-dimensional code normally, that is, the two-dimensional code can be used for specific objects, such as the two-dimensional code on the train ticket.[4]

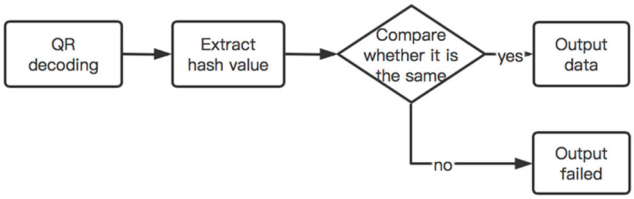

Fig. 5. The decoding process of introducing hash values.

4.1.2 Introduce Third Party Method

The market for QR codes is in disarray since there are no third-party management or certification systems, nor matching coding standards for the various uses of QR codes. By using third-party management and authentication, dangerous websites and fraudulent information transmitted by QR codes may be efficiently intercepted. Moreover, by offering an authentication method, the source's credibility can be increased. The steps involved are as follows: Prior to linking to the third-party server, the user's smartphone scans the information included in the QR code. Subsequently, the code number information included in the QR code is used by the third-party server to query the database. The database will return the queried website to a third-party resolution server, which will return the user's merchant link address, and finally link the user to the merchant address[5].

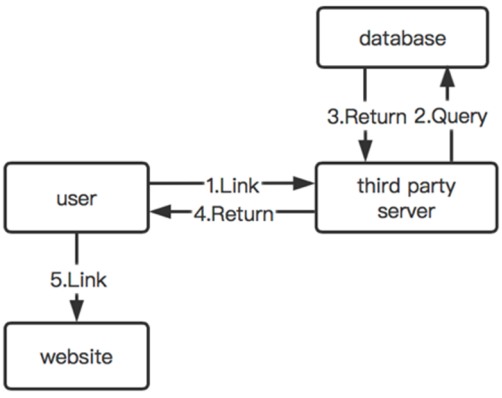

Fig. 6. Introduce a third party to manage the website.

4.1.3 Other methods

In addition to the password-based secure QR code method, there is also a QR code protection algorithm based on information hiding. This algorithm changes the shape of the QR code by embedding some secret information in the two-dimensional code, so that the attacker cannot know its content. The embedded information can be extracted normally to recover the QR code losslessly.

4.2 Non technical aspects

4.2.1 The state strengthens supervision

The first task of supervision is to supervise the QR code producers and publishers. This work mainly includes the following aspects: It is necessary for application stores to establish a long-term mechanism for the security detection, evaluation, and notification of QR code production and scanning software; guide users to choose QR code software with a high security level; the QR code application software developer signature mechanism should be implemented to make the application software traceable throughout the process. At the same time, it is necessary to standardize the network security management process of QR code release. In addition, the supervision also needs to encourage developers to develop and promote secure QR code software and improve the security detection capabilities of QR code production and scanning tools [6].

4.2.2 Users improve safety awareness

Users should master some knowledge, common criminal techniques and cases about QR codes, and improve their security awareness. At the same time, we should develop a good habit of using mobile phones. First, download the tool software on the official website. Second, do not scan the code casually. The QR code of unknown origin published on the street and online need to be vigilant. Then, anti-virus software needs to be installed in the phone. In addition, learn to use the law to safeguard the legitimate rights and interests of individuals.

5. Conclusion

At present, the widely used QR code has not only brought convenience to users, but also become the carrier and disseminator of malware, phishing, and other attacks. Therefore, it is of great significance for the security of the IoT to understand the potential threats of QR codes, analyze their potential attack methods, and propose defense plans. This paper briefly introduces the basic characteristics of the QR code, as well as some attack methods and potential threats against the QR code, and puts forward some preventive measures from the technical and non-technical aspects. The technical aspects include the combination of cryptography and the introduction of third-party management. The non-technical aspects are described at the national and user levels.

References

[1] Sun Qibo, Liu Jie, Li Xuan, Fan Chunxiao, Sun Juanjuan, “The Internet of Things: a review of the concept, architecture and key technologies [J],” Journal of Beijing University of Posts and Telecommunications, 2010, pp. 1-9.

[2] Chen Jinghua, Wang Jie, “Analysis on the Application and Development of Mobile QR Code in the Internet of Things [J],” Telecommunication Science, 2010, pp. 39-43.

[3] Gao Yanshou, “Security Implementation and Design Analysis of QR QR Code [D],” Nanjing University of Technology, 2013.

[4] Zeng Zijian, “Research and Implementation of QR QR Code Encoding and Decoding Technology [D],” University of Electronic Science and Technology of China, 2010.

[5] Lin Jiahua, Yang Yong, Ren Wei, “Attack Methods and Defense Measures of QR QR Code [J],” Information Network Security, 2013, pp. 29-32.

[6] Wang Weihua, “Research on the Prevention and Control Path of QR Code Crime Governance [J],” Journal of Liaoning Police College, 2022, pp. 68-76.