Optimized Secure Payment Solution Using QR Code Scanning based on Operation-payment Dual Devices

Ruohan Xu

Nanjing Foreign Language School, Nanjing 210008, China

Abstract. With the development of the internet and mobile payment technology, the mobile payment transaction volume in China is rising year by year. Likewise, an increasing number of people are using mobile payments for their convenience and stability. In recent years, however, security incidents involving these mobile payments have also occurred more frequently. Some lawbreakers have been known to add illegal information to QR codes so that the mobile phones of unwitting customers are infected with viruses when they scan the codes to make payments. These viruses result in losses of personal property. In view of this, we propose an optimized secure payment solution for QR code scanning based on Operating-payment dual devices. This sets a separation of the payment process by utilizing both an operating device and a payment device, so as to minimize losses when customers scan malware-infected QR codes. Through theoretical analysis, our proposed solution can effectively improve the security of QR code payments, and meet the requirements for secure payment in daily life.

Keywords: Mobile Payment; QR Code; Information Security; Optimized Payment Solution.

1. Introduction

As science and technology have continued to develop rapidly, mobile payments have made large inroads across various industries in China. The market survey shows that China's mobile payment transaction volume reached RMB 27.74 billion in 2018. We can conclude from Figure 1 [1] that China's third-party mobile payment transactions have increased significantly, with growth rates as high as 400% in 2014 and 2016. After 2017, the rate of development has gradually slowed down, although there is still a strong growth momentum. Overall, the development of third-party mobile payments in China is on the rise.

Figure 1. China Third Party Mobile Payment Transaction Scale and Projection in 2014-2018

Today, QR code payment has become the main method of payment day-to-day for the general public, with the vast majority of supermarkets and websites accepting payment by WeChat and Alipay. In the long run, China needs to promote digital RMB, which will be intrinsically linked to the basic payment method of scanning a QR code. QR code payments will become the mainstream payment method in the long run.

However, as mobile payment becomes more closely tied to people's work and personal lives, people are also becoming aware of the security problems involved in this type of payment method.

There are common cases of hackers gaining entry to payment systems using leaked passwords. If a virus is placed into a payment QR code, it is very likely to have an adverse impact on the scanning device. Therefore, improving payment security has become imperative.

In order to address this pressing issue, we propose an optimized secure payment solution for QR code scanning based on Operating-payment dual devices. The key components of this solution are as follows:

- 1). Divide the payment process into two parts: Operating-payment and payment-code scanning. This is very effective in avoiding attacks on the operating device from malware-infected QR codes.
- 2). Connect the operating device and the payment device through SSL. This can establish a reliable channel for exchanging information and ensure that the personal information held within the device will not be leaked.

2. Related Work

2.1 Multi-factor Authentication Technology

Multi-factor authentication technology[8] refers to the technology that applies two or more different conditions to verify users' identity. Passwords are usually combined with physical objects, as shown in Figure 2. This technology is widely used in the online payment industry since it can effectively improve the security and convenience of payments. The technology is designed to establish a multi-level defense system, making it more difficult for unauthorized people to access the computer system or network. In general, there are three different types of authentication:

(1) What does the user know? This low-security type of authentication is usually knowledge-based authentication, such as asking the user's mobile phone number and birthday. Once the user's information is leaked, the account is exposed to intruders.

(2) What does the user have? This generally refers to the identification items held by the user, such as a security token or smart card. Compared with "What does the user know?", this type of authentication has improved security.

(3) Who is the user? This high-security type of authentication is usually the user's biometric information, such as fingerprint or voice verification. However, the operation can be relatively complex, and sometimes the fingerprint or voice cannot be recognized.

Figure 2. Technology Model of Multifactorial Authentication Identification

With businesses' systems increasingly exposed to external users and ever more complex threats, the convenience inherent in passwords is far outweighed by the risks they can bring. As a result, many businesses adopt Multi-factor authentication technology to reduce the risks related to access control and liability.

2.2 SSL Connection Mode

In the traditional computer network system, the TCP/IP protocols have the benefit of secure and reliable transmission. However, following the maturity and development of network systems, it has become increasingly evident that the original TCP/IP protocols are insecure. Moreover, the requirements for data encryption performance are also becoming more demanding. SSL (Secure Socket Layer)[2][6] emerged as a result of these factors. This end-to-end connection mode proposed by Netscape has gradually become popular, so that many websites now support access based on SSL, and its identity verification and data encryption transmission functions can be fully utilized. Taking the GitHub website as an example, the cloud server and local devices can be connected through SSL in a fast and secure manner.

SSL protocol is similar to the TCP protocol, but with a few key differences. SSL protocol can be divided into two layers. The first layer is the SSL record protocol, which needs to be established on reliable transmission lines, in order to provide more service support for high-level protocols. The second layer is the SSL handshake protocol, which, unlike TCP's three-way handshake, needs to be built on the basis of the record protocol to confirm the identity of both sides of communication. These two layers of protocol support and complement each other to make SSL protocol one of the most secure and reliable transport protocols widely in use today.

The SSL protocol mainly offers the following services: ①Identify the target server to ensure that the data can be safely and accurately delivered to the target server; ②Protect the data during transmission to prevent data from being disturbed, stolen or even tampered with; ③Protect data integrity to prevent errors such as data loss, repetition and change during transmission. Because of the high security performance and confidentiality of the SSL protocol, SSL is used as the method of connection between the operating device and the payment device for the solution discussed in this paper.

2.3 QR Code Recognition Technology

With the rapid expansion of the internet, the number of internet users in China has increased year on year. According to the *Statistical Reports on Internet Development in China* released by the China Internet Network Information Center, Chinese internet users account for 20% of the world's total internet users, with the number reaching as high as 989 million[3]. The internet penetration rate in China amounts to 70.4%, which is higher than the global average. The "epidemic prevention health code", which is a QR code used to display COVID-19 infection status, was launched during the COVID-19 epidemic. More than 900 million people have now applied and it has been used more than 40 billion times. Evidently, the use of QR codes has become very important in our lives.

The QR code is a kind of matrix two-dimensional bar code [4] [5] developed by a Japanese company, Denso in September 1994. Compared with the instability and low information storage density of the one-dimensional code, QR codes are characterized by their strong stability, high reliability and large information capacity. In addition, they can represent more different forms of information containing numbers and letters, such as text, symbols and images, with strong secrecy and anti-counterfeiting performance. With the development of information technology, this coding method has become increasingly popular on mobile devices in recent years, as it can store more information and represent more data types than traditional bar codes.

As QR code recognition is specific and targeted, it is widely used in mobile payment. It is also very convenient for users to scan QR codes to make payments using only their mobile phones. However, QR code payments also have their disadvantages. For example, if a lawbreaker specially designs a malicious QR code to replace another original one, when an unknowing user scans the malicious QR code using their mobile device, the code can easily infect the device with a virus, thus causing users to suffer loss of property, disclosure of private information and other risks. Therefore, we need more secure payment methods to protect our private information.

3. Optimized Secure Payment Solution

3.1 Introduction to Operating-payment Secure Payment Devices

A. Operating device

Operating devices generally contain important content. If a device is attacked by a virus, the consequences can be disastrous. For this reason, it is particularly important to protect operating devices securely. In general, the operating device's system will strictly review the data entered into the device. In this paper, using an additional device to detect the exchanged data is also one of the commonly used solutions.

B. Payment device

As a bridge between the operating device and the QR code, the payment device, through physical shielding, divides the payment process into two parts: Operating-payment and payment-QR code. When we need to make an online payment, we have to scan the QR code with the payment device and open the contents of the QR code. If the payment device detects that the QR code is a normal payment channel, it will communicate with the operating device, and complete the final payment once confirmation is received from the operating device. However, if the detection result shows that the QR code contains illegal content, such as viruses, advertisements and blank pages, the transaction process will be promptly terminated. From the above-mentioned operations, it can be learned that payment device is required to form a strong defense against attacks. If the payment device encounters a virus when detecting a QR code and is infected, it should undergo several virus checking and killing operations, or even be reverted to default settings. The carrier of the payment device can be a mobile phone, a sports watch or a specific mobile terminal.

C. Reserved interface

For operating devices and payment devices some interfaces can be reserved to expand the functions of the existing system later. The reserved interfaces can include fingerprint recognition, facial recognition, voice recognition, nine-grid password, etc.

3.2 Operating-payment Secure Payment Process

A. Device initialization

1. Users need to download the corresponding application software on the operating device and set an account name, password and other account information. After they have completed their registration, users need to enter personal identity authentication information, such as their name, gender, ID card number, mobile phone number, email, QQ number, etc. Among them, the mobile phone number and email should be linked via the verification code, and the ID card number should match the name. After completing the personal identity authentication, it is necessary to set transaction commands, including passwords, fingerprints, face, etc. Transaction commands are specially used for managing changes of funds, and all fund changes can be carried out as normal only if the transaction commands are correct.

2. Users also need to download the corresponding application or install specific application programs on the payment device. Unlike the operating device, the payment device does not require personal information entry, but it requires users to register their account and set transaction commands. If you want the transaction process to be more secure, we recommend setting different transaction commands on the operating device and the payment device.

B. Device connection

After setting up the operating device and payment device, we need to connect the two devices. In this paper, we use the SSL protocol connection method[6]. For the first time connecting or replacing the device, the user needs to open the connection QR code of the payment device and scan the QR code with the operating device, so that the payment device can remember the IP address of the operating device. There is no need to repeat this for the next connection. In the case of network connection, the specific connection process between devices is as follows[7]:

Step 1: The payment device issues a https request. If it is the first time connecting, the user must scan the connection QR code;

Step 2: The operating device responds to the payment device and sends the digital certificate and the certificate public key to the payment device. The payment device finds the public key of the CA center locally, which is what we often call the root certificate, for authentication;

Step 3: The payment device authenticates that the certificate public key is correct and determines whether it has expired;

Step 4: After authentication is confirmed, a session key is generated;

Step 5: After the session key is encrypted with the public key of the operating device, the information is transferred to the payment device;

Step 6: After receiving the session key encrypted by the public key, the payment device decrypts it with its own private key to obtain the session key;

Step 7: Both the payment device and the server use this session key to encrypt the data to be transmitted for communication.

C. Device payment

First of all, the user must make sure that both the operating device and the payment device are logged in. They can then scan a QR code to make a payment with the payment device, and the payment device will detect the information contained in the QR code. If there is any abnormality detected, the transaction will be terminated immediately, and if no abnormality is detected, the customer enters the transaction password. After the transaction password is found to be correct, the payment device connects with the operating device, then the customer selects their payment method (Alipay, WeChat, bank card, digital RMB, etc.) on the operating device and confirms the amount and the payee. Next, after this information is confirmed to be correct, the customer must enter the transaction password correctly to complete the whole transaction process. After the transaction is complete, both the operating device and the payment device exit the transaction program and return to the original login state.

3.3 Analysis of Security

The solution uses the screen transfer method to further improve the security of mobile payments. Users need to use two linked devices to complete the entire payment. The improved security of this solution is reflected in the following features:

1). The operating device and the payment device are independent of each other and depend on each other in the payment process. Without either of them, the final transaction cannot be completed.

2). The connection method between the operating device and the payment device is an SSL connection, which ensures that the data transmitted by the two devices is correct, as well as encrypting the transmitted data. If the payment device is infected by a virus, but the data obtained by the virus on the payment device is encrypted, the private information and personal authentication information of the operating device will not be leaked.

3). At the beginning of the solution design, we also reserve the corresponding expansion interface. If the device detects that the user's identity is suspicious in the payment process, it can authenticate the user's identity again through fingerprint recognition and facial recognition to protect the property of the account and personal information.

4. Conclusion

This proposed solution provides a high level of security for mobile payments. Unlike the previous security improvement solutions which add various steps of authentication to one device, this solution improves security by adding a second device. Lawbreakers can only achieve an illegal payment if they have access to the account details, operating device and payment device at the same time. Moreover, account login, requires additional authentication methods such as fingerprints and SMS verification codes. Finally, although two devices are required to complete the payment, this does not

cause too much inconvenience to users, and the only additional step is the simple scanning of the QR code. Therefore, this proposed solution is still relatively simple and convenient.

References

- [1] Data Analysis and Projection of China Mobile Payment Market. [https:// www. askci. com/ news/ chanye/ 20180911/1553171131710.shtml](https://www.askci.com/news/chanye/20180911/1553171131710.shtml).
- [2] Hickman K, Elgamal T. The SSL protocol [J]. 1995.
- [3] The 47th release of Statistical Report of China Internet Development Situation[J]. News World, 2021 (03): 96.
- [4] Xu Xiwei. Talking about QR Codes and the Conception of its System Application [J]. China Technology Information, 2009(15):126-127.
- [5] Data Analysis of the China Mobile Payment Industry: In 2018 the total sum of mobile payments has reached 27.74 billion. <https://www.iimedia.cn/c1061/66170.html> 2774000000.
- [6] SSL Connection <https://baike.baidu.com/item/SSL%E8%BF%9E%E6%8E%A5/15976576?fr=Aladdin>.
- [7] SSL Principle and the Process of Building Connection [https://www. cnblogs. com/ fengfeng yang/ p/985 2481. html](https://www.cnblogs.com/fengfengyang/p/9852481.html).
- [8] Qiu Shuming. Design and Analysis of Multifactorial Safety Authentication Agreement[D]. Beijing University of Posts and Telecommunication, 2019.