

Mobile Security Payment Solution Based on Encrypted SMS Verification Code

Sai Li^{1, a *} and Xiaoyu Li^{1, b}

¹School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

^alisaizzucn@163.com, ^bixyli@zzu.edu.cn

Keywords: Mobile payment; Two-factor authentication; Encrypted SMS verification; RSA algorithm; SMS leakage

Abstract. Aiming at the problem that payment verification code is easy to leak during the process of mobile payment, a two-factor authentication mobile payment system based on encrypted SMS is proposed. The system is based on the public key system, uses PKI / CA authentication method to authenticate the server and the client online, and uses encrypted transaction verification SMS to ensure that even if the verification code ciphertext leakage, the attacker can not obtain the verification code, thus eliminating the risk of theft caused by the verification code leakage. The results compared the overall performance of the encryption and non-encryption solution, and the response time of the encrypted system is 0.8s higher on average than the non-encrypted system. Which can be concluded that the encrypted SMS verification code in the transmission process, the performance remained stable, to ensure that the user's payment verification code security.

Introduction

With the popularization of Internet and the rise of electronic commerce, financial payment has become a bottleneck restricting economic development, mobile payment is in this context came into being. In recent years, the Internet has brought great opportunities for innovation in various industries [1], which also makes the field of mobile payment has become a battleground for enterprises to pay. According to I Research's latest statistics show that in 2014, third-party mobile payment market transactions reached 5992.47 billion yuan, representing an increase of 391.3% in 2013, continue to show a high growth status. According to Erel forecast, 2018 mobile payment market transactions will be more than 18 trillion.

Such a large scale of transactions, one of the most central issue is the security of mobile payment [2], and the key problem of mobile payment is to establish a secure payment authentication mode [3]. For many important payment systems, if use the password as the only means of authentication, from the security point of view there is a big risk [4]. Therefore, in order to enhance the security of the website, most online payment platform or online banking will use two-factor authentication or multi-factor authentication [5].

In practical application scenarios, when using these authentication factors, should consider the pass rate, logical security, and customer security issues [6]. In general, SMS authentication is the lowest cost, easiest to implement and most convenient authentication scheme in secondary authentication. The binding of the client is strong, no extra equipment is needed, the cost of verification is very low, the pass rate is the highest, Operation of the best means of verification. However, in the present case, SMS verification code must be kept confidential, because once the SMS verification code was leaked due to various reasons, it may face the risk of account theft.

Therefore, personal protection can effectively prevent the leakage of SMS verification code, but can not completely avoid the leakage or theft of the verification code. Because criminals can use camouflage acquaintances social user account, to send messages to users to cheat the user's SMS verification code, or send a phishing link implanted mobile phone Trojan, so as to achieve the purpose of stealing user SMS verification code, and In this way to steal SMS verification code, often makes it difficult for users to identify the authenticity, thus deceived.

Based on the above considerations, this paper proposes a two-factor authentication mode based

on "User Password + Encryption Authentication SMS" to ensure that the mobile payment process can be safely completed in the case of verification code leakage [7], reduce the risk of loss of customer property.

Related Knowledge

Authentication

In the five functions of network information security (identity authentication, authorization, confidentiality, integrity and non-repudiation), identity authentication is the most basic and most important link. The role of identity authentication is to ensure that in the specific decision-making process, reflecting the true wishes of customers [8]. Typically, authentication has three elements:

- (1) Things only the user knows, such as passwords, security issues
- (2) Things only the user has, such as mobile phone verification code, U shield
- (3) Things only the user is, such as fingerprints, iris

From the point of view of cryptography, verification using any of the above two is called two-factor authentication [9]. In the current network environment, the use of single certification factors alone will have its problems and risks:

- (1) Things only the user knows: easy to forget, guess and pervasive information leakage caused by the collision
- (2) Things only the user has: easy to be fishing, lost
- (3) Things only the user is: the cost of certification is too high, vulnerable to attack

There are also differences in the security of these authentication factors, due to the difficulty of obtaining and forging, it is generally believed that the safety of the first category is worse than that of the second category, and the second category is worse than the third category. But it is need to be clear that, If only one of them is weak authentication, two or even three must be used. Secondary authentication is to use more than two kinds of authentication, it can ensure that the payment authentication is safe and effective.

Mobile Security Payment Proposal Based on SMS Authentication

To ensure the security of payment is necessary to establish a secure session mechanism, and then on this basis to complete the payment process. The entire payment process is divided into two phases. The first stage is the mutual authentication phase between the Server and the Client APP. [10] After the authentication phase is completed, the second phase is the payment phase [11]. It should be noted that: the authentication phase is completed during the Client APP installation process, the certification work can be done directly after the completion of the operation, in the future payment process does not require re-verification. Specific programs are as follows:

Table 1 The relevant symbols and description

| Symbol | Description |
|----------|---------------------------|
| S_{PK} | Server Public Key |
| S_{SK} | Server Private Key |
| C_{PK} | Client Public Key |
| C_{SK} | Client Private Key |
| REQ | Payment Request |
| VC | Payment Verification Code |

Server, Client Authentication Phase.

- 1) The information to be transmitted is calculated by the hash function to get a hash value, that is, the message digest (MD).

- 2) The server uses the server private key SSK through the RSA algorithm, The server uses the server private key S_{SK} to encrypt the MD to get the digital signature (DS).
- 3) The server encrypts the plaintext, the DS and the server public key S_{PK} through the encryption key SK of the symmetric encryption algorithm to obtain the encrypted information E .
- 4) Before sending the information, the server obtains the client public key C_{PK} of the client APP, encrypts the symmetric algorithm encryption key SK with C_{PK} , forms the digital envelope (DE).
- 5) The server transmits the encrypted information E and DE to the client APP.
- 6) The client APP decrypts DE with its own client private key C_{SK} to obtain encryption key SK .
- 7) The client APP uses SK to reduce E to plaintext, DS and server public key S_{PK} .
- 8) The client APP decrypts DS with the server public key SPK to obtain the MD.
- 9) The client APP then uses the Hash function to get a new message digest MD' .
- 10) Compare whether MD and MD' are equal, If the two are equal, the server connection can be confirmed to be successful, indicating that the Web server and the client terminal to establish a secure channel, if not equal, then refused to establish a connection.

The whole process as shown in Fig. 1:

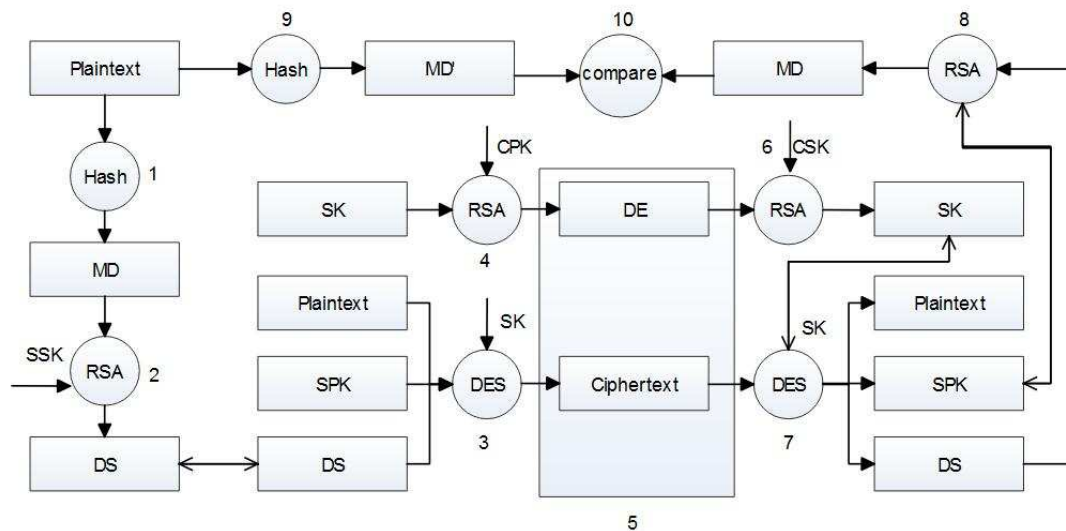


Fig. 1 User and the server authentication process

Payment Phase.

- 1) Confirm the establishment of a secure channel in the Web server and Client terminal, the user name and password that are used to log in to the Client APP are encrypted with the server public key S_{PK} and sent to the Web server for authentication, after entered the payment page, the client's payment request information REQ call server public key S_{PK} to encrypt, the encrypted information S_{PK} (REQ) sends a payment request to the Web server.
- 2) After receiving the payment request, the Web server decrypts the payment information in the payment request with the Server private key S_{SK} . After confirming the payment request, the Web server generates the verification code VC, and encrypts the verification code with the server private key S_{SK} to obtain a primary ciphertext verification code S_{SK} (VC). And then use the Client APP public key C_{PK} to encrypt to obtain the second ciphertext verification code $C_{PK} \{S_{SK} (VC)\}$. The server sends this secondary ciphertext verification code to the Client APP via SMS.
- 3) The user obtains the secondary ciphertext verification code $C_{PK} \{S_{SK} (VC)\}$ from the SMS, and then inputs it to the Client APP. The Client APP decrypts the secondary ciphertext verification code $C_{PK} \{S_{SK} (VC)\}$ with the client private key C_{SK} to obtain the primary ciphertext verification code $S_{SK} (VC)$, and then decrypts it with the server public key S_{PK} to get the original verification code VC.
- 4) The Client APP encrypts the original authentication code with the client private key C_{SK} and obtains the primary ciphertext $C_{SK} (VC)$, then encrypts the ciphertext with the server public key S_{PK}

to obtain the secondary ciphertext $S_{PK} \{C_{SK} (VC)\}$, and finally send the secondary ciphertext to the server.

5) The Web server decrypts the secondary ciphertext $S_{PK} \{C_{SK} (VC)\}$ with the server private key and obtains the primary plaintext $C_{SK} (VC)$, then use the client public key to decrypt the primary plaintext $C_{SK} (VC)$ and get original plaintext verification code VC, after the server matches the authentication information with the information stored in the server, the payment can be made.

It should be pointed out that both the server and client keys can be periodically updated (independently of each other) and the server can not obtain the private key of the client in order to ensure the security of the digital signature. Otherwise, the server can forge the signature of the user, resulting in payment problems. The payment model is shown in Fig. 2:

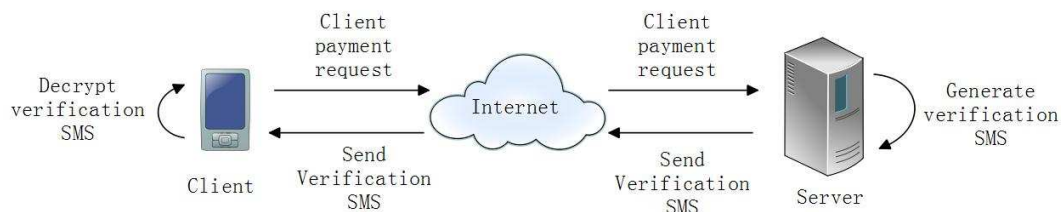


Fig. 2 Payment Model

1) In order to ensure the security verification in the replacement of mobile devices, it is necessary to set aside security questions when the users register.

2) When the mobile device is used for the first time, the application obtains the mobile device information to be sent to the server, and the server saves the user's device information and the user public key C_{PK} .

3) When the user log in account, the Client APP compares the acquired device information of the current device with the device information previously saved on the server. If the result is the same, it indicates that the user has not changed the mobile device, after verifying the login information, the user enters the application system. If the user want to reinstall the Client APP or upgrade the Client APP, the APP will check whether the current device has installed the Client APP before, if the Client APP have already been installed, then the currently installed Client APP no longer calls the key generator to regenerate the client public key C_{PK} and the private key C_{SK} .

4) If the device is lost or the device is replaced for other reasons, the client public key C_{PK} and private key C_{SK} will be regenerated after the Client APP is installed with the new device.

5) When the user logs on the account, the Client APP compares the device information of the new device with the device information previously saved on the server. Unlike the result of the comparison, the Client APP redirects to the reserved security question page.

6) If the user answers the security question correctly and confirms that the user is valid, then the generated client public key C_{PK} will be sent to the server for update saving. Client APP can be used normally.

7) Reserved security question answered incorrectly, authentication failed, the system will regard this user as illegal users, illegal users can not use the Client APP, in addition, the client public key saved by the server remains unchanged. When the legitimate user logs in to the client, the system prompts the user that an illegal user tries to log in to the system and recommends that the user change the password. So that illegal access to customer names, passwords can not pretend to operate the user himself, in order to avoid losses caused by loss of equipment problems.

Security Analysis

In this paper, based on the SMS verification code mobile payment solution, First of all, it can effectively prevent the fraudulent illegal users, Specifically: In the installation of the Client APP, there will be mutual authentication between the server and the Client APP, and establish a secure channel to ensure the smooth payment. In the process of authentication, the server will save will save the client public key transmitted by Client APP and verifies the user's credibility by digital

signature, so that the illegal client can not pass the authentication and can not continue the payment operation. And because customers in the registration information set up to set aside security issues, in the replacement of equipment, reserved for security issues must be answered to properly use Client APP, thus avoid the illegal acts lead to the occurrence of property losses.

Secondly, because the traditional SMS messages are not encrypted during the transmission and the server of the operator, the secondary authentication of the traditional SMS has serious security risks: Trojans, replenishment card attacks and radio monitoring. In this paper, the solution is to encrypt the message authentication code, the authentication information is transmitted in ciphertext, even if it is stolen in the channel or intercepted by the pseudo-base station, the content can not be identified, only after decryption with customer private key and converted to plaintext. As the user authentication has independent security measures, even if the verification code leak, the attacker can not complete the payment, thus ensuring the safety of funds.

Because the RSA algorithm is a public key cryptosystem based on the problem of large integer factorization, the security of RSA depends on the difficulty of the inversion of the mathematical function of the encryption algorithm. While the modulus factorization is more difficult to crack, so the encryption algorithm used in the signature key length should not be less than 1204 in the RSA (bit), which is in order to ensure the best computer deciphering the ciphertext requires about 33000000 1GHz CPU years, so it is able to ensure safety.

The main purpose of this paper is using the RSA encryption algorithm is 8 decimal integer plaintext verification code (64 binary string) encrypted by the server sent to the client, to ensure that users receive the verification code even in the case of disclosure does not occur the risk of loss of property. Too long key bit length will make the encrypted verification code ciphertext is too long, affecting the user experience. Under comprehensive consideration, the RSA encryption key length used in this paper is 64 bits (bit), the encrypted ciphertext on the best computer is about to be cracked at about 3.5 1GHz CPU hours. The validity of the verification code is usually only a few minutes, so that although this program can not guarantee absolute security, but can ensure the security in fact.

Experimental Results and Analysis

The experimental server-side processor with AMD Athlon™ X4 750 Processor 3.40GHz, 4GB of memory. The operating system is 64-bit Windows10. Programming based on Eclipse Mars (JDK1.7 development kit) platform, and configure the Android SDK development kit.

Fig. 3 is a comparison of the use of RSA encryption algorithm to encrypt the plaintext ciphertext data, the results can be seen from the figure, in the selected key length (length modulus) 64 (bit) cases, the encrypted data length is not fixed, but encrypted ciphertext length is basically 64 (bit), which is determined by the formula RSA encryption algorithm, and because in the actual operation mode value has a relationship with the generation algorithm of prime number, prime number generator generated primes is close to 64 (bit) of the prime (not always 64), so in the process of generating ciphertext the size of encryption is also about 8Byte, can be converted to 8 decimal integer. Users can easily input manually in client APP. Such payment verification code ciphertext length in the case of security, will not affect the user's experience.

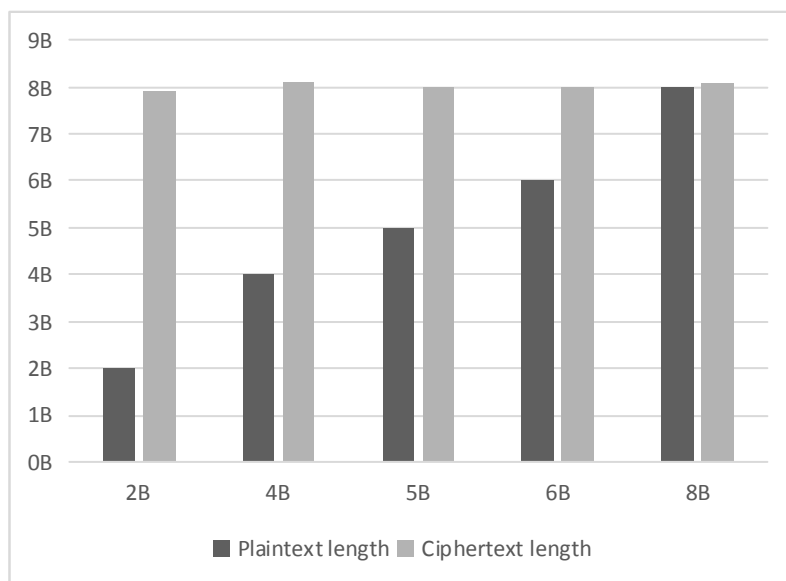


Fig. 3 The comparison of RSA encrypted ciphertext and plaintext data

Fig. 4 the horizontal axis represents the mobile phone side of concurrent visit, the vertical axis is the average response time of payment verification SMS. Figure three curves are represented using the Mob interface, Juhe interface(Mob and Juhe are commercial interface), and the Mob interface encryption (experimental method in this paper) the response time of payment verification SMS, we can see that with the increase of customers and influence the equipment performance, the average response time of 3 kinds of system increases, the greater the amount of concurrency increases will increase however, growth is linear, its growth rate is not fast, so there is no system performance with the increase of the number of users fell sharply. This system can support a large number of concurrent user access, its robustness is better. It should be noted that the average response time of the system is not the waiting time for the customer to receive the message, because the time that the customer actually receives the message is decided by various factors.

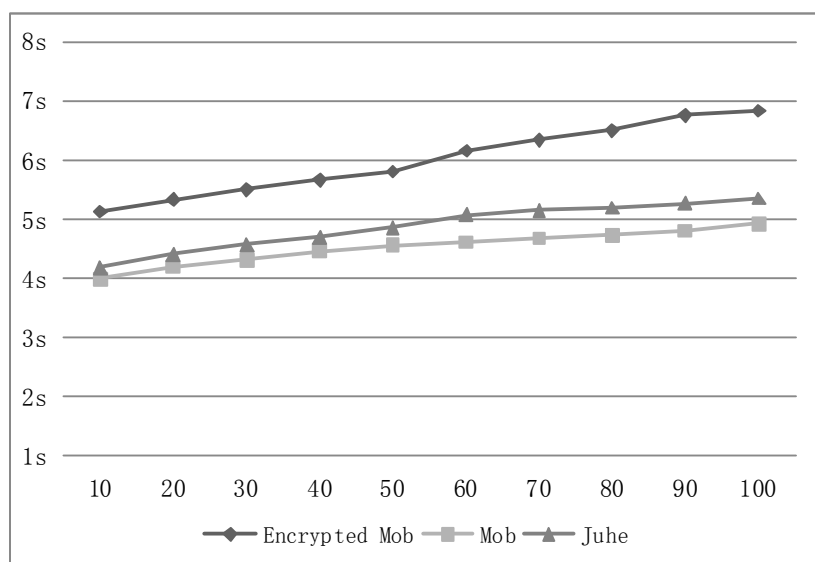


Fig. 4 The average response time of the system - the amount of concurrent access to the mobile terminal

Conclusion

Mobile security payment solution based on encrypted SMS verification code guarantees the security of mobile payment in many ways. The principle of SMS verification code in the payment

verification process is to allow users to perceive the payment behavior is taking place, increase the difficulty of illegal user fraudulent user account, because illegal users may get the payment password, but may not have the user Phone. And users in the absence of payment behavior received a payment SMS verification code, will realize that the account may be stolen, thereby improving the security.

However, the traditional SMS verification code as a means of payment security verification, as it is sent in plaintext, it has the risk of being intercepted and forwarded during communication, once intercepted and forwarded, the transmitted information loses its security, all kinds of fraud by deceiving users, resulting in a leak of the verification code scam, is aimed at this weakness. The two-factor authentication mobile security payment scheme based on encrypted SMS verification code proposed in this paper guarantees the security of mobile payment by preventing the occurrence of unsafe payment behavior to some extent by using ciphertext in all phases of the payment process.

Acknowledgments

The work in this paper was partially founded by the National Natural Science Foundation of China grant (61472412) and Natural Science Foundation of Henan Province Education Department grant (14A520012).

References

- [1] China Internet Network Information Center, the 37th China Internet Development Statistics Report[R]. Beijing, 2016.
- [2] V. Goyal, Dr. U. S. Pandey, S. Batra: Mobile Banking in India: Practices, Challenges and Security Issues[J].International Journal of Advanced Trends in Computer Science and Engineering,2012,1(2),p.56.
- [3] T. Dahlberg, J. Guo, J. Ondrus: A critical review of mobile payment research [J]. Electronic Commerce Research and Applications, 2015, 14(5), p. 265.
- [4] N. Arvidsson: Consumer attitudes on mobile payment services-results from a proof of concept test [J].International Journal of Bank Marketing, 2014, 32(2), p. 150.
- [5] Z.M. Xu, T. Zhang, Y.J. Zeng et al: A Secure Mobile Payment Framework Based on Face Authentication [J].Lecture Notes in Engineering and Computer Science, 2015, 2215(1), p.4.
- [6] L.D. Chen. A model of consumer acceptance of mobile payment [J]. International Journal of Mobile Communications, 2008, 6(1), p. 32.
- [7] Q.L. Zhao: A study on mobile payment security [J].Electronic Design Engineering, 2014(15), p.59. (In Chinese)
- [8] Y. Feng: Analysis and research of identity authentication in mobile payment [J]. Information Communication, 2012(3), p. 107. (In Chinese)
- [9] W. Cao, Y. Zhao: Research on the Technology of Mobile Payment Security Based on Two-factor Authentication [J].Information Security and Technology, 2014, 5(2), p. 10. (In Chinese)
- [10] Q.Y. Ge, L.J. Che: The study of network security payment model based on multi factor authentication [J]. Information Network Security, 2015(12), p. 48. (In Chinese)
- [11] R. Duan, N.Y. Xu, A. Q. Hu: Research on the security of authentication protocol based on formal analysis tools [J].Information Network Security, 2015(7), p. 71. (In Chinese)