Research on Multiple Security Authentication Schemes for Mobile Applications of Power Trading Platforms

SHI Shuhong\textsuperscript{1,2}, WANG Lei\textsuperscript{1,2}, ZHENG Shiqiang\textsuperscript{1,2}, LV Jingwei\textsuperscript{1,2,*} and ZHANG Qian\textsuperscript{1,2}

\textsuperscript{1}Nari Group Corporation/State Grid Electric Power Research Institute, Nanjing, China
\textsuperscript{2}Beijing Kedong Electric Power Control System Co., Ltd, Beijing, China

\textsuperscript{*}Email: lvjingwei1993@163.com

Abstract. The development of mobile technology and the Internet has brought many potential threats while bringing convenience to users. Aiming at the leakage of private data and transaction sensitive information in mobile trading market, we study the multi-security authentication support technology of mobile transaction mobile application, and analyse the common mobile application content, document protection technology and mobile signature protection technology. Based on the identity authentication technology of mobile application and the security considerations of members and transaction data in the power trading market, an identity authentication technology using SMS verification code, mobile phone shield, face recognition and fingerprint identification is proposed to protect the mobile transaction mobile application transaction. Anti-leakage of market member privacy data and transaction-sensitive information. In order to verify the effectiveness of the proposed scheme, we carry out the simulation experiment. The experimental results show that the proposed scheme can effectively protect the privacy of users.

1. Introduction

The emergence and popularity of smart terminals has convenience to users, but it also has brought many potential threats, such as illegal tampering and illegal access of information, using the operating system to modify relevant terminal information, and destroying the system through viruses and malicious code [1-2]. Because trading platform data contains a lot of sensitive information, how to control unauthorized access, handle sensitive data interference or abuse network services is a problem that mobile security authentication technology must consider [3]. Security certification provides effective security for mobility management and mobile applications, and authentication is a prerequisite for access control and billing [4]. Therefore, establishing a secure authentication system for mobile trading mobile applications is a fundamental requirement for the security of mobile trading mobile applications [5].

We propose an application to solve the problem of leakage of private data and transaction sensitive information in the mobile trading market, using SMS authentication code, mobile phone shield, face recognition and fingerprint identification. A multi-security authentication scheme for mobile applications on the power trading platform. In view of the mobile network security certification of electronic trading system, starting from the basic theory of mobile network security, the security analysis is relatively complete, and the key technology of transaction platform security authentication is studied to overcome the above problems in mobile terminals such as PDAs, smart phones and
customized terminals. In this way, the fast and secure mobile office function can be achieved, so that anyone can provide any service within his rights at any time and any place.

2. Multiple security authentication scheme

2.1 Overview of the scheme
We propose a multi-security authentication method for mobile applications on mobile trading platforms (as shown in Figure 1). The specific steps are as follows:

Figure 1 Multiple Security Certification Scheme

1) The user initiates an authentication request to the identity authentication server. The mobile user initiates an authentication request to the identity authentication server by using the mobile device held by the mobile user, and the identity authentication server issues an identity authentication request to the client.

2) Identity authentication server authenticates the user
   After receiving the identity authentication request sent by the identity authentication server, the client first requires the user to input a signature password, and the identity authentication server performs digital signature authentication by using the user public key stored on the server.

3) The client authenticates the identity of the server
   The identity authentication server performs digital signature using the server private key stored on the server side, and the client uses the server public key stored in the client for signature authentication.

4) Server and client complete two-way authentication
   The client device that authenticates the server and the client for two-way authentication can access the authorized application service by using the secure channel established between the server and the identity held by the server.

2.2 Concrete realization
The multiple security authentication method proposed in this paper for the mobile application platform mobile application is shown in Figure 2, including the following steps:
Users USIM platform

Send a business request

- Request user signature
  - Request user to enter a signature password (PIN)
  - Signature password passed verification
  - Complete digital signature
  - User signature information

- Certification pass information
- Demand server signature
- Server signature information
- Card end authentication server signature

Secure communication

Authentication

Server-side signature

Check user status

Figure 2 Multiple security authentication methods for mobile trading platform

Step 1: The mobile user initiates an authentication request to the identity authentication server by using the mobile device held by the mobile user, and the identity authentication server sends an identity authentication request to the client.

The mobile user initiates an identity authentication request to the identity authentication server by using the mobile device held by the mobile user, and the client first asks the user to input his/her personal PIN code to perform the user identity authentication;

After the user's individual identity authentication is passed, the mobile client sends the request to the mobile identity authentication platform.

The authentication server checks whether the identity of the user has passed the verification. If the authentication fails, the identity authentication server issues an identity authentication request to the client.

Where $X \rightarrow Y$ indicates that entity $X$ sends a message to entity $Y$; $H()$ represents a one-way function; $\text{Sign}_K()$ represents a signature algorithm, $K$ is a key; and $(E_K(), D_K())$ represents an encryption algorithm and a decryption algorithm.

(1) Integrity check request message:

\[
\text{USIM} \rightarrow \text{ME} : \text{Request}, \text{rand}_{\text{USIM}}, \text{UID}, \text{Cert}_{\text{USIM}}
\]  

In this step, the Universal Subscriber Identity Module (USIM) generates and stores a random number $\text{rand}_{\text{USIM}}$, and constructs a request message for checking the integrity of the mobile device (ME, Mobile Equipment), and the message further includes: a UID. And the USIM certificate.

(2) ME reply message:

\[
\text{ME} \rightarrow \text{USIM} : \text{Result}, \text{ID}_{\text{ME}}, \text{rand}_{\text{ME}}, \text{Sign}_{\text{ME}}(\text{rand}_{\text{USIM}}, \text{UID}, \text{rand}_{\text{ME}}, \text{result})_{\text{ME}}
\]  

After the Cert_{ME} receives the request message, the MTM stores the random number $\text{rand}_{\text{USIM}}$, and then the MTM generates a new random number $\text{rand}_{\text{ME}}$. MTM signs the results of the integrity check, $\text{rand}_{\text{ME}}, \text{rand}_{\text{USIM}}$, and UID. And construct a reply message, and reply the signature to the USIM along with the ID_{ME}, rand_{USIM} and ME certificates.

(3) Authentication request message:

\[
\text{USIM} \rightarrow \text{ME} : E_{\text{ME}}(E_{\text{K}}, \text{ID}_{\text{ME}}, \text{rand}_{\text{ME}}), \text{Sign}_{\text{USIM}}(\text{rand}_{\text{USIM}}, \text{UID}, 0, E_{\text{ME}}(E_{\text{K}}, \text{ID}_{\text{ME}}, \text{rand}_{\text{ME}}))
\]  

After receiving the reply message, the USIM verifies the results of the previous legality and integrity check. Then, the USIM checks if the random number $\text{rand}_{\text{USIM}}$ contained in the signature is the same as that saved by itself. The main requirement of this step is that if the MTM and the USIM have the same certificate authority (CA), since the USIM has the certificate of the own CA, the
verification of the MTM certificate can be omitted. Otherwise, the verification of the certificate requires additional overhead.

After completing the check of the reply message, the USIM generates a key \( EK \) for encryption between the USIM and the MTM. The USIM encrypts \( EK \), \( ID_{ME} \), and \( rand_{ME} \) using the ME's public key and signs the encrypted message, \( rand_{USIM} \), \( UID \), and \( O \). The constructed authentication request message is then sent to the ME.

(4) Certification reply message:

\[
ME \rightarrow USIM : \text{Sign}_{USIM}(EK, rand_{USIM}, UID, 0)
\]  

After the ME receives the authentication request message, it verifies the validity of the signature and calculates the signature of the same content (where 0 uses the value stored in the MTM) and decrypts the message body. If the signature is legal and the calculated signature is the same as the one received, the USIM and MTM owners are the same; if the signature is legal, but the calculated signature is different from the one received, the USIM owner is different from the MTM owner. The ME signs the \( EK \), \( rand_{USIM} \), \( ID_{ME} \), and \( 0 \), and sends the message as an authentication reply message to the USIM. The 0 used by this message is the value stored in the MTM.

When the USIM receives the message, it verifies the validity of the signature and determines if the ME has the same owner as itself.

The first four steps implement the USIM for ME integrity check and support mutual authentication between USIM and MTM. At the same time, the negotiation of the encryption key between the USIM and the ME is also implemented. And the verification of the signature can also complete the judgment of the owner of the ME, USIM. After the first four steps are completed, the ME obtains the user's identity characteristics from the User according to the requirements of the protocol implementation.

(5) User information collected:

\[
USIM \rightarrow ME : E_{Ek}(rand_{ME}, H(PW) or BD), \text{Sign}_{ME}(E_{Ek}(rand_{ME}, H(PW) or BD))
\]

The secure mobile platform guarantees the integrity of the hardware and the integrity of the software system. In this step, the ME collects a user-entered password (PW) or biometric data (BD, Biometric Data) through BR or KB. To ensure the security of the transmission of the password or BD data between the USIM and the ME, the MTM encrypts the \( rand_{ME} \), \( H(PW) \) or \( BD \) using the previously negotiated encryption key \( EK \), and signs the encrypted message body and sends it to the USIM as the collected user information.

(6) Authentication result reply message:

\[
ME \rightarrow USIM : E_{Ek}(rand_{ME}, rand_{USIM}, result), \text{Sign}_{USIM}(E_{Ek}(rand_{ME}, rand_{USIM}, result))
\]

After receiving the user message, the USIM verifies the signature and decrypts the message, obtaining \( H(PW) \) or BD. Then perform parity verification on the password or BD.

The USIM encrypts the verification result, signs the encrypted message, and sends the reply message as an authentication result to the ME.

Step 2: After receiving the identity authentication request sent by the identity authentication server, the client first requests the user to input a signature password, and the identity authentication server performs digital signature authentication by using the user public key stored on the server.

The method uses the RSA algorithm to realize digital signature. The key of the RSA algorithm is to determine the prime numbers \( p \) and \( q \) of the Euler function \( \varphi(n) \).

After receiving the identity authentication request sent by the identity authentication server, the client first requires the user to input a signature password (the PIN code of the USIM card). If the client verifies that the signature password is correct, the client completes the digital signature by using the user private key stored in the client, and Send the signed content to the authentication server again.

After receiving the digital signature of the client, the identity authentication server performs digital signature authentication by using the public key stored on the server, and the client identity authentication sends the signature verification pass information to the client through the rear server.
Step 3: The identity authentication server performs digital signature by using the server private key stored on the server side, and the client uses the server public key stored in the client to perform signature verification.

After receiving the authentication pass information of the identity authentication server, the client sends a message requesting authentication of the identity of the server.

After receiving the client's server identity authentication request, the identity authentication server digitally signs the server private key stored on the server and sends the signature information to the client.

After receiving the digital signature information sent by the identity authentication server, the client uses the server public key stored in the client for signature authentication.

Step 4: Through the identity authentication server and the client two-way identity authentication client device, the authorized application service can be accessed by using the secure channel established between the server and the held identity.

It can be seen from the above steps that the solution proposed in this paper performs security authentication on the mobile application platform mobile application, and can provide a set of mechanisms that can solve most security problems, such as static password vulnerability, data integrity problem, non-repudiation problem, key Generate, transfer problems, device loss issues, etc. The safety certification method that comprehensively considers the application process of the entire trading platform is clear and suitable for promotion.

3. Evaluation
In order to verify the effectiveness of the proposed scheme, we compare and analyse the scheme of this paper with the traditional identity authentication scheme and the emerging identity authentication scheme. The results are shown in Table 1.

Table 1. Analysis of Advantages and Disadvantages of Each Identity Authentication Scheme

| Category                  | Advantages                                                                 | Disadvantages                                                                 |
|---------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| Market member name/password | Simple implementation, is the most commonly used authentication method   | Single factor authentication is a very insecure way of identity authentication |
| smart card                | Is a two-factor authentication method, market members will not be impersonated | It is easy to intercept the authentication information of market members, and there are certain security risks. |
| Traditional authentication scheme | Adopting a one-time method to ensure the security of market membership | a legitimate market member may not be able to log in; when there is a disoperation, it may be inconvenient to use. |
| Dynamic password          | One-time strong two-factor authentication mode solves the contradiction between security and ease of use. | Need to install mobile digital certificate |
| USB Key                   | Has good security, reliability and effectiveness,                          | Biometric recognition technology is not suitable for everyone                  |
| Biometric technology      |                                                                           |                                                                               |
Our scheme | Good system security, reliability, confidentiality, and mechanisms to solve most security problems | More identity authentication technology, certification time will increase
---|---|---

In view of the privacy problem of the mobile application platform mobile application, we carried out a simulation experiment, and the result is shown in Figure 3.

**Figure 3** Privacy curves for different scenarios

In Figure 3, 1-r represents the scheme privacy estimate, the lower the value, the better the scheme privacy protection. As shown in Figure 3, in most cases, the privacy estimate of the proposed scheme is lower than the privacy estimates of other schemes. Therefore, it can be considered that our scheme has more advantages in terms of privacy protection.

4. Conclusion
The popularity of mobile terminals such as smartphones and tablets has brought convenience and at the same time causes users to face the risk of privacy leakage. We study the multi-security authentication support technology of mobile transaction mobile application, and analyse the common mobile application content and document protection technology, mobile signature protection technology and mobile application-based identity authentication technology. In terms of sexual considerations, an identity authentication technology using SMS verification code, mobile phone shield, face recognition and fingerprint recognition is proposed to ensure the leakage prevention of privacy data and transaction sensitive information of members of the power trading market. Finally, the simulation experiments prove that the proposed scheme can effectively protect the privacy of users.

ACKNOWLEDGMENT
This work was supported by the technical project of state grid corporation of China “Research on Key Technologies of Mobile Application and Big Data Analysis in Power Trading Platform”.

References
[1] anaee Z, Abolfazli S, Gani A, et al. Heterogeneity in mobile cloud computing: taxonomy and open challenges[J]. *Communications Surveys & Tutorials, IEEE*, 2014.
[2] Hui-Juan W , Yong J , Gao-Feng Z , et al. Arithmetic Correlation Used in Mobile Cloud ID-Based Multiple Authentication[C]. *IEEE International Conference on Big Data Security on Cloud*, IEEE, 2016.
[3] Khan S H, Ali Akbar M, Shahzad F, et al. Secure biometric template generation for multi-factor authentication[J]. *Pattern Recognition*, 2015, 48(2):458-472.
[4] Nguyen T A T, Nguyen D T, et al. A Multi-factor Biometric Based Remote Authentication Using Fuzzy Commitment and Non-invertible Transformation[M], *Information and Communication Technology*. Springer International Publishing, 2015.
[5] Liu Y, Ling J, Liu Z, et al. Finger vein secure biometric template generation based on deep learning[J]. *Soft Computing*, 2017, 22(7).