Research on Dynamic Identity Authentication Mechanism Based on Digital Signature

Weishu Zhan*, Xin Xin Ye
University of Northern Iowa, Cedar Falls, 50613, United States
*Corresponding author's e-mail: zhanw@uni.edu

Abstract. With the economic development of globalization, the widespread Internet and the continuous establishment of national informatization, information security has become the focus of the national security guarantee system. Identity authentication is the first line of defense of the network communication system and the network security portal. Cryptography is the core content of the information security system and is widely used in various applications such as network security and data security. As the cornerstone of network security, since passwords are easy to be stolen or lost, it is not safe to authenticate identity with static passwords alone. Therefore, dynamic identity authentication came into being. It effectively resists the main security threats and attacks faced by static password authentication, solves the main drawbacks of static password authentication technology, and effectively prevents replay attacks. In addition, dynamic identity authentication solves the problem of static passwords being stolen in the database or stolen during transmission, thereby preventing illegal users from intruding and accessing the system. This article first studies the principle of digital signature technology and the design idea of dynamic identity authentication, and combines the advantages of both to propose a new dynamic identity authentication system based on digital signature technology.

1. Introduction

Information network is an important infrastructure of modern society and is closely related to people's lives. The development of network technology has facilitated communication and exchanges between people and provided people with convenient information resources. The e-commerce platform supported by network technology provides businesses with a new type of operation mode. The continuous progress of network technology has driven the development of a number of emerging industries and the upgrading of traditional industries, and has promoted the progress and innovation of computing science and communication technology. Network security technology includes many contents. Cryptographic technology is an important tool to ensure the confidentiality of information in the network and is the foundation of network security. In practical applications, people are more concerned about the authenticity and integrity of information. In order to solve this problem, people put forward the idea of digital signature. At present, most digital signature algorithms are based on public key cryptography, and the realization of network security protocols is inseparable from the support of digital signature technology. With the deepening of basic theoretical research, new theoretical tools suitable for digital signature applications are constantly being proposed. In addition, the continuous changes in the application environment also require us to continuously improve the existing signature algorithms. In this article, we will study the above-mentioned problems.
2. Basic principles of digital signature
Since asymmetric encryption algorithms require that both the encryption key (private key) and the decryption key (public key) be derived from one and the other is computationally infeasible, this type of algorithm is widely used in the field of digital signatures. Theoretically, the disclosure of the public key will not pose any threat to the security of the private key, so the public key can be sent to multiple verifiers on demand, and the security of the private key must be guaranteed [1]. At present, digital signatures mainly include digital signatures with symmetric key systems and digital signatures with asymmetric key systems. The digital signature scheme designed in this article uses digital signatures with asymmetric key systems.

2.1. Digital signature of symmetric key system
The digital signature requires an authoritative trust center as a third party, and all keys are kept by it. Each user chooses a key and passes it directly to a third party. Therefore, only users and third parties know the key. If user A needs to send a file to user B, the process is shown in Figure 1:

![Figure 1. Digital signature process of symmetric key system](image)

The specific process is as follows:
First, user A encrypts the plaintext W with its own key to obtain $K_A(W)$, and sends it to a third party.
Second, the third part decrypts $K_A(W)$ to get W, and then creates a new message (A+D+W) composed of A's name, address, date, and plaintext. Then encrypt it with a secret key N that is secret to anyone, generate N(A+D+W), and send it back to A. In this way, the third party can confirm that the request is indeed from A, because only A and the third party know $K_A$. If an impostor sends a message to a third party, the message decrypted by $K_A$ will be meaningless.
Third, user A sends N(A+D+W) to user B.
Fourth, user B first sends N(A+D+W) to a third party, requesting $K_B(A+D+W)$ as the result.
Fifth, user B decrypts $K_B(A+D+W)$ to obtain plaintext information A, D and W.

2.2. Digital signature of asymmetric key system
The key problem of using symmetric key system for digital signature is that everyone trusts the third party, because the third party saves all keys and reads all signed ciphertexts. But some people do not trust third parties. Therefore, it would be better for only the signing parties to participate when signing documents, and an asymmetric key system can meet this requirement. Therefore, it would be better for only the signing parties to participate when signing documents, and an asymmetric key system can meet this requirement. Second, encrypt H(W) with your own private key $PR_A$ to get the digital signature $E_A(H(W))$. Finally, A sends the digital signature $E_A(H(W))$ and the plaintext W to the B user. After receiving the message, user B first separates $E_A(H(W))$ from W. Secondly, use A's public key $PU_A$ to decrypt to obtain H(W). Then, B uses the same hash function to perform a hash operation on W to obtain the message digest H(W). Finally, H(W) and H'(W) are compared. If they are equal, the original text has not been tampered with and the signature is credible. Otherwise, this document will not be valid.
3. Design idea and mechanism of dynamic identity authentication

3.1. The design idea of dynamic identity authentication
The design idea of the dynamic password authentication mechanism is mainly based on a certain cryptographic algorithm. In the encryption and decryption algorithm, a certain identity information of the user or a certain uncertainty factor is used as an input parameter. Through a series of algorithm changes, the result obtained is different each time, which is the so-called dynamic password. Then the user inputs the one-time password as the dynamic password for logging in, and transmits it to the authentication server through the network. The authentication server also generates a one-time dynamic password through the same mechanism, and compares this result with the one-time password transmitted by the user. If the same, the user request is agreed and the user request is accepted. The advantage of this mechanism is that the dynamic password is changeable, and the user does not need to remember it. A password is only used once, and the repeated use of the password will be rejected by the system as an illegal login. The user inputs the password generated by the dynamic token into the client, the server uses the same algorithm mechanism as the client to obtain the dynamic password, and compares it with the password entered by the user to achieve identity authentication. Only legal users with dynamic tokens can generate legal passwords, and the dynamic password mechanism changes one time at a time. Even if hackers intercept the password, they cannot use this password to impersonate a legitimate user.

3.2. Dynamic identity authentication mechanism
This paper optimizes the design based on the challenge/response dynamic password mechanism, which is asynchronous. The challenge/response dynamic password uses an encryption algorithm or one-way
hash function for dynamic password production. When receiving a user's login request, the authentication server generates a challenge code and sends it to the user. The client performs a hash operation, and the input parameters of the hash operation are the challenge code and the secret key. The hash operation generates a dynamic password and sends it to the authentication server. In the same way, the authentication server uses the same one-way hash function to verify the user's identity. The authentication process includes four steps, namely: (1) The client enters user information and sends a login request to the authentication server. (2) The server verifies the user's information, and if the user information is correct, it generates a challenge code and sends it back to the client. (3) The client executes a one-way hash function operation, with the key and challenge code as the input parameters of the function, generates a random response code and sends it to the server. (4) The server executes the same function as the client, generates a response code, and compares it with the response code sent by the client to obtain the verification result and send it to the client, as shown in Figure 4.

4. Improvement in dynamic identity authentication mechanism

This paper adopts the challenge-response system, because its security is higher than the time synchronization authentication method and the event synchronization mechanism, and it has low cost and is easy to implement. This article sacrifices time in exchange for its high security. In addition, the process of generating dynamic passwords has been improved.

Improvements in the registration phase:
- First, When the user registers, the user password $PW_i$ is transmitted using its hash value $H(PW_i)$ during the transmission process, and the user password does not appear in plain text.
- Second, after the user's registration information is successfully verified, the server sets the number of successful logins $m$ to 1, and generates the EL Gamal algorithm key. Before the message is transmitted, the message is signed and then encrypted, which greatly improves its security. In addition, two random number keys $K1$ and $K2$ are generated for random XOR operation.
- Third, when the server issues a user certificate, the user's information and the server's unique identifier SD are stored after being processed by XOR, and the smart card has a PIN code.

Improved login authentication phase:
- First, when verifying whether $ID_i$ and $PW_i$ are correct, they are authenticated in the local smart card after hashing them, which saves time and improves efficiency.
- Second, when transmitting the challenge code challenge Num, connect the user login times $m$ and the server's unique identifier SD $(m||SD)$ and perform a hash operation $(H(m||SD))$, and finally sign
SK2 (H(m||SD)), finally connect the challenge code and the signature, and get PK1(challenge Num||
SK2(H(m||SD))) after encryption. This improves its safety.

- Third, connect the user's \( H(ID_i), H(PW_i) \), challenge Num and the number of user logins m to obtain \( H(ID_i)|| H(PW_i)||\text{challenge Num}||m \), and then adopt a random order XOR interleaving operation, the result obtained is marked as str, because of the randomness of the calculation sequence and improved security.
- Fourth, perform MD5 hash operation on str to get H(str), and XOR the result of two or two bytes, then take the last character as one bit of the dynamic code, and finally get the 8-bit dynamic verification code Auto Password. The generation complexity of the dynamic code is improved, and the security is improved.
- Fifth, the dynamic code Auto Password is transmitted together with the random numbers a and b. The random number is processed to obtain SK1(a||b), and then Auto Password is connected with SK1(a||b) to obtain Auto Password||SK1(a||b), and then encrypt it to get PK2(Auto Password||SK1(a||b)), double-layer encryption improves security.

5. Conference
This paper studies various technologies and methods of dynamic identity authentication, analyzes and compares the advantages and disadvantages of authentication schemes based on event synchronization, challenge-response and time synchronization mechanisms, and studies encryption and decryption technologies. It researches the existing dynamic identity authentication technology, mainly explain the related concepts of identity authentication, the classification of identity authentication, the idea of dynamic password identity authentication, the generation method and advantages of dynamic password identity authentication, and the threats encountered by dynamic identity authentication. This article improves the traditional dynamic identity authentication scheme. Specific instructions are given from the user registration, user login authentication, detailed technical improvements in the scheme, and finally the application of the dynamic identity authentication scheme on the cloud platform.

Reference
[1] Wang, Y. (2007) Research on Digital Signature Technology and Its Application in Electronic Government Affairs. Chengdu: Southwest Jiaotong University.
[2] Xu, C. S., Guo, F. Y. (2020) Research and Design of Dynamic Identity Authentication Mechanism Based on Digital Signature. Computer Knowledge and Technology, 16(11):22-23.
[3] Cao, Y. (2018) Key agreement scheme for dynamic identity authentication in multi-server environment. Computer Technology and Development, 28(05):131-134.
[4] Zhang, S. T., Xie, Y., Wu, L., et al. (2017) Design of Security Protection Architecture of Electric Power Communication Network Based on SDN. Electronic Design Engineering, 25(19):136-140.
[5] Shi, L., Chen, N., Zhang, J. (2019) Research on access trust technology of big data platform based on dynamic and continuous authentication of identity. Cyberspace Security, 10(07):66-72.
[6] Huang, G. B., Ma, J. B., Jia, R. X., et al. (2019) Identity authentication management service based on SMS dynamic password. Electronic Measurement Technology, 42(02):108-111.
[7] Cheng, C. H. (2020) Overview of Digital Signature Technology. Information Security and Communication Confidentiality, (07):48-62.
[8] Zhang, J. H., Zhou Q. L., Han Y. J. (2020) A cleanable signature scheme based on ring signature and short signature. Computer Science, 47(S1):386-390+399.
[9] Jiang, Z. Y. (2020) A brief talk on cryptography and its role in computer network security. Value Engineering, 39(16):189-191.
[10] Ma J. H., Huang, X. Y., Xu J. P., et al. (2020) A publicly auditable and amendable signature scheme. Journal of Electronics & Information Technology, 42(05):1079-1086.