

Research on User Identity Authentication Based on Two-way Confirmation in Data Transmission

Qin Li¹, Caiming Liu^{1,2,*}, Siyuan Jing^{1,2}, and Lijun Du¹

¹Leshan Normal University, School of Computer Science, 614000 Leshan, China

²Leshan Normal University, Key Lab of Internet Natural Language Processing of Sichuan Provincial Education Department, 614000 Leshan, China

Abstract. User identity authentication is the foundation of data transmission in the complicated network environment. Moreover, the key issue is the effective identity authentication of both sides in data transmission. An authentication method for user identity based on two-way confirmation in data transmission is proposed in this paper. The public key, private key, information of traditional identity authentication, one-time transmission key, timestamp, authentication lifecycle for timestamp and other authentication elements are constructed. Based on guaranteeing the timeliness of data transmission, the two-way user identity authentication process for sending terminal and receiving terminal is set up through using the information of traditional identity authentication and one-time transmission key.

1 Introduction

The security of data transmission is the foundation of running the Internet safely. Massive data always flow in the Internet. How to verify the valid identity of data sender and receiver is crucial to keep data transmission in security. It makes authentication technologies for user identities be vitally important [1]. In recent years, security events about data transmission broke out frequently, such as data leak of 20 million hotel records. These events were concerned by the society and caused huge economy loss. Overall, the rising severe situation of data transmission security has caused user identity authentication technologies for data transmission be one of hot topics in the field of network security.

2 Research background

User identity authentication technologies have been widely applied to network areas such as finances [2], e-mails [3], wireless networks [4], etc. They are critical to verify the valid identity of users in network systems [5]. Traditional user identity authentication technologies mostly function based on user names and passwords [6]. Currently, identifying codes are adopted to strengthen the security of user identity authentications. However, the authentication method of identifying codes has a few security vulnerabilities because image recognition technologies constantly improved. The following problems exist in traditional identity authentication technologies for network users. First, user names and passwords are easily be intercepted when they are transmitted. Second, it is hard to keep the balance of the confidentiality and usefulness between passwords and

identifying codes which are easy cracked by brute force attacks. Therefore, the transmission security requirements for complicated network environments can't be satisfied anymore by traditional identity authentication technologies.

Hu [7] proposed an authentication architecture for unified identities to centrally and remotely administrate, verify and authorize users. The method of unified management for user information resources resolves the dispersity of users. Zhang et al. [8] proposed a trusted and anonymous authentication protocol. Fake names prestored in mobile terminals are used to hide the real names. Integrity verification is realized through a third authentication center. Li et al. [9] proposed an user authentication model based on dynamic identities which is aimed at remote login environments. The model can verify the real identity when users login remote servers. David et al. [10] proposed an authentication model for multimedia servers and clients based on dynamic identities and developed a medical multimedia system to check the effectiveness of the proposed model. Amin et al. [11] designed an user authentication and key exchange protocol for accessing the remote medical server, which is used to make it safe when doctors share medical services. Existed identity authentication technologies for data transmission highlight the identity validation for data sender, and the authentication for data receivers is ignored, which are considered to be legal by default. However, in the complicated network security environment, unauthorized personnel may design a trap to let network flows be transmitted to some devices, and then the flows could be analyzed, cracked and leaked.

When network data are transmitted in the open network environment, they confronted the dangers which

* Corresponding author: caiming_liu@163.com

are to be intercepted, modified and faked. The large-scale and dynamical network data make the user identity authentication be extremely difficult. Therefore, the user identity authentication for massive data in Internet is one of the key technologies expected to be resolved.

To improve the safety of transmitted data in networks, an authentication method for user identity based on two-way confirmation in data transmission is proposed in this paper. In the following, the architecture and its operational principle of the proposed method are summarized, the authentication elements and process are described in Section III. Section IV concludes this paper.

3 Authentication method

3.1 Summary of the proposed method

The architecture of the proposed method is shown in Figure 1. The communication operation of the data sender is with respect to the receiver's. The proposed method is summarized in the following.

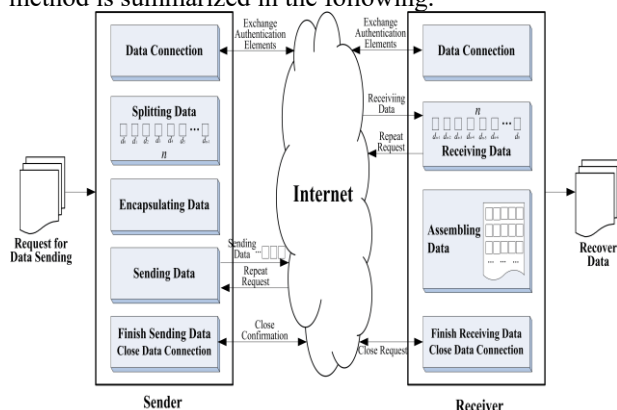


Fig. 1. The Architecture of The Proposed Method.

The sender and receiver send data connection information to each other and exchange authentication elements when transmitting data.

The sender begins to communicate with the receiver and creates a data connection when its traditional identity authentication elements are verified by the receiver. It is the single-way authentication of the sender. The sender takes the operations of splitting, encapsulation and sending to transmit data to the receiver.

The receiver takes the operations of receiving, decryption and assembling to recover the original data. When it gets a datum, it uses the one-time transmission key to decrypt the datum. It is the single-way authentication of the receiver.

The authentications of the sender and receiver form the user identity authentication based on two-way confirmation to ensure the data communication be in security. The data connection is kept alive until the data transmission finishes.

3.2 Authentication elements

The encryption information of public keys, private keys and time which constitute the authentication elements of the proposed method, is applied to the proposed method to advance the creditability and security of the sender and receiver. The authentication elements are shown in Figure 2.

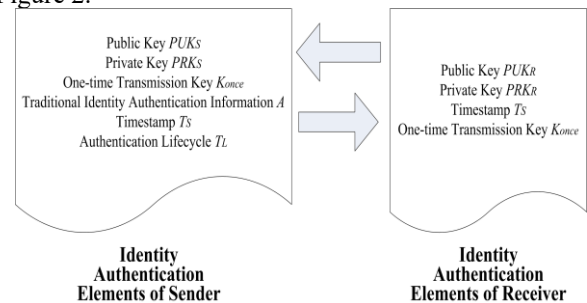


Fig. 2. The Authentication Elements.

3.2.1 Data Sender's Authentication Elements

The authentication elements of the data sender consist of public key, private key, traditional identity authentication information, one-time transmission key, timestamp and authentication lifecycle.

Let the sender's public key be PUK_S , private key be PRK_S . Both keys form the digital identity information of the sender. PUK_S is sent to the data receiver who encrypts transmission data with PUK_S . PRK_S is only stored in the data sender who decrypts the confidential transmission data with PUK_S .

Let the traditional identity authentication information of the sender be A which is shown in Equation (1).

$$A = \{ \langle name, password \rangle \} \quad (1)$$

where, $name, password \in ASCII \text{ Character Set}$, they are the traditional name and password respectively to be used to log on.

Let the one-time transmission key of the sender be K_{once} which is shown in Equation (2).

$$K_{once} = f_{Generate} () \quad (2)$$

where, $K_{once} \in ASCII \text{ Character Set}$. K_{once} can be generated according to the actual situation, for example, randomly or duly. However, it should be strong enough. Let the timestamp of the sender be T_s , which denotes the moment when the sender sends the data to the receiver. Also, it records the beginning moment of the authentication lifecycle.

Let the authentication lifecycle of the sender's timestamp be T_L , which denotes the legal time space between when the sender sends and the receiver receives the transmission data. Both the sender and receiver receive transmission data, they compare the timestamp with the current time. If the time space is less than or equal to T_L , the transmission data are valid. Or else, the transmission data are invalid and the new data are requested to be sent again.

3.2.2 Data Receiver's Authentication Elements

The authentication elements of the receiver consists of public key, private key, timestamp and one-time transmission key.

Let the receiver's public key be PUK_R , private key be PRK_R . Both keys form the digital identity information of the receiver. They have the same meanings as the sender's.

Let the timestamp of the receiver be T_R , which has the same meaning as the sender's.

The one-time transmission key of the receiver is the same as the sender's. It is received to verify whether the receiver's identity is legal when the sender creates the data connection. The authentication mechanism of the proposed method requires both the sender and receiver to be verified by each other with the one-time transmission key and the traditional identity information.

3.3 Authentication process

The authentication process includes 5 stages: data connection, splitting data, encapsulating and sending data, receiving and assembling data, connection close. The stages are described separately in the following.

3.3.1 Data Connection

Let the data connection information of the sender be C_{S1} , which is shown in Equation (3).

$$C_{S1} = \langle PUK_S, T_S, T_L, n \rangle \quad (3)$$

where, PUK_S is the sender's public key, T_S is the sender's timestamp, T_L is the lifecycle of the timestamp, $n \in N$, N is a natural number set, n denotes the amount of the data to be sent.

After the receiver gets C_{S1} , it sends its public key and timestamp to the sender. Its public key and timestamp are merged into C_{R1} , which is shown in Equation (4).

$$C_{R1} = \langle PUK_R, T_R \rangle, \text{ if } T - T_S \leq T_L \quad (4)$$

where, PUK_R is the receiver's public key, T_R is the receiver's timestamp, T is the current time.

After the sender gets C_{R1} , it merges the one-time transmission key and traditional identity authentication information into C_{S2} and sends C_{S2} to the receiver. C_{S2} is shown in Equation (5).

$$C_{S2} = \langle A, f_{PUK_R}(K_{once}), T_S \rangle, \text{ if } T - T_R \leq T_L \quad (5)$$

After the receiver gets C_{S2} , it compares the traditional identity authentication information A in C_{S2} with the receiver's authentication information. If A is verified, the receiver returns a successful information which is C_{R2} to the sender. C_{R2} is shown in Equation (6).

$$C_{R2} = \langle f_{PUK_S}(\text{"Connection OK"}), T_R \rangle, \text{ if } T - T_S \leq T_L \quad (6)$$

where, $f_{PUK_S}(\)$ is a encryption algorithm with public keys.

3.3.2 Splitting Data

Let the data to be sent be D , which is shown in Equation (7).

$$D = \begin{pmatrix} d_{0,0}, & d_{0,1}, & \dots, & d_{0,m-1} \\ d_{1,0}, & d_{1,1}, & \dots, & d_{1,m-1} \\ \dots, & \dots, & \dots, & \dots \\ d_{n-1,0}, & d_{n-1,1}, & \dots, & d_{n-1,m-1} \end{pmatrix} \quad (7)$$

According to what the transmission system requires, D is split into n data blocks. Let the i th data block be d_i , which is shown in Equation (8).

$$d_i = \langle d_{i,0}, d_{i,1}, \dots, d_{i,m-1} \rangle \quad (8)$$

where, $0 \leq i \leq n-1$

The data to be sent could be presented as $D = \langle d_0, d_1, \dots, d_{n-1} \rangle$.

3.3.3 Encapsulating and Sending Data

The authentication elements are used to pack each split datum into a cryptographic unit. Let the cryptographic unit be d_{si} , which is shown in Equation (9). It is about to be sent to the receiver.

$$d_{si} = \langle f_{K_{once}}(d_i), T_S \rangle, \text{ if } T - T_R \leq T_L \quad (9)$$

where, $f_{K_{once}}(\)$ is a symmetric encryption algorithm. If the timestamp of the receiver expires, d_{si} will not be transmit. If the receiver requires to repeat, d_{si} will be sent again.

3.3.4 Receiving and Assembling Data

When the receiver gets a single unit d_{si} it decrypt d_{si} to $f_{K_{once}}(d_i)$ and T_S . If $T - T_R \leq T_L$ is not satisfied, the receiver sends a repeat requirement R , which is shown in Equation (10).

$$R = \langle f_{PUK_S}(\text{"Repeat"}), T_R, i \rangle \quad (10)$$

where, i is the serial number of the unit to be sent again. The receiver sends R in every T_L until it receives the correct d_{si} .

After the receiver get the correct d_{si} , it decrypts $f_{K_{once}}(d_i)$. The receiver which is the only valid one and has the one-time transmission key can recover the original data with a normal method. The unique valid receiver receives the one-time transmission key K_{once} when the data connection is created. The invalid

receivers which do not have K_{once} can not get the original data easily.

The above process represents the single-way authentication for the receiver after the receiver gets a confidential datum unit. The data transmission based on two-way authentication in the proposed method continues if the single-way authentication is passed.

After all transmission data are received, the receiver assembles the data and recovers the original data from the sender. Let the original data be D' , which is shown in Equation (11).

$$D' = \sum_{i=0}^{n-1} d_i, 0 \leq i \leq n-1 \quad (11)$$

3.3.5 Connection Close

When the receiver finishes the data acceptance, it returns a notification message for data connection close to the sender. Let the notification message be C , which is shown in Equation (12).

$$C = \langle f_{PUK_s}(\text{"Connection Close"}), T_R \rangle \quad (12)$$

If the authentication lifecycle is satisfied by T_R , the sender decrypts the message C with its private key. Then it stop sending data and close the data connection.

4 Conclusion

The existed single-way authentication in data transmission ensures data sender to be in security to an extent. However it doesn't verify the identity of the data receiver. An authentication method based on two-way confirmation is proposed in this paper to conquer the above vulnerability. The encryption technologies of public keys and symmetric keys are applied to the proposed method. Based on the traditional identity authentication technology, the one-time transmission key is used to verify the receiver. The timestamp mechanism is adopted to ensure transmission data in time. Both the sender and receiver are confirmed by each other with the proposed authentication method to improve the security of data transmission in networks.

Acknowledgments

This work is supported by the Leshan Science and Technology Plan (No. 17GZD032), the Applied Basic Research Plans of Sichuan Province (No. 2015JY0105), the Scientific Research Fund of Sichuan Provincial Education Department (No. 15ZA0274, 18ZA0233 and

17ZA0201) and the Scientific Research Project of Leshan Normal University (No. Z1415).

References

1. C.L. Li, L.F. Wang, Z.J. Jiang, X. P. Chen. Security Architecture Research Based on Authentication Technology. *Microelectronics & Computer*, **22**(4):8-11 (2005).
2. L. Zhu. A network identity authentication protocol of bank account system based on fingerprint identification and mixed encryption. *Manufacture Information Engineering of China*, **8878**(4):88782C-88782C-4 (2013).
3. R. M. Abdul, D. Anandhavalli. Implementation of image based authentication to ensure the security of mail server. *International Conference on Advanced Communication Control and Computing Technologies*, **2015**:555-558 (2015).
4. P. Gope, T. Hwang. A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Industrial Electronics*, **63**(11):7124-7132 (2016).
5. J. Xiong, J. Zhu. Study on the Security of Network Database in Transmitting. *Computer Science*, **32**(11):127-129 (2005).
6. Y. Niu. User Authentication Protocol Based on Multi-Server Mutual Authentication. *Computer Simulation*, **33**(2):350-354 (2016).
7. X.Y. Hu. Remote Call and Manament of Users' Information of Unified Identity Authentication System. *Journal of Xi'an Technological University*, **35**(9):715-719 (2015).
8. X. Zhang, X.Y. Yang, S.S. Zhu. Trusted and anonymous authentication protocol for mobile networks. *Journal of Computer Applications*, **36**(8):2231-2235 (2016).
9. C.T. Li, C.C. Lee, C.Y. Weng. A dynamic identity-based user authentication scheme for remote login systems. *Security & Communication Networks*, **8**(18):3372-3382 (2016).
10. D.B. David, M. Rajappa, T. Karupuswamy, et al. A Dynamic-Identity Based Multimedia Server Client Authentication Scheme for Tele-Care Multimedia Medical Information System. *Wireless Personal Communications An International Journal*, **85**(1):241-261 (2015).
11. R. Amin, G.P. Biswas. A Novel User Authentication and Key Agreement Protocol for Accessing Multi-Medical Server Usable in TMIS. *Journal of Medical Systems*, **39**(3):33 (2015).