Research on Mobile Security Communication Based on Digital Fingerprint Encryption

Guofang Zhang

Hainan College of software Technology, Qionghai, China

zgf100200@163.com

Keywords: wireless communication; WAP gateway; client; server

Abstract: WAP gateway connects wireless network with wired network, which makes it convenient for mobile terminals to access network servers anytime and anywhere. Traditional mobile clients need to go through WAP gateway to access network servers. Because of the difference between WAP and TCP/IP, the security protocols WTLS for wireless and TLS for wired cannot be unified. When WTLS and TLS are converted in WAP gateway memory, plaintext appears. Once WAP gateway is attacked, it is easy to cause information leakage. To solve this problem, this paper proposes a secure communication scheme from mobile client to network server using public key digital fingerprint technology, which solves the problem of user information leakage and realize the communication security from mobile terminal to network server.

1. Introduce

The innovation of communication technology has promoted the development of mobile internet. Mainly in two aspects, on the one hand, more and enterprises and businesses are transferring their business to the internet. The internet has become the main channel for them to carry out their business. On the other hand, with the popularity of smart mobile phone and the free access to various life software, mobile users prefer to use smart phones for social activities, entertainment, online shopping, living expense and other activities at anytime and anywhere. Users use smart mobile phones to carry out these activities and generate a large amount of data through wireless and wired channels in the network. These data may include user personal identity information, bank card account information, commodity information, mobile phone contacts and another user information. With the rapid development of China's finance and communication industry, the crime of false information fraud has spread in china. Criminals fabricate false information and set up fraudulent schemes by means of communication tools such as telephone and network and modern internet banking technology. Long-distance and non-contact fraud against victims. Encouraging victims to pay or transfer money to criminals causes great losses to the people. Mobile card real-name identity card authentication can be solving the identity authentication relationship between mobile phone and mobile phone holder. But it can't solve the problem of data security transmission from mobile terminal to network server. How to ensure the security of data between mobile terminals and network servers become a problem to be solved. Many mobile communication security incidents have sounded alarms for people, and people have begun to pay attention to the security of mobile communications. To solve these problems, a new solution is proposed in this paper. Using digital public key as the basis of identity authentication and data encryption and data encryption for both parties.

One of the aims of public key fingerprint technology is to enable authentication before mobile terminals communicate with network servers. To carry out public key digital fingerprint authentication, both sides need to make their own digital fingerprints public. How to carry out bidirectional authentication after publishing their own public key digital fingerprints is the first point of this research. The second purpose of digital fingerprint technology is to encrypt and transmit the transmitted data point to point by both parties through authentication. How to ensure that the data

encrypted by the sender can only be deciphered by the receive, this is the second point of this paper. Due to the progress of network detection technology, attackers use the middle position between mobile terminal and network server to obtain the public digital fingerprint forgery data of both sides to deceive. How to solve the problem of middleman deception is the third point of this research. Public key digital fingerprint as the identity of both sides of communication should be secure and unique. How to select the identity of mobile terminal and network server to produce unique public key digital fingerprint is the fourth point of this paper.

2. Vulnerabilities in data conversion between two protocols

Packet communication between mobile client and wired server involves wireless network and wired network. Packets are encapsulated differently in wireless network and wired network. Wireless application protocol (WAP) is used in wireless mobile network communication. TCP/IP protocol is used in wired network. Wireless network is connected to wired network through WAP gateway. WAP gateway is responsible for the conversion, data encoding/decoding and user agent of WAP protocol in wireless network and TCP/IP protocol in internet. These two protocols are structured as shown in Figure 1

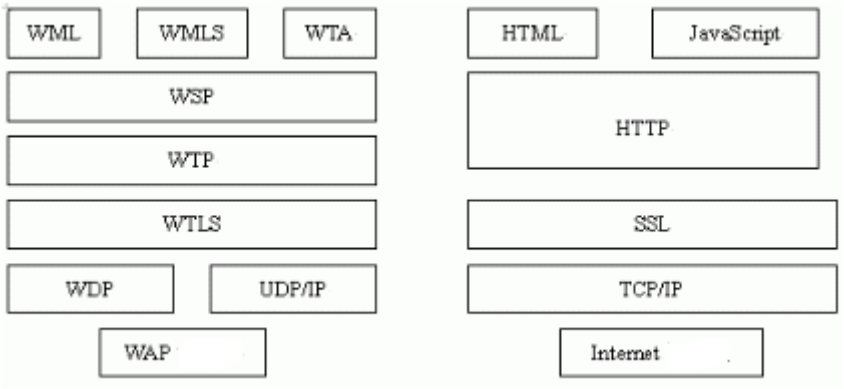

Fig 1 the structure of two protocols

Because WAP protocol guarantees the secure transmission of information in wireless communication through WTLS protocol, and TCP/IP protocol on internet communication security through TLS, consequently, the WAP gateway is responsible for the conversion of WTLS and TLS protocols. As a result, plain text will appear in the memory of the gateway when the encrypted information is converted to WTLS/TLS at the gateway. This easily led to the difficulty of ensuring end-to end information security from wireless mobile terminals to wired servers. To realized end-to-end secure communication between mobile terminal and wired server, it is necessary to ensure that user's personal information does not appear in clear text at WAP gateway. At the same time, gateway can access information without encrypting protection, and the functions of gateway data encoding/decoding, proxy and other functions. A secure access solution for communication between mobile terminal and wired server in this paper. The security layer protocol of TCP/IP is TLS, which is between application layer and transport layer. TLS requires a reliable transport layer, which is guaranteed by protocol. WAP wireless transport layer security protocol WTLS is a TLS-based security protocol and is optimized for narrow-band channels used in mobile communication. The security protocol TLS on the internet cannot be directly applied to wireless communication security. This means that wireless mobile data need to be converted between two encryption mechanisms before it is encrypted by WTLS and encrypted by TLS on the internet. The conversion of these two encryption mechanisms is carried out within the WAP gateway. In the cache of WAP gateway, information will exist in plain text for a certain period. If the gateway is controlled by hackers. The information of the user's personal information will be unsafe, which is a serious security risk.

3. Wireless network security

Data streams sent by mobile wireless clients must pass through AP to reach other mobile clients or wired clients located elsewhere. No direct communication between clients. After the mobile client authenticates to the wireless access point AP, it can relate to other mobile terminals or wired clients. Obviously, the security of this wireless communication is very suitable for implementation at AP. In the early wireless communication, the client authenticated AP in the following ways.

3.1 Open authentication

Open authentication does not need to provide any credentials, SSID is the only credential that need to be provided. Although this makes authentication simple and easy, it cannot control access to WLAN. This authentication method method does not provide measures to encrypt data transmitted through WLAN.

3.2 Shared key authentication

This authentication method stores a wireless equivalent protocol (WEP) key on the wireless client and AP side. When the client wants to join the WLAN, AP sends a challenge phrase to client. The client must use challenge phrase and WEP secret key to calculate a public shared value and send it to AP. At the same time, AP calculates a shared value using its own WEP secret key and challenge phrase. If the two shared values are the same, the client will pass the authentication.

The secret key of this authentication method is also used to encrypt the data of wireless communication. The secret key and the encrypted cipher text are sent to the remote end. After receiving the data from the remote end, the original text is decrypt with the received secret key. This kind of communication has the danger that the secret key is acquired by a third party.

3.3 A method based on external authentication and authorization

Extensible authentication protocol (EAP) is a kind of security authentication protocol. Many wireless security authentication methods are based on this protocol. For example, LEAP, EAP-TLS,PEAP,etc. EAP-TLS uses transport layer security protocol (TLS) to ensure the security of client authentication. EAP-TLS uses digital certificates as authentication. Both the wireless client and the AP terminal must have a digital certificate. These certificates are issued by the CA of the authentication authority center. Both sides authenticate their identities through the authentication server. This security method can also realize the the encryption of wireless data. The secret key of data encryption is realized by automatically generating WEP secret key when the authentication server requests the client to re-authenticate. When the wireless client authenticates, it will use different TLS session keys. When the client wants to join the WLAN, AP sends a challenge phrase. The client uses the challenge phrase and the TLS session key to derive the unique WEP key. The WEP key is used to encrypt the wireless data.

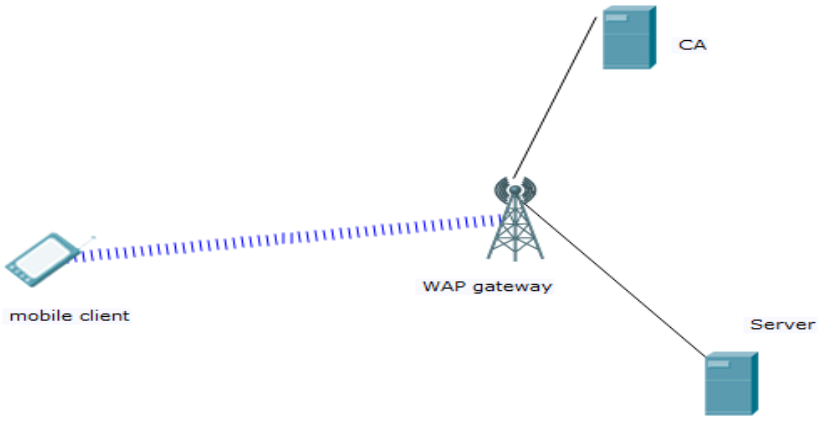

Fig 2 communication between wireless client and server

4. Public key digital fingerprint scheme

Digital fingerprint is a public mark of communicator on digital certificate based on RSA asymmetric encryption algorithm. The mobile client uses the public key digital fingerprint of the digital certificate of the network server as the key to encrypt data, and the network server uses the public key digital fingerprint of the digital certificate of the mobile client as the encrypt data, which can ensure the communication security between the mobile client and the network server. The scheme of using public key digital fingerprint to realize secure communication between mobile client and server is as follows.

4.1 Generating digital fingerprints

Servers,clients, mailboes and website on the network can apply for their own digital certificates. The institutions responsible for generation digital certificates are CA, and CA is the authority of digital certification. Generating digital certificates for servers and clients requires detailed information from both servers and clients. For security, it is necessary to provide MAC address, domain names, manager's identities and telephone information of servers. To apply for digital certificates for mobile clients, information such as MAC address of mobile clients, identity card of mobile client holders, access telephone and so on are needed.

4.2 Storage of digital certificate

When CA generates digital certificate, it generates the private key corresponding to the digital certificate, which is issued by CA to the client and server respectively. When CA issues the digital certificate to the server, it also sends the private key of the server to the server, which is saved by the server. Clients store their private keys and digital certificates on their devices. Because private keys can only be held by clients and servers, they need to be stored securely and cannot be leaked, so the server and the client should keep their private key well. The server's public key digital fingerprint is stored on the server's digital certificate as the unique identity of the server, and the client's public key digital fingerprint is stored on the client as the unique identity of the client.

4.3 Identity authentication process

The mobile communication security scheme proposed in this paper involves three-party communication identify authentication, client and AP identity authentication, AP and server identity authentication, client and server identity authentication. When the client and AP authenticate, both sides provide their digital certificates to each other, and then both sides want the authoritative CA center to inquire. When the CA authentication is passed, both sides pass the authentication. The same is true for AP and server authentication, client and server authentication.

4.4 Implementation of secure communication

After the identity authentication of wireless client, WAP gateway and server, data should be encrypted for the sake of communication security. The communication between client and WAP gateway is wireless communication, while the communication between WAP gateway and server is wired communication. Because of the difference between WTLS and TLS on data format, the WAP gateway needs to be converted. The secure communication scheme in this paper is based on secondary encryption. First, the client uses the server's public key to encrypt the data for the first time, then uses the WAP gateway's public key to encrypt the data for the second time, and then the data is sent to the WAP gateway. At the WAP, the wireless encrypted data is decrypted. The decrypted data is encrypted by the server's public key, which is signed by the client. The encrypted data between the WAP gateway and the server is sent to the server using TLS encryption algorithm. When the server transmits data to the client, it uses the client's public key to encrypt the data, uses the WAP's public key to encrypt the data for the second time, sends the data to the WAP. The data

was decrypted In the WAP gateway, and then the data was encrypted in WTLS encryption algorithm and was transmitted to client. The client decrypt the received data, verifying, and then decodes it after verification,then getting the plain text.

5. Conclusion

In this paper, the communication scheme of double encryption between mobile client and server by using digital public key encryption is proposed. When the information is converted to WTLS/TLS in WAP gateway, no plaintext information will appear in the memory of WAP gateway. This solves the problem of user information leakage caused by WAP gateway attack, and prevents the intermediate hijacking attack by signing data, thus guaranteeing the communication security between mobile terminal and server.

Acknowledgements

This paper is supported by “Hainan Provincial Natural Science Foundation of China:618MS080”

References

[1] GUO-FANG ZHANG. The solution and management of VPN based IPSec technology. International Journal of Technology Management 2014.7.

[2] Guofang Zhang Weitao Li. A security reinforcement scheme for the server.

[3] WOP in education social sciences and psychology. 2018.7

[4] Bai Maren, Security reinforcement of the server.

[5] http://baijiahao.baidu.com/s?id=1569896489965322&wfr=spider&for=pc.

[6] Samland, server security reinforcement and service optimization.

[7] https://wenku.baidu.com/view/fe2d56b0312b3169a551a4ef.html

[8] Windows 2003 server safty reinforcement scheme.