An Improved TLS handshake protocol

LI Xian-Zhu[1], LIU Jun[2]

[1]Postgraduate Team, Institute of Command information system, PLA University of Science and Technology,Nanjing 210007, China;

[2.]Institute of Command information system, PLAUST

13770828947@sina. cn

Keywords: transport layer security, TLS, identity based encryption

Abstract: The transport layer security protocol (TLS) used in the Internet exist complex certificate management shortcomings and highly handshake delay due to the use of the certificate, IBE avoid the above problems by not using the certificate. he article introduces the identity based encryption system into the TLS handshake protocol, and design a new handshake protocol. Analysis shows that, compared with the identity based encryption system on certificate based scheme, the cipher algorithm processing time increases slightly, communication amount has reduced, the handshake delay is significantly reduced and the protocol efficiency is greatly improved.

Introduction

Nowadays, the main protocol to realize secure communication in transport layer are SSL (Secure Socket Layer) and TLS (Transport Layer Security). SSL and TLS based on Reliable TCP and lie between transport layer and application layer. The TLS protocol is developed from the SSL protocol. So application layer could transport all kinds of data transparently to guarantee data's security and confidentiality through TLS. Having been widely used on the Internet, TLS has been widely accepted in transport layer security. Nowadays, the long handshake delay is the important deficiency of TLS. Because TLS uses Public Key certificate in the authentication process between client and server, the process of certificate's transmission and dispose result in the long handshake delay. This article designed a new TLS handshake protocol based on Identity-based cryptograph (IBC). Made improvements to existing protocol, it reduces the handshake delay and gives consideration to security. Also, it can improve the performance of the protocol.

TLS protocol

TLS handshake protocol. TLS is one of the widest used security protocol on the Internet currently. It is widely applied to electronic Commerce and Electronic Government to ensure systems running. Through long-term application and development, the security and practicability of TLS have got universal approval .TLS is made up of recording protocol and handshake protocol: Recording protocol lying in the low player of ILS is used to package Upper-layer protocol transparently .Recording protocol groups and compressing disposes data and submits transport layer protocol after encryption when it sends information in the process of communication. Recording protocol Decrypt and check first, decompresses and then sends data to upper layer's client when it accepts l messages in the process of communication. Handshake protocol lying in the upper layer of TLS is the hard core. It is used to establish session for communication between two parties, including cryptographic algorithm's consulting, session key generating and other functions. It's the premise of securely communication between two parties. Handshake protocol's message process [1] as illustrated in FIG 1. There, client is the side to send chaining and server is the side to accept chaining.

Step one: Client sends "client Hello" and Server sends "Server Hello". Both sides consult Cryptographic Algorithm, key exchange algorithm, MAC Algorithm and so on used in communicate and consult Security Parameters.

Step two: If server should be authenticated, “certificate” is sent to client to check identify. Server sends “Server Key Exchange” for key exchange with client. If client should be authenticated, “Certificate Request” is sent to request client to sent certificate. At last, send “Server Hello Done” to show message finishing.

Step three：After receiving the message, client validate the legality of Server’s Certificates first, and check that Security Parameters demanded by server can be received or not. Client sends “Certificate” to Server to supply certificate. And then send “Client Key Exchange” to exchange the secret key and send “certificate verify” to assure Server’s certificate.

Step four: Both sides send “Change Cipher Spec” to Switch to the new cryptographic algorithms and send “Finished” to finish secure connection’s establishment. So far, secure connection is ok and application layer could communicate security.

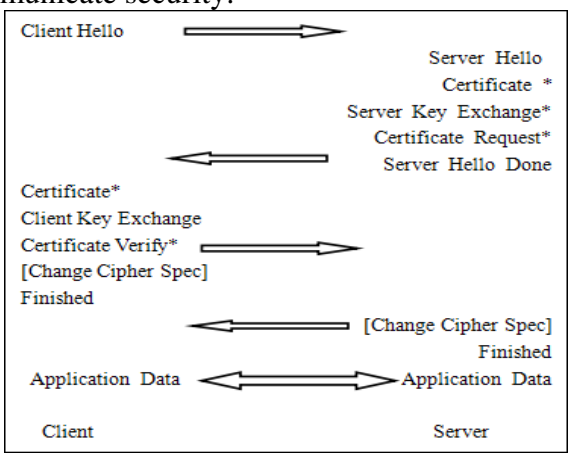

Figure 1 TLS handshake message flow

encryption scheme used by TLS. To realize the mutual Authentication between Client and Server in TLS, Pre-shared Key symmetric cryptosystem or Certificated-based public key cryptosystem have been used. There are many advantages including less computing time, less amount of data transmission and shorter handshake delay to apply Pre-shared Key. However, Its key management is more complicated so that it’s not suitable for the application in large-scale network environment. By contrast, applying the public key cryptosystem is more common in practical applications.

Realizing authentication and Key Exchange is accomplished by PKI (public Key Infrastructure) ssuing the public key certificate in Certificate based TLS protocol. Public key cryptosystems that applied in TLS include RSA and elliptic curve cryptosystem (ECC). The public key cryptosystem based on RSA has been applied in a large number of existing systems. Contrasting RSA, ECC uses shorter secret key to achieve the same security strength. The TLS protocol based on certificate need to use certificate that issued by PKI so as to realize the link between the identity and public key. Certificate based TLS exist shortcoming of low efficiency of management in practical application. On the one hand, certificate exchange lead to more communication expenditure; On the other hand, the computational overhead of certificate inquiry result in delay increasing. In addition, the construction and maintaining of PKI need higher expense, and system complexity increase.

Based on the discussion above, this article put forward an IBC based TLS handshake protocol. The protocol designed on the basis of bilinear mapping principle. The public key can be calculated directly through identity information to avoid transmission overhead and certificate processing overhead due to the applying of the certificate. What’s more, it simplifies systems structure and increase protocol efficiency.

IBC based cryptosystem

Main idea of identity-based cryptosystem is to take the only user’s identity as a public key, rather than using a digital certificate. The public key can be defined by any meaningful fields related to user's identity, such as IP address, Email address, etc. While the Private Key is generated by the

PKG (Private Key Generator). IBC has the following advantages compared with PKI. 1) Public key defined by the user's public identity information, which don't need a trusted authority to store the public key. 2) Signature verification for entities, public key encrypting and session key calculating with public key directly and do not need to validate first. Identity-based cryptosystem avoid high cost and complex processing by applying the certificate.

The research of IBC. Shamir [2] proposed identity-based public key cryptosystem (IBC) in 1984. IBC mainly includes two parts, identity based encryption (IBE) and identity-based signature (IBS). There are two problems in the IBE system put forward by Shamir. 1) How to prove their identity to many trusted third party.2) How does the trusted third party send the user's private key security to the user Boneh [3] put forward the first practical IBE scheme in 2001.The encryption scheme based on identity with bilinear pairings .Since then, the bilinear mapping function has become the important means of identity based encryption system .But low computing efficiency is one of the main drawback, resulting in the difficulty in practical application. Later Boneh [4] proposed an effective IBE scheme. It is security under identity selected attack security model. And they put forward tow IBE systems based on determining bilinear Diffie-Hellman assumption and bilinear Diffie-Hellman substitution assumption.

In the current applications, the most frequently mentioned and widely used is Boneh-Franklin's idea. It is very classic by applying the bilinear mapping and Weil pairing principle .Its principle is as follows. Set G1 as a q order of additive group, G2 as a q order of the multiplicative group, q is a safety large prime Number, bilinear mapping e: $G1 \times G1 \rightarrow G2$ has the following properties [5]:

Bilinear For all the $P, Q \in G1$, $x, y \in G2$, exist $e(xP, yQ) = e(P, Q)^{xy}$.

non-degeneracy exist $P, Q \in G1$, making $e(P, Q) \neq 1_{G2}$.

Calculability There is an algorithm that for any $P, Q \in G1$, $e(P, Q)$ can be efficiently calculated.

Encryption scheme and digital signature scheme provide the confidentiality, integrity, non-repudiation and authentication security guarantees for the system .The research on IBC mainly covers encryption, digital signature and authentication key negotiation, etc. Since Boneh-Franklin IBE scheme was put forward, Boneh and Franklin's research constructs the first safe and practical identity based encryption scheme with bilinear mapping, making the identity-based public key cryptosystem to become the focus of research. A series of technology research based on the scheme appeared. Boneh-Franklin IBE has been written into the international standard of IBE. IETF released RFC 5091 [6] that describes the Boneh- Franklin IBE implementation of the algorithm in 2007. IETF released RFC 5409 [7] in 2009 show how to use Boneh-Franklin IBE algorithm with the cipher message syntax.

Identity Based Encryption. Boneh-Franklin IBE scheme [3] based on the bilinear mapping, Weil matching principle. The scheme is composed of four stages. Respectively they are the system parameters, the private key generation, encryption and decryption.

1) setup PKG produce a big prime number q with the safe parameter "t", put out params = < q, G1, G2, e, n, P, pub, H1, H2 > and the main secret key "s".G1 is the group of points of an elliptic curve over Fp and G2 is a subgroup of F *p 2. Therefore, we view G1as an additive group and G2 as a multiplicative group. A map e: $G1 \times G1 \rightarrow G2$ is said to be bilinear .N intends the length of plaintext, P is a generating element in G1, let s be a random number in Z_q^*, let s be the main key of the system, pub = sP, Hash functionH1: $\{0,1\}^* \rightarrow G1^*$, Hash function H2: $G2 \rightarrow \{0, 1\}^n$. PKG keep s and open params.

2) Extract PKG produce public-private key pairs for a given identity ID, calculating QID = H1 (ID), take the result QID as public key,then calculate $S_{ID} = sQ_{ID}$, take S_{ID} as the private key, Then pass the private key in security means.

3) Encrypt Plaintext M, With the public key calculated above, select a random number "r" randomly,and $r \in Z_q^*$, Calculated the ciphertext $C = < rP, M \oplus H_2(gr) >$, $g = e(Q_{ID}, P_{pub}) \in G_2^*$.

4) Decrypt The encrypted plaintext C = < U, V > With the public key related to identity ID, Decrypt it With the corresponding private key and get clear $V \oplus H_2(e(S_{ID}, U)) = M$, Because the

bilinear pairings' nature, e (S_{ID},U) = e (S_{ID}, rP) = e (Q_{ID}, P_{pub})^r = g^r, So the decryption is plaintext.

the secret key exchange protocol. Diffie and Hellman put forward Diffie-Hellman key exchange algorithm in their paper [1]. Nowadays, the algorithm is still considered the most effective and safe key exchange algorithm. The main idea of the algorithm based on the difficulty of computing discrete logarithm problem in finite domain, realizing the distribution of the key in public channel. But the algorithm does not support key authentication, but also can't resist the middle attack. Literature [8] improved the algorithm by adding user's identity information in the protocol, it implements key exchange and authentication at the same time, and improved the safety. Its key exchange process is as follows: Two large prime Numbers p, q, n = pq, calculating ((n) = (p - 1) (q - 1), g is a primitive root on GF(n), in the interval select two primes e, h in the interval (0, ϕ (n)), calculate the integer de = 1 mod ϕ (n).

1) According to customer's request, PKG select a random integer Xc, Then calculate the user identity IDc by h^{eXc} IDc=1modn ,PKG keep ϕ (n) and d ,open parameter n, g, e, hand user identity IDc Send X_c to clients.

2) Client C select a random integer Rc, with the open parameters, calculate T_c = ($h^{Xc}g^{Rc}$) modn, then send Tc to another client S.

3) WhenS received T_c, select a random integer Rs, calculate Ksc = ($T_c{}^e ID_c$)^{Rc}modn, and calculate T_s=($h^{Xs}g^{Rs}$)mod n. Send (T_s) to client C.

4) When C received Ts, calculate Kcs = ($T_s{}^e ID_s$)^{Rs}mod n. It can be proved that Kcs = Ksc, so we realized the distribution of Shared secret key.

An attacker that attempt to get the key by intercept the information, need to solve the large integer factorization and discrete logarithm problem at the same time. It is not feasible in calculation. Compared with Diffie-Hellman key exchange scheme, the protocol can realize the key exchange, but also resist the middle attack by identity authentication. The difficulty to crack the key will increase. The Authentication scheme are no longer in detail in this paper.

Handshake protocol design based on IBE

Handshake protocol based on RSA or ECC scheme need to pass certificate in the process of protocol, that takes a further communication overhead. This article proposes a new handshake protocol scheme based on IBE which realized no certificate authentication in the protocol. Thus effectively reduced the communication overhead, reduced the protocol handshake delay and improved the performance of the protocol. According to the practical application and security needs, designed a new handshake protocol based on the IBE mechanism, but also expand to record agreement to support new handshake protocol messages .We assume that the PKG generated system parameters and the private key before the handshake protocol .Finished generating main secret key, System parameters and the private key of each node, all parties of communication have the common system parameters and obtain their private key.

The message flow of TLS handshake protocol based on Boneh-Franklin IBE as shown in figure 2.Compared with traditional solutions as RSA, the server don't have to send certificate to the client for authentication due to the IBC encryption scheme. The client can directly get the server's public key when communicating .If the client authentication is required, server sent "Identity Request" to client to require the client to provide identification. The client also does not need to send the certificate for authentication and just need to provide authentication information. The protocol reduced the amount of messages in the process of shaking and reduced traffic, also it improved the efficiency.

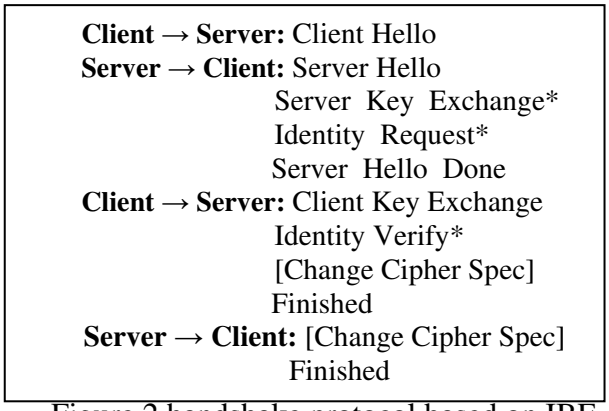

Figure 2 handshake protocol based on IBE

In the handshake protocol based on IBE, use the improved DH key exchange scheme mentioned above to generate session key. Assuming that the system PKG has set parameters for key exchange protocol before execution, including large prime numbers p, q and prime e, h on open interval (0, ϕ (n)), and set a random integer x_c to user ,then calculate the user identity according to h^{eXc} IDc =1modn, the protocol process is as follows.

Step 1 The Client sends the "Client Hello" message to the server, and declares the cipher suite supported. Server choose the same cipher suite and send message "Server Hello" to client,finish setting security parameters. The parameters for key exchange protocol has been generated before handshake protocol by PKG and sent to the user safety.

Step 2 Server select a random integer R_s, calculate Ts = ($h^{Xs}g^{Rs}$) modn, Encrypt Ts with the client's public key $Q_c = H_1(ID_c)$ and get $K_{pubc}[T_s]$, Then send it to client in message "Server Key Exchange", send message "Identity Request" at the same time to request the client authentication. If client authentication is not required, send Ts to cilent for key exchange directly. The server send the finish message "Server Hello Done" at last.

Step 3 If client authentication is required, Client decrypt the message with its own private key and get Ts when message arrived .Client get Ts directly if client authentication is not required. The client choose the random integer R_c, calculate T_c = ($h^{Xc}g^{Rc}$) modn, Encrypt T_c with the server's public key $Q_s = H_1 (ID_s)$ and get $K_{pubs} [T_c]$, Then send it to server in message "Client Key Exchange". Client send message" Identity verify" for verifying. Client and server can calculate the session key after the above steps. The client calculated Kcs = ($T_s^e ID_s$) Rsmodn, the server calculated Ksc = ($T_c^e ID_c$) Rcmodn. It can be proved that Kcs = Ksc according to the above content .The session key 'k' can be calculated according to the rules of cipher suite. Then, Client and Server get the same session key 'k'.

Step 4 When handshake is completed, client and server send message "Change Cipher Spec" to each other, and switch to the new cryptographic algorithms, send message "Finished" to check the validity of the session key. The establishment of a secure connection has completed and the communication began.

Security and performance analysis

Security analysis. Next we analyst the security of the protocol scheme respectively from the IBC based system itself and the handshake protocol.

The security of the IBC has been widely accepted. BF-IBE has been proved that it can resist chosen ciphertext attack in the random oracle model. The secret key which generated in the protocol of this article is randomness. Its security based on solving the large integer factorization and discrete logarithm problem at the same time [8]. The attacker need to solve above two problems at the same time to get the exchanged key from information delivered .We believe that there exist no algorithm to solve the problems above in polynomial time. So the IBC is considered to be safe base on the assumption.

Considering with the security mechanism of TLS, the TLS handshake protocol based on the IBC has features including security, confidentiality, integrity and non-repudiation. We assume that both server and client have got their own public-private key pairs from PKG before communication.

Authentication: In the process of handshake, the Client sends the message “Client Hello” to the server, containing the Client identity information. And encrypt it with server’s public key to ensure that only the server could decrypt the message with its own private key. Then server send message “Server Hello” to client, it’s encrypted with the client's public key. Only the client has the access to decrypt with its private key and assure that only the Server could send message “Server Hello”, Which realized the identity authentication.

confidentiality: During the process of communication, the two sides get a session secret key with shared secret key consultation scheme and encrypt communication data with the session key. The secret key agreement protocol ensures that only can communication parties get the session key, which guarantees the communication content’s confidentiality.

Integrity: The communication parties need to declare the cipher suite selected when shaking hands in the first time. generate the message authentication codes through the hash function, it can prevent the data from being delayed, rearranged, deleted, etc, which realized the integrity protection.

In addition, due to the applying of identity-based encryption system, it can also resist the middle attack while guaranteeing the authentication. A new random number will be generated every time exchange the key. The generated session secret key is fresh to resist replay attacks. The protocol is forward secure, the attacker is unable to get the secret key of the session even if the attacker got the private key.

Performance analysis. Considering the cipher algorithm processing time, the IBC cost more time than the traditional RSA and ECC, etc. But with the development of technology and the gradual improvement of the computer performance, processing ability rise, the processing time of IBC will decrease more. Now a variety of more efficient operation methods have been proposed, which makes the processing time of IBC get closer and closer to the RSA algorithm. Compared with the handshake delay reduction by reducing the interactions and traffic, the cipher algorithm processing time increased is not too much.

, Time for certificate parsing is generally long when parsing the message. The message processing time of IBC based handshake scheme effectively reduced because there is no Certificate. The transmission delay in certificate-based scheme is much longer as transmission of certificate chain cost more time. However, because there is no certificate to transport, scheme based on IBC effectively reduced the traffic, and greatly reduced transmission delay for fewer handshakes.

In conclusion, the handshake delay of IBC based TLS handshake protocol is shorter than certificate based scheme, and effectively improved the Performance of the protocol. It is more suitable for lower-speed transmission networks, such as wireless network or space network environment.

Summary

This article introduces identity-based cryptosystem into the TLS handshake protocol, and proposes a new protocol without certificate. The protocol avoids overhead of transmission and processing of certificate, and efficiency improved. The analysis shows that, the cryptographic algorithm processing time of this scheme is close to the certificate based scheme, furthermore, it greatly reduced the handshake delay, improve the efficiency of the protocol.

How to reduce cipher algorithm processing time of handshake protocol and reduce the computational overhead will still be the focus in next research, and research to optimize the service side and improve practicability .In addition, the complex network environments, such as the space network, should be considered, which requires to design better handshake protocol that adapt to the network environment .

References

[1] BONEH D; FRANKLIN M K. Identity-based encryption from the Weil pairing, 2001.

[2] BONEH D; BOYEN X. Efficient selective ID secure identity based encryption without random oracles, 2004.

[3] BOYEN X; MARTIN L. Identity-based cryptography standard (IBCS) # 1: supersingular curve implementations of the BF and BB1 cryptosystems, 2007.

[4] Li Jialan; Lu Jian; Zhu Jianzhang. The authentication key exchange that resist the middleattack, 2005

[5] MARTIN L; SCHERTLER M. Using the Boneh-Franklin and Boneh-Boyen identity-based encryption algorithms with the cryptographic message syntax (CMS) , 2009.

[6] Peng Changyan; Zhang Quan; Tang Chaojing The IBC based TLS handshake protocol design and analysis, 2009.

[7] SHAMIR A. Identity-based cryptosystems and signature schemes, 1984.