Design and realization of a network security model

Jiahai Wang, Fangxi Han
School of Computer Science & Technology, Shandong University

Zheng Tang, Hiroki Tamura and Masahiro Ishii
Faculty of Engineering, Toyama University

Abstract: The security of information is a key problem in the development of network technology. The basic requirements of security of information clearly include confidentiality, integrity, authentication and non-repudiation. This paper proposes a network security model that is composed of security system, security connection and communication, and key management. The model carries out encrypting, decrypting, signature and ensures confidentiality, integrity, authentication and non-repudiation. Finally, the paper analyses the merits of the model.

Key words: information security; security connection; data transmission; key management

1. Introduction

We live in a world of computer and electronic network. Governments and businesses rely heavily on computerized processes for most, if not all, of their day-to-day activities. Citizens sending E-mails from their home computer, head office communicating with branch plants, and nations sharing critical information all contribute to the skyrocketing increase in Internet usage. It is the Internet that is well on the way to becoming the primary platform for global commerce and communications. The very openness that has encouraged the Internet's explosive growth, however, also makes it difficult to ensure that Internet secure. Before committing their sensitive communications to the Internet, users require specific assurances: protecting privacy by ensuring that electronic communications are not intercepted and read by unauthorized persons; assuring the integrity of electronic communications by ensuring that they are not altered during communication; verifying the identity of the parties involved in an electronic communication; ensuring that no party involved in an electronic communication can deny their involvement in the communication. In a word, secure Internet needs confidentiality, integrity, authentication and non-repudiation.

2. Cryptography technology[1][2]

Cryptography technology is a key technology that can ensure the secure transmission of information and end-to-end security of the communication.

An encryption algorithm is a procedure which takes the original message (plaintext) and a small piece of information arranged in advance between sender and recipient (the key) and creates an encoded version of the message (the cipher text).There are two kinds of cryptographic algorithm: the private key algorithm (symmetrical algorithm) [1] and the public key cryptographic algorithm (asymmetrical algorithm) [2]. In the private key algorithm, the encryption key is the same to the decryption key, if sender and recipient want to exchange encrypted information, they both need to possess one private key, which is kept secretly between them. This key is needed for both encryption and decryption of the message. So the security depends on the same secretly key shared by both sides. The best-known and most widely used private key algorithm is the U.S. Data Encryption Standard (DES).

But in the public key algorithm, the encryption key (the public key), is significantly different from the decryption key (the private key). The public key is used to encrypt a message and the private is kept secret, Every person has a unique key pairs, for example, everyone can encrypt message to recipient with recipient's public key, but only recipient will be capable of decrypting the message, by using its secret key. The security depends on the fact that it is computationally impossible to attempt to derive the private key from the public key. RSA is a famous public key algorithm.

Cryptography allows data to be transmitted across a vast public network such as the Internet while preserving the confidentiality of its contents. Message digest function aims to prevent anybody from altering the data, so it can keep the integrality of information. A typical message digest function (commonly is a one-way hash function) takes a variable-length message and produces a exclusive fixed-length hash. Given the hash it is computationally impossible to find a message with that hash, in fact one can't determine any usable information about a message with that hash, not even a single bit. It's also computationally impossible to determine two messages which produce the same hash. Changing even a single letter of information would cause the message digest to become completely different. The best commonly used message digest function is MD5, it produces a 128-bit hash.

For guaranteeing somebody's identity and preventing somebody from denying his dealing, we must use digital signature technology. Digital signature can be used to uniquely sign an electronic document. Similar to the RSA public key algorithm, but this time using the private key to encrypt the electronic document, as long as you don't let anybody know what your private key is, it will take impossibly large amounts of computing power to forge your digital signature. It is an extremely good idea to sign electronic documents by using your private key to encrypt the message digest of the document. A message digest is a relatively short block of numbers that prevents anybody from altering you document.

3. Design and realization of network security model

3.1 The architecture of model

Now, we can use the technologies mentioned to design a network security model that provides all operation. The model consists of three parts: security system, network connection and data transmission, key management. The model architecture is shown in Fig.1.

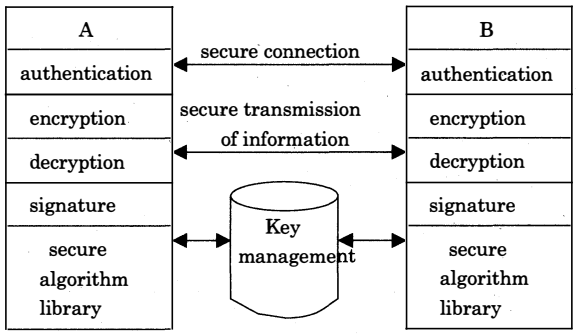

Fig.1: The architecture of model

Security system is a mixed encryption system including private encryption algorithm DES, public encryption algorithm RSA, message digest function MD5, algorithm for generating key and algorithm for producing random number. It is the main provider of security function[3][4][5].

As the network connection and data transmission, when both sides want to communicate with each other, they must transmit the information of authentication to guarantee identity of each other according to authentication protocol. After successful authentication, both sides can transmit data[6].

Key management has several basic functions including key generating, registration, storing, distribution, retrieving, updating and revocation. It runs through whole process of information transmission. This model adopts distributed key management scheme, in which every user generates his own key pairs. The key distributed center (KDC) manages all the generated public keys of users, but the generated private key is kept by themselves. Every local network's user group has a KDC that is called local KDC. The local KDCs directly manages each user of the local network's user group. If a lot of local networks are interconnected, all the local KDC are also interconnected and form the structure like a tree[7].

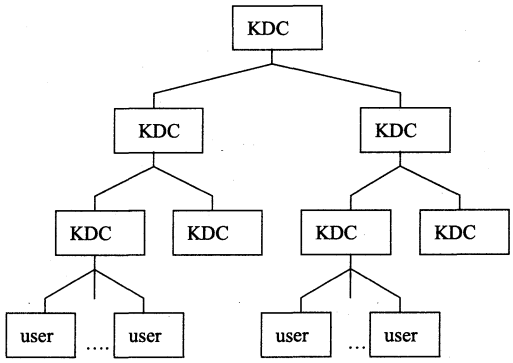

Fig.2 :The structure of distributed KDC

In the figure, the leaf node denotes user. Each KDC contains lower level KDC and users. Higher level KDC looks lower level KDCs as common users.

KDC has several functions:

1: Key registration: Adding the public key of new users to the address list of KDC after checking up the user's identity.

2.: Key Updating: When KDC receives user's requirement of updating public key, KDC then accepts the public key which user has produced and updates the user public key list.

3: Key retrieving: When KDC receives user's requirement of retrieving public key, KDC returns the corresponding public key by the way of recursive retrieving.

4: Key revocation: When KDC receives user's requirement of public key revocation, KDC then delete is the corresponding public key and the item of address list.

4. Security layer of the model

Internet bases on TCP/IP protocols including application layer, transport layer, Internet layer and network interface layer. This model adds a "security layer" between application layer and transport layer as shown in Fig.3. All the security functions are carried out by the security layer. The information transmission bases on TCP protocol that is connection-oriented.

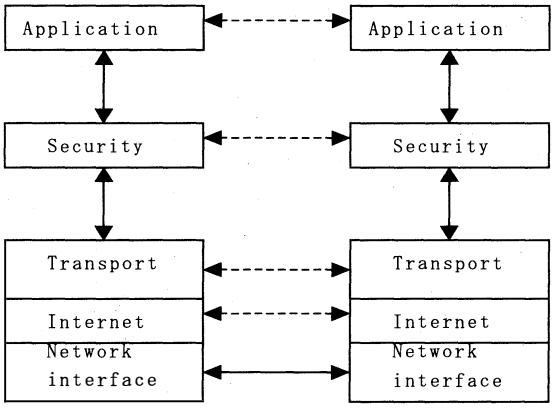

Fig.3: The model of the a "security layer" between application layer and transport layer

The best thing about all these encryption, decryption, verifying and authenticating processes is that "security layer" does them all transparently, so that both sides receive the assurances they need without having actually to engage in computations themselves.

5. The process of the model

5.1 Getting the public key of both sides

The public keys are placed in the KDC, so if user A wants to communicate with user B, A at first he will find out what B's public key is, so he will send a request to the key server (KDC) to get the public key.

The process of getting the public key of each other is: at first, A sends a request to the KDC to get B's public key, then KDC researches the address of B in the local address list. If KDC finds B, it indicates that A and B belong to the same user group managed by KDC. So KDC returns B's public key to A, at the same time, it returns A's public key to B. Else if KDC does not find B in the local address list, it indicates that B belongs to other user group. In this case, the request of getting public key is handed on through every layer of distributed KDC by the recursive way until local KDC that manages the B directly is found. Then the local KDC returns B's public key to A and returns A's public key to B. So both sides get the public key of the other side.

5.2 setting up the security connection

Having got the recipient's public key, authentication information is transmitted between sender (A) and recipient (B). The whole process is shown in Fig.4.

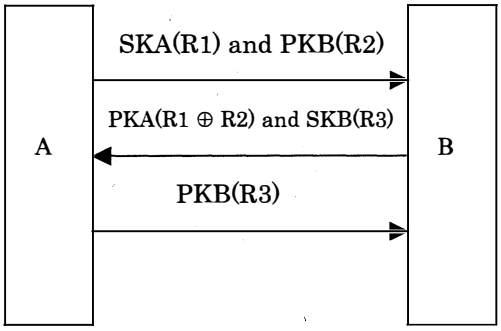

Fig.4: The process of identity authentication

First, sender generates two random numbers R1 and R2, then encrypts R1 using his own private key SKA and encrypts R2 using recipient's public key PBK. The results of encryption are SKA (R1) and PKB (R2) and sender sends SKA (R1) and PKB (R2) .

Next, when having received the SKA (R1) and PKB (R2) , recipient decrypts SKA (R1) using sender's public key PKA and decrypts PKB (R2) using his own private key SKB, the results of decryption are PKA (SKA (R1)) =R1 and SKB (PKB (R2)) =R2. Then the recipient generates a random number R3, and encrypts (R1⊕R2) using sender's public key PKA and encrypts R3 using his own private key SKB . The results of encryption are PKA (R1⊕R2) and SKB (R3) , and recipient sends PKA (R1⊕R2) and SKB (R3) .

Finally, when having received the PKA (R1 ⊕R2) and SKB (R3) , sender decrypts PKA (R1⊕R2) using his own private key and decrypts SKB (R3) using recipient's public key, the results of decryption are R and R3. If R equals the original number (R1⊕R2), then sender encrypts R3 using recipient's public key, the result of encryption is PKB (R3) , else sender breaks the connection and stops communication because it indicates that "recipient" is not a real person with which sender wants to communicate. When recipient recieves the PKB (R3) , he decrypts it using his own private key, if the result of decryption equals original number R3, recipient thinks the "sender" is a real person with which he wants to communicate, else he breaks the connection.

Sender encrypts the message using recipient's public key. Because recipient keeps his own private key, only he can successfully decrypts the message. Sender signs the message using his own private key, so recipient can identify the source of information. The whole process of handshake completes the authentication.

5.3 Data transmission

Data transmission is based on TCP protocol that is connection-oriented. The whole data process includes encryption, signature, decryption and validation and ensures confidentiality, integrity, authentication and non-repudiation.

Sender applies MD5 algorithm to the message, converting it to a fix-length (128 bit) string called a message digest. This message digest acts as a "digital fingerprint" of the original message. If the original message is changed in any way, it will not produce the same message digest when the hash function is applied. Sender encrypts the message digest using his private key, and produces a digital signature of the message.

Then he encrypts the message to which the digital signature is "attached" using a one-use private key (the session key) that has been randomly generated specifically for the message and gets the digitally signed, encrypted message. And, he encrypts the session key using recipient's public key. Since the message-specific private key (the session key) is typically small in comparison with the message, the combined encryption approach provides the speed benefits of private key encryption along with the manageability of public key encryption.

Finally he transmits the digitally signed, encrypted message and the encrypted session key.

When recipient receives the digitally signed, encrypted message and the encrypted session key, he firstly uses his private key to decrypt the encrypted session key. Then he uses the session key to decrypt the digitally signed, encrypted message. As only his private key can decrypt a message encrypted with his public key, the confidentiality of the message is assured.

Recipient then uses sender's public key to decrypt the digital signature, revealing the message digest. Since only sender's public key can decrypt the digital signature, he is able to

verify that sender is the true sender of the message. To verify the message content, Recipient applies the same MD5 algorithm to the message he received from sender. The message digests should be identical. If they are, recipient knows the message has not been changed and he is assured of its integrity.
The whole process of data transmission is shown in Fig.5.

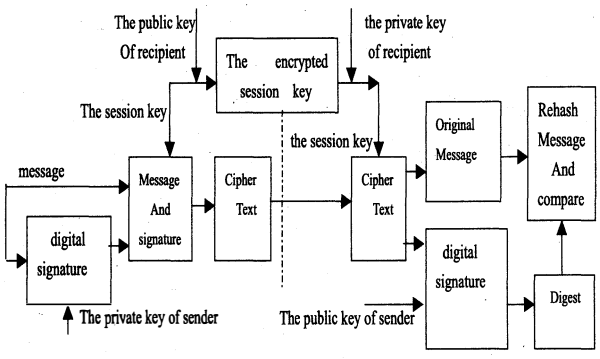

Fig.5: The whole process of data transmission

6. Conclusions

The proposed network security model has following merits:

(1) The model introduces the secure function smoothly. Some security schemes introduce the secure function at IP layer or TCP layer. IP is oriented to connectionless, so it is unreliable and the diagrams arrive out of order. TCP is oriented to connection and reliable, but TCP protocol itself will be changed if secure function is introduced at TCP layer. This model adds a "security layer" between application layer and transport layer, so all the protocols needn't be changed. Security layer performs encryption, decryption and identity-verifying functions invisibly to both communication sides, while ensuring that their communication is nearly as private and secure as a face-to-face meeting, so all operation is transparent and seamless.

(2) Inherent disadvantage in private key encryption is the problem of secure distribution. For example, if someone want to send other person an encrypted message, he has to securely send the other side the secret key first. This creates a chicken-and-egg dilemma: to set up a secure communication system, he needs a secure communication system. Public key encryption solves this problem using key pairs. Data encrypted with one key in the pair is decrypted using the other key. Thus we can encrypt the message with recipient's public key which, as its name implies, is not a secret. Decryption requires recipient's private key, which only recipient possess. At the same time, the private key algorithm is very quick, but the public key algorithm itself is very slow. So we use the private key algorithm-DES to encrypt the long message, and use the public Key algorithm-RSA to distribute the key of the private key algorithm.

It is an extremely good idea to sign the long message by using the private key to encrypt the message digest of the message. For a message digest is a relatively short block of numbers that prevents anybody from altering your message, so the speed of signature is hisher.

(3) The proposed model adopts a simple and secure one-use session key mode. Before transmission data in the common encryption system, both sides must exchange the session key. This model uses different session key that has been randomly generated and transmitted with the encrypted message in different data transmission presses. So the model avoids the session key exchanging. This improves the security of the system, because next data transmission does not be effected in case of the session key leaks. At the same time, when one session is completed, session key needs not to be restored, which makes key management easier and simpler.

(4) The model has a secure, and greatly efficient key management scheme. Centralized key management scheme commonly used in

practical distributes the user's key through channel which must be secure. Users' public key and, specially, private key are generated by key management center, which then distributes the key to users, so the key management center interposes users' privacy and can be easy to counterfeit users' identity. All users must communicate with the key management center, so all private information of users can be wiretapped, at the same time, the communication burden of the key management center is so high that it becomes bottleneck of communication. This model adopts distributed key management scheme in which every user produces his own key pairs, and the public keys of users in every user group are managed by distributed KDC, but users' private keys are produced and managed by themselves, which protects privacy of users. At the same time, there is no central node in the distributed KDC, so it has no the problem of bottleneck of communication.

REFERENCES

[1]G. Brassard, *Modern Cryptology,* A Tutorial, volume 325 of LNCS. Springer, (1988)

[2]D.W.Davies, *Price Security For Computer Network,* John Wiley and Sons, LTD,(1992)

[3] A.S. Tanenbaum, *Computer Networks,Third Edition,* Prentice-Hall International, Inc

[4] B.Schneier, *Applied Cryptography, Protocol, Algorithms, and Source Code in C, Second Edition.* John Wiley&Sons, Inc. (1996)

[5] A. Weber, B. Carter, B. Pfitzmann, M. Schunter, C. Stanford, and M. Waidner. *Secure international payment and information transfer,* Technical report, CAFE Project,(1995)

[6]B.C.Neuman and T.T.Kerberos: *"An Authentication Service for Computer Networks", IEEE Communications,* Vol 32, no 9, pp.33-38. September (1994)

[7] R.Ramaswamy, *"A Key Management Algorithm for Secure Communication in Open Systems", Interconnections Architecture,* Computer&Security, Vol.9, No. 1 (1990)