ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 26-29 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

Secure Data Using Identity Based IP Network Encryptor

Swati R. Salunke
Dept. of Computer Engineering, Institute Of Knowledge College Of Engineering, Pune, India
Email: Salunke.swati277@gmail.com,

Abstract*:* To protect the data across the network layer, network layer encryption offers an efficient and proven method for providing the data privacy. At the network layer encryption such as IPSec is more flexible than higher layer solution since it is not application dependent and can protect at end to end traffics which goes between two hosts .Before sending the information over the network IPSec establish a session key. In this paper we present an how a identity based encryption(IBE) scheme is used to calculate the encryption key far per packet by using the IP address of destination host without using the expensive key generator as in IPSec. This mechanism is compatible with the current IP protocol and. And also this mechanism compare with the RSA algorithm in cryptosystem. This result shows that this module provides encryption to the per-packet encryption for end to end secure communications that is ideal for consumer electronic application.

Key words: Network encryptors, Identity-based encryption (IBE), Internet key Exchange Protocol (IKE).

INTRODUCTION

Network encryption (sometimes called network layer encryption) is a network security process that applies crypto services at the network transfer layer-above the data link layer, but below the application layer. Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption process used network encryptor provides end-to end security to the data send from the these node to the destination node. Compared to application layer encryption, such as S/MIME and PGP, which only works for a specific application and requires installation of programs in the client workstations and server hosts, network encryptor is independent of applications and is completely transparent to the end users [1].

Internet Protocol Security (IPSec), which operates at the network layer protocol, that provides end to end encryption for security of IP communications. In this IPSec, both the sender and receiver must use the Internet Key exchange Protocol(IKE or IKEv2).This Internet Key Exchange Protocol(IKE or IKE2) is used for to set up security association for generating the encryption and authentication keys before an IPSec –protected communication can be set up. These generated encryption and authentication keys are then reused throughout the life time of association [1].

A model of IP security based on software encryption has been implemented. The implementation was done on Encryption servers, that support encryption and authentication of forwarded IP packets and function as secure gateways to the Internet [11] Due to which the complex software setup it prevent the such security system to scale to future-high speed networks and the large per-host setup task also presents a significant challenge to system a administrators of large corporations with thousands of clients.

In this paper we provide, we present the end-to-end network encryption using the identity based encryption (IBE)**.**The IP address of a target host is used as its identity for encryption. Following are the advantages of network encryptor:

1) Because of the simplicity of IBE scheme, the encryptor can be implemented in hardware, for eliminating any need of per-host software setup. Hence it has the potential to scale with future high-speed network.
2) By using the IBE, complicated key management and exchange process as in IPSec are unnecessary. As a result, the overhead of this encryption scheme is small when compared to IPSec.
3) There is no need of complex key generation is not needed, in this each packet is encrypted using a different key, eliminating the risk of key-hijacking. Compared to traditional public-key encryption such as RSA and Elliptic Curve Diffie-Hellman public key system (ECDH), this scheme eliminates the burden of complex key management from this server.
4) The presence of KEY Generating Server (KGS) is not required for data.
5) In this scheme Key Generating Scheme is not needed for data communication.
6) Provide end to end security along with each packet rather than network security.
7) If there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. This system assumes that, once issued, keys are always valid. The majority of derivatives of this system which have key revocation lose this system.

The use of identity-based cryptosystems have been proposed under various different contexts .In[6],an identity based encryption scheme was proposed to provide secure and anonymous roaming wireless access ,which improves on schemes such as [2]that utilizes symmetric key encryption. Similarly, an identity-based key exchange scheme was used in [3] to address man-in-the-middle attack of their previously proposed FEA_M scheme [4].However, we are not aware of any prior work utilizing such identity-based scheme for IP network traffic encryption.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 26-29 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

BACKGROUND

The concept of IBE was introduced by Shamir in 1984 [7].The idea is to let a user's identity to be used as his public key. In IBE is a public key cryptosystem in which each user has two keys, one is public key and another is private key. In this encryption and decryption is done by using two different keys. In public key cryptosystem one key is published, namely, a public key while the other one is kept as a secret, namely ,a private key. For example, when Alice wants to send a private message to Bob, she encrypts the message by using the Bob's public key. And at the receiver side Bob decrypt message by using its own private key shown in following figure (1).

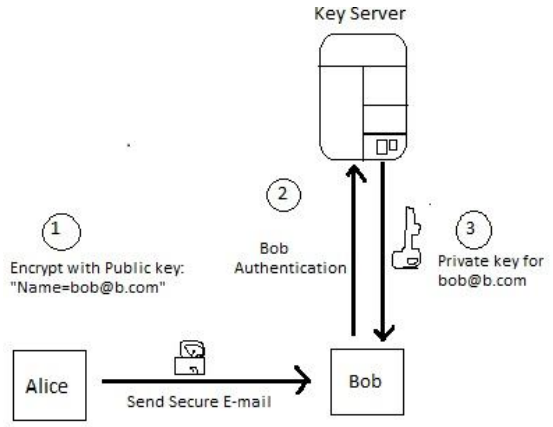

Fig 1: How a Alice send a message to Bob

In 2001, Bonech and Franklin [8] invented the first feasible solution for IBE using the Weil pairing on elliptic curves. Since then, many ID-based key agreement protocols and signature schemes using bilinear pairing have been suggested [9]. The corresponding private key of a user can be generated by a publicly trusted Key Generating Server (KGS) using the user's public key and the master secret key of the KGS. We propose to use the Bonech-Franklin IBE scheme [8] to encrypt IP packets. In this scheme, IP address is used as identity of network hosts and so any message sender can calculate the public key of the message receiver using his IP address. Tate pairing [5] on an elliptic curve, *E* is used to generate the shared secret between the message sender and receiver. Such shared secret is used as the per-packet key for encrypting the IP packet. Tate pairing was chosen in this scheme because of its relatively low computational cost.

PROPOSED ENCRYPTION SYSTEM

There are two distinct phases in this encryption scheme. First, a user must register with a central key generating server (KGS) to obtain its private key. The KGS holds the master key of the system which is required for generating the private key of a user [1]. Once equipped with his private key, a user may then engage in encrypted communicate on with another user without contacting the KGS again. In this sense, the workload of the KGS is much lower than a certificate authority (CA) of a conventional public key infrastructure [1].

At the network layer data is present in packet format to provide the encryption technique to the network layer; we encrypt each individual packet with a unique key before it sends to the receiver. For example, when a user A wants to transmit a stream of packets to another user B, user A encrypt each individual packet with a unique key generated based on the IP address of B. Each time a 40 byte of information is decrypted. This encrypted packet is travel through routers, only header part and its corresponding packet payload are modified in place. At the receiver side user B decrypt each packet by using the own private key. Following are the steps for encryption and decryption of information and how to generate a master key.

A. Adding extra information with each packet

Before sending each packet to the receiver some extra bits are added with the each packet for increasing the security level.

B. For generating Master Key and user registration

For each instance of this IBE system, the KGS must first generate a set of parameters according to the following steps:

Step i : Select a point P on E.
Step ii : Generate a field x from F(2^m)
Step iii : Find xP

This x is kept by the KGS as the master key; P and xP are announce to all users as the public parameters for the system. When a user registers with the KGS, the latter generates the private key based on his IP address using the following steps:

Step i : Calculate the public key, A for the user.
Step ii : Calculate the private key of Alice, xA
Step iii : Send this xA to user Sender through a secure channel.

C. Encrypting IP packets

When a sender sends a stream of IP packet to Bob, each packet is encrypted using the following steps:

Step i : Calculate the public key of receiver using his IP address.
Step ii : Select random number from F (2^m).
Step iii : Find rP.
Step iv : Select s shared secret key s from F (2^{4m}).
Step v : Convert s into m bits and use it with per packet key Ks.
Ks =s1+s2+s3+s4
Step vi : Encrypts the packet by using RC4 stream cipher using Ks as the encryption key.
Step vii : Send encrypted packets to the Bob.

D. Decryption of IP packets

When Bob receives an encrypted IP packet, he performs following steps to decrypt the packet:

Step i : Extract X (rP) from the received packet.
Step ii : Find s from his private key, xB.
Step iii : Convert s to a key of length of m bits and use it as the per-packet key, Ks.
Step iv : Decrypts the received IP packet by a RC4 stream cipher using Ks as the decryption key.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.3, Pages : 26-29 (2013)
Special Issue of ICCSIE 2013 - Held during 24 May, 2013 Bangalore, India

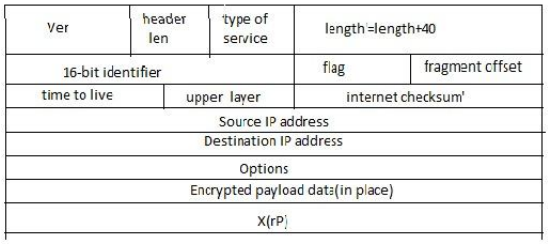

Fig 2: Packet format for Encrypted IP

Description about (Fig. 2)

Ver: It describe the version of protocol

Header type: In this field type of header is specify.

Type of service: Contains a 4 bit service bits, and 1 unused bit.

These services bits can be:

Minimize delay	1000
Maximize throughput	0100
Maximize reliability	0010
Minimize monetary cost	0001

Length': In the case of unfragmented packet, together with the EPT, a total of 40 bytes is appended to the original IP packet. As a result, both the checksum and the length fields of the header must be modified accordingly [1].

Identifier: for uniquely identifies the datagram. Usually incremented by 1 each time a datagram is send.

Flag and fragment offset: used for fragmentation.

Source IP address: in this field IP address of sender is present.

Destination IP address: in this field IP address of destination is present.

Option: Option data

Encrypted payload data (in place): In this field encrypted data is present.

Some extra information is also added in original packet, the resulting packet must be exceed maximum transmission unit(MTU) of 1500 bytes[11].for such cases the original packet is fragmented into two encrypted packets first contains the encrypted payload and second contains X (rP) payload.

SECURITY CONSIDERATION

The network encryptor provides end-to-end encryption of data over IP network so they cannot be attacked by the unauthorized entity .When the encryptor works in the transport mode, in which only the data part of the information is protected but header information is not protected, attacker may find some useful information from the unprotected header information to attack the network equipped with the network encryptors. On the other hand, at the network encryptor only provides confidentiality but not the authentication and message integrity. Thus, it can only protect against passive attacks such as eavesdropping and sniffing of data as it pass over the network but not active attacks such as altering data and masque reading as another individual to send data over the network.

Other security considerations are:

Chosen-Plaintext Attack

As any user in the system can use the encryptor to encrypt any chosen plaintext, the system is subject to chosen-plaintext attack in which an attacker can choose the plaintext that gets encrypt and obtain the corresponding cipher text from the output of the encryptor .However ,as a 238-bit RC4 cipher is used for the encryption, it is unlikely to discover the key for the encryption by simply analyzing the plaintext-cipher text pairs[1] .In addition, each IP datagram is encrypted by a unique per-packet key. Therefore, the security of the system will not be seriously affected even if one of the keys is discovered by the attacker.

Key Escrow

As the KGS is in possession of the master secret, *x*, it encompasses the full knowledge of private keys of all users, allowing it to decrypt any message send to any user. There are two ways to reduce the risk of breaking the entire IBE system owing to the compromise of the KGS:

1. By using distributed key generating servers, and
2. By using short-lived master key.

APPLICATIONS

Dynamic Host Configuration

Dynamic Host Configuration (DHCP) is a protocol used for assigning IP addresses to individual networked devices dynamically for operation in an IP network. As a fundamental assumption of this proposed IBE scheme is to utilize the IP address of the receiver as the unique identity for public key calculation, this scheme cannot work with an IP network using DHCP that randomly assigns IP addresses to users [1]. However, as many DHCP servers do, it is possible to fix the mapping between a MAC address and the corresponding assigned IP address. With such a mapping, this scheme may then perform as expected.

Mobile IP

Mobile IP is an extension to the Internet Protocol which enables mobile computers to stay connected to the Internet regardless of their locations and without changing their IP addresses. Mobile IP uses two types of routing protocols, namely, indirect routing and direct routing.

In indirect routing protocol, IP packets sent to the mobile user use its home address. Since the destination address of an IP datagram remains pointing to the original home IP address, this proposed network encryption scheme, which requires only the destination address for encryption, works without any modification in this case.

In direct routing protocol, the following techniques can be used:

During the link setup phase in which the correspondent user gets the care-of-address of the mobile user from the home agent, the encryptor connected to the correspondent user sniffs the packets sent between the correspondent user and the home agent, obtains the care-of address of the mobile user, and associates it with the home address of the mobile user[1]. When the corresponding user actually sends data to the mobile user using his care-of address, the encryptor uses the care-of-address to look up the home address of the mobile user and uses the home address as the public key for encryption.

CONCLUSION

In this paper a Secure Data using identity based IP Network Encryptor, is presented. The destination public key IP address of an IP datagram is used to generate unique keys to encrypt each individual IP datagram. Since all information required to generate encryption key is available with the sender, no communication with KGS is needed. Also a new per-packet key is generated for each individual packet, due to which the risk of hijacking is virtually eliminated. In addition, design considerations when this IP-centric encryption scheme must coexist with common network protocols, including DHCP and NAT. In the future, we plan to implement the IBE encryption scheme entirely in FPGA so as to provide the needed speed to cope with live traffic in a 10Gbps Ethernet network.

REFERENCES

[1] Sammy H.M. Kwok, IEEE," Zero-configuration Identity-based IP Network Encryptor", in *IEEE Transactions on Consumer Electronics*, Vol. 56, No. 2, May 2010.

[2] J. Zhu; J. Ma, "A new authentication scheme with anonymity for wireless environments," *Consumer Electronics, IEEE Transactions on* , vol.50, no.1, pp. 231-235, Feb 2004.

[3] X. Yi, C. H. Tan, C.K. Siew and M. R. Syed, "ID-based key agreement for multimedia encryption," *Consumer Electronics, IEEE Transactions on* , vol.48, no.2, pp.298-303, May 2002.

[4] X. Yi, C. H. Tan, C.K. Siew and M. R. Syed, "Fast encryption for multimedia," *Consumer Electronics, IEEE Transactions on*, vol.47, no.1, pp.101-107, Feb 2001.

[5] G. Frey *et al.*, "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," *Information Theory, IEEE Transactions on*, vol. 45, no. 5, pp. 1717-1719, Jul 1999.

[6] Z. Wan, K. Ren, and B. Preneel "A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks," in *Proceedings of the First ACM Conference on Wireless Network Security (WiSec '08)*, Mar. 31 –Apr. 02, 2008, ACM, New York, NY, pp. 62-67.

[7] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO'84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 47-53.

[8] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO'01*. London, UK: Springer-Verlag,2001, pp. 213-229.

[9] L. Martin, *Introduction to Identity-Based Encryption*,1st ed. Artech House Publishers, Jan 2008.

[10] J. Mogul and S. Deering, Path MTU Discovery, *RFC1191*, Nov 1990.

[11] Encryption Servers: A scalable distributed method for Internet security by Vivek Pathak Thesis, Under the Director of: Liviu Iftode, New Brunswick, New Jersey, May 2001.