Using IBE Key Distribution Strategies to Development of DDoS Attack Detection and Prevention

Qing Tan[1, a]

[1]College of Information Technology, Luoyang Normal University, Luoyang, 471022, China

[a]email: edutanqing@163.com

Keywords: DDoS; IBE; Key distribution

Abstract. System based on public key of the certificate biggest problem is the management of the certificate, the certificate inside bind the user ID and the user's public key. To solve this problem, some researchers have proposed the identity-based IBE public key system. The DDoS attacks performer, can be any type of network node. Based on the user's private key distribution scheme identity-based cryptogram system, will give an escrow agent system private key escrow, users have at least a proxy information fragments collected can calculate their private key. The paper proposes using IBE key distribution strategies to development of DDoS attack detection and prevention.

Introduction

IBE public key can be any string on the user's identity, as long as the string that uniquely identifies the user's identity; Users own identity, and access to the private key to a trusted third party certification, a process that can receive an encrypted message before also after; trusted third party CA (Certificate Authority), can service multiple users; Finally, as Shamir pointed out: identity-based encryption scheme is inherently key managed because a trusted third party know about all the user's private key.

The self-similar network traffic and time series analysis can only detect DDoS attacks, the test results are delayed, false positive and false negative phenomenon, even if detected neither DDoS attack nor defense [1]. IP packet filtering technology to better defend DDoS attacks, but the technology used in the amount of data is very large, the query and update data need to take up a lot of system resources (such as CPU and memory) to increase system overhead, and only use the IP packet filtering technology can not detect DDoS attacks.

System based on public key of the certificate biggest problem is the management of the certificate, the certificate inside bind the user ID and the user's public key. To solve this problem, some researchers have proposed the identity-based public key system. Identity-based key system, the user ID is equivalent to the user's public key to this, there is no authority in CA, do not need a dedicated directory to store the certificate, which greatly reduces the administrative burden of the system. The paper proposes using IBE key distribution strategies to development of DDoS attack detection and prevention.

The IBE Key Distribution Program Analysis

In the traditional public key system, public / private key pair is created in pairs, and public key, in identity-based public key system, the public key is the user identity to ID or from ID derived, key generation center KGC user private key is generated, intelligent and to the user issuing personal card, smart card contains a microprocessor, input the output port, random access memory and has the private key and the encryption and decryption, signature program [2]. Because the public key from ID directly calculate, in use process need not store the public key certificate directory, also do not need to use third party (CA) to provide all related services. In the Shamir scheme, all the smart card issued after, even KGC can also turn off.

In the aspect of information protection and authentication, the more popular is the public key infrastructure PKI (Public Key Infrastructure) technology. PKI consists of 4 main parts: the strategy

approved center PAA, PCA certificate, certificate authentication center strategy CA and ORA registry center. In use process, PKI was found to exist many unsatisfactory areas, the need to explore new methods, new system to solve problems. Presented here does not depend on the identity authentication, as the key ideas, think this is perhaps the best way to simplify the public-key cryptography, as is shown by equation1.

$$\begin{aligned}\hat{s}(k)_{\mathrm{MAP}} &= \mu_{s|a} \\ &= \left[\beta(k)^{\mathrm{T}}\Sigma_{\varepsilon(k)}^{-1}\beta(k)+\frac{1}{\sigma_{s(k)}^{2}}\right]^{-1} \\ &\times\left\{\beta(k)^{\mathrm{T}}\Sigma_{\varepsilon(k)}^{-1}\left(a(k)-\alpha(k)\right)+\frac{s_0(k)}{\sigma_{s(k)}^{2}}\right\}\end{aligned} \tag{1}$$

In the public key system is widely used in public key certificate, the distribution (Certificate) to achieve, certificate contains the signature public key, ID number of the user and the authority of the certificate. Digital certificates provide an authenticated on Internet way, its function is similar to the driver's license or daily life ID. It is composed of an authorized by the authority -- CA Certificate (Certificate Authority) electronic document center issued identity, people can use it to identify each other in the Internet communication.

Using the IBE system, key management center PKG without public key and certificate to save a large number of users like PKI CA center, the user can use public key encryption, also passes through the certification process does not need complex. Unfortunately, IBE system must solve two problems faced in the application: key escrow and key update. Key escrow, the user's private key or symmetric key centralized production and management. Application for signature, key escrow should be avoided, can see the user's private key is generated by the PKG center, then the user private key in the IBE system is the beginning of the key escrow [3].

$$h(k)=\frac{T(k-1)A(k-1)}{A(k-1)^{T}T(k-1)A(k-1)+1/(1-UC)} \tag{2}$$

The dependent PKI digital certificates to bind a public key and a public key belongs digital certificate database must be run online; IBE does not require digital certificates, personal identifier is the public key corresponding to the public key is used to decrypt the private key known only toned to get time off, even if access to the private key can decrypt the file.

See from the above comparison can: system certificate system is suitable for large scale based on certificate management, but it is very troublesome. Although the identity based system may still have problems, but the advantage is obviously: save the certificate management problem, no longer need to CA signature, no longer need to verify the CA signature, no longer need to CA certification, greatly simplifying the system cost, the IBE system easier to maintain and management, as is shown by equation3.

$$C=\sum_{i=0}^{L-1}p_i\log_2\frac{p_i}{q_i} \tag{3}$$

Using the discrete logarithm of key distribution scheme of user identity in Cryptosystem Based on the intractability, whose security is based on discrete logarithm, therefore selected must be large enough, such as | |=512; and -1 must have at least one big prime factor [4]. The system can accommodate multiple users, here we consider the users mutual collusion, to obtain confidential information, partial information about each user's.

In the distribution system of this simple, just a simple realization of the user identity information is transmitted to the information center, information center by the user private key is generated after his own private key information will be kept confidential, delivered to the user through a secure channel, and the communication between users to directly use the user private key, no user security information for authentication, as is shown by figure1.

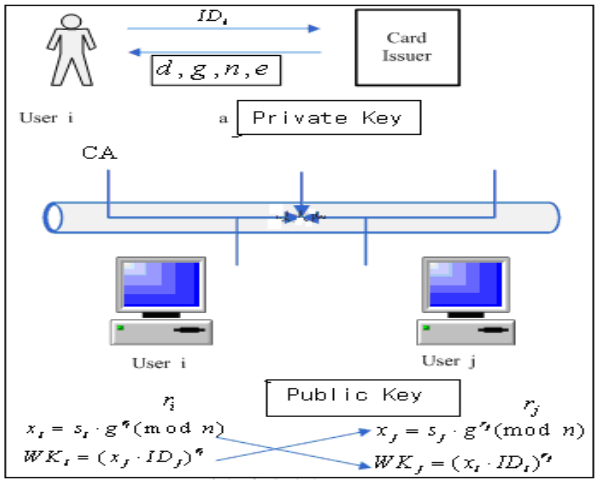

Fig.1. IBE key distribution figure

There is an information center system, responsible for the selection of system parameters, generating system of public and private key pair, as well as to the escrow agent distribution of the key pieces; an escrow agent, every escrow agent have a public information and the corresponding key pieces, at least an escrow agent cooperation can calculate the user's private key; there are a number of communication user [5]. Public key cryptography and one-way encryption function used in our scheme. The scheme function modules include: system initialization process, user key and authentication and shared key generation process.

Digital certificate process generally: the user first generates a key for oneself, and the public key and the part of personal identity information is transmitted to the certification center. Certification Center in the verification of identity, will perform the necessary steps to make sure that the request, is sent by the user and, then, the certification center will be sent to the user of a digital certificate, the certificate contains the user's personal information and other public information, information signature also accompanied by certification center. The user can carry out various activities related to the use of their own digital certificate. The digital certificate issued by independent certification organization (CA) released, as is shown by equation4.

$$\sigma_{\Omega}^{2} = \frac{1}{A_{\Omega}} \iint_{(x,y)\in\Omega} [(I(x,y) - \bar{I}_{\Omega}]^{2} \mathrm{d}x\mathrm{d}y \tag{4}$$

IBE password system, all the user's private key is generated by the key center, and then sent to the user, therefore, the key generation center knows all the user's private key, the key escrow problem which is called IBE. In order to solve the above problem, this paper is on this basis, we introduce the RSA algorithm and threshold scheme improvement ideas, successfully solves the key escrow problem existing in cryptosystem.

Using IBE Key Distribution Strategies to Development of DDoS Attack Detection and Prevention

In the IKE routing protocol for DDoS attacks, the attacker from a large number of fake IP address to initiate a connection request, in an attempt to make the response of memory and CPU resources are consumed. In the implementation, if it is determined whether the first message sent by the originator of the IP address is it true IP address response R can not, then the response with the least amount of CPU resources and does not need to record the contents of the SA, this would not be effective intrusion.

Because the IKEv2 negotiation of two is not protected by encryption, so the attacker can rob in the real negotiation response before sending the reply message in an attempt to destroy the normal connection. In view of this situation, IKEv2 sponsors allow multiple response in response to the first message, and the response of all as a legitimate and response [6]. The initiator to send some message, upon receipt of a valid encryption response message, the response message other ignored, and the other entire invalid semijoin discarded, so in the negotiations to avoid attack by DDoS.

$$C(t) = \frac{E[B(t), B(-t)]}{E[B(t)^2]} = 2^{2H-1} \tag{5}$$

Flooding DDoS attacks, the most important feature is the distributed architecture, collaborative attack and a large number of attack packets to the annihilation of the target machine. With the attack technology development, flooding DDoS attacks no longer just targeted to the nodes in the network, the network congestion has gradually become a new target for flooding DDoS attacks. The traditional flooding DDoS attacks can cause network congestion to some extent. The use of the programming language is as the standard C++ language, as is shown by figure2.

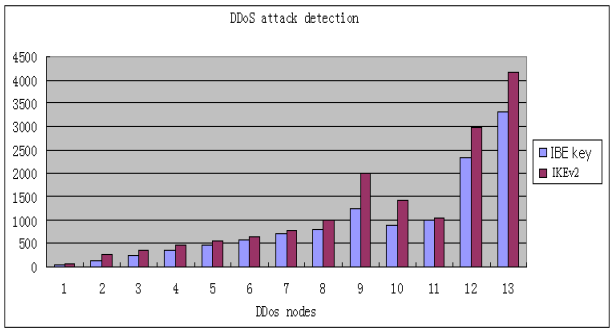

Fig.2. Compare of DDoS attack detection and prevention based on the IKEv2 protocol with IBE key algorithm

The paper proposes using IBE key distribution strategies to development of DDoS attack detection and prevention. The DDoS attacks performer, can be any type of network node. Attack aircraft controlled by the host computer, and install specific attack procedures received attack instructions from the host computer to send a large number of attack packets to the target machine.

Conclusion

DDoS attack can be any type of initiator, nodes in the network. Attack the host first control puppet machine much, and install the control program in the puppet machine. Based on the certificate system and it is the need for a directory to store the user's certificate (public key). Based on the identity of the system, because the public key calculated by ID, without requiring a separate directory to store user certificate.

References

[1] Hossein HADDAD, Hadi MIRMOHAMADI, “Comparative Evaluation of Successor Protocols to Internet Key Exchange (IKE)”, IEEE Intemational Conference on Industrial Informatics (INDIN), 2005 3rd.

[2] MontMC, Bramhall P. IBE applied to privacy and identity management. Trusted Systems Laboratory. HP Laboratories Bristol, 2003.

[3] Li-Chiou Chen, Thomas A. Longstaff, Kathieen M. Carley.Charterization of defense mechanisms against distributed denial of service attacks.Computer & Security, 2004,(23):665-678.

[4] Park K., Lee H..On the effectiveness of routebased packet filtering for distributed DoS attack prevention in PowerLaw internets.presented at the ACM SIGCOMM, San Diego, CA, 2001

[5]Do-Yoon Ha, Chang-Yong Lee, Hyun-Cheol Jeong, Bong-Nam Noh, "Design and Implementation of SIP-aware DDoS Attack Detection System", AISS, Vol. 2, No. 4, pp. 25 ~ 32, 2010

[6] Jiqiang Zhai, Keqi Wang, "A Distributed Method for DDoS Attack Tree Construction", IJACT, Vol. 4, No. 23, pp. 538 ~ 545, 2012.