Development of DDoS Attack Defense System Based on IKEv2 Protocol

Qing Tan and Xiaojing Yue

Abstract IKE version second (IKEv2) simplifies the redundant function of IKEv1 and enhances the security of internet. This paper uses a DDoS attack detection technology, if the detection detected the DDoS attacks, with the establishment of good faith database TD filtering the network data flow, defense DDoS attack. The paper presents development of DDoS attack defense system based on IKEv2 protocol. This paper designs a secure and practical IKEv2 system implementation scheme.

Keywords IKEv2 · DDoS · Key distribution

1 Introduction

Flooding DDoS attacks, RoQ attack has several features: distributed, collaboratively large-scale attack (RoQ attack in pulse attacks stages) and a single-packet undetectable [1]. Exhausted the resources of the target machine, DDoS attacks target a port or multiple ports to send a large number of service requests or take advantage of the reflection server network implementation of DDoS attacks. A large number of attack packets bound to make some of the network traffic characteristics can be changed; through the study of changes in these characteristics, it can effectively detect DDoS attacks.

As a security protocol, the important point is the ability to resist attacks. Although the IKEv1 protocol developed a number of mechanisms to enhance its

Q. Tan (✉)
College of Information Technology, Luoyang Normal University, Luoyang 471022, China
e-mail: edutanqing@163.com

X. Yue
The High School Affiliated to Luoyang Normal University, Luoyang 471022, China

S. Patnaik and X. Li (eds.), *Proceedings of International Conference on Soft Computing Techniques and Engineering Application*, Advances in Intelligent Systems and Computing 250, DOI: 10.1007/978-81-322-1695-7_4,

security, there are still some security vulnerabilities, making it easy to attack, of which the most important is the Distributed Denial of Service (DDoS). So, here, we will mainly describe the improved IKE version second (IKEv2) attack that is against DDoS. The paper presents development of DDoS attack defense system based on IKEv2 protocol.

2 IKEv2 Protocol Analysis and Design

The IKE protocol plays a vital role in the whole IPsec system. It is a hybrid protocol, based on the Internet security association and key management protocol (ISAKMP) defined frame. IKE uses two stages of the ISAKMP, defines four kinds of mode [2]. In the first stage, it is regardless of the use of main mode or savage mode and it can use four kinds of authentication methods: pre-shared key, digital signature, public key encryption, and improved public key encryption.

As the certificate cannot be forged, the certificate can be placed in a directory for participants to access; the user can also directly send the certificate to other users. Certification Center (CA) plays a key role in the public key system, responsible for the management of the system, all users' (including people, all kinds of applications, host) certificate. We describe Certification Center (CA) that PKI's main purpose is to automatically manage keys and certificates for users to establish a secure network operating environment in a variety of application environments, allowing the users to easily use data encryption and signature technology to ensure the network data confidentiality, integrity, and effectiveness.

Key material IKEv1 in the calculation, due to the presence of significant flaw in the design of the protocol itself, can cause security vulnerabilities. The IETF working group took note of this point, and in IKEv2, using the new design avoids these defects, as is shown by Eq. 1.

$$X_{i+1,V}(m) = \bar{H}_i^* X_{i,V}(m) + \sum_{r=1}^{q-1} \bar{G}_{r,i}^* X_{i,r,D}(m) \tag{1}$$

Between IKEv2 and IKEv1, a major difference is that the new agreement is a new definition of the independent encryption loads. For the IKE_AUTH stage message, the CREATE_CHILD_SA, and exchange of information messages, the message removed from the head outside portion is encrypted, and the encrypted portions on the encrypted IKE payload field are the encrypted payloads. Message encryption load must be placed in the tail of the message. From the defined encrypted payload, opinion from outside intuitive, the entire message contains only a payload (encrypted payload).

Exchange of IKEv2 corresponding to the first stage of IKEv1 is called the IKE_SA_INIT exchange, and in the basic exchange, the number of packets correspondingly reduced to two. IKEv2 from the IKE_SA_INIT exchange nonce's and the establishment of Diffie-Hellman is sharing to calculate a key seed secret

(SKEYSEED). The SKEYSEED is further used to calculate the seven key for other materials: SK_d is used to generate CHILD_SA key, only if he does not divide the direction; SK_ai and SK_ar were used as the integrity verification, and IKE_SA_INIT subsequent exchange of key materials: SK_ei and SK_er are used to encrypt and decrypt subsequent exchange; SK_pi and SK_pr is used to generate the AUTH load. The 6 keys for both sides of communication is different, SK_ai, SK_ei and SK_pi used to protect the originator of the message, SK_ar, SK_er and SK_pr used to protect the response message, as is shown by Eq. 2:

$$\begin{aligned} \mathrm{M} = \sigma_{\mathrm{s|a}}^2 &= \mathrm{cov}(s(\not{k}) \mid a(\not{k})) \\ &= E\{[s(\not{k}) - \mu_{s|a}]^2 \mid a(\not{k})\} \\ &= \beta(\not{k})^{\mathrm{T}} \Sigma_{\varepsilon(\not{k})}^{-1} \beta(\not{k}) + \sigma_{s(\not{k})}^{-2} \end{aligned} \tag{2}$$

The kernel of IKEv2 system and IPsec protocol are used to provide VPN security gateway together. The system is the realization of the IKEv2 protocol; its ultimate aim is to peer entities in the system that provides the IPsec security protocol for secure network connections needed to establish security alliance. The IKEv2 system is responsible for handling user management configuration commands, the physical interaction, negotiation of packet encryption authentication, and the same kernel SAD interaction.

The IKEv2 message negotiation process IKEv1, a great improvement. IKEv1 negotiation process is very complex, with two stages and four modes. The main mode or aggressive mode is selected in the first stage, in which in the main mode, there are six exchange messages, and the second phase of the fast mode requires three exchange messages. And the messages exchanged are also different depending on the method of authentication barrier, making the entire negotiation process more complicated.

IPsec security protocol has two modes of operation: transport mode and tunnel mode (Transport Mode) (Tunnel Mode). Transport mode is used in the upper-layer protocol to protect IP packet; it is inserted into a special IPsec header between IP and upper-layer protocol header. Tunnel mode is used to protect the whole IP packet; in tunnel mode, to transmit, the IP packets are encapsulated and inserted into an IPsec head between the external and internal IP head [3]. Two kinds of IPsec security protocol (AH and ESP) can also be used in transport mode and tunnel mode, as is shown by Eq. 3.

$$\begin{bmatrix} X_{M-1}^T & X_{M-2}^T & \cdots & X_1^T \end{bmatrix} \begin{bmatrix} w_{M-1} \\ w_{M-2} \\ \vdots \\ w_1 \end{bmatrix} = X_M^T \tag{3}$$

Information exchange is mainly used for error handling in IKE negotiation and solving the communication configuration; the messages carrying one or more deleted loads will be used for determining deleted SA SPI value. The best

exchange of information is only after the completion of the initial exchange, so that it is protected by the negotiated IKE_SA. An IKE_SA control message must be sent under the protection of the IKE_SA, and part of a CHILD_SA control message must be produced under the protection of the IKE_SA CHILD_SA sent.

IKE provides key information to generate the encryption key and the authentication key for IPsec communication. Similarly, IKE using ISAKMP is used for other IPsec protocols' (AH and ESP) negotiation of SA. Later, with the higher requirements to the performance, security, there is a need to increase the NAT genetic authentication, remote address acquisition, and other contents, so the content of the agreement is getting more and more complex, with the lack of consistency in it [4]. IKE is of vital importance to the structure in the IPsec position and is used very frequently, so the performance inefficiency has become the bottleneck to the system. Therefore, the urgent need to reduce the complexity is performed by IKEv1. Therefore, IETF since the beginning of February 2002, IKE version second (IKEv2) of the drafting work, was released in October 2005, official version of IKEv2, as is shown by Eq. 4.

$$Wf(j,\,k) = 2^{-\frac{j}{2}} \sum_{n=0}^{N-1} f(n)\phi(2^{-j}n,\, n-k) \tag{4}$$

IKEv2 initial exchange in the first stage is equivalent to the IKEv1 exchange, usually consisting four new, in response to that attack by DoS circumstances, will add two more. All exchange messages in the IKEv2 appear in pairs. Before the initial exchange of messages called IKE_SA_INIT exchange, negotiation encryption algorithm, nonce value, Diffie-Hellman exchange, and various keys are needed after the value calculation. Second in the message is called the IKE_AUTH exchange, which is the authenticated message exchange front, has identity and certificate (optional), determines the traffic selectors, and establishes the first CHILD_SA. The two IKE_AUTH message exchanges are the encryption and authentication; encryption and authentication using key is generated in IKE_-SA_INIT exchange, to protect the identities of both sides of the play.

Corresponding the first version of the second stage in IKEv2 is the IKE_AUTH exchange. CHILD_SAs can be established through exchange of IKE_AUTH, also may establish the exchange by CREATE_CHILD_SA. The following key material generated in the way: KEYMAT = prf + (SK_d, Ni | Nr) if the establishment of the first CHILD_SA, then Ni, and Nr, is done by IKE_SA_INIT exchange in the nonces value; if not, then Ni and Nr are derived from CREATE_CHILD_SA exchange, as is shown by Eq. 5.

$$\sum h(n)h(n+2k) = \delta_{k,0} \tag{5}$$

In order to be more flexible during forward compatibility, IKEv2 defines "1" and "0" for critical marks "*C*". The critical mark for "0" implies : the sender wants response but could not identify the next receiving load types of the load, and skips the load. The critical mark for "1": the sender wants response but could not

identify the next receiving load types of the load, and refused to accept the message. If the receiver of the message is to identify the types of loads then it is neglecting the domain.

In the second stage, IKEv2 function and IKEv1 CREATE_CHILD_SA exchange in the exchange of similar are negotiating a new CHILD_SA. This exchange is from the two message composition. If the initial exchange is completed, it may be initiated by the exchange of any party, so the CREATE_CHILD_SA exchange in the initiator and the initial exchange of sponsors may be different. The use of exchanging the initial exchange of negotiating encryption and authentication algorithms is to protect the message. Sponsors include our proposal in SA load, nonce load in nonce value will be used to calculate the CHILD_SA key generation, KE load is optional, and the use of KE load can guarantee CHILD_SA a perfect forward protection. If Diffie-Hellman group is used in SA, then the message must contain a KE load, as is shown by Fig. 1. The response contains the accepted recommendations in SA load; if KEi load is the originator of the message, the responder of the message must have KEr load.

In the process of message exchange, a party may wish to send control messages; notification occurs with some errors or events [5]. In order to accomplish these operations, IKEv2 defines information exchange. If message exchange of information contains zero or more notice, delete, configuration load, an INFORMATIONAL message is received, and a party must response, and response message may not contain any load. Origination message can also do not contain any load; the sponsors may determine whether the other is survived by this method.

Each IKE message starts at IKE message header, followed by one or more IKE payload. IKE message header with biggest change is the initiator and responder of SPI IKEv2 message header instead of IKEv1 header initiator and responder cookie value.

A CREATE_CHILD_SA exchange can generate more than one SA, so according to the method, if IKEv2 protocol extends the key definition extends KEYMAT to less than the required length, and each key sequence capture is certainly required. Rules for determining key sequence are as follows: First of all, key all SA from the initiator to the response direction, all the keys of all SA direction are received from the direction response to initiator. The consultation of multiple IPsec protocol is keys in order to intercept data packet protocol head appeared in the package. If there is a single agreement with the encryption key and the authentication key, then take the encryption key and then the authentication key.

The main version and the major version are designed for compatibility with IKEv1. The main version of IKEv2 must be 2, while the main version of IKEv1 is 1, which is greater than the major version number 2 that was not accepted. Must be the version of IKEv2 implementation based on the minor version number that is set to 0. IKEv2 redefines the exchange type, number of 34–37, IKE_AUTH, representing the IKE_SA_INIT, CREATE_CHILD_SA, and INFORMATIONAL exchange. While retaining, the 0–33 number is compatible with IKEv1, as shown by Eq. 6:

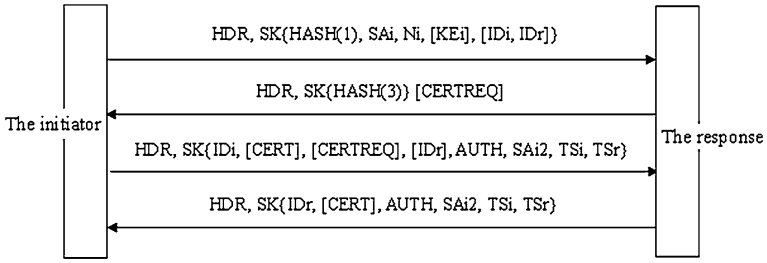

Fig. 1 The IKEv2 information exchange figure

$$P^{(\eta)}(m, s) = W_X^* \bar{P}^{(\eta)}(m, s) W_X \tag{6}$$

IKEv2 has canceled the three loads, the different structure security alliance load (substructure) according to the level relation together. IKEv2 SA load allows the inclusion of more suggested substructure, they must be in accordance with the arrangement from the best to the suboptimal order; each substructure can contain multiple IPsec protocol (e.g., IKE, esp., AH); each IPsec protocol can contain multiple transform substructure (e.g., encryption algorithm, integrity check algorithm, D-H group); transform structure can contain multiple attribute structure (e.g., key length).

The number of transformation of substructure is decided by both parties to choose the agreement, AH must implement a transform through integrity verification algorithm; ESP usually needs two transformations: encryption and integrity check algorithm. IKE needs four transformations: D-H group, integrity verification algorithm, PRF algorithm, and encryption algorithm. According to the different types of transformation and that defines the transformation of ID different, it appears in each transform head this definition and IKEv1 have great difference. In IKEv1 protocol, the protocol requires multiple algorithms, there is usually an algorithm in transform reflected, while the rest of the algorithm on the property is in contrast to the IKEv2 definition more clear.

IKEv2 do not record the state cookie (stateless cookie). In IKEv2, if a party is suspected of legitimacy of the request, it may request the other party with a cookie request, and it does not record any state or do any complex operation before such a request is received. So, when the receiver receives a large number of half open (half-open) of the IKE_SA request, it will reject them, unless the receipt notices of a load with cookie. This will enable the ability to resist DDoS attack greatly enhanced.

Network communication subsystem is responsible for the network interface. To provide communication, IKEv2 application and network complete the receiving and sending of IKEv2 messages. The module will do local message negotiation of IKEv2 consultation message encapsulation system generated into UDP packets and is sent out; UDP data packet stripping IKEv2 message is received and passed

to the upper hand by message negotiation processing subsystem. The programming interface module of the full realization of the network socket and monitor is performed in the 500 and 4,500 ports, respectively.

3 Development of DDoS Attack Defense System Based on IKEv2 Protocol

Reflector DDoS attacks can be described as follows: First, the attacker host controls a large number of vulnerabilities puppet machine, in these puppets on placement control procedure and attack procedures. Then, attack the host attack instructions sent to the host computer; the host computer received attack instructions for the source IP address, the IP address of the target machine sends service requests (or packets) to the reflector server. Finally, the reflection to the server upon receiving a service request (or packets) of the source IP address in response to a large number of data packets, thus, forming the reflector DDoS attacks.

DDoS attacks in order to resist the IP source tracking IP attack packets generally use IP spoofing technology. In this way, even if detected, DDoS attacks cannot trace the source of the attack according to the source IP address in the IP packet items. The length of the IPv4 IP address is 32, the IP address entry in the database of traditional IP packet filtering technology. If the database stores all IP address, probably occupied a space of $232 = 4G$, then it is a very large number.

For stationary time, series can be analyzed by AR model and MA model. The PDD time series is nonstationary time series; DDoS attack detection and online analysis, therefore, used the online analysis ability and strong adaptive autoregressive (AAR) model to describe the PDD time series. Parameter sequence is fitting as a stationary current state (or generalized stationary time series) [6]. The PDD time series for arbitrary is the definition of P order AAR model.

IKEv2 for all messages appear in pairs; in each of the message, the initiator is responsible for retransmission event, response without retransmission of the response message, unless requested a retransmission for each other. Avoid both initiation and retransmission, resulting in a waste of resources, but also can prevent the attacker intercepting the message, disguised as a negotiator who is constantly sending out the retransmission of the message, the two parties of the resource consumption. The IKEv2 protocol is a very complex security protocols, engineering complex and difficult. The IKEv2 system for Fedora Core 4 operating system, and it is Linux 2.6.11 kernel. The use of the programming language is as the standard C++ language, as shown by Fig. 2.

At present, the distributed DDoS attack defense system structure is the trend of development, dynamic IP packet filtering technology, if the nodes in a distributed manner used in the network (such as servers, switches, and boundary router), each node to a certain extent filtering part of a DDoS attack packets, the target hit by

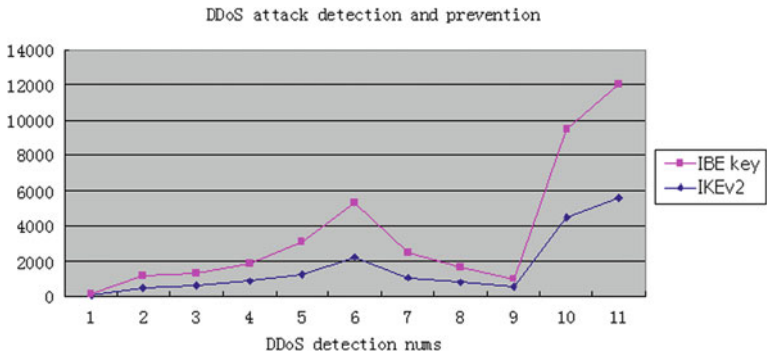

Fig. 2 Comparison of DDoS attack detection and prevention based on the IKEv2 protocol with IBE key algorithm

DDoS attacks will be greatly diminished, conductive to the realization of defense strategy of DDoS attack on the target machine. The paper proposes the strategies of DDoS attack detection and prevention based on the IKEv2 protocol and IBE key distribution.

4 Conclusions

IKEv2 in agreement with SA is divided into two steps: first, the establishment of a certified safety channel in the communication between the two sides, namely the establishment of IKE SA and then under the security channel protection. Second, IPsec security service negotiating SA, namely the establishment of IPsec SA. In IKEv2, the IKE SA is still called IKE SA, and IPsec SA is called CHILD SA.

References

1. Soussi, H., Hussain, M., Afifi, H., Seret, D.: IKEv1 and IKEv2: A quantitative analyses. The 4th World Enformatika Conference (2005)
2. Zhao, L., Li, X., Dong, Q., Shi, L.: An IKEv2 based security authentication scheme for mobile network. AISS **3**(9), 191–198 (2011)
3. Kwok, Y.K., Tripathi, R., Chen, Y., Hwang, K.: HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks. ICCNMC, pp. 423–432 (2005)
4. Yan, H., Wang, F., Cao, Z., Lin, F., Chen, C.: A novel method to defense against web DDoS. JDCTA **6**(19), 162–170 (2012)
5. Fan, L., Zeng, W., Jiang, Y., Li, J., Liang, Q.: A group tracing and filtering tree for REST DDos in cloud. JDCTA **4**(9), 212–224 (2010)
6. Perlman, R., Kaufman, C.: Key exchange in IPsec: Analysis of IKE. IEEE Internet Comput. **4**(6), 50–56 (2000)