A Distributed Communication Model of Intrusion Detection System in Active Network

Soo-Young Park*, and Sang-Gug Park**

* Department of Computer Engineering, Uiduk University, Kyung-ju, Kyungpook, Korea
(Tel : +82-54-760-1652; E-mail: sypark@uu.ac.kr)
** Department of Computer Engineering, Uiduk University, Kyung-ju, Kyungpook, Korea
(Tel : +82-54-760-1656; E-mail: skpark@uu.ac.kr)

Abstract: With remarkable growth of using Internet, attempts to try intrusions on network are now increasing. Intrusion Detection System is a security system which detects and copes illegal intrusions. Especially with increasing dispersive attacks through network, concerns for this Distributed Intrusion Detection are also rising. The previous Intrusion Detection System has difficulty in coping cause it detects intrusions only on particular network and only same segment. About same attacks, system lacks capacity of combining information and related data. Also it lacks cooperations against intrusions. Systematic and general security controls can make it possible to detect intrusions and deal with intrusions and predict. This paper considers Distributed Intrusion Detection preventing attacks and suggests the way sending active packets between nodes safely and performing in corresponding active node certainly. This study suggested improved E-IDS system which prevents service attacks and also studied sending messages safely by encoding. Encoding decreases security attacks in active network. Also described effective ways of dealing intrusions when misuses happens thorough case study. Previous network nodes can't deal with hacking and misuses happened in the middle nodes at all, cause it just encodes ends. With above suggested ideas, problems caused by security services can be improved.

Keywords: DDoS, E-IDS, Active Network, Intrusion Detection

1. INTRODUCTION

With remarkable growth of using Internet, attempts to try intrusions on network are now increasing. Intrusion Detection System is a security system which detects and copes illegal intrusions. Especially with increasing dispersive attacks through network, concerns for this Distributed Intrusion Detection are also rising. The previous Intrusion Detection System has difficulty in coping cause it detects intrusions only on particular network and only same segment. About same attacks, system lacks capacity of combining information and related data. Also it lacks cooperations against intrusions. Systematic and general security controls can make it possible to detect intrusions and deal with intrusions and predict. This paper considers Distributed Intrusion Detection preventing attacks and suggests the way sending active packets between nodes safely and performing in corresponding active node certainly.

2. DISTRIBUTED INTRUSION DETECTION SYSTEM

2.1 Outlines of Intrusion Detection System

Intrusions means groups of acts which disturbs integrity, confidentiality, availability of resources on computer or acts destroying Security Policy[1]. Intrusion Detection System is mostly connected to intrusion interception system and its administrator can detect intrusions like abnormal using, misuse in the steps of network or host. And also it can detect Anomaly Detection, Misuse Detection[1-4]. Anomaly detection is the case which approaches out of model cases and Misuse Detection is corresponding model cases. Also, Host-Based IDS detects intrusions only hosts which connected Web Service. Network-based IDS detects intrusions on the specified network only[5-6].

2.2 Structures of Distributed Intrusion Detection System

To supply information security service, the conditional problems of previous information security service can be solved by dispersing security node thorough wide network and managing it in center. To handle increasing traffics and various attacks effectively, managing network is needed by expanding local security surroundings and using frameworks based on a policy foundation which can make each systematic and organic movements. Also can use hierarchic integration analysis technique to collect information and analyze.

Therefore, fragmentary and conditional problems can be solved by dispersing intrusion detection and managing it in center, policy decision can be made and global networking security controls, too.

The biggest problem in network security is DDoS(Distributed Denial of Service) attack. Cause it isn't predictable and can't be distinguished from normal traffic. The extent of damage is also very large thorough network. Besides it makes excessive traffics run into network, it causes serious troubles by exhausting resources thorough network security and managing. Intrusion detection and general analyzing supplies unified analysis techniques between SGS(Security Gateway System) and high lank policy servers. So, actually damages can be minimized by perceiving changes of traffic running thorough network ingress point early.

2.3 Enhanced Intrusion Detection System

The previous IDS only detects intrusion and alarms but improved IDS can deal with intrusion progressively. Also can defend hackers by making E-IDS paralyzed. This is a structure which defends DoS attack, that is the most frequent attack[7]. This structure disturbs hacker's passive sniffing or active detecting by making IDS host invisible. It disturbs trials trying to stop E-IDS host by relocating host and important IDS process with mobile agent technique. This new IDS structure has so strong mechanisms that it can defend DoS attack in active network.

3. PROTECTING WAY OF ACTIVE PACKET

3.1 The framework of Network and Currents of Active Packet

E-IDS suggests following ways to stop misuse while forwarding messages among hosts. In this chapter, Active Node and Passive Node exists together for suggested schemes as followings figure 1.

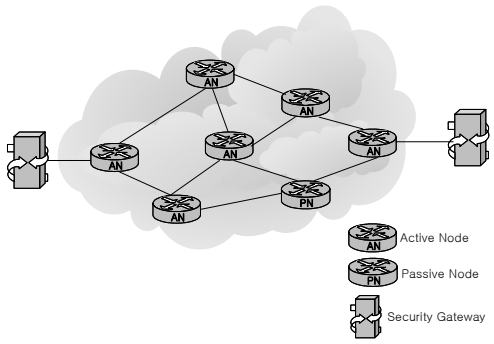

Fig. 1 Network establishment.

Basically when receives active packet, previous node simply forwards neighbor node unlike active node. Active node accomplishes programs and forwards in active node environment. This paper suggests the method of coding and decoding for packet forwarding. After sending node creates active packet which has codes, it decodes payload with secret key coding process[8].

Active packet structure(Fig. 2) is consisted of an IP header, IP address of sender, active packet header and payload. Payload has an possible code.

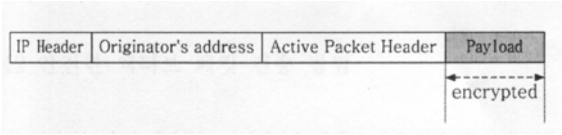

Fig. 2 Active packet format.

Cause Sending node doesn't know addresses of neighbor node's, sending node broadcasts neighbor nodes. If passive node receives this active packet, it ignores packet and forwards. If neighbor active nodes receive encoded active packet, they create massages asking secret key(symmetric encoding system) and active packet which has its public key(public key encoding system). And then Receiving Node can get IP address of Sending Node from the Header, it transmits active packet to corresponding address. When Sending node receives active packet, after it checks Header and Payload, it encodes its secret key with public key encoding method(RSA etc.). This public key is in payload of received active packet. Sending node creates active packet having coded secret key and then sends it to receiving node. After receiving this packet, receiving node decodes encoded secret key by using private key(public key encoding system). With this secret key, receiving node gets possible codes from coded active packet. After executing each codes, receiving node creates newly-encoded active packet and broadcast it into neighbor node.

3.2 Safe Ways of Transmitting Active Packet

In this paragraph, we'll make several assumptions to clarify proposed ideas. And then explains proposed schemes for movements in detail after defining its marks.

3.2.1 Assumptions

- Active node doesn't know IP addresses of neighbors.
- Each domains has one CA(Certified Authority).
- Each active node on domains are already registered in CA.
- Each active node has its own secret key and RSA pair.
- Authentication issues a digital signed certificate to each node when it registered. Digital signature scheme uses Schnorr signature which uses proper Hash function or RSA signature .
- Possible code of active packet is executed in all middle nodes located in division node.

3.2.2 Notifications

The following are notifications of this paper schemes

- KU_A : The public key of active node A(pUblic Key)
- KR_A : The private key of active node A(pRivate Key)
- KS_A : The secrete key of active node A(Secret Key)
- CERT_A : The certificate of active node A(CERTificate)
- PGM : execution possible codes which includes a active packet
- ENCX(Y) : Y encoding with key X using public key encoding system
- DECX(Y) : y decoding with key X using public key encoding system
- EX(Y) : Y encoding with key X using symmetric key encoding system
- DX(Y) : Y decoding with key X using symmetric key encoding system

- SIGX(Y) : Y encoding with key X using digital signature scheme
- VER(S) : verification of signature S
- CA : Certification organization(Certification Authority)
- KR_CA : private key of certification organization for issue a certification authority
- KU_CA : public key of certification organization
- INFO : information which includes certification authority(e.g., used encoding algorithm, the term of validity, issue date of certification authority, etc.)
- REQ(Y) : request message to get Y

3.2.3 Processing

Figure 3 shows a proposed processing for safe active packet between Active Node A(sending node) and Active Node B(receiving node).

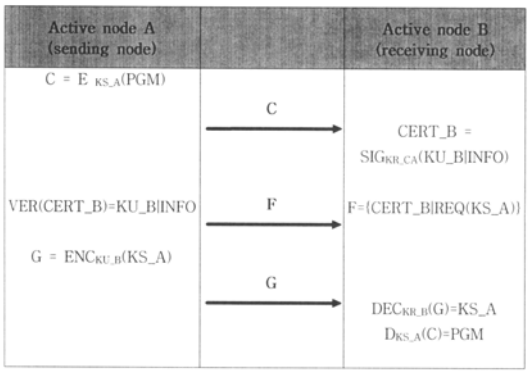

Fig. 3 Transmission process of safe active packet.

Active Node A has a execution code from another node or created itself. It has to be transmitted well into next Active Node. Sending node transmits this possible code into neighbor active node. Also wants all middle active nodes to execute all active nodes. Processing are as followings;

(1) Active node A creates active packet. Possible code is included in this payload of active packet. Sending node encodes this payload with symmetric key encoding method.

C = EKS_A(PGM)

(2) Active node A doesn't know IP addresses of neighbor nodes, so broadcasts it to neighbor nodes.

(3) If neighbor active node B receives encoded active packet(=C), it checks active packet thorough active packet header. Then it records IP address of sending active packet and C on its table.

(4) Cause active node B needs secret KS_A for decoding C, active node B requires active node A it. First of all, by using digital signature scheme prepares own CERT_B which signed with KR_CA. CERT_B includes INFO which has KU_N and code algorithm and valid dates, certificates issued dates.

CERT_B = SIGKR_CA(KU_B|INFO)

(5) Active node B creates new active packet F having message REQ(KS_A) for acquiring CERT_B and KS_A. And from own table , it sends IP address of active node A to corresponding IP address.

F = {CERT_B | REQ(KS_A)}

(6) If active node A receives F from active node B, it checks active packet header and payload. Then gets KU_B and INFO after inspecting CERT_B with KU_CA. IN this case processing differs from digital signature scheme.

VER(CERT_B) = KU_B | INFO

(7) Active node A records active packet IP addresses, KU_B, CERT_B and F on the table.

(8) Active node A encodes KS_A with its KU_B using RSA. After getting active node B address from its table, it sends G to IP address.

G = ENCKU_B(KS_A)

(9) If active node B receives G, it decodes secret key G with KR_B. Then active node A gets KS_A. By decoding active packet C with coded KS_A, gets possible code.

DECKR_B(G) = KS_A

DKS_A(C) = PGM

(10) Receiving node B executes this program and records results on its table. Then repeats this process to send results safely to neighbor nodes.

3.3 Case study

Figure 4 shows Policy-based Security Management Structure which includes E-IDS.

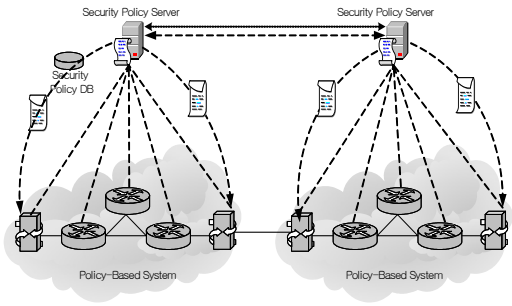

Fig. 4 Policy-based Security Management Structure.

E-IDS framework has a policy server, policy DB, policy subject. Policy server is organized by policy management and policy decision. Policy DB can exist alone apart from policy server. Policy object is E-IDS. E-IDS prevents intrusions and performs policy from policy server.

Policy server is consisted of security policy modeling technology and security policy managing system, policy expressions and inspection, alarming and detecting intrusion technology and security system. Security gateway has analyzing intrusion engine and coping engine, traffic forwarding engine, security policy performing engine, alarming engine and traffic measuring engine. Figure 5 shows E-IDS behavior diagram in Policy-based Security Management Structure.

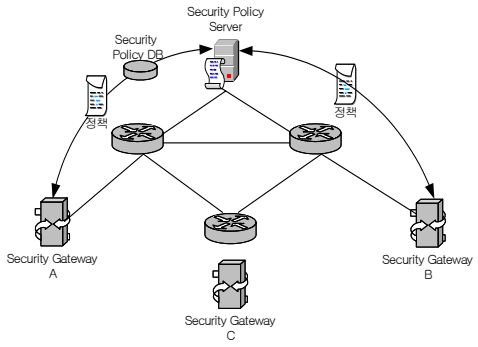

Fig. 5 E-IDS behavior diagram in Policy-based Security Management Structure.

When Intrusions happens in this structure, framework detects and copes with intrusions as followings;

(1) Hackers scans weak points to do DoS attack.
(2) E-IDS(security gateway in figure 5) is in proxy server. It detects attacks but hackers can't identify E-IDS information.
(3) E-IDS informs Policy Security System of intrusions. Informing Messages are coded.
(4) Policy DB stores new policy rules as subjects.
(5) Policy server brings policy messages from policy DB.
(6) Policy server sends policy rules to corresponding E-IDS after encoding and changing rules into applicable form with E-IDS.
(7) After receiving policy messages, E-IDS performs policy and informs policy server. If necessary, it sends messages to other hosts(switch, router).

All of messages used above procedures are coded. Although hackers snatch messages between clients and server, they can't know contents of messages at all.

4. CONCLUSIONS

With remarkable growth of using Internet and various services, present network service can't be satisfactory. Active network appeared as a new alternative plan. Previous network simply sends packets to next node after checking headers. But active network sends program codes and DB in packet together. Also performs program codes in network nodes like switch and router. Active network introduces a new flexible network service paradigm.

Present network security technology protects only specified domains and has Intrusion Detection System for detecting intrusions and fire walls preventing invader's traffics and packet filtering router. Limits of present network security technology are local detecting and lacks of adaptation and lacks of cooperations. Besides there hasn't been studied about proper prevention.

This study suggested improved E-IDS system which prevents service attacks and also studied sending messages safely by encoding. Encoding decreases security attacks in active network. Also described effective ways of dealing intrusions when misuses happens thorough case study.

Previous network nodes can't deal with hacking and misuses happened in the middle nodes at all, cause it just encodes ends. With above suggested ideas, problems caused by security services can be improved. Future studies as another types of case studies and studies about encoding node and traffic abilities are needed.

REFERENCES

[1] Debra Anderson, "Detecting Unusual Program Behavior Using the NIDES Statistical Component", IDS Report Sri Project 2596, Contract Number 910097C(Trusted Information Systems) under F30602-91-C-0067(Rome Labs), 1995.

[2] H. Debar and A. Wespi, "Aggregation and Correlation of Intrusion Detection Alerts", RAID 2001, LNCS 2212, pp. 85-103, 2001.

[3] T. Lunt, H. Javitz, and A. Valdes, et. al., " A Real-Time Intrusion Detection Export System(IDES)", SPI Project 6784, SRI International Technical Report, Feb. 1992.

[4] The Computer Misuse Detection System. http://www.cmds.net, 1998.

[5] Thomas E. Daniels, Eugene H. Spafford, "Identification of host audit data to detect attacks on low-level IP vulnerabilities", Journal of Computer Security, 7(1), pp. 3-35, 1999.

[6] Chris Herringshaw, "Detecting Attack on Network", IEEE Computer Magazine, pp. 16-17, Dec. 1997.

[7] David Del Elson, Instrusion Detection, Theory and Practice, ICSA Intrusion Detection System Buyer's Guide, March 27, pp. 50-58, 2000

[8] William Stallings, Cryptography and Network Security, Prentice-Hall, pp. 99-105, 1999.