The security system for response within the border router of the local network that the attacker belongs to

MINHO HAN, JUNGCHAN NA, SEUNGWON SOHN
Network Security Department, Information Security Technology Division, ETRI
161 Kajong-Dong, Yusong-Gu, Taejon 305-600
KOREA

Abstract: - A current security system detects intrusion and does individual response in local network domain. Therefore, it is important that construction of infra to do response in all system environment through sharing intrusion detection information between different network domains. This paper proposes the novel method of detection, tracing, and response about intrusion using packet filtering, active network, cryptographic technology with the minimum change of the network structure

Key-Words: - **Active network, Active packet, Active node, IDS, packet filtering, detection, tracing, response**

1 Introduction

This paper proposes the security system structure that shares intrusion detection information between different network domains, not limited to any local network domain. When the network domain that the attacker belongs to is found through tracing, the security system does any response within that domain.

A current security system detects intrusion and does individual response in local network domain. Therefore, it is important that construction of infra to do response in all system environment through sharing intrusion detection information between different network domains. New technologies to overcome such systematic response have been proposed, and remarkable things among them are Intrusion Detection and Isolation Protocol (IDIP) and Decentralized Source Identification of Intrusion Source (DecIdUouS) [1][2]. However, they require that all network structures be changed. Therefore, this paper proposes the novel method of detection, tracing, and response about intrusion using packet filtering, active network and cryptographic technology with the minimum change of the network structure.

2 Active Security System

This paper defines the security system that shares intrusion detection information between different network domains and responses within the domain of the attacker through the tracing as 'Active Security System'.

3 Requirement

To construct the Active Security System, it must be met the following three requirements.

- The border router of local network must be able to perform the packet filtering.
- The border router of local network should be consisted of active node architecture.
- The CA server for the security of the active packet and the safety of the active node must exists in ISP.

All intrusions are begun in local network. Therefore, if the border router of local network performs the packet filtering not to transmit the packets that have different network address outside, we can prevent IP spoofing and know the local network that the attacker belongs to [3]. Fig.1 shows the packet filtering method of the local network border router

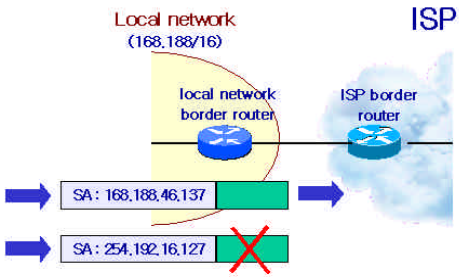

Fig.1 the packet filtering method of the local network border router

In case the intrusion detection system detects the attack, the attack information (attacker IP address, port number, etc.) must be sent to the local network border router that the attacker belongs to. If the local network border router receives the attacker information from the intrusion detection system of own local network, the local network border router performs the blocking of attacker packet using filtering and transfers the active packet that has the attack information to the local network border router [4][5]. Fig.2 shows the process of the generating and transferring of active packet in the local network border router. Thus, when the active packet passes the route that attacker passed by, the local network border router (active node) recognizes an active packet and can do a response.

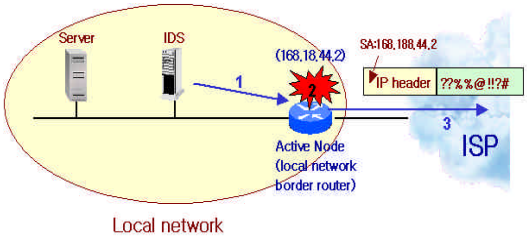

Fig.2 the process of the generating and transferring of active packet in the local network border router

When the local network border router transfers the active packet that has the attack information to the local network border that the attacker belongs to, this active packet must be able to keep a security. To do this, the CA server has the public key of each local network border router and permits the reliable active node to access the public key of active nodes in key table. The local network border router transfers the encrypted active packet using own private key and the local network border router that receives the encrypted active packet decrypts it using the public key that brought from CA Server. [Fig 3] shows the decryption of active packet in local network border router using public key.

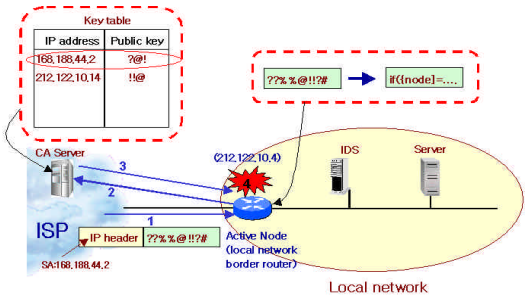

Fig.3 the decryption of active packet in local network border router

4 The structure of Active Security System

Fig.4 shows the structure of Active Security System. The border routers of local networks are consisted of active node and the CA server exists in ISP

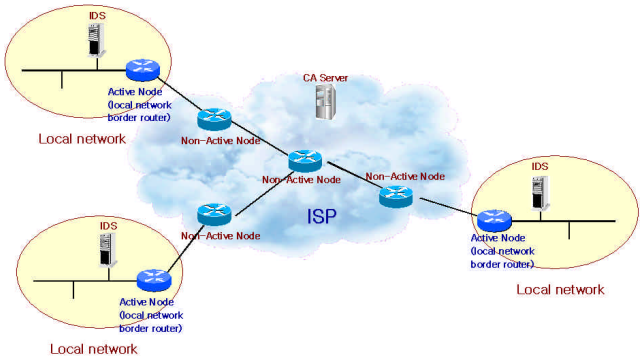

Fig.4 the structure of Active Security System

5 The process of Intrusion Detection, Tracing and Response

Fig.5 illustartes how Active Security System accomplishes intrusion detection, tracing and Response:

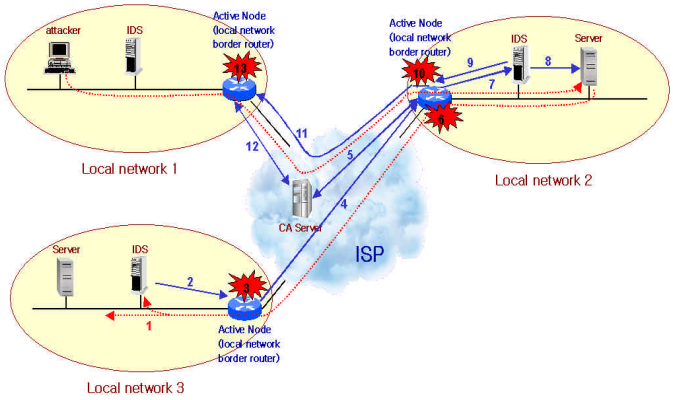

Fig.5 the process of intrusion detection, tracing and response

(1) In case the attacker in Local Network 1 tries attacking the Server in Local network 3 via the Server in Local Network 2,; (2) the IDS of Local Network 3 detects the attack and sends the attacker information (IP address and port number of the Server of Local Network 2) to the border router of Local Network 3; (3) The border router of Local Network 3 performs

the blocking of attacker packet (packet from the Server of Local Network 2) using filtering; and (4) transfers the encrypted active packet that has the attacker information to the attacker (the Server of Local network 2); (5) When the border router of Local network 2 receives the encrypted active packet, it brings the public key for decrypting this packet from CA server; (6) The border router of Local Network 2 performs the blocking of attacker packet (packet from the Server of Local Network 2) using the information in active packet; and (7) informs this information to IDS of Local network 2; (8) The IDS of Local Network 2 scans the Server of Local Network 2 and detects the attacker of Local network 1; (9) The IDS of Local Network 2 sends the attacker information (IP address, port number of attacker of Local Network 1) to the border router of Local Network 2; (10) The border router of Local Network 2 performs the blocking of attacker packet (packet form the attacker of Local Network 1) using filtering; and (11) transfers the encrypted active packet that has the attacker information to the attacker of Local Network 1; (12) When the border router of Local network 1 receives the encrypted active packet, it brings the public key for decrypting this packet from CA server; (13) The border router of Local Network 1 performs the blocking of attacker packet (packet from the attacker of Local Network1) using filtering.

6 Conclusion

Active Security System that proposes in this paper can do detection, tracing and isolation about the attack of different network domains through the minimum change of the network structure. But it needs to alter the border router of local network and the border router of local network must be guarantee not to transmit the packet that have different network address outside.

References:

[1] Dan schnackenberg, Kelly Djahandari et al, *Infrastructure for Intrusion Detection and Response*, the Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX) 2000.

[2] H.Y. Chang, C. Sargor et al, *DecIDUouS : Decentralized Source Identification for Network-Based Intrusion*, 6th IFIP/IEEE International Symposium on Integrated Network Management, 1999.

[3] P. Ferguson et al, *Defeating Denial of Service Attacks which employ IP Source Address Spoofing*, RFC 2267, January 1998.

[4] Calvert K. et al, *Architecture Framework for Active Network*, AN Working Group Draft, July 1999.

[5] David L. Tennenhouse et al, *A Survey of Active Network Research*, IEEE communication magazine, Jan 1997.