Immunity-based Security Architecture for Active Switch

Pan Jingsong

Abstract - **This paper proposes one kind of active network security technique which combined artificial immune intrusion detection system (IDS) and firewall, it can omni-directional carry on protection to the computers and networks.**

Keywords – **Firewall, Active Network, Active Switch, Network Security**

I. INTRODUCTION

With high speed development of the Internet, network intrusion methods diversification, network security is increasingly outstanding. When faced with different types or new methods of attack that intrusion detection realizing efficient performance, enhanced system security, so the administrator can more quickly and accurately carry out counter-action. Hackers to make attacks with abnormal packet transmission to reach the goal, parts of the attack with a single packet to identify, but the Hacker may also be using fake normal packet or an excess of normal packets to intrusion and attack, if only simple method to analyze a single packet that may not be effective to determine whether the attack, the follow-up time needed to analyze the contents of the packet. Passive network which we used today can forward packets only. Active network can compute and process packets before forwarding them, for example, to copy the packet, and to modify the context of packet or reroute and reforward it without according the packet's header [1]. Thus, active network can solve many problems of passive network like vulnerability. Today, the procedures of the network security system are: Computer collects information and logs security event automatically; Computer would have basic response judged by the information and advises administrator; Administrator confirms the response by computer and solves the problem thoroughly.

II. INTRUSION DETECTION COMPONENTS

Intrusion detection system is designed to ensure information security, the purpose of the find the abnormal network of behavior phenomenon. Intrusion detection system shall be subjected to a host system intrusions, can effectively detect the attack behavior, and inform the administrator, the loss of minimum decreased , and in the invasion process, learn from experience, to collect information about the invasion modules to enhance the overall system defense capabilities. In order to detect whether the network's behavior is malicious attacks, computer software and hardware device must have a surveillance network behavior ability, to provide relevant information with the IDS [2]. The computer network system information contained operating system audit log , the network packet header file (Fig.1) and so on.

IDSs are becoming the logical next step for many organizations after deploying firewall technology at the network perimeter. An intrusion-detection system collects information about its environment to perform the diagnosis on its security status. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. A typical intrusion-detection system is shown in Fig. 2. Many different intrusion detection systems are designed to detect different types of intrusions. These systems may not be able to achieve the common goal of detecting when working alone.

- Data collection module: data collection module to collect after through the firewall to filter packets , its usually like the type of open source libpcap packet capture program.
- Analysis Engine module: This module is the main components of the IDS, used to analysis of operating procedures for security risks.
- Event Generator module: This part is responsible for the find invasion of invasion response and handling, the intrusion-detection system can react in a number of ways -- from alerting a systems administrator and recommending various actions to automatically kicking the intruder off the network. But in practical application, it's difficult to hold back intrusion of action, timeless was poor, so in order to achieve these objectives, need to change firewall rules, and strengthen the interaction firewall and the response part.

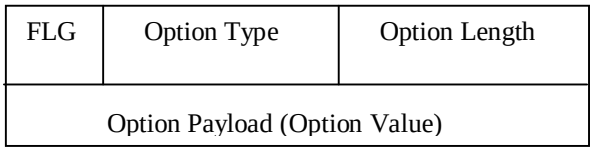

Fig. 1 Active network encapsulation protocol option format

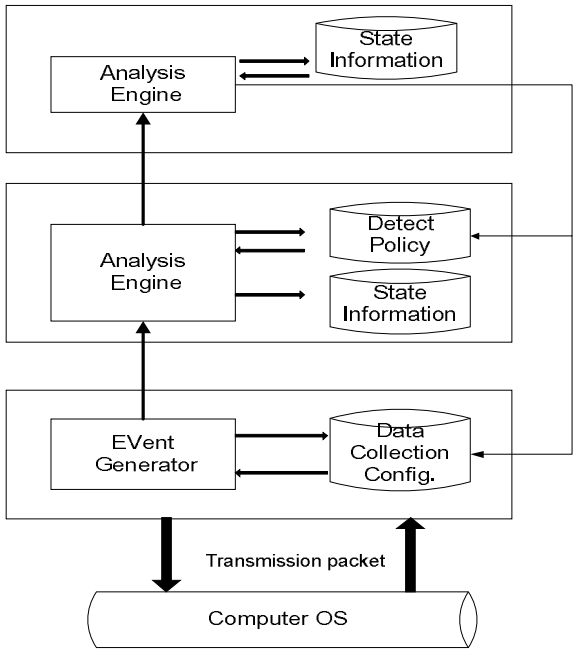

Fig. 2 Intrusion detection components

Pan Jingsong - College of Computer Science Yangtze University, Jingzhou, Hubei , China,
E-mail: pjs00488@gmail.com

III. Architecture for Active Switch

In order to establish fully defense mechanism to cope with DoS and its variants. IDS is based on detection of packet application layer and system layer, usually attached in the firewall's internal network, with conduct the relevant audit work, which can dynamically analyze and identify intrusion behavior to deal with the changeful intrusion attacks, and list their threat sequences.We must consider every situation of each type DoS attack. We will discuss attacker and intermediary attacker computers attached on active switch (Fig. 3). Protection process in accordance with the following order:

Step 1: Scanning and attack packets from active switch.

Step 2: The detection service will request filter service on the same active node to block the malicious packet immediately.

Step 3: Detection service sends signature of the packet to manager server.

Step 4; Antivirus administrator analysis the type and source of attack packets.

Step 5: Manager service updates signature database on signature database on IDS.

Step 6: The filter service will remove these packets in the block list automatically in order to reduce the load of system.

Step 7: Alert service sends warning message to the malicious packet sender.

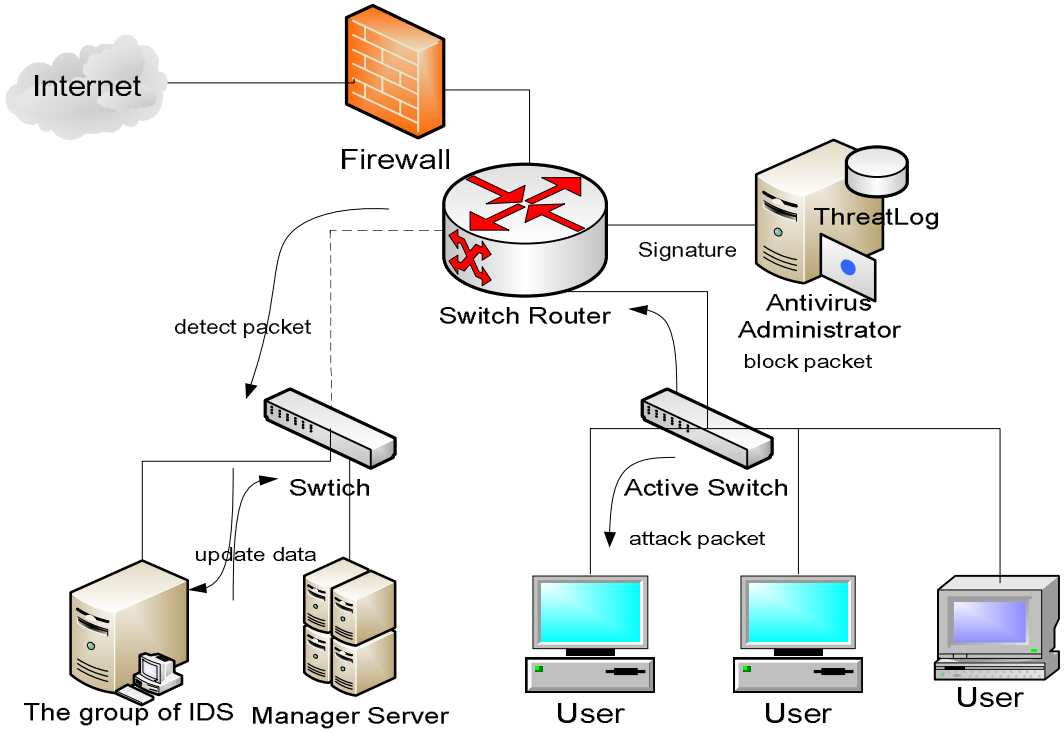

Fig. 3 Attack attached on active switch

IV. Conclusion

In this paper present artificial immune intrusion detection systems and firewalls make a dynamic combination for attack attach on a Active switch, to overcome the use of simple firewall technology which cannot meet the hacker of incessantly expanding harm and renewed technologies.

References

[1] Tao Li, “An immune based dynamic intrusion detection model,” *Chinese Science Bulletin.* pp. 2650-2657, 1. Nov. 2005

[2] Ping Yi, Yiping Zhong, Shiyong Zhang, “An immunity-based security architecture for mobile ad hoc networks,” *Journal of Electronics*, pp.417, May.2006.

[3] Nikolaos Nanas, Anne Roeck, “Autopoiesis, the immune system, and adaptive information filtering,” *Natural Computing,* pp.387-427, Jun. 2009.

[4] D. Dasgupta, F. Gonzalez, “An immunity-based technique to characterize intrusions in computer networks,” *IEEE Transactions on Evolutionary Computation*, pp. 281-291, Jun. 2002.

[5] F. Esponda, S. Forrest, P. Helman. ”A formal framework for positive and negative detection schemes,” *IEEE Transactions on Systems, Man and Cybernetics, Part B (Cybernetics)*, pp. 357-373, Feb. 2004.

[6] E. Eskin. “Anomaly detection over noisy data using learned probability distributions,” *In Proc. 17th International Conf. on Machine Learning*, pp. 255–262. Morgan Kaufmann, San Francisco, CA, 2000.

[7] Bowen, R.; Sahin, F, “A System of Systems approach to model an Artificial Immune System using Discrete Event Specification,” *IEEE International Conference on System of Systems Engineering, 2009*,Jun.2009, pp.1-6.