A NOVEL APPROACH FOR PROTECTING EXPOSED INTRANET FROM INTRUSIONS

K.B.Chandradeep

Department of Centre for Educational Technology,
IIT Kharagpur, Kharagpur, India
kbchandradeep@gmail.com

ABSTRACT

This paper proposes a novel approach for protecting groups of computers in an intranet from malicious attacks. The proposed scheme uses a distributed intrusion detection system as the primary source of security mechanism along with micro-firewalls at the host level to enable dynamic policy update for the intranet as and when the threat pattern changes. The authentication mechanism used for authenticating the hosts along with the communication mechanism used for communicating the policy update to the hosts is presented.

KEYWORDS

Intrusion Detection, Network Intrusion Detection System, Micro-Firewall, Security Policy

1. INTRODUCTION

There has been an explosive growth in the number of connected hosts in recent times. With the commence of e-commerce several firms are relying more and more on internet for all their business transactions. Without adequate protection or network security many individuals and companies are at a high risk. If the network hosts and servers are exposed to the public access through the internet then such an exposed intranet can be attacked by intruders either from outside the intranet or an intruder can penetrate the intranet and become a threat from inside. In this paper we present a security solution which solves the security problem of all the nodes present in the intranet.

In our scheme Network based Intrusion Detection Systems are configured at several places in the network to perform the role of a distributed intrusion detection system to detect intrusions and report the same to a central management node. This central management station then comes up with a new dynamic security policy for the entire intranet which has to be physically transmitted to all the nodes present in the intranet where this policy gets implemented. The new security policy is then implemented at all the nodes present in the intranet using a linux firewall.

A lot of research work has been done in the past in the area of network security and specifically in the area of intrusion detection. Linux IDS were developed for linux systems. Bellovin introduced the concept of Distributed Firewall [11]. The dynamic security concept was suggested by Petkac and B.Lee [4]. Different policy update mechanisms were evaluated by Kai Hwang and Muralidaran Gangadharan [5]. In this paper we present a scheme for utilizing the existing network based intrusion detection system and the micro-firewall so as to provide a security solution for the intranet and also discuss the authentication and communication mechanism between the management node and the different hosts present in the network.

DOI : 10.5121/ijcnc.2010.2412

The rest of the paper is organized as follows. Section II indicates how distributed intrusion detection system is obtained using multiple network based intrusion detection system sensors at several places in the network and also the placement of these sensors at different places in the network. It gives a brief description about the network based intrusion detection system used. Section III explains the mechanism used for making a policy update dynamically to all the hosts present in the network as and when an intrusion is detected. Section IV deals with the procedure used for implementing the new policy at the linux firewall of the hosts. Finally, we conclude by giving the advantages of the proposed solution.

2. INTRUSION DETECTION SYSTEM

An intrusion detection system is hardware, software or a combination of both used to detect intruder activity. The intrusion detection system can be of different types viz. host based IDS, network based IDS or distributed IDS. The intrusion detection system we have used is a completely software based system. We have used the open source network based intrusion detection system Snort at several places in the network so as to implement the distributed intrusion detection system.

2.1. Distributed Intrusion Detection System

The network based intrusion detection system Snort is configured at several places in the network as shown in the Fig.1. The NIDS1 is used for detecting any intrusions occurring from outside the intranet and is connected to the spanning port of the DMZ switch. The NIDS2 detects any intrusions that occur when the internal servers in the intranet are accessed. The NIDS3 is used for detecting any intrusions which might occur among the hosts.

The network based intrusion detection sensors pass the alert information or the intrusion data to a central NIDS management station where the intrusion data is analyzed and stored in a database. The advantage of having multiple sensors is that the rules which these sensors use to detect intrusions can be tailored to meet the specific needs of that particular network. The NIDS management station then comes up with a new security policy which is then implemented on the gateway firewall and also the hosts in the network. The policy which is implemented on the gateway firewall is the global security policy which is different from the security policy which gets implemented on the hosts. The mechanism used for implementing this policy update is explained in section III.

2.2. Snort IDS

The network based intrusion detection system used is the Snort Intrusion Detection System. Snort is capable of packet sniffing and packet logging in addition to intrusion detection. Snort employs both signature based techniques and anomaly based techniques to detect intrusion. Snort has an alert generating mechanism which generates an alert as and when an intrusion is detected. This alert is used by the overall system to identify the occurrence of an intrusion at any location in the network.

The rich rule set that snort possesses has been used to detect any intrusion based on the signature present in either the header of the packet or the payload of the packet. The rule set of the snort intrusion detection system is updated on a regular basis so as to keep snort up to date with the latest intrusion signatures. Snort also has several output modules which indicate the occurrence of alert in various output forms.

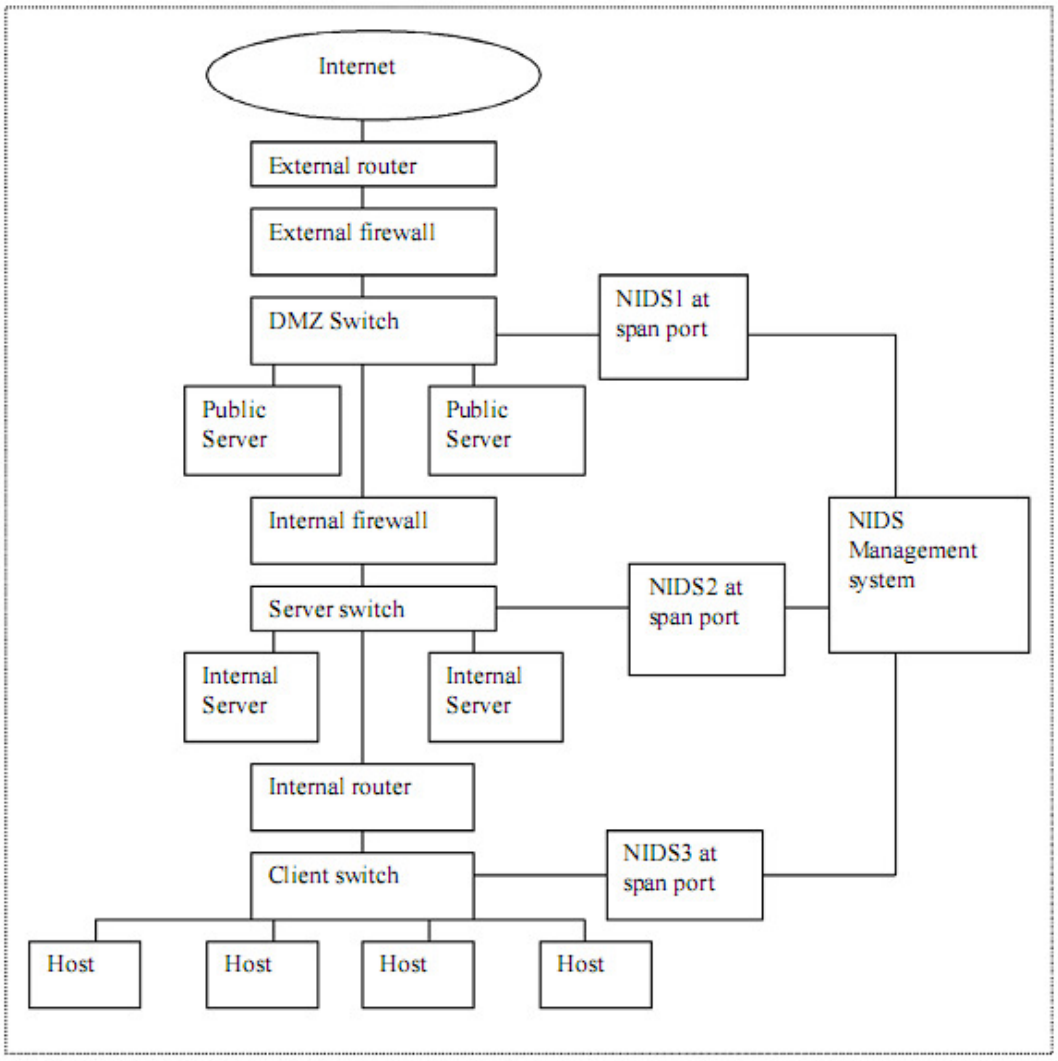

Figure 1. Distributed IDS

3. AGENT COMMUNICATION

The communication between the central management station and the hosts is carried out using mobile agents. Mobile agents are capable of migrating from one computer to another autonomously and continue execution on the destination computer. A mobile agent platform is responsible for the creation, execution, migration, sending, receiving and destroying of the mobile agents. When these mobile agents are deployed in an intranet or a large scale distributed network, security is an issue to be considered. It is to be ensured that the mobile agents do not access resources for which they do not have the required permissions. The receiving hosts also need to make sure that the agents are not malicious.

In order to implement the policy update on all the hosts in the intranet we employ a secure mobile agent platform which includes the following.

- Agents which carry the new policy from the central management station to the hosts and implement the policy at the hosts.

- An agent coordination system at the central management station which is responsible for creating, executing, sending, suspending and destroying the agents.

- Certification Authority that provides public and private keys for authenticating the mobile agents.

3.1 Authentication Mechanism

Whenever the mobile agents move from the agent coordination system to the hosts, the agent coordination system signs the agent digitally. The mobile agent with the signature of the agent coordination system, the signature of its owner is sent to the hosts. When the hosts receive the mobile agents they verify the identity of the mobile agent platform which sent the mobile agents. It then decides to accept it or reject it based on the level of trust the host has on the sending platform.

3.2 Communication between the mobile agents

The communication between the mobile agents is achieved using java RMI. Each agent defines its own access control policy. Based on the definition given by the mobile agents, stub and skeletal classes are generated. These classes contain the security modules which are implemented. The stubs and skeletons make sure that only authorized capabilities are exchanged between the agents. When a client agent communicates with a server agent, the client stub sends a message along with a capability for access. Based on the message received the server agent sends a reply message granting access to the client.

4. IMPLEMENTING THE POLICY UPDATE ON THE LINUX FIREWALL

Once the new policy reaches the hosts through the mobile agents the policy is implemented using the IPtables on the linux firewall. An IP filter is a packet filtering mechanism which looks at the header of a packet and decides whether to drop it or accept it. Under linux, packet filtering is built into the kernel as a kernel module. Netfilter is a general framework inside the linux kernel into which the IPtables module can be plugged into. The IPtables communicates with the kernel and tells the kernel what packets to filter. The IPtables tool inserts and deletes the rules from the kernel's packet filtering table. IPtables has different tables like NAT table, mangle table, filter table. For the purpose of packet filtering, filter table is used.

Filter table has three in-built chains. These chains are input chain, output chain and forward chain for input packets, output packets and forward packets respectively. In our system all linux hosts have packet filtering options built into the kernel. The IPtables enforce the update in the policy provided. The kernel's packet filtering module is updated with the new security policy.

5. Conclusions

In this paper we proposed the design and implementation of a distributed intrusion detection system capable of analyzing network traffic flowing in any part of the network and generating an alert whenever an intrusion is detected by any of the network intrusion detection sensors used. The NIDS used for this purpose was presented. The mechanism employed for updating the security policy as a part of intrusion response on the firewalls of the host systems is given. The tool used at the firewalls of linux is mentioned.

A. Advantages of the proposed distributed intrusion detection system

- Our system is not restricted to external traffic alone. It can analyze both internal and external traffic, i.e. all traffic which flows in any part of the network is analyzed.
- We have used the approach of mobile agents for dynamic policy update and this has a high scalability.
- If enough hosts on the inside generate large amount of traffic, a single gateway firewall will become a bottleneck since it cannot process the packets fast enough. By easing the firewall rules at the gateway and distributing the firewall rules out into the network, this bottleneck is removed.
- At the host level, our system reduces the possibility of further penetration into the network or prevents the widespread of the attacks.

REFERENCES

[1] L.Vokorokos, A.Kleinova, O.Latka, "Network Security on the Intrusion Detection System Level", Intelligent Engineering Systems, INES 2006. Proceedings international conference, pp: 270-275, 2006.

[2] Q.Xue, J.Sun, Z.Wei, "TJIDS: an intrusion detection architecture for distributed network", Electrical and Computer Engineering, IEEE CCECE 2003.
Canadian Conference Volume 2, pp: 709-712, 4-7 May 2003.

[3] A.Berqia, G.Nacsimento, "A distributed approach for intrusion detection systems", Information and Communication Technologies: From Theory to Applications, 2004. Proceedings 2004 International Conference pp:493-494, 19-23 April 2004.

[4] M.Petkac and B.Lee, "Security agility in response to intrusion detection", Proceedings of the applied computer security associates conference 2000, Louisiana, USA, Dec. 11-15, 2000.

[5] K.Hwang and M.Gangadharan, "Micro-firewalls for Dynamic Network Security with Distributed Intrusion Detection", IEEE international Symposium on Network Computing and Applications", 8-10 Oct 2001, pp: 68-79.

[6] Rafeeq Ur Rehman, "Intrusion Detection Systems with Snort, Pearson Education inc. 2003

[7] Jay Beale, James C Foster, Brian Caswell, "Snort 2.0 Intrusion Detection", Syngress Publishing inc., 2003.

[8] Sun Microsystems, Java RMI Specification", http://java.sun.com/docs/books/tutorial/rmi/ index.html

[9] http://www.netfilter.org/documentation/ index.html#documentation-howto for IPtables.

[10] http://www.snort.org for snort IDS.

[11] S.M.Bellovin, "Distributed firewalls", Journal of Login, Nov 1999, pp:37-3

. **Authors**

K.B.Chandradeep received his M.Tech degree from IIT Kharagpur. India and B.tech degree from J.N.T.U. Hyderabad, India in Electronics and Communications.

At IIT Kharagpur his work was in the area of network security related to intrusion detection and distributed firewall. His current interests include wireless network security for wireless LAN controllers and light weight access points.