Proceedings of the 2004 IEEE
International Conference on Networking, Sensing & Control
Taipei, Taiwan, March 21-23, 2004

An Active Network-Based Intrusion Detection and Response Systems

Han-Pang Huang* **and Chia-Ming Chang**+

Robotics Laboratory, Department of Mechanical Engineering, National Taiwan University, Taipei, 10660, TAIWAN

TEL/FAX: (886) 2-23633875, Email: hanpang@ntu.edu.tw

*Professor and correspondence addressee, Graduate student

Abstract — ***The network security is getting more important because of increasing worms and network attacks in recent years. More and more security mechanisms are introduced to protect from attack, such as firewalls and intrusion detection systems (IDS). This paper proposes an active network programming model. Comparing to a traditional network, active network gives the nodes programmable ability. It adopts the active network technology. The response, service deployment and service update schemes rely on this technology. The proposed intrusion detection and response system (IDRS) can stop attacks at the first line and respond as fast as possible to reduce the damage caused by intruders. It provides the abilities of detection, report and response. The proposed prototype system adopts the novel data mining technology-support vector machine to enhance the detection function.***

1 Introduction

1.1 Objectives and Motivation

With the wide spread of internet, various kinds of Internet Services are developed, such as e-commerce, web services. Network security is an important issue. According to the report of Carnegie Mellon University's Computer Emergency Response Team's (CERT) [21] Coordination Center, the sophistication of attacks is dramatically increasing and there are usually several stages involved in one attack. The firewalls can protect a system from external attacks, but it cannot keep up with new attacks. The intrusion detection system (IDS) is much more dynamic and can provide advance network defence mechanism. The previous IDS are mostly focused on passive model, which aims at detection and alerting. The present IDS are static and lack the functionality of adding new features and system reconfiguring. Active network is a novel approach to network architecture in which the nodes of the network perform customized computations on the messages flowing through them. This paper proposes a scalable intrusion detection system based on active network technology. The system can tailor the detection mechanisms to the system and replace them with improved detection model. Current IDSs have limited mechanism and emphasize on detecting attacks. The delay time in alert and response may affect the influences of the attacks. Therefore, an automated intrusion response system combined with IDS is necessary. Responding in time and taking appropriate measures can make the system immune to the similar types of the attacks. Unlike the traditional network, which only passively transforms the packets, active network allows the network node to execute the mobile code within packets. The proposed IDS combines distributed monitoring and data mining approach (through individual host and LAN monitors) with centralized data analysis (through the Intrusion Detection Center).

1.2 Background Knowledge Survey

Active network [1][2][4][10][15][16][17][19][20] is a novel approach to network architecture in network nodes, such as switches, routers, hubs, bridges, gateway. The network nodes perform customized computation for the packets flowing through them. The essential feature of active network is the programmability. New network feature and service can be dynamically added to the network infrastructure on demand. Note that active network is different from programmable networks [5][7][9][14]. Active networks carry executable code within packets, while programmable networks are focused on a standard programming interface for network control. Intrusion detection is defined as the process of monitoring and analyzing events occurred in a computer or network and present the results to the administrator. The related research on intrusion detection started in the early 1980s. It has continued through several major DARPA (and other Government) programs. In the beginning of the 1990s, intrusion detection becomes red hot research topic and commercial IDS starts to emerge.

2 Active Network-Based Intrusion Detection System Design

In this paper, an intrusion detection system is designed for detecting both well-known and unknown intrusion behaviors. The system is composed of intrusion detection system (IDS), management center and intrusion detection center (IDC). The relationship among them is shown in Figure 1.

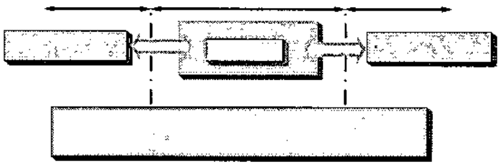

Figure 1 Service Management

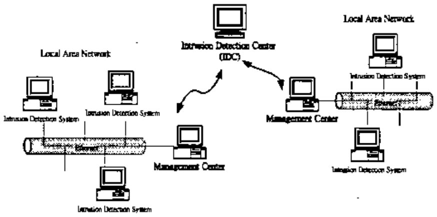
Local Area Network
Intrusion Detection Center
(IDC)
Local Area Nerwork
Intrusion Detection System
Intrusion Detection System
Intrusion Detection System
Ethernet
Management Center
Management Center
Ethernet
Intrusion Detection System
Intrusion Detection System

Figure 2 System Architecture

If any suspected activities are discovered, the corresponding responses of IDS are sent to IDC for further analyzing. Management has the ability to dispatch service agents. The active node can get the desired services form the Management center according to its needs and environment. It also allows the IDC to update the detection model. The overall architecture is shown in Figure 2. Each management center is responsible for a subnet. Its duty is to deploy and update the services. It also maintains and monitors the status *of agents of the active node. In addition to handling these* events, IDC provides the detection modules for IDS. It dispatches them by applying mobile agent technology to satisfy the need of different environments.

2.1 Intrusion Detection Systems

An intrusion detection system (IDS) is composed of node manager, active network monitor, intrusion detection agent, intrusion response agent and network management agent. Each component will be introduced in the following sections.

2.1.1 Node Manager

A node manager is built in every host to provide the transient agent execution environment so that various agents can perform tasks. It can be seen as the cooperation of agents that reside within the agent-based EE. A node manager can monitor agents. It has to check any illegal operations and filter out malicious behaviors. The main function of a node manager is to cooperate all agents according to the host system information.

2.1.2 Active Network Monitor

Active network monitor (ANM) which plays the important role in the system is a programmable traffic monitor. It captures packets from internet according to the user's instructions. It allows the remote manager to dynamically specify the packet type. The manager can get the analysis results and know the quality and traffic of the whole network.

2.1.3 Intrusion Detection Agent

The intrusion detection 1gent (IDA) implements data mining methods, e.g., neural network and support vector machine. It is responsible for the actual intrusion detection job. There are two kinds of intrusion detection agents: services-specified mode and general mode, as shown in Figure 3.

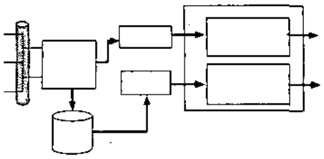

Figure 3 Detection mode of Intrusion Response Agents

2.1.4 Intrusion Response Agent

Intrusion response agent (IRA) is like the commander in the IDS. It is an agent responsible for what action should take when receiving an event or report. It sends out the response commands based on the security policy. For those locally intrusions, it takes responses such as reconfiguring the filter rules, terminating the connections. If no existing knowledge or rules are available, it will pass the message to IDC in a standard format.

2.1.5 Network Management Agent

The purpose of the research is to integrate the IDS and NMS in terms of audit sources, analysis techniques and deployment strategies. This is the responsibility of the Network Management Agent (NMA). The integration of intrusion detection and network management systems will provides a unified view of network security status to the system manager and significantly improve the security management.

2.2 Management Center

Management center is responsible for service deployment and service update. It is service-domain independent and performs tasks without knowing the detail of the service. It is like data warehouse which reposits the agents or mobile codes to deploy service. If IDS or other applications, such as video conference and network management, intend to update the agents, they just send the revised or new edition agent to the management center. It will automatically retrieve the related client software modules according to its node information.

2.3 Intrusion Detection Center

Since the IDS detects suspected activities, the DMA will send the report and related information to intrusion detection center for further analysis. When IDC receives the intrusion reports, they will be sent to the event manager. The decision will be made based on the information, such as attack type and priority. Basically, the intrusion will be sent to detection module to compare with previously known patterns. If the discovered pattern is indistinct, it may need other experts to identify whether they are normal patterns or intrusion. If it is really an intrusion pattern, it will update the knowledge base.

2.4 Programming Model

The programming model is intended to support a general class of active networks. It uses ANEP [3] as the basic transformation protocol. The programming model adopts Java programming language in order to be operating system independent. Besides, programs based on this model should be seamlessly executed on different execution environments. The user should inherit and overwrite the *ANPacket* class of the model to define the unique communication mechanism. Therefore, every active packet can be executed to perform the user-specified action on the active node which it has traveled through. New service can be developed by extending the abstract classes of the programming model. The basic components of the network service in the programming model *are Active Packet, Active Service Base, ANApplication,* and *ANDaemon.*Figure 4 illustrates a general view of the programming model. A new protocol and service can be developed by extending *ANPacket, ANBase,* and *ANApplication.* Based on this programming model, it provides a convenient way to construct the active network-based services. In this paper, the proposed active network-based intrusion detection system is based on this model.

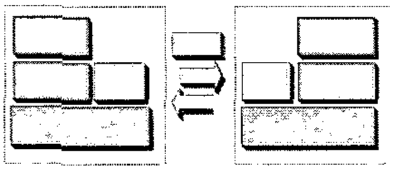

Figure 4 Active network Programming Model

2.5 IDS based active network Model

Based on the programming model mentioned in the previous section, the proposed IDS is constructed. The user should overwrite the *ANPacket, ANBase* and *ANApplication* to create and integrate components to provide the service.
The main classes based on this programming model are *IDSPacket, IDSBase,* and *IDSApplicatopn:*

- IDSPacket

The static portion can be used as a new header. The system is represented by the specified IDS. The *Services ID* is used to identify services. In the proposed prototype IDS, only the general model and web service are defined. The web service is the only implementation of service specified services. *Services Type* is used to specify the environment of the www services. The *Class ID* is used to identify the type of this *ANPacket*. According to the above information, the variation part can be further processed. The variable portion can be a mobile code or just data. The user can handle and execute it in the *ANBase* or *ANApplication*.

- IDSBase

It extends the abstract class *ANBase*. The node manager has the implementation of the *IDSBase*. It provides the context for the program that inherits *IDSApplicaion*. It also exports the basic function of the API for effiency.

- IDSApplcation

It extends the abstract class *ANApplicaiton*. Active network monitor, intrusion detection agent, intrusion response agent, and network management agent are all the implementation of the *IDSApplication*. For the creation of the *IDSApplication*, it should designate the *ANBase*. Then, the node manager can monitor and control these components by the default mechanism of the *ANBase* and *ANApplication*. Each component can easily communicate with other components to perform tasks.

2.6 Protocol

Several protocols are used in our proposed prototype system. These protocols implemented for interoperability are described in the following section.

- ANEP

The Active Network Encapsulation Protocol (ANEP) [3] is defined for interoperability. The ANEP header format is shown in Figure 5.

The Intrusion Detection Message Exchange Format (IDMEF)[6] is an Extensible Markup Language (XML) Document Type Definition (DTD) developed by the Intrusion Detection Exchange Format Working Group (IDWG) [22] of the Internet Engineering Task Force (IETF), which is an IETF working group aims at defining common data formats and exchanging protocols for information sharing among intrusion detection and response systems, and management systems.

2.7 Intrusion Responses

Passive Response

Passive responses of the IDS are used to notify the proper authority. They can provide useful information to the manager. Several passive responses are used in the proposed prototype system and will be described as followed.

Alarms are the common responses adopted in the IDS. They inform users when attacks are detected. They provide the detailed information in the alarm message about the events, such as the source and target IP addresses of the attack, the suspicious activities, and the event priority.

Active Responses

Active IDS responses are automated actions taken when the corresponding suspicious behavior is detected. In general, the IDSs will produce plenty of false alarms. The false alarm will waste system resources and cause packet loss when the network traffic overloads. The prototype system will gather the information about the suspicious target and intruder hosts by increasing the sensitivity of detection. The additional information can help resolve the detection of intrusions. Another active response is to stop the attack in progress by blocking the subsequent access of intruder. The prototype system resides the target host will disconnect all the connections from the intruders, and notifies the routers and firewalls to block the network packets from the attacker. When attacks occur, it is import to respond as fast as possible to reduce damage. The prototype system will trace the intruder. It will notify and update the active node services to isolate the intruder. The IDS system will follow the policy to take action according to the event. The proposed prototype system reports the system status to the network management system. The IDS contains the network management agent that can send SNMP traps and messages to post alarms and alerts to the central network management consoles. Hence, it is easy to detect the abnormal events and report to the manager.

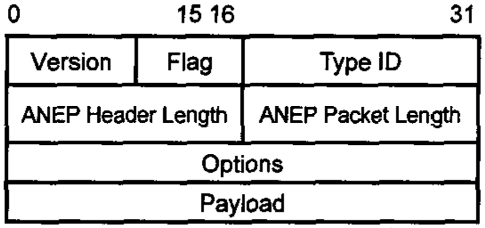

Figure 5 Active Network Encapsulation Protocol (ANEP) header format

2.7.1 Deployment Scheme

The framework provides the flexibility and convenience for service deployment. It adopts mobile agent technology to construct the active network-based services. Each service can negotiate to decide the format of the protocol and the parameters of the specified services. The deployment steps are represented below:

Step 1: The node manager creates the mobile agent according to the user configuration and system environment.

Step 2: The designed mobile agent is sent to the management center. The mobile agent negotiates with the management center to get the specific service.

Step 3: The management center which is responsible for providing services can dispatch the appropriate mobile agents to the client according to the information carried by the previous user's mobile agent.

Step 4: When the mobile agents arrive at the client host and reside into the node manager, they begin to perform the assigned tasks or services. Besides, they can communicate with the predefined protocol.

2.8 Service Update Scheme

Management center deploys the services according to the user's demand and save the related information. When it is necessary to update the Agent version, the Management Center can retrieve the software module from other servers and check the database. Then, the server searches the Management Table by corresponding System ID, Service ID, and Service Type to find out the agent and its position to update the module.

3 Modeling and Methodology

3.1 Detection Models

The general model deals with the general situation and is independent of the system environment. The service specified model is for the specified services. The attack approach of the IIS is quite different from Apache. If the host does not have the web server, it is unnecessary to construct the web attack detection services. The IDC will prepare the web intrusion detection of three different editions (IIS, Apache and others).

3.2 General Development Procedures

3.2.1 Data Format

General Model

Three groups of features defined by KDD Cup are listed below

1. Basic features of individual TCP connections
2. Time based features
3. Connection based features

Service Specified Model

In case of service specified model, only the content of the connections are concerned. The data format is only concern about keywords shown in Table 1 and Table 2.

Table 1 General Keywords of WWW Server Specified Service Model

General Keyword	System, winnt, Html ,GET, HEAD, Host, HTTP, scripts , www, Exe, Connnection, Close, Accept, DLL, IIS, MICROSOFT,Content,Server,Ranges,windows

Table 2 Selected Individual Intrusion Keywords

Intrusion	Keyword
WEB-IIS ISAPI .ida attempt	Ida, GetTickCount, LoadLibraryA
EXPERIMENTAL WEB-IIS .asp HTTP header buffer overflow attempt	SmartSaver, abch, MSOFFICE9
WEB-IIS cmd.exe access	Lwrite, msadc,cmd
WEB-MISC cross site scripting attempt	mute, Src, Compatible
WEB-MISC Transfer-Encoding: chunked	PHP, Powered, Transfer
WEB-IIS CodeRed v2 root.exe access	MSADC, Root, c+dir

3.2.2 Data preprocessing

General Model

The five-fold cross validation is used in the training dataset to find out which parameters which have better performance.

Service Specified Model

Every connection between the client and server can be viewed as a document. Then, the text categorization technique uses the keyword as the feature to represent the connection. So each connection can be coded as a feature vector depending on the content, if it contains the keyword from the feature list. In the service specified model of WWW attack, keywords are selected as features to represent every connection.

Feature Selection

The word features comes form two parts: basic common words and keywords from intrusion. Twenty words are selected to represent these kinds of features. Finally, the last keywords are selected according to the $IDF(W_i,d)$. The selected method is based on the $IDF(W_i,d)$ function.

$$IDF(W_i) = \log({}^{DF(W_i,d)}\!/_{DF(W_i)}) \qquad (1)$$

Here, W_i is the keyword. $DF(W_i)$ represents the number of connections that the word W_i occurs in the total number of training connections. $DF(W_i,d)$ represents the number of connections that the word W_i occurs in the specified intrusion. Intuitively, the inverse document frequency (IDF) of a word is low if it occurs in many connections and occurs only few times in the intrusion d. It is the highest one if it occurs in few total connections and occurs only every intrusion d.

3.2.3 Detection Algorithms

Different detection models are implemented by the development procedure described in the previous section. The detection algorithm lists below.

Step1: Receive network packets of connections.

Step2: For each detection model, preprocess the packets to feature vectors according to the detection model profile.

Step3: Classify these specified feature vectors using data mining algorithm such as support vector machine.

Step4: If the intrusion is identified by the service specified intrusion detection agent, the related information will forward to intrusion response agent. The intrusion response agent will handle the event.

4 Experimental Results

In this section, we try to compare the different data mining methods and data processing techniques that are implemented in IDC for constructing the detection model.

4.1 Performances Measures

Some experiments made for verification of accuracy (general and service specified detection model). First, we try to analyze the DARPA KDD Cup 1999 data and compare the result with the champion. Second, the proposed service specified is verified by accuracy and false alarm rate. We use different data mining methods such as neural network and support vector machine to compare the results. The SVM kernel adopts the LIBSVM -a simple and easy-to-use support vector machine tool for classification [23].

4.2 Experimental Results

General model

In order to verify the result, the experiment results are compared to the Bagged Boosting [24]-the winner of the KDDCUP. In summary, the final predictor was an ensemble of 50x10 C5 decision trees [24]. The SVM is relatively insensitive to the size of the dataset and is less independent of dimensionality of feature space [8]. Therefore, there are some experiments made by using SVM [11][12][13] to IDS. The experiments show high accuracy and low training time. Although it has tremendous high accuracy, the result can not compare with the champion. Because it rearranges the source dataset, the new dataset only has two classes: intrusion and normal. It does not imply that the SVM can not solve the multi-class problem. Hence, some experiments are conducted by applying SVM to the KDDCUP multi-class dataset. In addition, the general intrusion mode needs to identify probe, normal, DOS. These three classes have similar attributes and are system independent. That is why we use them to construct the general model. The SVM kernel function used in the experiment is radial basis function. The parameters used are that gamma is 0.00001 and cost is 55. Neural network is also used to compare with the SVM. There are 40 hidden nodes used in the three-layer neural network. Table3 and Table 4 show the comparing results. SVM has better result in the probe class and similar result. But NN has lower performance. In short, the SVM, winner's accuracy and false alarm rate are close. It still has better performance because the testing examples are enormous. The results show that SVM can be applied to multi-class intrusion detection model with excellent performance.

Table 3 Class Accuracy of the Algorithms in the KDDCup 99 Data Set

Class	Winner	SVM	NN
normal	99.47%	99.50%	99.34%
probe	83.30%	86.89%	73.26%
DOS	97.10%	97.09%	97.07%

Table 4 False Alarm Rate of the Algorithms in the KDDCup 99 Data Set

Class	Winner	SVM	NN
normal	8.79%	9.99%	10.25%
probe	31.16%	6.8%	8.44%
DOS	0.11%	0.25%	0.45%

Service specified model

Table 5 shows that both results are good. But it may be questionable whether the new intrusion can be detected. It may need further evaluation. At last, the known intrusions can be detected.

Table 5 Service Specified Model with Different Approaches

Algorithms	False Negatives Rate	False Positive Rate
SVM	100%	0
NN	100%	0

5. Conclusions

This paper proposes an active network model and develops the IDS based on the model. The system is flexible and scalable. It enables the dynamic service deployment and update scheme. The software components are lightweight and dynamically updateable. It also has the mechanism of automated response to intrusions. It can reduce the reaction time to lower the damage. The system detection models can be divided into general model and service specified model for the rapid development of the data mining detection model.

References

[1]. N. Achir, M. S. P. Fonseca, Y.M. Ghamri Doudane, N. Agoulmine, and A. Mehaoua, "Active Networking System Evaluation: A Practical Experience," *7th International Workshop on Mobile Multimedia Communications*, MoMuC'2000, Tokyo, Japan, Oct. 2000.

[2]. D. S. Alexander, M. Shaw, S. M. Nettles, and J. M. Smith, "Active Bridging," *Proceedings of the ACM SIGCOMM'97 Conference, Cannes, France*, Sep. 1997

[3]. D. S. Alexander, B. Braden, C. A. Gunter, A. W. Jackson, A. D. Keromytis, G. J. Minden, D. Wetherall, "Active Network Encapsulation Protocol (ANEP)," Request for Comments: DRAFT, July 1997.

[4]. K. Calvert, S. Bhattacharjee, E. Zegura, and J. Sterbenz, "Directions in active networks," *IEEE Communications Magazine, Special Issue on Programmable Networks*, Oct. 1998.

[5]. A. T. Campbell, H. G. De Meer, M. E. Kounavis, K. Miki, J. B. Vicente, and D. Villela, "A Survey of Programmable Networks," *ACM Computer Communications. Rev.*, vol. 29, pp. 7-23, April 1999.

[6]. D. Curry and H. Debar, "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition," draft-ietf-idwg-idmef-xml-03 (work in progress), Feb. 2001.

[7]. J. Gao, P. Steenkiste, E. Takahashi, and Al. Fisher, "A Programmable Router Architecture Supporting Control Plane Extensibility," *IEEE Communications Magazine*, March 2000.

[8]. T. Joachims, "Estimating the Generalization Performance of a SVM Efficiently," *Proceedings of the International Conference on Machine Learning*, Morgan Kaufman, 2000

[9]. R. Keller, J. Ramamirtham, T. Wolf, and B. Plattner, "Active Pipes: Service Composition for Programmable Networks," *Milcom 2001*, Lean VA, Oct. 2001.

[10]. A. Kulkarni, G. Minden, R. Hill, Y. Wijata, S. Sheth, F. Wahhab, H. Pindi and A. Nagarajan, "Implementation of a Prototype active network," *OPENARCH '98*, San Francisco, CA, April 1998.

[11]. S. Mukkamala, G. Janowski and A. H. Sung, "Intrusion Detection Using Support Vector Machines," *Proceedings of the High Performance Computing Symposium – HPC 2002*, pp. 178-183, April 2002.

[12]. S. Mukkamala, G. Janowski, and A. H. Sung, "Intrusion Detection Using Neural Networks and Support Vector Machines," *Proceedings of IEEE IJCNN*, pp. 1702-1707, May 2002

[13]. S. Mukkamala and A. H. Sung, "Feature Ranking and Selection for Intrusion Detection," *Proceedings of the International Conference on Information and Knowledge Engineering – IKE 2002*, pp. 503-509, June 2002.

[14]. L. Peterson, Y. Gottlieb, M. Hibler, P. Tullmann, J. Lepreau, S. Schwab, H. Dandekar, A. Purtell, and J. Hartman, "An OS Interface for Active Routers," *IEEE Journal on Selected Areas in Communications*, vol.19, no.3, March 2001.

[15]. K. Psounis, "Active Networks; Applications, Security, Safety and Architectures," *IEEE Communications Surveys*, vol. 2, no. 1, 1999.

[16]. D. Tennenhouse and D. Wetherall, "Toward an active network Architecture," ___*ACM SigComm's Communication Review*, April 1996.

[17]. D. L. Tennenhouse, J. M. Smith, W. D. Sincoskie, D. J. Wetherall, and G. J. Minden, "A Survey of active

network Research," *IEEE Communications Magazine*, vol. 35, no. 1, pp. 80-86, Jan. 1997.

[18]. G. Vigna and R. A. Kemmerer, "NetSTAT: a network-based intrusiondetection approach," *Proceedings of the 14th Computer Security Applications Conference*, pp. 25-34, 1998.

[19]. D. J. Wetherall and D. L. Tennenhouse, "Towards an active network Architecture", *Computer Communication Review*, pp. 5-18, April 1996.

[20]. D. J. Wetherall, U. Legedza, and J. Guttag, "Introducing New Internet Services: Why and How," *IEEE Network Magazine*, July 1998.

[21]. CERT coordination center, ***http: //www.cert.org/***

[22]. Intrusion Detection Exchange Format (idwg), *http://www.ietf.org/html.charters/idwg-charter.html*

[23]. LIBSVM - A Library for Support Vector Machines, http://www.csie.ntu.edu.tw/~cjlin/libsvm/index.html

[24]. Winning the KDD99 Classification Cup, http://www.ai.univie.ac.at/~bernhard/kddcup99.html