The Defense Framework For Large-scale Computer Network System

JIANCHUN JIANG, WEIFENG CHEN, SIHAN QING,DENGGUO FENG

Engineering Research Center for Information Security Technology
Chinese Academy of Sciences, Beijing 100080,P.R.China
{jianchun, chwf, qsh,fengdg} @ercist.iscas.ac.cn

Key words: network security, attack, defense

Abstract: This paper proposes a defense framework for large-scale computer network system(DFLCNS) to cope with potential threats. The DFLCNS is composed of prevention subsystem, intrusive detect subsystem, response subsystem, anti-attack subsystem. These subsystems co-work with each other to provide defense services.The new idea of the DFLCNS is active and cooperative comparing with others. Finally, the paper illustrates the prototype of the DFLCNS and conclude with future works.

1. INTRODUCTION

The modern society is growing increasingly dependent upon large-scale networked systems, which improve the efficiency and effectiveness of organizations. However, such networked systems are accompanied by elevated risks of intrusion and compromise. Because the networked systems are large-scale, they are very difficult to administrate, and then they suffer from a lot of security threats: worms, break-ins, hijacking, spoofing, denial-of-service, and so on[7, 8, 9, 10]. Contemporary many networked computer system are protected against external threats by traditional network security technology such as firewall[13, 14]. Serving as system guardians, firewalls are only part of a comprehensive network protection scheme. Completely

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35515-3_53

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

preventing breaches of security appear unrealistic. The main reasons are listed as follows[4, 5, 6, 7]:

bad design, wrong implementations and poor integration
cryptographic methods problems
no cooperation between defense subsystems and response slowly
human operating error
passive defense

With all aspects carefully considered, it is very necessary that the defense framework is designed so as to prevent unauthorized access to system resources and data. We proposes a defense framework for large-scale computer network system(DFLCNS) to cope with potential threats. The DFLCNS is composed of prevention subsystem, intrusive detect subsystem, response subsystem, anti-attack subsystem. The prevention subsystem(PS) can stop these intrusion actions. The intrusive detect subsystem(IDS) can try to detect these intrusion attempts so that action may be taken to repair the damage later. The response subsystem(RS) can restore and repair the compromised system. The anti-attack subsystem (AS) can counter hacker's actions.

This paper is organized as follows: Section 2 describes design issues and overall architecture of DFLCNS, Section 3 gives detailed design for each defensive subsystem of DFLCNS, Section 4 describes implementation issues and illustrates the prototype of the DFLCNS, Finally, we conclude with future works.

2. OVERVIEW OF DFLCNS

2.1 Design Issues

The DFLCNS provides prevention control, intrusive detect, response action, and anti-attack defense services. The basic idea of defense frame is to cooperate with defense subsystem,and then DFLCNS is able to prevent dynamically, detect intrusive action, counter attacker actively and recover duly. Unlike the traditional security measures that only defense passively such as firewall. A key characteristic of DFLCNS is its capability to counter intruder in the face of attack, and is an wide automated defense system.. Using DFLCNS, a variety of attacks will be detected and counter. Upon an attack being launched, defense subsystem will alert each other of the attack and a subsystem will be selected to initiate an automated response. The responses of DFLCNS will vary with the attack.

2.2 Overall Architecture of DFLCNS

As shown in Figure.1,DFLCNS is composed of four defense subsystems.

Prevention subsystem (PS): it is composed of packet filter component, proxy component, verify component, and access control component. components. PS provides identication, authentication and filter services. To enter the defensed network system, a user should submit his identity, password, and role name to the identication component. Using user information, the prevention subsystem decide whether it permit to pass. Generally, it block dangerous services like TFTP, the X Window System and the "r" services(rlogin, rsh, etc).PS still communicate with the other defensive subsystem. Once it receives attack signal from intrusive detect sub-system, it will carry out prevent actions.

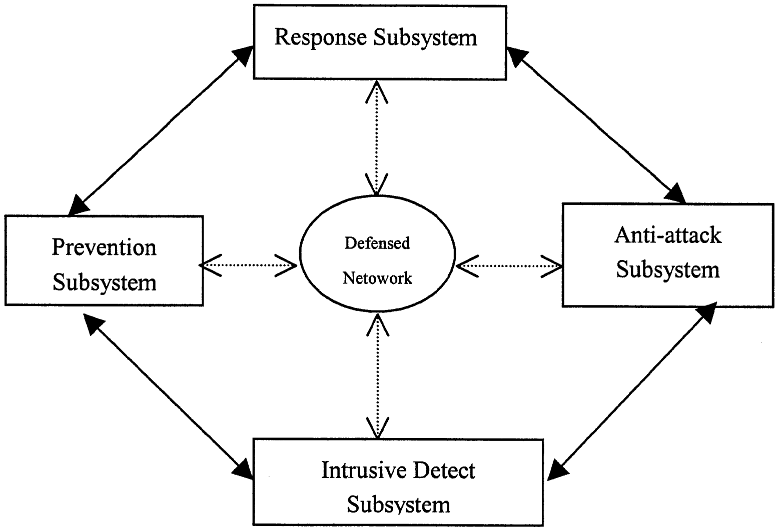

Figure 1 Defense System Architecture

Intrusive Detect Subsystem (IDS) : It is composed of misuse detection component and anomaly detection component. It dynamically find intruder's actions and advise the other defensive subsystem in large network. Although it is not possible to build a completely secure system in practice [6, 7]. If there are attacks on a system, we would like to detect them as soon as possible (in real-time) and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. So that action may be taken to repair the damage and enhance system security later.

Anti-attack Subsystem (AS): It is composed of audit component, deception component and track component. These components make

DFLCNS represents the active characteristic. The audit component record the actives of network system, for example user login. Using audit trails, we can find suspicious active, and decide whether the system is intruded. Certainly, These audit records are used to hacker's evidence. The deception component deal with those malicious intrusive actions. The security administrator can take advantage of deception component to counter effectively attacker. Doing so, it gains the following advantages[4, 5]:

(1) increases the attacker's workload
(2) see attacks coming well ahead of time
(3) exhaust the attacker's resource
(4) decentralization the attacker's attention
(5) track attacker attempts and respond in advance

Response Subsystem (RS): it dynamically adopt emergency actions and communicate with the other defense subsystems in large-scale network. There is no ideal security system, and so there should have response measures. The RS set up some strategies and disposes in advance to handle security incident after an intrusion has occurred.. The task of the RS is to evaluate the network situation, alarm notice, snapshot the compromised system, restore and recover the destroyed system. The RS make DFLCNS own the survivability characteristic

3. DETAILED DESIGN OF DFLCNS

3.1 Prevention Subsystem

As shown in Fig.2 the prevent subsystem includes packet filter, authentication, and access control.

The algorithm of the PS is described as follows:

1. packet filter component prevent malicious packet from incoming defensed network; if pass goto step 2 else prevent user 's operation;
2. authentication component confirm user identity; if pass goto step 3 else prevent user 's operation;
3. access control component limit user 's operation;
4. repeat step 1,step2,step 3;

3.2 Intrusive Detect Subsystem (IDS)

As shown in Fig.3, this is intrusive detection subsystem architecture. The IDS attempts to detect an intruder breaking into system or a legitimate user

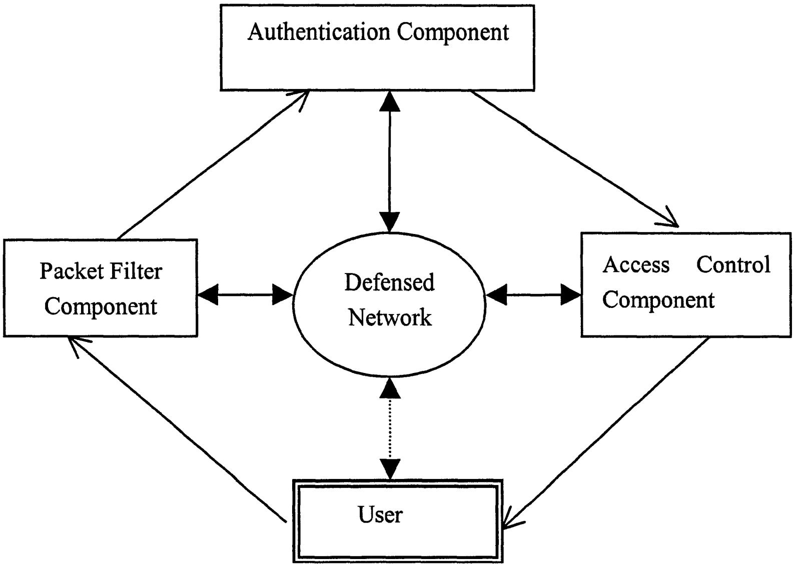

Figure. 2 Prevent Subsystem

misusing system resources. Traditionally, intrusions detection technique can be categorized into misuse intrusion detection and anomaly intrusion detection[11]. The first approach try to recognize known "bad" behavior. For attacks on known weak points of a system, they can be detected by watching for activity that corresponds to certain intrusion signatures or system vulnerabilities. For example, an attempt to create a setuid file can be caught by examining log messages resulting from system calls. As misuse intrusions follow well-defined patterns, The main difficulties in this approach are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity.The last approach attempt to detect intrusion by observing significant deviations from normal behavior. It firstly assume that all intrusive activities are necessarily anomalous. This approach is to establishing a "normal activity profile" for a system or user behaviour, then detect intrusion attempts by observing significant deviations from the established profile. The normal profile maybe include average CPU load, I/O usage, number of network connections per minute, number of processes per user and so on. It are harder to detect, since there are no fixed patterns in anomaly intrusion detection that can be monitored for, so a more "fuzzy" approach have to be taken. At present, there have been a few major approaches to anomaly intrusion detection systems, some of which are statistical approaches, predictive pattern generation neural networks [11, 12].Every techniques have long and short. Our viewpoint is to integrate these technique into an IDS so as to make use of their advantages. The following is given main processing steps of intrusive detect subsystem :

Step 1: collect raw source data from audit records on host, network traffic ;

Step 2: parse data ;

Step 3: analysis data and judge ;
Step 4: send alarm to the other defensive subsystem

How to collect raw data is very important for IDS. The IDS can collect raw data from audit trail, application software log and network traffic. And then the IDS parse these raw data, search attack signature and build normal profile to observe abnormal activity. During designing the IDS, we should take into account the following issues [3, 12]:

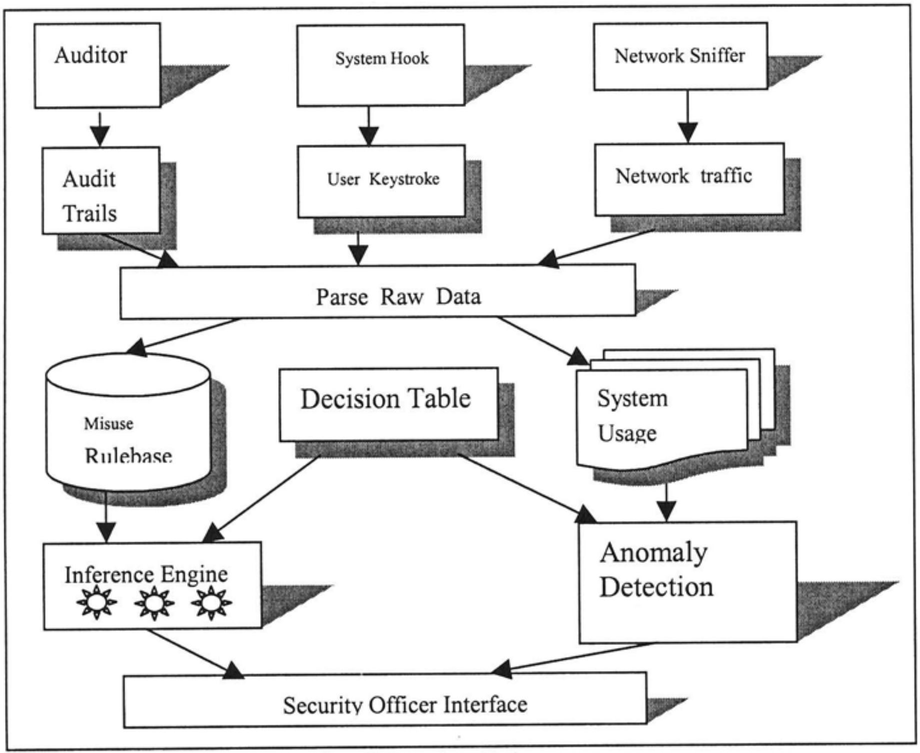

Figure3 Intrusion Detection Subsystem

Accuracy. It has low false intrusive alarm.

Fault tolerant. It must survive a system crash and not have its knowledge-base rebuilt at restart.

Anti-attack. It must resist subversion. The system can monitor itself to ensure that it has not been subverted. it must be difficult to fool.

Performance. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.

Scalability. It must be easily tailored to the system in question. Every system has a different usage pattern, and the defense mechanism should adapt easily to these patterns.

Adjustability. It must cope with changing system behavior over time as new applications are being added. The system profile will change over time, and the IDS must be able to adapt.

Timeliness. The IDS has to perform and propagate its analysis as quickly as possible to enable the other defense subsystem to react before much damage has been done.

Completeness. Incompletness occurs when the IDS fails to detect an attack.

3.3 Response Subsystem

Using this response defense subsystem, a variety of attacks will response in time, and so network don't suffer from more damage. As shown in Figure. 4, response defense subsystem are composed of decision engine, response policy database, response engine and so on. decision engine analyer intrusive signal against response policy database. Then decision engine give the result to response engine. response engine carry out policy script. These responsive actions may be network disconnection, packet filter, packet injection etc.

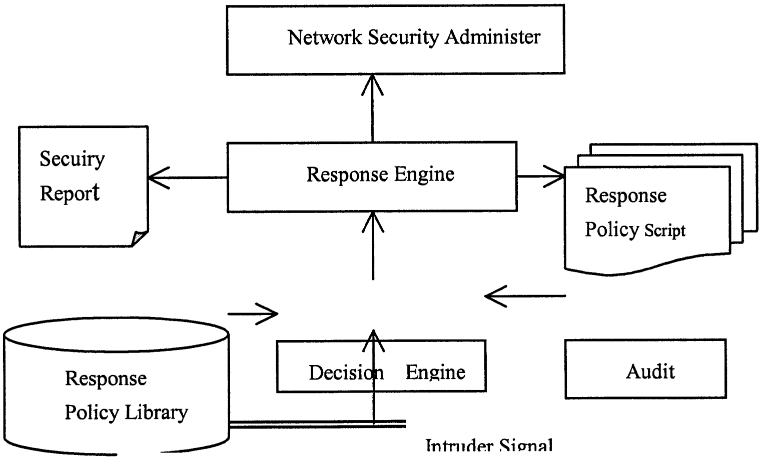

Figure 4 Response Defense Subsystem

However, when the RS response attacks, it maybe impact on normal users' operating and some network services. We will have to consider how to solve the problem during responsing attacks. After all, we don't want the response to be more harmful than the attack itself. So the RS should meet the following requirement[1]:

availability: the RS can't increase too much burden of system;

scalability: the functions of RS are tailored or added;

practicability: the actions of RS can be carried out in real system environment;

3.4 Anti-attack Subsystem

Generally, there are two approaches to mitigating attacks on a network system. The first approaches, known as safeguard, involves taking some protective action before a attack has occurred. The second approach, known as countermeasure, involves taking some protective action after a attack has occurred. The two approaches consider defender from frontal. It's defensive idea is passive, but anti-attack defensive subsystem is active. It can be assume itself is attacker. This is very important for counter attacker. For example, we can run SATAN to detect network system. On the other hand, the anti-attack defensive subsystem construct false information or services [4, 5]. We all know attacker like to crack password. If we supply a fake password file, it must take attacker much time and energy to crack, but it is no harm for us. We know that an attack could be considered to be comprised of three phases, viz preparation, execution, and post-attack [2]. In the preparation phase, the attacker gathers information needed to launch the attack. The actual attack occurs in the execution phase. In the post-attack phase, the desired effects of the attack are observable. Naturally, we first use deception to counter attacker before the last phase.

The anti-attack defensive subsystem is shown in Figure 5.

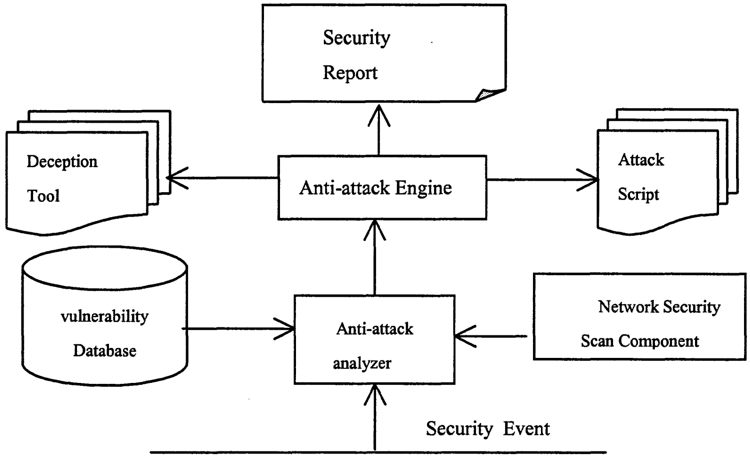

Figure 5 Anti-attack Defense Subsystem

4. IMPLEMENTATION ISSUES

The prototype of the DFLCNS described so far has been implemented and tested. We apply it in defending WWW information system. Four different corporate entities have been brought together to produce the defence system: WWW Guard System. It is shown in Figure 6.

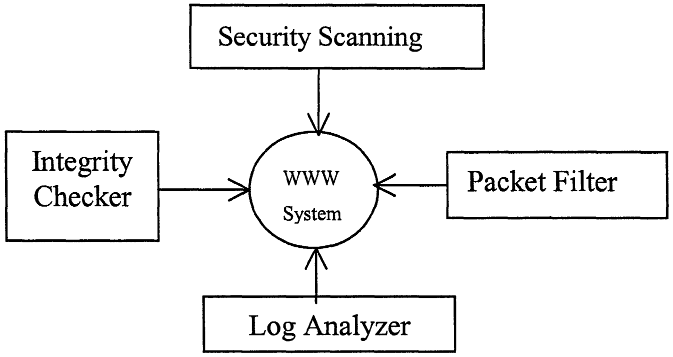

Figure 6 WWW Guard System

In WWW guard system, The function of different defence subsystem are listed in the following:

Log Analyzer: analyze WWW log files and operating system log files so that it search for some intrusion actions.

Integrity Checker: check the integrity of the WWW file system so that the WWW guard system can restore it in time.

Packer Filter: prevent illegal packet entering into WWW system and restrict services access

Security Scanning: Scans all accessible TCP ports on WWW server and then analyzes the data and generates a report detailing the security vulnerabilities of each service, along with possible corrective actions

We feel that the idea of DFLCNS is useful and scalability in practice. It can be integrated into a single component. For example packet filter can be designed to own ability to counter attack. Certainly, it can be viewed a idea to protect network system.

5. CONCLUSIONS

We have discussed a framework to defend network security. Most networks are insecure as the hosts that are attached to the network and the network must be protected against attacker(insiders and outsiders).

The paper establishes a defensive framework (called the DFLCNS) for coping With network attack. The DFLCNS may be a single component software, or several software component integration as long as they can cooperate with each other.

The paper also presents a model of defense, the model reflecting the defensive phases of prevent, detect, counter and response. These defensive phases effect and cooperate each other. Finally, we remark that our present work.

However, there are still several open problems and much new work to be done in the DFLCNS.

Can we implement a defensive protocol which make PS, IDS,RS, and AS cooperate easily?

How we describe a intrusion action using a language?

Are there good method to detect intruder in the large network system?

Are there effective ways to evaluate the defensive system?

6. REFERENCES:

[1] http://seclab.cs.ucdavis.edu/response/

[2] L.Todd Heberlein,Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee,Jeff wood and David Wolber 1990 IEEE Computer Society Symposium on Research in Security and Privacy

[3] http://www.cerias.purdue.edu/coast/intrusion-detection/detection.html

[4] http://all.net/journal/journal/ntb/mathdeception/mathdeception.html

[5] http://all.net/journal /journal/ntb/deception.html

[6] Dorothy E Denning. An Intrusion Detection Model. In IEEE Transactions on Software Engineering, Number 2, page 222, February 1987

[7] Edward Amoroso, AT&T Bell Laboratories. Fundamentals of Computer Security Technology. Prentice Hall International, Inc.

[8] S.M. Bellovin Security problems in the TCP/IP protocol suite, Computer Communication Review,Vol 19,No.2,pp32-48,April 1989

[9] Marco de Vivo,Gabriela O. De Vivo, Germinal Isern Internet Security Attacks at the Basic Levels, OPERATING SYSTEM REVIEW,1998

[10] TCP SYN Flooding and IP Spoofing Attacks. CERT Advisory CA-96.21

[11] Sandeep Kumar. Classification and Detection of Computer Intrusions. Ph.D. Dissertation, August 1995.

[12] Herve.Debar, Marc Dacier, Andreas Wespi Towards a taxonomy of intrusion-detection systems, Computer Networks Vol 31 pp805-822,1999

[13] W.Cheswick and Sibellovin. Firewall and Internet Security. Addsion –Wesley,1995

[14] D.B.Chapman and E.D.Zwicky.Building Internet Firewalls. O-Reilly & Associates. Inc.. 1995.