Honeynet Based Distributed Adaptive Network Forensics and Active Real Time Investigation

Wei Ren
Department of Computer Science, School of Information, Zhongnan University of Economics and Law, Wuluo Road 114, Wuhan, P.R.China 430064
+86-27-88045625
renw@public.wh.hb.cn

Hai Jin
Cluster and Grid Computing Lab, School of Computer, Huazhong University of Science & Technology, Luoyu Road 1037, Wuhan, P.R.China 430074
+86-27-87543529
hjin@hust.edu.cn

ABSTRACT
Network forensics and honeynet systems have the same features of collecting information about the computer misuses. Honeynet system can lure attackers and gain information about new types of intrusions. Network forensics system can analysis and reconstruct the attack behaviors. These two systems integrating together can help to build an active self-learning and response system to profile the intrusion behavior features and investigate the attack original source. In this paper, we present a design of honeynet based active network intrusion response system. The features of our system are distributed adaptive network forensics and active real time network investigation.

Categories and Subject Descriptors
C.2.4 **[Distributed Systems]**: Distributed Applications – *distributed trap system, network forensics system.* C.3 **[Special-Purpose and Application-based Systems]**: Real-time Systems – *active response and network investigation*

General Terms
Management, Design, Security

Keywords
Network Security, Honeynet, Network Forensics, Network, Computer Forensics, Digital Forensics

1. INTRODUCTION
Honeynet system attempts to attain the unknown attacking signature by setting up a controlled environment similar to the service system, inveigling attackers, gaining information about new type intrusions to aid the corresponding security system [1].

Computer forensics is defined as the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Network forensics is used to describe the task of analyzing information collected on active networks from various intrusion detection, auditing, and monitoring capabilities for the purpose of protection [2].

In this paper, we present the design of a network forensics system in the honeynet environment. The novel approaches in our system are dumping the traffic adaptively by the mechanism of the analysis of log data, which are gathered from the distributed agents on the different host. The real time forensic analysis on the forensics server can guide the investigation behavior on the network investigator machine. The investigation to the attack source is active and at real time.

2. FUNCTIONS AND COMPONENTS
One basic function is to capture network traffic and log data efficiently. To capture the whole traffic can get the detail of the forensics data. The other essential function is to analyze the traffic and log data according to the user's needs. The traffic can be retrieved according to the rules, such as IP, protocol and so on. The analysis of the traffic can replay the attack behavior.

There are four elements in our network forensics system. They are network forensics server, network forensics agents, network monitor, network investigator.

Network forensics server integrate the forensics data and analysis them. It also guides the network packet filter and captures behavior on the network monitor. It can launch the investigation program on the network investigator as the response to the sensitive attacks. Network forensics agents are engine of the data gathering, data extraction and data secure transportation. It also gives the mechanism of digital signature to data integration, communication, command and control. These agents are deployed on the monitored host and network. Network monitor is a packet capture machine to adaptively capture the network traffics. Network investigator is the network survey machine. It can provide the mapping topology data and so on. It can actively investigate target when server gives the command. It can launch the real time investigation response to the network intrusion.

SAC'05, March 13-17, 2005, Santa Fe, New Mexico, USA.

3. SYSTEM FEATURES

3.1 Architecture

Figure1 gives the architecture of the network intrusion forensics system. There two local area network in the architecture. One LAN is monitored honeynet network. The other is forensics LAN, which is high-speed and utilizes the SSL (Secure Socket Layer) techniques to secure transportation.

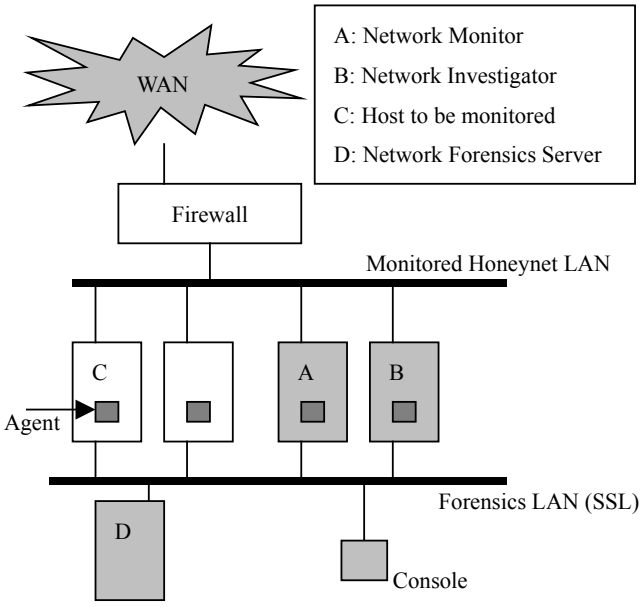

Figure 1. System Architecture.

3.2 Honeynet Deployment Policies

There are four different methods of honeynet employment. They include deception services, weakened systems, hardened systems and user mode servers. Hardened systems will apply all known security patches to the operating system in an effort to make each of the exposed services as secure as possible. User mode servers are simply functional servers that have been nested within the application space of the host operating system. When an Internet user transmits a request to the IP address of one of the user mode servers, the host accepts the request and routes it to the proper user mode instance. We deploy the hardened systems and user mode servers in the honeynet, together with the firewall and IDS system. Data control measures will prevent the compromised machine being a gangplank and protect the record data.

3.3 Secure Distributed Log Data Fusion

Our network forensics system can integrate the log and audit system of the honeynet, such as server log, host log, IDS alert, and so on. The system can build an integrate database, we call it LOGDB. The data mining analysis approaches will be used to learn the features, such as hostile IP address, MAC address, attacking ports and so on. We deploy log gathering agents components in the honeynet system.

3.4 Adaptive Network Traffic Capture

Capture module can capture the fully network traffic, so it require a large amount of disk space. But to keep the efficiency of capture network traffic, we select the data to save: such as a record of the source/origin, destination, service port, duration, bytes transferred for every TCP connection occurring on the network. Under some circumstances, we might eliminate irrelevant traffic by applying a filter.

Our network forensics system can adaptively capture the network traffic in the honeynet. System can automatically to change the policies to filter and dump packets according to the traffic burden. Packets capture module is deployed in the honeynet environment. We run packet dump module on a host linking to the hub. This module can adaptively change the filter rules.

3.5 Active and Real Time Investigation

To analysis the attack behavior by replay the attacking procedure. Network forensics tools can reorganize the packets into individual transport-layer connections between machines. Protocol parsing and analysis is the major work of network forensics analysis. In the analysis, the POP3, HTTP, FTP and telnet protocols need to be paid more attention. After the protocol parsing, we may find the covert channel or data hiding in the traffic, which add the burden of the investigation. Some artificial intelligence and data mining approaches can be used to forensics analysis.

In the investigation we can use some methods to trace a steady stream of anonymous Internet packets back towards their source. IP trace back and mapping the IP to the geographic location are the most important approaches in the network investigator. The response is real time, so that once the IDS gives the alert, the network forensics server will send the command to the network investigator. Another approach can be used is remote OS fingerprinting. It can obtain the general OS type of the target host. Surveying the domain name of an IP address can obtain some details of the malicious origin, such as DNS surveying. Many tools are integrated in the system, such as the ping, traceroute, nslookup, whois and so on.

We will build a database to profile the hostile person or organization. We store the IP address, attacking features, the location of the hackers in the database.

4. CONCLUSION

We describe a framework for utilizing deception technology in network forensics systems. We give an implementation design of an adaptive network forensics and active real time investigation system.

5. REFERENCES

[1] Know Your Enemy: GenII Honeynets, November 2003. http://project.honeynet.org/papers/gen2/

[2] Gary Palmer, A Road Map for Digital Forensic Research, Technical Report DTRT0010-01, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS)