Implementation of an Emulation Environment for Large Scale Network Security Experiments

Cui Yimin, Liu Li, Jin Qi, Kuang Xiaohui
National Key Laboratory of Science and Technology on Information System Security
Anxiang Beili 10#, Chaoyang District, Beijing, China
tsiu-min@163.com

Abstract: Large scale network attack, for instance worm, DDoS, will have serious impacts on network service and network infrastructure. Because of the difficult points that the experiment needs complicated network topology and various defense schemes, researches on test and evaluation of large scale network attack are less. This paper presents metrics and indices of effectiveness evaluation of large scale network attack and defense, and introduces in detail the major methods used to implement an emulation environment.

Key-Words: Network security; Experiment; Emulation environment; Metrics

1 Introduction
Research on large scale network attack and defense needs to do experiment. But the experiment can not be carried out on real network; moreover, devices in laboratory are limited in types and quantity. So an emulation environment which can be used to simulate large scale network attacks and deploy different protection policies is needed to collect experiment data and analyze the efficiency of the policy enforcement. This paper introduces the implementation of an emulation environment for large scale network security experiment and the evaluation system.

2 Related Work
Implementation methods of Network security experiment environment are divided into packet level simulation, network emulation, test bed and hybrid emulation.

The experiment environment implemented by packet level simulation method, such as PDNS[1] and GTNetS[2] has so good scalability that a single simulation instance can simulates a network of hundreds and thousands nodes. This kind of experiment environment has network characteristics such as bandwidth, congestion, delay, topology, throughput and loss etc.

The experiment environment implemented by network emulation method builds corresponding relationship between real devices and experiment nodes, and it has high fidelity in characteristics at both network and end system levels. Network emulation is furthermore subdivided into test bed and overlay network. Emulab[3] and DETER[4] belong to the former, Planetlab[5] belong to the latter. The scale of experiment environment implemented by network emulation method is limited to the quantity of real devices.

Test bed is built by using the software and hardware which are consistent with real network, so it is real network system.

In order to balance the contradiction between scalability and fidelity, hybrid method is proposed, which is subdivided into packet level simulation combining with parser model and network emulation combining with packet level simulation. For the former, M. Liljenstam etc.[6] made use of packet level simulation combining with parser model method to implement a hybrid worm simulation experiment environment on the basis of SSFNET simulator. Deterlab and Emulab etc. made use of network emulation combining with packet level simulation method to implement a large network experiment environment.

The later method can take advantage of not only high scalability of packet level simulation method, but also high fidelity of network emulation method, furthermore, because the environment implemented by adopting the simulation idea of hardware in loop, and it can interface with real network device and software, it can be directly used to analyze and evaluate the efficiency of defense mechanisms.

DETER[7,8,9] have done much more researches in detail on effectiveness measuring of Worm and DDoS attacks.

3 Emulation Environment
In order to study defense policy against large scale network attacks, we have implemented an emulation environment which has multiple-level fidelity and
supports large scale network security experiments by using the packet level simulation combining with network emulation method. The test shows that the environment could support researches on large scale network attacks.

3.1 Architecture of the Environment
The function architecture of the emulation environment is shown in Fig. 1.

The large scale network security experiment emulation environment is composed of control network and test network. The control network bears management, resource configuration and monitoring of the emulation environment. The test network comprises all kinds of nodes connected by programmable interconnected network, such as IP network simulation nodes, router emulation nodes, end nodes, kernel routers, network devices etc. The IP network simulation node is used to simulate certain scale network using network simulation method based on discrete events, and realize packet level interaction between virtual network nodes and real network devices. The router emulation node is used to emulate router device using soft routing technology.

Packet parsing and reconstructing technology uses BPF (Berkeley Packets Filter) to capture the packets in real-time which arrive at the network interface of the local host, or the packets needed to be retransmitted. The packet is parsed to get its destination address, port and payload, then, it is converted to virtual network packet, next, it is forwarded to the virtual network.

When a packet of virtual network arrives at boarder gateway node, the TTL of real network packet is reset according to the virtual one, and then it is sent to real network by BPF. In order that the packets can be correctly routed, a router table which can be updated in real-time is built in the simulation instance through packet retransmitting based on dynamic router table method. When the real network packet is converted to the virtual network packet, the destination IP address is used to search dynamic route table. If it is in the address table, virtual network packet is created by using corresponding simulated node address as destination address of virtual network packet. Otherwise, the emulation node interface route table is searched and the corresponding virtual network boarder node address is used to create virtual network packet. So, the real network packet is correctly retransmitted in virtual network.

3.2 Network Simulation Method Based on Discrete Events
On the basis of NS2 network simulator, that the packets are converted and routed correctly between virtual network and real one is realized by using packet parsing and reconstructing technology and packet retransmitting based on dynamic route table technology, as shown in fig. 2 and 3.
When the virtual network packets are converted to real network packets, the real network packet address is directly used to query the interface route table to determine the retransmitting interface because the payload of the virtual network packet is real network packet. Then, the correct routing is realized.

In order to verify the emulation functions of large scale network, a test network is constructed by 6 high performance PCs, a Juniper router and a real network. The real network comprises a switch and some personal computers. The configuration of each PC is as following: CPU 1.6Hz, memory 512M, 4 network interfaces, and bandwidth of each interface 100Mbps, as shown in fig. 4.

The experiment network created by the topology generating tool[10] of the large scale network security experiment emulation environment was composed of auto systems, routers and end systems. There were 4 Autonomous Systems (AS), 160 route nodes and 20000 host nodes. Due to too many nodes, fig. 5 only shows router level topology. The number of the nodes connected to each router was created in random, BGP4 route protocol is used between ASs, OSPF route protocol is used inside ASs, and there were total 3 kinds of background traffic: CBR, FTP and HTTP.

3.3 Simulation of Defense mechanism
Defence policy can be divided into active policy and reactive policy. Active policy is defined according to the protection strategy and is used to protect the network at usual time, while the reaction policy is defined according to the characteristic of the attack, and it is distributed while the network is under attack.

Active defense doesn’t rely on concrete characteristics of the attack, the means of which contains various security mechanisms such as firewall, IDS, OS access control, etc. The distribution of the active policy is divided into distribution on real nodes and simulation distribution on virtual nodes.

For the convenience of the actual policy distribution, popular OS, firewall and IDS are collected, which can be put to use according to the requirements. The policy distribution on virtual node is realized via two steps: first, abstract characteristic of the policy, then translate it to proper format by the translation tool. The enforced controls by policy distribution include connection control: control the connection relationship between the nodes; interface control: control the availability of the interface of the node; access control: control the access to every kind of resource, such as file system; protocol control: control the protocol the node can process.

Reactive policy is created after the attack is identified. It is distributed on the same way as active policy.

4 Effectiveness Evaluation
The effectiveness of simulated attack and defence is evaluated according to the variation of the network performance.

4.1 Metrics
Generally speaking, network attack and defense capabilities are composite. Attack capability can be divided into network scanning capability, system penetration capability, blocking and disturbing capability, evading and elusion capability, and so on. Network defense capabilities can be divided into identification capability, protection capability and
response capability and so on. Emulation environment is mainly used to study the impacts made by large scale network attacks, so as to find out valid protection policy. So, metrics are mainly defined to measure the effectiveness of blocking and disturbing attack.

Attack effectiveness can be measured in multi-levels, such as link level, network level and application level:

- **Application layer**: IP phone voice traffic, percent of call completed, call setup time etc.
- **Transport layer**: end-to-end TCP connection packet loss, UDP packet transmission delay, delay jitter;
- **Network layer**: router IP packet throughput, point-to-point or end-to-end connectivity, IP packet transmission delay, delay jitter, packet loss, loss rate;
- **Data link layer**: frame throughput, frame transmission delay, frame loss rate.

The attack effectiveness should be evaluated according to the extent of the damage which the attack made. Different groups of people care about different layer metrics. Generally, the users care mostly about the metrics on transport layer and application layer. Different network services and applications relate to different metrics. The performance metrics listed above all make certain impacts on network services and applications. If we want to evaluate attack impacts on special users, we should first define the user requirements, then collect data from the emulation environment, finally calculate and draw the result.

This paper suggests the following as basic metrics: delay, delay jitter, loss, bandwidth, throughput etc. In order to evaluate the impacts on the network users, some metrics should be introduced, such as server connection time, server connection completion rate, server concurrency connection number, server response time etc.

Three indices are introduced: total service performance index, total transmission performance index, penetration index. Total service performance index represents the performance change value of all the services in the network. Penetration index is the ratio of total number of machines infected by worm or virus to the total number of all machines on the network.

### 4.2 Experiment Evaluation System

Based on the emulation environment, an evaluation system is implemented; its architecture is introduced as follows.

The evaluation system comprises the following modules:

- **Attack description module**: describes attack schemes including attack steps, interval between the steps, targets of each attack;
- **Target network description module**: describes information of the emulated network including its topology, node types, distribution of the servers, quality requirements of the users. The creation of the topology of very large network need assistant tool.
- **Defense policy description module**: describes the active and reactive policies, the former is distributed before the attack, the later is distributed during the attack.
- **Evaluation and display module**: calculates the value of each metric and display the evaluation result.
- **Network configuration module**: configures the test network to emulate the experiment network.
- **Traffic creation module**: creates background traffic flow and attack flow.
- **Data collection module**: collect network performance data related to each metric and store in database.
5 Conclusion
This paper introduces an implementation of an emulation environment for large scale network security experiments, presents the method to measure the impacts of network attack and defense. In the future, we will make use of the environment to study the efficiency of different network defense mechanisms under the large scale network attack, such as worm or DDoS.

References:
[10] Jin Li, xiaohui Kuang, Hong Tang; Research on Creation of Large Scale Network Topology; Computer Engineering and Science; 2009.2