Modeling Framework for Developing and Testing Network Security Techniques against DDoS Attacks

Konstantin Borisenko[#1], Ivan Kholod[#2] and Andrey Shorov[#3],
[#]Faculty of Computer Science and Technology,
Saint Petersburg Electrotechnical University (LETI),
Professor Popov str. 5, St.Petersburg, 197376, Russia
[1]borisenkoforleti@mail.ru, [2]iiholod@mail.ru, [3]ashxz@mail.ru

***Abstract* — In the paper we introduce a hybrid system for simulating DDoS attacks and computer network protection techniques. The developed system makes it possible to create various network topologies, perform experiments with DDoS attack simulation, develop new protection methods and test the existing ones. The suggested system not only allows us to design virtual networks, but also makes it possible to connect real network nodes for improving the accuracy of the experiments.**

Massive DDoS attacks often affect websites of governments and government bodies of various countries, websites of leading IT-corporations. The world leaders in the area of information security consider DDoS detection and DDoS resistance as a primary task in their research and developments.

To study DDoS attacks and to develop new defense mechanisms researchers mostly use simulation methods. However, DDoS attack simulation often causes problems of the accuracy of the attack simulation on application level. Furthermore, depending on the software installed on a server this server can function in a different way. Also multi-level network construction in reality often requires dozens of time and resources

Thus, we suggest to integrate simulation and testbed methods. Using simulation, we create attacking network and connect it to the real server. A virtual network is very similar to a real one. In case of using DDoS attack traffic generators defense can be placed only on attacked server. Our approach allows to develop defense mechanisms, which can be placed anywhere in the attacking network. Furthermore protection mechanisms can be architecture-dependent, which is important for performing experiments in a way very close to a real network. An important advantage is the possibility of connecting real nodes to a virtual network, which will improve the accuracy of our experiments and allow us to test different settings and types of servers.

System development was performed using the discrete-event simulation system OMNeT++. The INET library was used for making network settings and packet switching. The ReaSE library was completed for creating topology settings. The system has special network interface, which allows to redirect traffic from the simulated network to real network and vice versa.

The verification of the system was successfully made. Comparison was made between system and networks constructed using Planetlab.

Authors have made series of experiments with different attack scenarios: SYN-Flooding attack, HTTP attack. Experiments were made without any defense methods and with filtering methods (Ingress, Egress). The network topology for conducting experiments consisted of 7 routers, 204 clients and 1 real server. The delays between network nodes are equal to 1 microsecond.

Now consider the analysis of scenario experiments for SYN Flooding using the Egress Filtering method and without using protection techniques. During SYN-Flooding attack, 20% of the total number of network clients (40 computers) participated in the attack. SYN cookies were switched off on the server for a successful SYN Flooding attack. At the beginning of the attack, at the 10th second, the number of server applications is increasing because more and more virtual clients are starting to take part in an attack. Till the 15th second the server is coping with the task of processing all requests and then the TCP stack is overflowed and the server is unable to process the increasing flow of applications. In the period from the 15th second till the 57th second the server provided no response to all arriving SYN-packets.

A series of experiments has been performed with the use of a filter with 2, 3, or 4 routers in a virtual network. At the same time the clients attacking the server continuously were located in the local network of a router that did not use Egress Filtering. With the increase of the number of filters the power of a server attack decreased.

The developed system can be used for studying DDoS-attacks and the protection techniques against them. Network administrators can quickly and precisely reproduce a network they are servicing, execute load testing, estimate server stableness to attacks, network capacity, and the quality of protection mechanism performance.

The paper has been prepared within the scope of the state project ”Organization of scientific research” of the main part of the state plan of the Board of Education of Russia as well as project part of the state plan of the Board of Education of Russia (task # 2.136.2014/K).