Simulation Environment for Investigation of Cooperative Distributed Attacks and Defense

Igor Kotenko, Alexander Ulanov
Computer Security Research Group, Saint-Petersburg Institute for Informatics and Automation (SPIIRAS)
{ivkote, ulanov}@iias.sbp.su

Nowadays we are witnesses of increasing number of distributed attacks on global computer networks. Much of them are aimed on the distributed denial of service (DDoS) of critical information resources. These attacks are realized due to joint efforts of many malicious software components that are deployed on compromised Internet hosts. The general approach to DDoS defense includes mechanisms of *attack prevention, detection, tracing the malicious traffic sources and attack counteraction*. Because of gravity and complexity of DDoS the design of effective defense is a complicated scientific and technical problem. It is sufficiently hard to examine and evaluate the effectiveness and efficiency of defense mechanisms in practice. However these mechanisms might be simulated with the necessary fidelity and thoroughly analyzed.

We propose *the approach and developed software environment intended for simulation and investigation of distributed cooperative attacks and defense systems*. The main attention is given to the *integrated agent-oriented and packet-level approach to the simulation of security processes in the Internet*. It can provide the acceptable fidelity and scalability of implementing computer attacks and defenses. The special attention is given to *cooperative distributed defense mechanisms that are based on the deployment of defense components in various Internet subnets*. That is intended for simulating the interactions of various ISPs security elements.

The cybernetic counteraction is supposed to be represented as the interaction of the teams of malefactors and the teams of security agents. The agent teams can be opposed to each other or cooperate. Attack agents are subdivided at least into two classes: “daemons” and “masters”. To simulate distributed cooperative defense, the security agents belong to the following classes: information processing (“samplers”); attack detection (“detectors”); filtering and balancing (“filters”); traceback and investigation (“investigators”).

The proposed simulation approach presumes the following components of the simulation environment developed: (1) Discrete-event Simulation Framework (implemented on OMNeT++), (2) Internet Simulation Framework (using OMNeT++ INET Framework), (3) Attack and Defense Framework (Library of attacks and defenses), (4) Multi-Agent Simulation Framework. Attack and Defense Framework includes attack and defense modules and the modules that expand the hosts of INET Framework: filter table and packet analyzer.

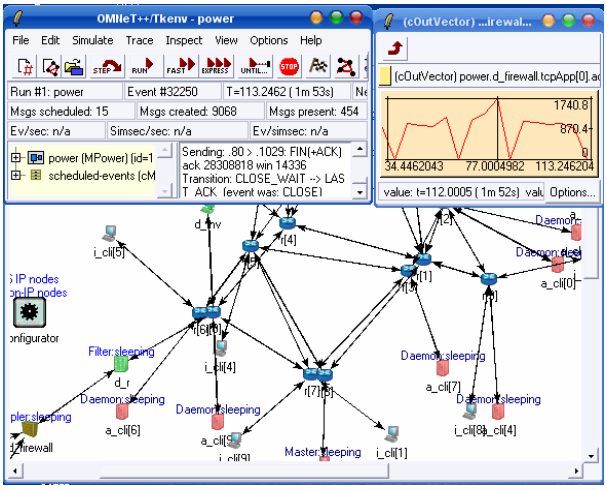

Fig. 1. User interface of simulation environment

The basic window *the simulation environment* developed (Fig.1) shows a simulated computer network (hosts and channels). Hosts can fulfill different functionality depending on chosen parameters and internal modules. Internal modules are responsible for functioning of protocols and applications at various levels of OSI model. Applications (including agents) are established on hosts. The window for simulation management allows looking through and changing simulation parameters. It is important that it is possible to see the events which are valuable for understanding attack and defense on time scale. Corresponding windows show the current status of agent teams. It is possible to open windows which characterize functioning of particular hosts, protocols, agents, defense methods, see contents of the packets, etc. The following *parameters are used in the environment to define the attack*: victim type; type of attack; attack rate dynamics; impact on a victim; persistence of agent set; possibility of exposure; source address validity; degree of automation. *Defense mechanisms are determined in the environment* by the following parameters: deployment location; mechanism of component cooperation; covered defense stages; attack detection technique; attack source detection technique; attack prevention and counteraction technique; model data gathering technique; determination of deviation from model data technique.

The environment allows to analyze various classes of attack and defense mechanisms. The abstract and poster is devoted to the investigation of *the models of cooperation between distributed defense teams*: (1) *filter-level cooperation*: the team whose network is under attack can apply filtering rules on the filters of other teams; (2) *sampler-level cooperation*: the team whose network is under attack can get the traffic information from the samplers of other teams; (3) *“poor” cooperation*: the teams can get the traffic information from the samplers of some other teams and apply filtering rules on the filters of some other teams (each team knows a subset of other teams depending on the cooperation degree); (4) *“full” cooperation*: the team whose network is under attack can get the traffic information from all samplers of other teams and apply filtering rules on all filters of other teams. Such cooperation schemas are used in the cooperative DDoS defense methods: COSSACK, Perimeter-based DDoS defense, DefCOM, Gateway-based, ACC pushback, MbSQD, SOS, tIP router architecture, etc. The cooperation schemas can be investigated and compared using the analysis of various parameters: (1) incoming traffic before and after filters; (2) normal and attack traffic rate from the whole traffic coming into defended network; (3) false positives and false negatives rates, (4) detection and reaction times, etc.

In the *future research* we are planning to expand the attacks and defenses library, elaborate particular components functionalities. The important constituent of future research is numerous experiments to investigate various attacks, defense mechanisms (attack prevention, detection, tracing the attack sources and counteraction) and optimal defense combinations.