Software Environment for Simulation and Evaluation of a Security Operation Center

Julien Bourgeois[1], Abdoul Karim Ganame[1], Igor Kotenko[2] and Alexander Ulanov[2]

[1]LIFC, Universite de Franche Comte, 4, place Tharradin, 25211 Montbeliard, France
{ganame, bourgeois}@lifc.univ-fcomte.fr
[2]St. Petersburg Institute for Informatics and Automation (SPIIRAS), 39, 14 Linia, St.Petersburg, 199178, Russia {ivkote, ulanov}@comsec.spb.ru

Abstract. It is somewhat problematic to evaluate the performance of security systems in the Internet due to complexity of these systems and the Internet itself. Therefore, modeling and simulation are becoming more and more important in optimizing the behavior of security systems, including security components intended for protecting various distributed geographic information systems (GIS). This paper presents an approach and software simulation environment for comprehensive investigation of the Security Operation Center (SOCBox) system which is in essence an intrusion detection "metasystem". SOCBox collects data from a wide range of sources (intrusion detection systems (IDS), firewalls, routers, workstations, etc.) and therefore has a global view on the network. The simulation environment has been developed formerly for Distributed Denial of Service (DDoS) attacks and defense simulation. This tool is characterized by agent-oriented approach, the packet-based imitation of network security processes and the open library of different attacks and defense mechanisms. We consider the SOCBox structure, the simulation environment architecture, the SOCBox models in the simulation environment and peculiarities of SOCBox simulation.

Keywords: Security modeling and simulation, infrastructure security, intrusion detection, DDoS.

1 Introduction

The design of reliable defense system for complex and distributed computer systems including geographic information systems (GIS) is a complicated problem. Such a system has to include the mechanisms of prevention, detection, unauthorized access (or attack) source tracing and

malicious actions counteraction. It is obvious that the more useful data such system has the more effective it is. This especially concerns the detection mechanisms. The large-scaled system of distributed sensors gives the following opportunity: one can represent the more complete picture of current state and detect an attack in a long distance from the attack goal and then take some countermeasures.

Such approach is suggested in the Security Operation Center (SOCBox) [1-3], that could be called intrusion detection "metasystem". SOCBox collects data from a wide range of sources (intrusion detection systems (IDS), firewalls, routers, workstations, etc.) and therefore has a global view on the network. The SOCBox analysis engine can correlate all messages generated by all network components and find patterns of intrusion. However, the implementation of SOCBox is a complicated problem.

An advanced hardware test bed is needed to debug, test and evaluate the effectiveness of SOCBox. It can be a laborious independent network or the Internet fragment. A.K.Ganame et al. [3] describe different experiments conducted with SOCBox. They presented the intrusion detection capabilities and performance of SOCBox in comparison with Snort IDS. Experiments were carried out in a real Internet service provider (ISP) network for over a week. This ISP manages more than 50000 subscribers. But, it is hard (or impossible) to implement a set of periodical global experiments in the networks of real ISP (e.g. when applying a new detection technique). Furthermore, the important conditions for a scientific experiment are repetition and controllability. These conditions are hard to fulfill on a hardware test bed, but they can be provided in a simulation environment.

The choice of simulation type depends on scalability and fidelity requirements. The variety of simulation tools spreads from hardware test beds to analytical models. Hardware test beds, e.g., EmuLab [4, 5], offer the real network incorporating hundreds or even thousands of hosts. One can simulate up to dozens of thousands of hosts using the network emulation, e.g., NetLab [4, 5], ModelNet [4, 6]. Both hardware test beds as well as emulation systems are by definition executed in real-time. Next alternative is a packet-level simulation: OMNeT++ INET Framework [7, 8, 9], NS-2, SSFNet, J-Sim INET Framework [7, 8]. Packet-level simulation exhibits one of the best tradeoffs between scalability and fidelity. Mixed simulation is a combination of packet-level simulation and analytical models [4, 10]. The latter is the most scalable but the most simplified simulation approach [4, 11].

Test beds and SOCBox itself can be simulated with the given scalability and fidelity (accounting for certain assumptions). Multi-agent simulation