Cloud-based Security Research Testbed: A DDoS Use Case

Tomáš Jirsík, Martin Husák, Pavel Čeleda
Institute of Computer Science, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
{*jirsik* | *husakm* | *celeda*}@ics.muni.cz

Zdenek Eichler
Faculty of Informatics, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
zdenek.eichler@mail.muni.cz

***Abstract*—In this paper we present a cloud-based research testbed designed to aid network security managers. The testbed enables operators to emulate various network topologies, services, and to analyze attacks threatening these systems. A possibility to test results of network management measures is desired, since testing these measures in a production environment is always not possible. We demonstrate a testbed use case, which aids to scrutinize network behavior under attack. Our use case is based on a large DDoS attack which targeted network infrastructure and web servers in Czech Republic in March, 2013.**

I. Introduction

Introducing new services and network management measures represents a difficult task, since it is not easy to make this change without proper testing. Testing in a real environment, however, is not a suitable solution, as we need to maintain already running services and network configuration. A network simulation is a possible solution to this problem. Since there are various types of network topologies, services, and use-cases to test, a simulation testbed should be able to emulate the whole infrastructure, and capture the relevant network properties. Moreover, it should gain full control over all emulated activities. In our work, we focus on network security simulation and management, as cyber attacks have become ubiquitous.

Cybernetic Proving Ground[1] (CPG) is a testbed designed especially for a network security management and simulation [1]. It is a scalable, universal solution which is designed for deployment in clouds managed by OpenNebula[2]. CPG provides an assisted generic network topologies emulation and an isolated virtual environments facilitation, which is used for controlled attack analysis. Moreover, it can serve as a cyber security training tool. The outputs can be used for research into new detection methods and for network management.

The purpose of this paper is to demonstrate an example of a network attack simulation in CPG. The demonstration focuses on a facilitation of network topology emulation, retaining main attack characteristics and real-world aspects of the simulation. We reproduced the Distributed Denial of Service (DDoS) attack against the internet infrastructure of the Czech Republic that took place in March, 2013 [2]. To reach our goal we had to specify a scenario based on the observed attacks, set up the testbed and run the experiment described in the scenario.

II. Testbed Description

We need to create a scenario (a set of descriptive documents for both users and CPG itself) to run the security experiment. The scenario includes several configuration parts, namely network topology, logical topology, nodes setup, measurement infrastructure setup, executive instructions, and the textual description for users.

CPG automatically creates a sandbox for attack simulation based on the description in the scenario. Virtual machines are configured according to nodes setup, where additional software and settings can be specified. The network topology describes network links and assignments of nodes into subnets. Networking devices do not need to be specified unless there are some specific requirements on them. CPG completes the network topology with networking devices and simulates the background network traffic if needed. The measurement infrastructure consists of monitoring probes (NetFlow, IPFIX) located at the networking nodes to provide a traffic overview. Logical topology assigns roles to the nodes and subnets, e.g., the role of an attacker, victim, etc. Assignment is fairly intuitive and is used mainly as a description in the visualization. Figure 2 shows the network and logical topology visualization. When the testbed is ready, the scenario contains instructions how to execute an experiment. These instructions typically contain time from start of the experiment and command executed by CPG at that time. Additional information provides a description of what happens and what the user should be aware of. Table I provides an example containing the outline proposed in our DDoS scenario.

Time	Action	Scenario state
0:00	–	The beginning of the scenario
01:00	Configuration of attacking machines	Common network traffic
02:00	The attacker attacks from two machines	Start of the attack
03:00	The attacker adds another machines	Increasing intensity of attack
04:00	The attacker adds another machines	Maximum attack intensity
06:40	The attacker stops the attack	Common network traffic
09:00	–	The end of scenario

TABLE I: DDoS use-case outline

The experiment results are presented via a visualization in CPG user interface, see Figure 1. The interface is web-based and is implemented using Liferay Portal. Multiple portlets form the user's screen, and each portlet is responsible for a particular visualization. Portlets can be linked together and create so-called nested portlets (the blue portlet no. ④ on Figure 1).

[1] http://www.muni.cz/ics/kypo

[2] http://opennebula.org/

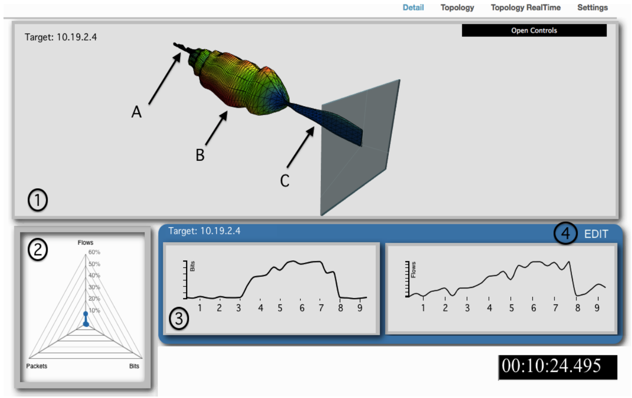

Fig. 1: Security Research Testbed: User Interface

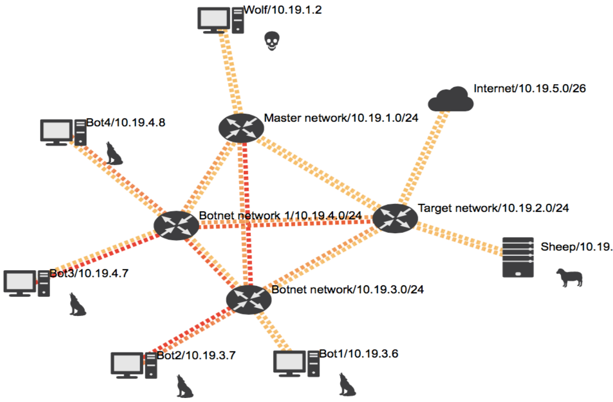
Wolf/10.19.1.2
Internet/10.19.5.0/26
Bot4/10.19.4.8
Master network/10.19.1.0/24
Botnet network 1/10.19.4.0/24
Target network/10.19.2.0/24
Sheep/10.19.2.4
Bot3/10.19.4.7
Botnet network/10.19.3.0/24
Bot2/10.19.3.7
Bot1/10.19.3.6

Fig. 2: Network Topology Visualization

Visualizations in CPG follow the Shneiderman's visualization mantra: *Overview first, zoom and filter, then details-on-demand*. The general overview (Figure 1, portlet ①) is provided by a 3D sequenced time-ordered radar chart (further referred to as overview chart). The graph visualizes multiple variables in time. The surface of the solid figure is a result of the composition of ordinary radar charts along a time scale. This visualization provides a general overview and helps to identify areas (variable and time) worth further investigation. Such areas are usually peaks and/or valleys on the surface, which are highlighted by color. The solid figure is semitransparent, thus it is possible to see such a highlighted areas even on the far side. The graph supports common interactions such as rotation around the time axis, move and zoom.

The above mentioned overview visualization is accompanied by an ordinary radar chart (Figure 1, portlet ②). The radar chart and the overview chart are interdependent. The main purpose of the radar chart is to present a selected point in time on the overview chart in appropriate detail – without perspective and overlap. The second purpose is to allow the manipulation of variables, particularly adding, removing and changing order of variables. This interaction affects the overview chart. The testbed visualization supports ordinary line charts (Figure 1, portlet ③), which display one variable in time. The charts are not all displayed by default, since they can be raised by the user as *details-on-demand*.

An example of network topology visualization is presented in Figure 2. This visualization operates in two modes: *(i)* network topology only, and *(ii)* topology with data flow. The first mode displays routers, links, computers and servers. Every node in the topology can be accompanied by a small sign, which represents the role of the node in the running scenario. The second mode is extended by the visualization of data flow on particular links. The traffic displays upload, and download separately. We use colour and movement to indicate traffic characteristics.

III. DDoS Attack Demonstration

We present a proof-of-concept scenario that CPG is able to simulate, measure, and visualize user specified scenarios. Our scenario is based on the real DDoS TCP SYN flood attacks, therefore we had the basic idea what to simulate, observe, and how to execute the attack. Network topology had to be reduced in comparison to the original attack as it is not possible to emulate the whole Internet. We have focused on the victim and the botnet under the attacker's control. The botnet is split into two subnets different from botmaster's subnet to represent multiple attack sources. The botmaster uses IRC protocol and *irssi*[3] tool to send commands to the attacking machines equipped with LOIC[4], a tool for performing DDoS attacks. The order of actions is defined in Table I.

On Figure 1, portlet ①, there is a visualization of three variables, packets per second, flows per second and bits per second, measured on the victim's downlink. Particularly, the rear thin part of the solid figure (A) presents common traffic before attack, the wide red part of the solid figure (B) represents traffic during attack, and the thin part in front of the camera (C) refers to common network traffic after the attack.

IV. Conclusion

We have presented a cloud-based research testbed CPG for simulation and visualization of network attacks. We propose a use case which focuses on DDoS attacks against network infrastructure. We are able to simulate given network, connected devices, and perform various types of attacks to examine vulnerabilities and discover potential pitfalls of a simulated system. Since the proposed testbed architecture has been described very briefly, we recommend reading the full paper [1] that provides details of the current testbed's implementation.

Acknowledgements

This work has been supported by the project "Cybernetic Proving Ground" (VG20132015103) funded by the Ministry of the Interior of the Czech Republic.

References

[1] D. Kouřil, T. Rebok, T. Jirsík, J. Čegan, M. Drašar, M. Vizváry, and J. Vykopal, "Cloud-based Testbed for Simulation of Cyber Attacks," in *Proceedings of the 2014 IEEE Network Operations and Management Symposium, NOMS 2014*, 2014, to appear.

[2] M. Husák and M. Vizváry, "POSTER: Reflected Attacks Abusing Honeypots," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013, pp. 1449–1452. [Online]. Available: http://doi.acm.org/10.1145/2508859.2512523

[3] http://irssi.org/

[4] http://hivemindloic.sourceforge.net/wiki/Main_Page