KYPO: A Tool for Collaborative Study of Cyberattacks in Safe Cloud Environment

Zdenek Eichler, Radek Ošlejšek, Dalibor Toth
Masaryk University,
Faculty of Informatics,
602 00, Brno, Czech Republic,
xeichler|oslejsek|xtoth2@fi.muni.cz

November 7, 2014

1 Introduction

This paper introduces the KYPO – a cloud-based virtual environment faithfully simulating real networks and enabling users to study cyber attacks as well as to train users in isolated and controlled environment. The paper focuses on the user environment and visualizations, providing views and interactions improving the understanding of processes emerged during experiments.

Cyber attacks become more and more sophisticated and frequent. Internet users face cyber attacks on everyday basis in the form of phishing e-mails, infected attachments or intrusion attempts. A viable option to study attacks and to train users is the simulation of cyber threats in isolated, controlled, scalable and flexible cloud-based environment enabling participants to experience and replay various scenarios in order to understand the impact of the attack on users and devices involved in the infrastructure.

2 Training Programs

Our main focus is the security training programs, where the main advantage of our approach is the authenticity. Instead of describing the key principles of cyber attacks theoretically, we rather let students to try to perform a real cyber attacks or let them e.g. to become victims of a phishing attack, all in safe virtual environment. The system provides easy to use user environment, where a lector is able to easily define a huge amount of attributes which will be measured in the network during cyber experiments and then presented to students in realtime or after experiment.

Since our tool is designed for students, sandboxes must be easy remotely accessible. Accessibility was ensured by employing the concept of Web applications with minimal requirements on web browsers. As the most fitting approach

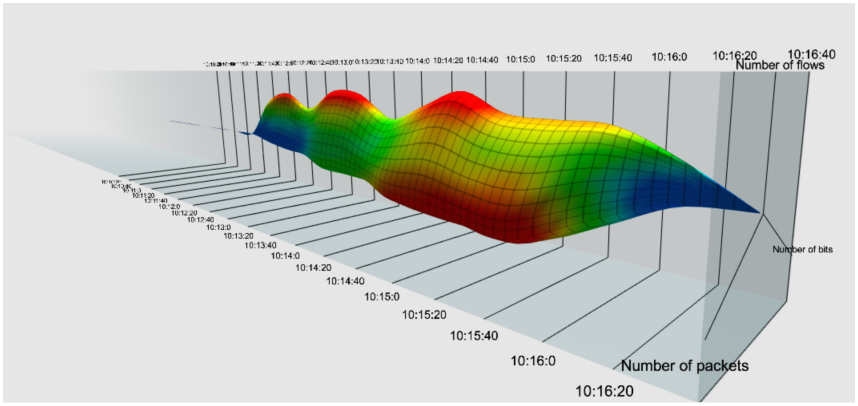

Figure 1: 3D sequences radar chart

was chosen an unifying environment of enterprise portal according to its component based architecture.

Security scenarios can significantly differ in the way how the users collaborate. For example, during a DDoS attack demonstration, all users can share a single sandbox with same data, where every user has its own visualizations enabling student to replay the scenario and examine the impacts of the DDoS on network. On the contrary, imagine a different scenario, where the users should try to compromise some computer, then every participant should have its own private sandbox, in order to handle the attack on its own. Also mixed approach is supported, where few students share particular sandbox and every student has it's own role in the scenario, operating different computers (e.g. one student is attacker and other student is defender of system under attack). Another case of mixed approach is sharing of one computer in a sandbox by multiple users.

The system provides various visualizations developed specially for educational purposes, where tutor defines which visualizations should be accessible, depending on particular scenario. All visualizations are interactive and follow the Shneiderman's visualization mantra: *Overview first, zoom and filter, then details-on-demand*. One of provided visualization developed for education is a 3D sequenced radar chart, which visualizes multiple variables in time. The visualization is implemented in WebGL in order to deliver accelerated visualization in Web environment. The surface of the solid figure (Figure 1) is a result of the composition of ordinary radar charts along a time scale.

A network topology visualization is presented in Figure 2. Subjects of visualization are 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 (e.g. attacker or victim). Supported is also visualization of data flow on particular links. This visualization also enables students to open e.g. a VNC (remote access) connection to the computer in sandbox and share

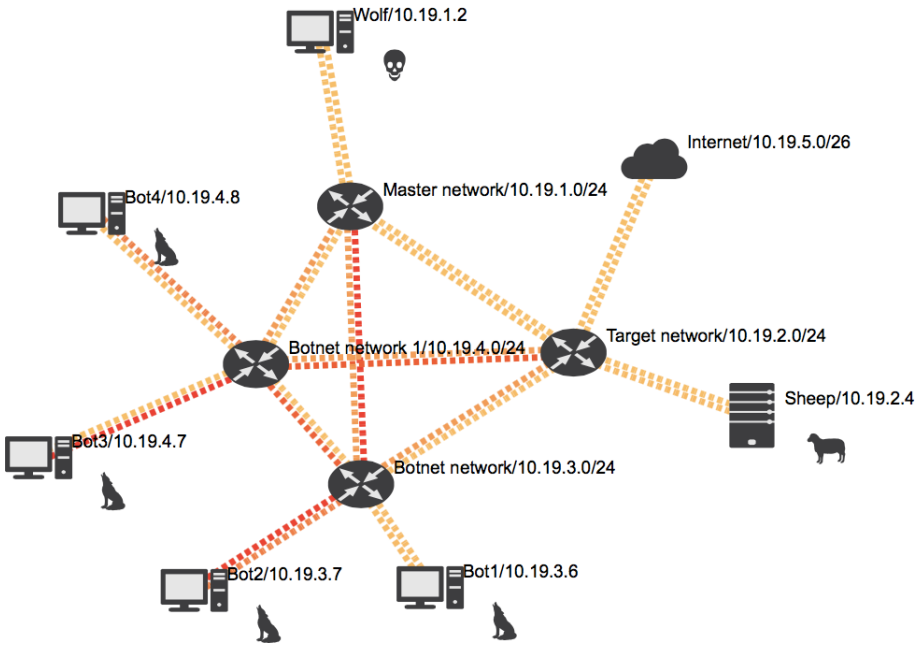

Figure 2: Visualization of network topology

the screen of remote computer with other students or lecturer.

3 Evaluation

Our system was already used on workshop focussed on cyber security. Also, a pilot testing on academic course with 10 students was conducted with promising results: at the beginning, subjects were asked to evaluate their knowledge about hacking (infiltration to the system) and DDoS attack. Then, we provided our system to the users, where every three or two students shared a sandbox and collaborated in order to complete the task. Instructions were provided to users in a form of a level based game, which leads the students through the scenario. The goal was to compromise target system and then run DDoS attack from the compromised system. Students were able to collaborate by sharing the screen of the attacker's computer through our web portal and view various visualizations described above. When all subjects finished the game, the subjects were asked to the same questions again (same as before the course). Particularly, the subjects evaluated their knowledge of DDoS and hacking on five-point Lickert scale (1 for I do not know nothing about that, 5 for I'm able to perform such attack). The difference between before and after the course showed increased knowledge in all subjects, where MODE of the increment was 1 on both questions. Subjects also evaluated the course itself, on five-point Lickert scale (1 for Strongly Disagree,

5 for Strongly Agree) on following statements:

- I enjoyed the course. (MODE = 4)
- I learned something new. (MODE = 4)
- I enjoyed the ability to perform real attack in safe and collaborative environment. (MODE = 5)