KYPO: A TOOL FOR COLLABORATIVE STUDY OF CYBERATTACKS IN SAFE CLOUD ENVIRONMENT

HCII'2015

Tuesday 7th July, 2015

Radek Ošlejšek

Zdenek Eichler, Dalibor Toth

oslejsek@fi.muni.cz

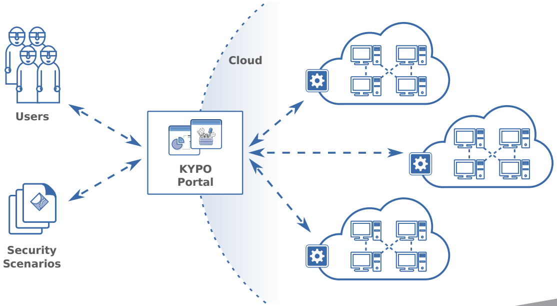
KYPO

BY CSIRT-MU

KYPO Overview and Architecture

KYPO Provides:

- **Isolated environment** for building virtual computer networks, running experiments and analysing results **safely**.
- **Analytic tools** to study various cyber attacks (forensic analysis).
- Cyber security **training programs**, e.g. “capture the flag” games.



KYPO Portal: Challenge

Problem: Diversity of users and their objectives

- **Diversity of users:** Security expert vs. students.
- **Diversity of objectives:** Finding hidden data coherence vs. learning how some attack behaves.
- **Diversity of workflows (security scenarios):** Forensic analysis vs. "capture the flag" game vs. concrete attack learning, etc.

Requirements:

- Intuitive web-based access without installing anything on client side.
- Shneiderman's visualization mantra (overview first, zoom and filter, then details-on demand).
- Variable GUI (pre-configured layouts, configurable interactions and visualizations, etc.).
- Variable collaboration modes.

KYPO Portal: Technologies

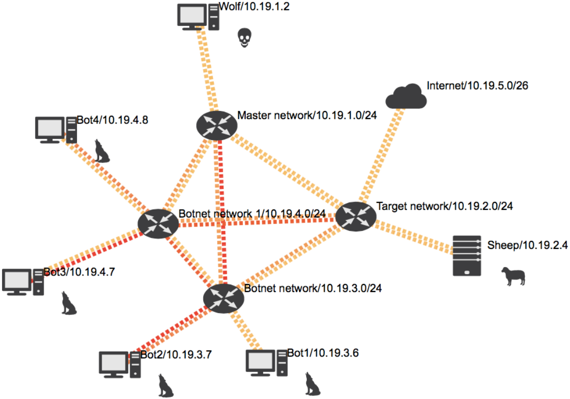
Web Portal

- Complies JSR standards for web portals.
- **LifeRay:** Popular framework for corporate webs.
- Portlets: “independent” windows (text, table, graph, . . .) implemented in various languages (Java, Javascript, WebGL, . . .).
- Pages composed of portlets + inter-portlet communications.

LifeRay = platform for building security-scenario-related GUI

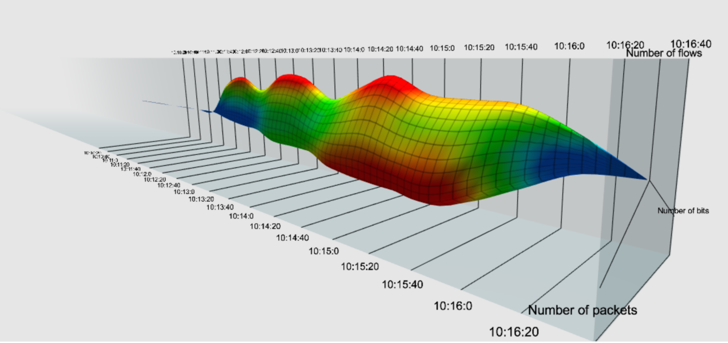
Visualization Portlets: Network topology

VNC connection, physical/logical roles of nodes, links utilization, . . .


Wolf/10.19.1.2
Internet/10.19.5.0/26
Master network/10.19.1.0/24
Bot4/10.19.4.8
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

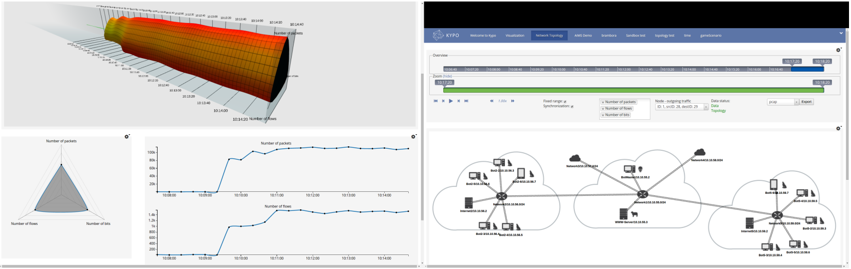
Visualization Portlets: 3D Chart

- Special visualizations for educational purposes.
- WebGL, fully interactive, supports gesture-based inetraction



Workbenches (predefined layouts)

- Predefined pages (tabs of web browsers) for user roles.
- Timeline portlet synchronizing other portlets.

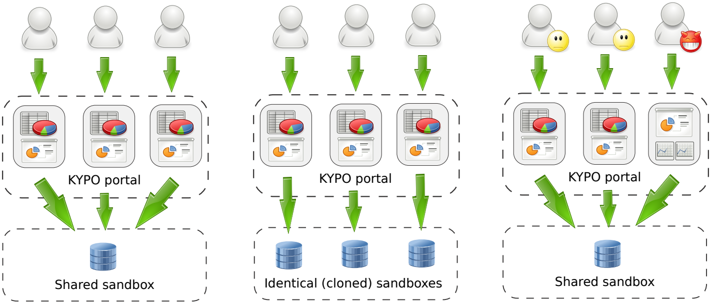


Fixed range: ☑
Synchronization: ☑
Node - outgoing traffic: ID: 1, srcID: 28, destID: 29
Data status: Data Topology
pcap

KYPO portal (dual display mode)

Collaboration Modes

- Individual views on shared data.
- Individual sandboxes.
- Role-based collaboration.



Evaluation: Online demos and exercises

- Online tutorial at AIMS 2014: 20 participants, DDoS attack demonstration followed by hands-on training of compromising and abusing a server, 40 virtual machines in 6 sub-networks.
- Online "capture the flag" game at TF/CSIRT Technical Colloquium in 2015, 25 participants.
- Cyber Czech 2015: In preparation, with Czech National Security Authority, about 20 players (cyber security experts) in 6 teams will defend their network of 15 servers and desktops against known vulnerabilites, misconfigurations and attacks.

Formal Evaluation

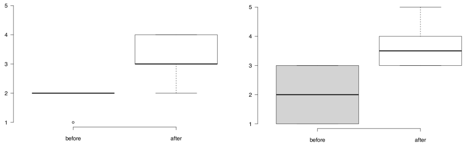
Evaluation process:

- 10 university students of the Faculty of Informatics MU.
- Subjects were asked to evaluate their knowledge about hacking and DDoS attacks.
- Subjects played level based game which led the students through the scenario. The goal was to compromise target server and then run DDoS attack.
- Subjects were asked to evaluate their knowledge again.

Formal Evaluation (cont.)

Results: Knowledge about hacking and DDoS

- 1 = I don't know nothing about that
- 5 = I'm able to perform an attack



Results: Evaluation of the course itself

- 1 = Strongly disagree; 5 = Strongly agree
- Most often appeared values:
  - I enjoyed the ability to perform real attack: 5
  - I learned something new: 4
  - I enjoyed the course: 4

Conclusion and Future Work

- KYPO Lab: 4K projector, multitouch wall, videoconference, . . .
- Techniques for remote collaboration.
- Complete support for visual analytics workflow.
- KYPO as a service.

QUESTIONS AND ANSWERS

www.kypo.cz

@csirtmu

Radek Ošlejšek

oslejsek@fi.muni.cz