Cybernetic Proving Ground

Cyber Exercise & Research Platform

Jakub Čegan et al.

cegan@ics.muni.cz

Institute of Computer Science, Masaryk University

Recent activities & projects

Current projects

- Czech CyberCrime Centre of Excellence
- *Cybernetic Proving Ground*
- And more ...

Our activities

- CSIRT-MU: Security supervision, trainings & education
- Cyber Europe 2014: European cyber crisis cooperation exercises

Cybernetic Proving Ground (CPG)

Features

- Simulation of networks, systems, services and applications.
- Monitoring of network behaviour, detection and mitigation of anomalies and attacks.
- Environment for investigation of cyber threats.

Cloud

- Enables computing of resource-intensive tasks.
- Remote secure access of users around the world.
- Enables providing CPG to third parties as a service.

Project Technologies

Traffic monitoring

- Implemented by IPFIX infrastructure.

Cloud & Networking

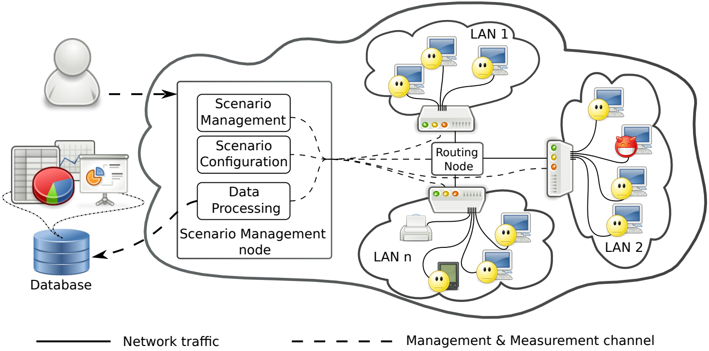
- Currently using OpenNebula a cloud middleware.
- Resources are provided by CERIT-SC project.
- Made possible by VLANs and Open vSwitch.

MetaCentrum

SC cerit scientific cloud

OpenNebula.org

CPG Architecture



Benefits for Users

Easier investigation of cyber threats and attack

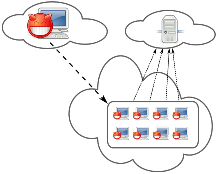
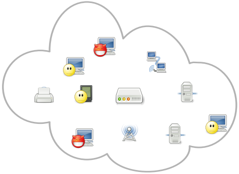
- Automated gathering and processing of data generated during security scenarios.
- Training of a penetration testing as well as a defense.
- Visualization of significant aspects of the scenarios.

Traffic analysis and forensics

- Acquisition, storage, and analysis of network statistics.
- Analysis of malware at infected host and in a network.
- Validation of processes of an incident response.

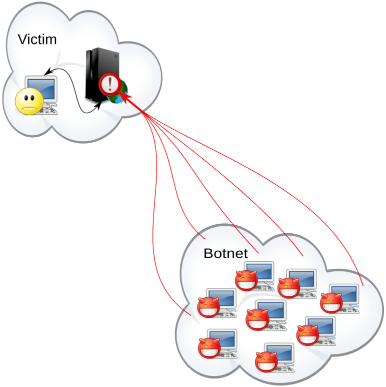
Project Roadmap

- Started in April 2013.
- Finishing in September 2015.
- Focused on topic each year.

2013 (Year One)	2014 (Year Two)	2015 (Year Three)
		
Distributed Denial of Service attack	Critical Inrastructure	Infrastructure as a Service

Pilot Security Scenario (2013)

DDoS attacks against Czech Rep. in March 2013



Critical Infrastructure (2014)

Critical infrastructure of the Internet – DNS

- Research & developement.
- Testing attack and defence tools.

Forensic analysis

- Observation of infected files and applications
- Monitoring of captured artifacts.
- Scenario repeatability.

Penetration testing

- Testing of detection tools.
- Training and education of penetration testers.

Final Security Scenario (2015)

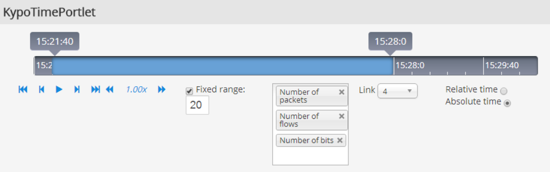
Training of security teams

- Commented analysis of scenarios.
- Cyber war game scenario in CPG.

CPG as a service

- Remote access to CPG to third parties.
- New complex scenarios *on demand*.

WUI – CPG Main Page



KypoTimePortlet

☑ Fixed range: 20

Number of packets ×

Number of flows ×

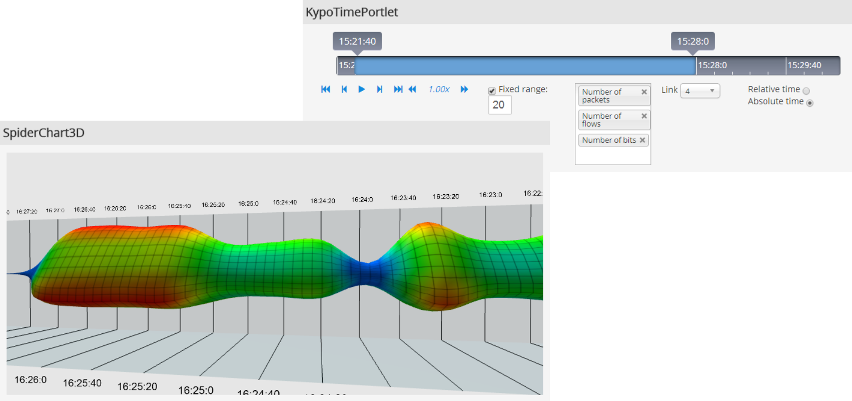
Number of bits ×

Link 4

Relative time ○

Absolute time ●

WUI – CPG Main Page



KypoTimePortlet

15:21:40 — 15:28:0

☑ Fixed range: 20

Number of packets ×

Number of flows ×

Number of bits ×

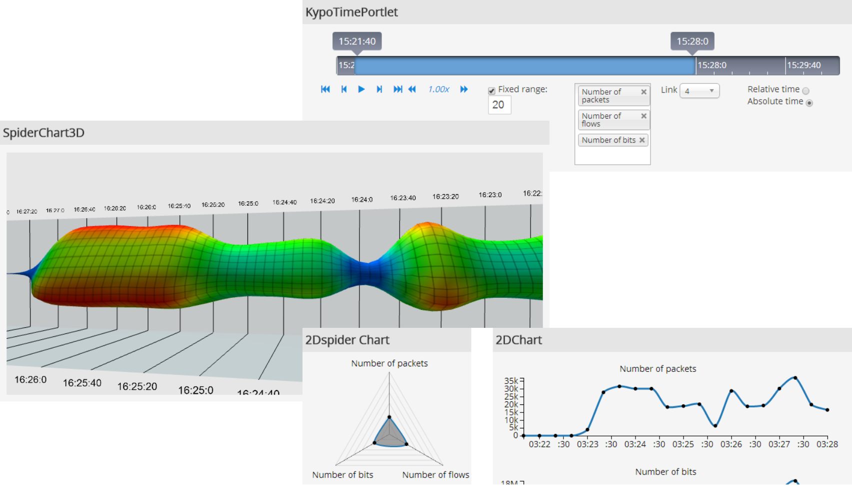
Link 4

Relative time ○

Absolute time ●

SpiderChart3D

WUI – CPG Main Page



KypoTimePortlet

☑ Fixed range: 20

Link 4

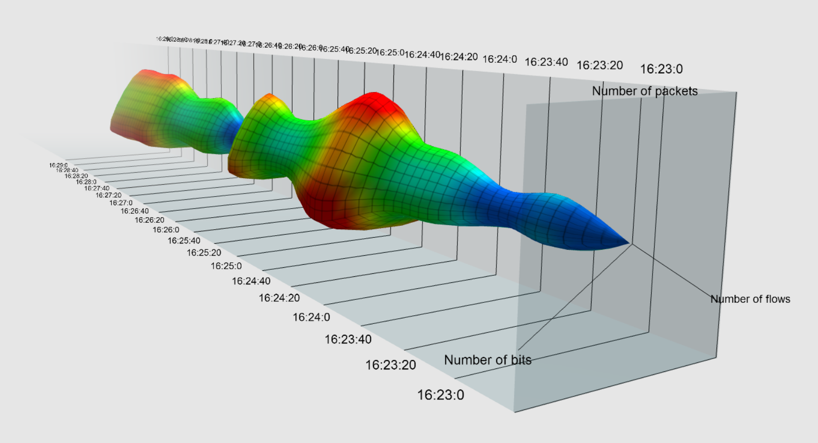
Relative time ○
Absolute time ●

SpiderChart3D

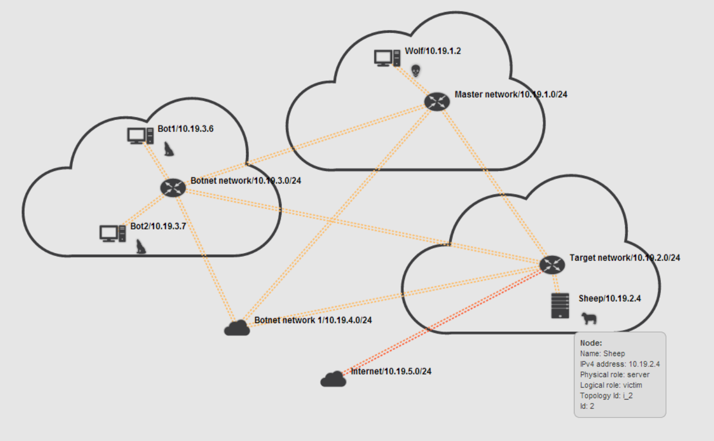
2Dspider Chart

2DChart

WUI – Network Traffic Visualization

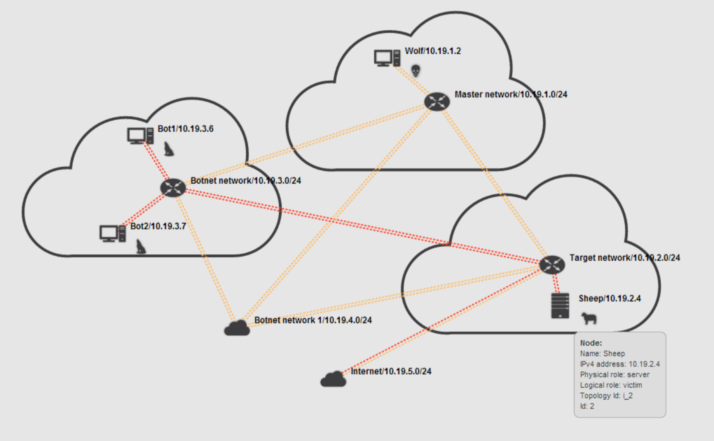


WUI – Network Topology


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

Node:
Name: Sheep
IPv4 address: 10.19.2.4
Physical role: server
Logical role: victim
Topology Id: i_2
Id: 2

WUI – Network Topology

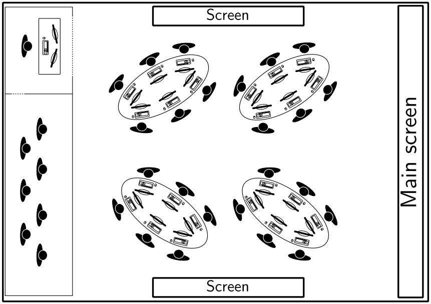

Wolf/10.19.1.2
Master network/10.19.1.0/24
Bot1/10.19.3.6
Botnet network/10.19.3.0/24
Bot2/10.19.3.7
Target network/10.19.2.0/24
Sheep/10.19.2.4
Botnet network 1/10.19.4.0/24
Internet/10.19.5.0/24

Node:
Name: Sheep
IPv4 address: 10.19.2.4
Physical role: server
Logical role: victim
Topology Id: i_2
Id: 2

CPG Hall in Brno

Room for education, training and collaboration

- Environment for education and training.
- Trainings of response to security incidents.
- Environment for testing of real malware.



Conclusion

Summary

- Complete and real-life network can be simulated.
- End users can set up entire environment very quickly.
- Security scenarios provide a generic way to describe an attack.
- Scenario can be re-run and evaluated.
- CPG is a *platform* for various applications.

Co-operation offers

- Propose topics that you would like to see as scenarios.
- Use CPG to run your scenarios.
- Participate in pilot training and exercises.

Thank you for your attention!

Cybernetic Proving Ground

Jakub Čegan et al.

cegan@ics.muni.cz

Thank you for your attention!

KYPO: Cyber Exercise & Research Platform

Project Webpage

http://www.muni.cz/ics/kypo

Jakub Čegan et al.

cegan@ics.muni.cz