TOWARDS A UNIFIED DATA STORAGE AND GENERIC VISUALIZATIONS IN CYBER RANGES

Oslejsek R., Toth D., Eichler Z., Burska K.

LAB OF SOFTWARE
ARCHITECTURES AND
INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY

Cyber Ranges

- Emulate computer networks
- Enables to perform cyber security exercises and experiments
- They differ in
  - emulation possibilities (traffic emulation),
  - application domain (training, learning, forensic analysis),
  - architecture (IaaS, PaaS, **SaaS**, ...)
  - ...

Cyber Ranges – Common Features

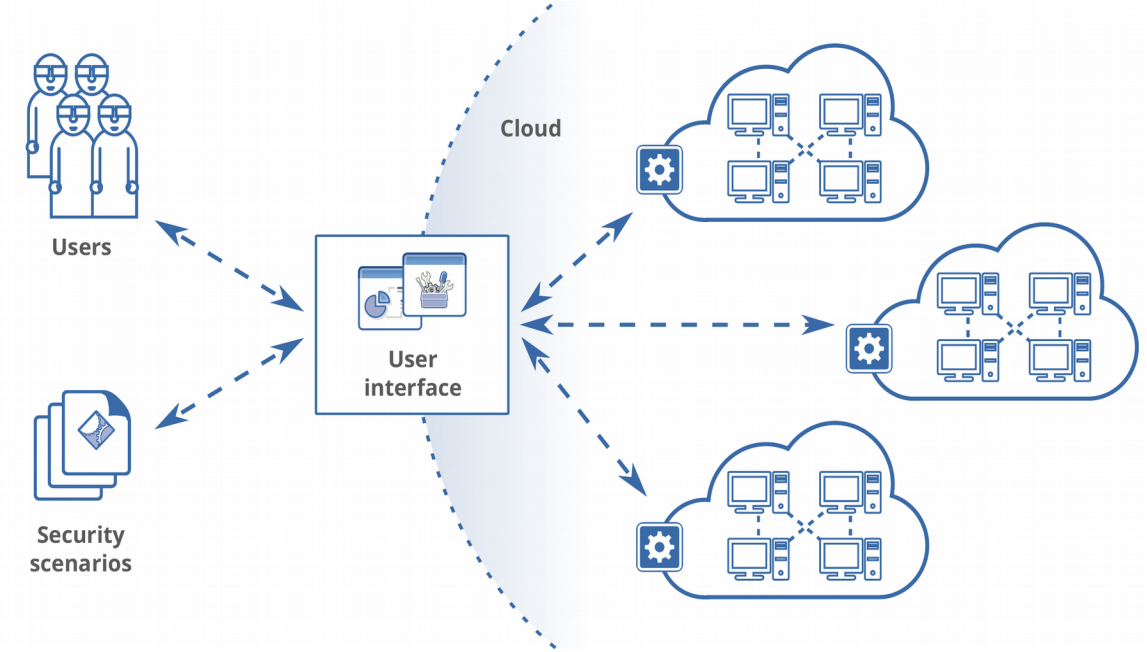
Common services provided by cyber ranges:

- *Resource management* – allocation of network infrastructure with required topology and running applications.
- *Interaction of users with hosts* – allowing users to log into hosts and run applications there.
- ***Data monitoring*** – network activities are monitored on the fly and measured data is stored for further analysis and mediation to users.
- ***Providing insight into cyber threats*** – by providing users with interactive visualizations, analytical tools, and other interactive techniques.

lasaris

KYPO Cyber Range – Key Features

- **Cloud-based** virtualization
  - Allocation of (multiple) sandboxes on demand
  - SW emulation of links, switches, hosts, ...
- Generic cyber range supporting **user-defined security scenarios**
- Goal: KYPO **as a service** (SaaS)
  - End users can interact with sandboxes easily via predefined user interfaces and without the need to install anything by themselves



Challenge 1: Data Monitoring

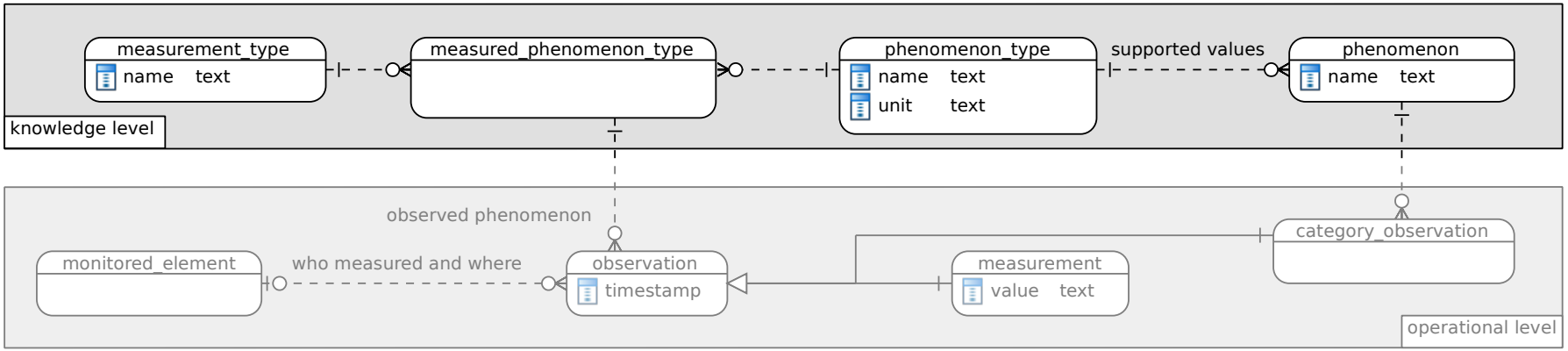
Data monitoring

- We do not know in advance what data are to be monitored for particular scenario.
- **Common phenomena** monitored natively
  - Ex.: packets, flows, CPU load
- **Scenario-specific phenomena** monitored by specialized probes integrated to the cyber range infrastructure
  - Ex.: availability of services, average link throughput, ...
  - Requires access to the virtualization layer or to the low-level cyber range infrastructure
  - Requires skills, competences and deep knowledge of the cyber range
  - It is annoying and time consuming for end users (domain experts)
- **Goal:** Provide a unified data monitoring and storage infrastructure at the user level (as a service)

lasaris

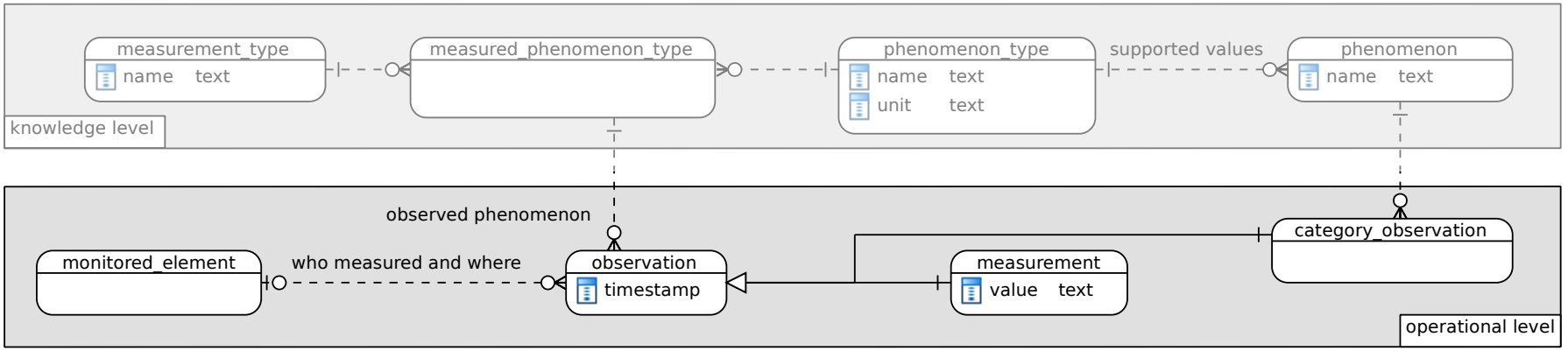
Unified Scheme for Data Storage

- Adapted *Observation* pattern of Martin Fowler
- **Knowledge level**
  - What is to be measured => **scenario-specific data**
  - `phenomenon_type` = common network phenomena
  - `phenomenon` = predefined values of network phenomena
  - `measurement_type` = aggregated data (higher-level interpretation, e.g. *average throughput in 5 min interval*)



Unified Scheme for Data Storage (cont.)

- **Operational level**
  - Data measured by probes => **exercise-specific data**
  - `measurement` = value from "unlimited" domain (e.g. numerical)
  - `category_observation` = predefined value



Challenge 2: Data Visualization

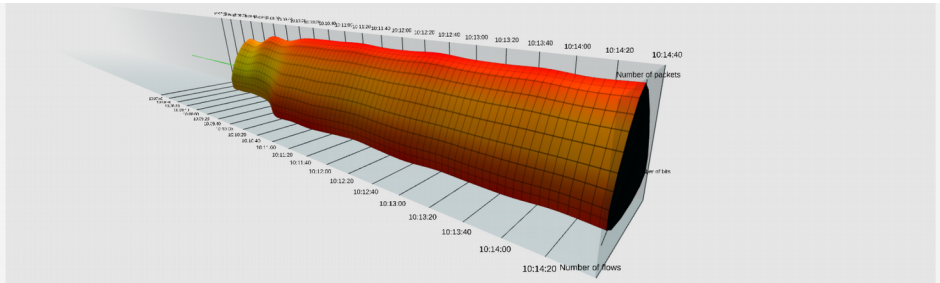
Mediation of data to users

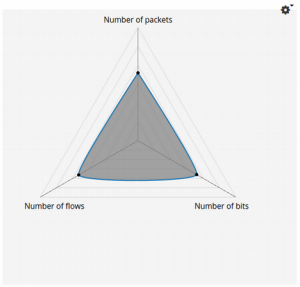
- Variable data
  - Scenario-specific data
- Variable user interests
  - The same data analyzed in different ways by different domain experts
- **Approach 1:** Use specialized analytical or visualization tools deployed in sandboxes by users themselves
  - Tools usually require a specific format of data sources => adaptation of the monitoring infrastructure
- **Approach 2:** Provide user interfaces as a service
  - A scenarist composes scenario-specific user interfaces from predefined visual/interactive blocks
  - End users (domain experts) utilize them directly

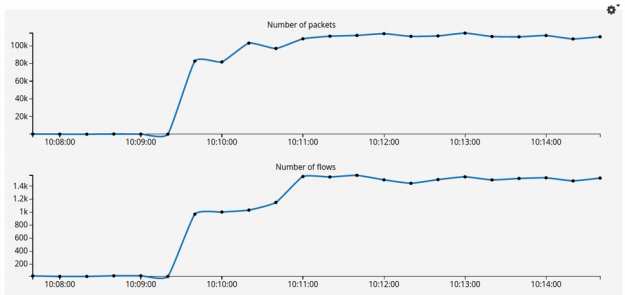
lasaris

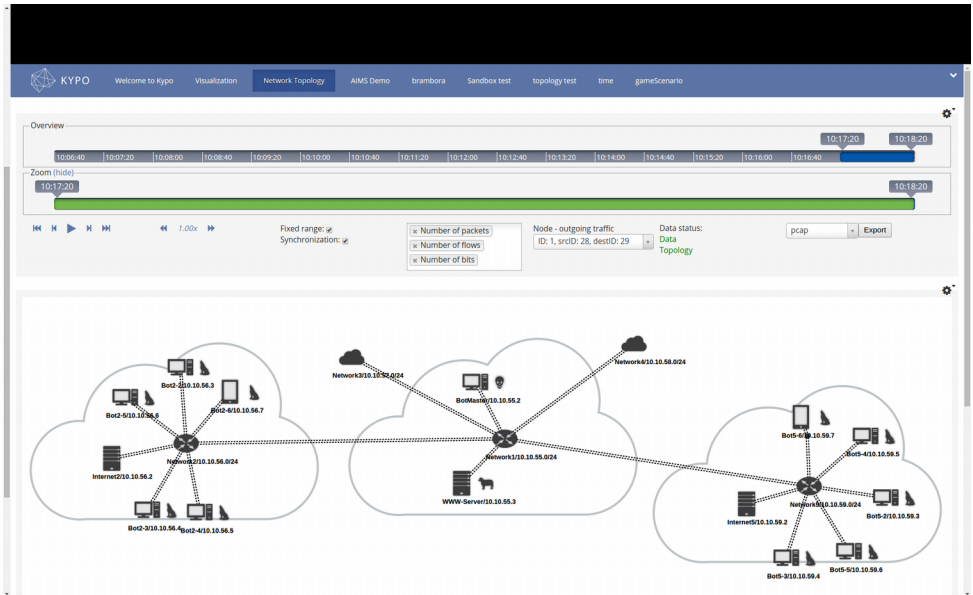
Adaptable User Interfaces

- Enterprise web portals (JSR 168 and JSR 286)
- *Portlets* integrated to *page templates* and *site templates* interactively at the user level
- Portlets:
  - Narrowly focused
  - Mutually connectable to provide higher-level interactions
  - Highly configurable









Evaluation

- Attack demonstrations
  - DDOS and phishing scenarios for security experts
- Hacking games
  - Cca 10 capture-the-flag games
  - From kids to security experts
- Cyber Czech Defense Exercise
  - Realistic 2 days defense exercise in the cooperation with Czech National Security Authority
  - 6 runs, complex scenario with 5 defending and 1 attacking teams
- KYPO Lab – regular cyber-security course
  - Students design their own security scenarios inspired by real threats and attacks
  - Other students play these scenarios at the end of semester

lasaris

Conclusion and Future Work

- Unified monitoring.
  - Setting up the monitoring infrastructure is very laborious and still far from automation.
- NoSQL databases.
  - Possibly better adaptation to variable data.
  - Do not solve the problem of data interpretation and mediation to users.
- Configurability of portlets.
  - Visualization and interaction features depending on dynamic (scenario-specific) roles, e.g. attacker vs. defender.

lasaris

Questions?

Thank you for your attention

www.kypo.cz

FACULTAS ARTIS INFORMATICÆ • UNIVERSITAS MASARYKIANA

lasaris
Lab of Software Architectures and Information Systems FI MU

UNIVERSITAS MASARYKIANA BRUNENSIS • INSTITUTUM REI COMPUTATORIÆ •

CSIRT-MU

lasaris