CRUSOE: DATA MODEL FOR CYBER SITUATIONAL AWARENESS

Tuesday 28th August, 2018

Martin Husák
Jana Komárková
Martin Laštovička
Daniel Tovarňák

CSIRT-MU

Introduction and Motivation

Cyber Situational Awareness

Situational Awareness

- *"Perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."* [Endsley, 1988]

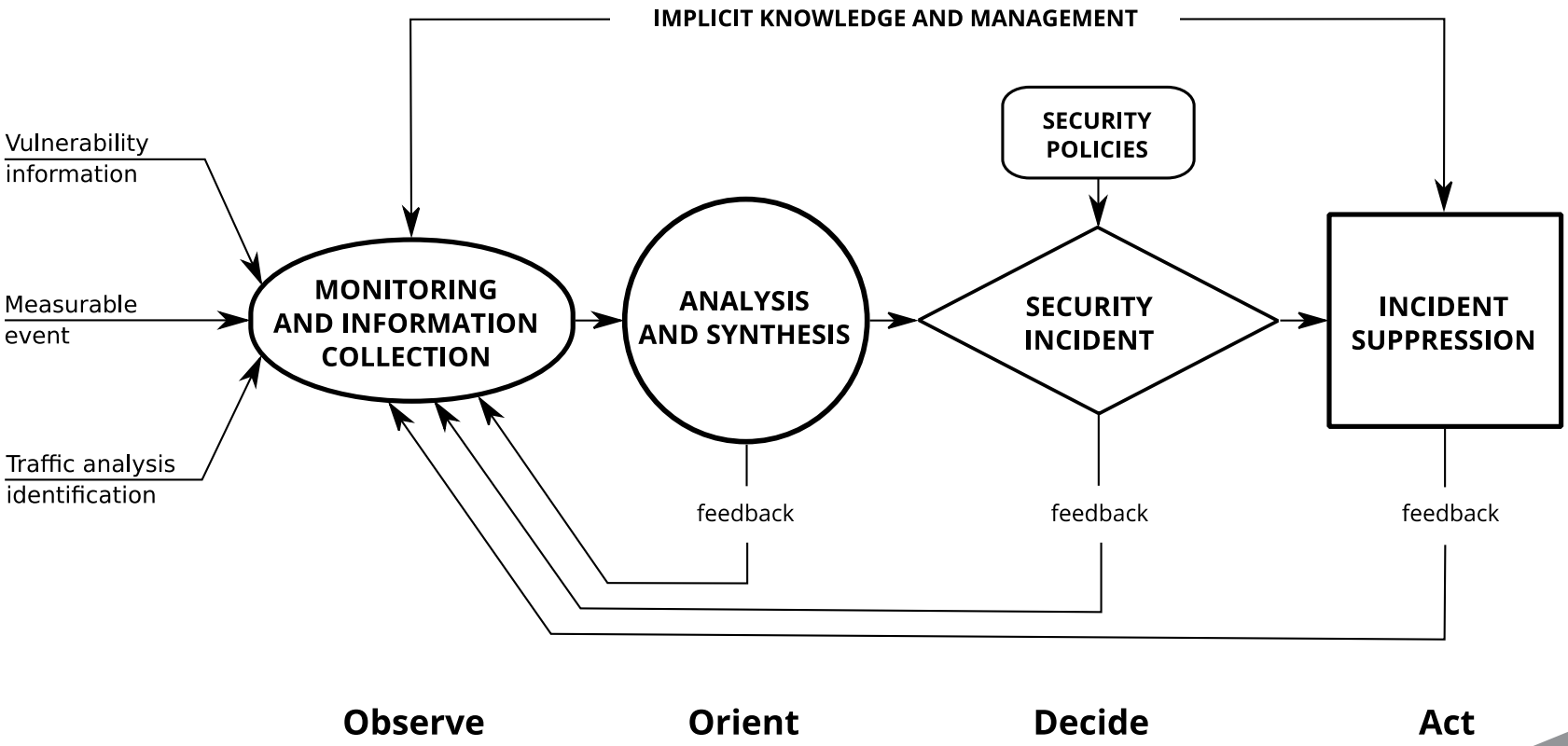
Network-wide Situational Awareness

- Network Awareness
- Threat/Attack Awareness
- Operation/Mission Awareness
- Prediction & Data Fusion

  [Evancich, 2014]

OODA Loop

Observe, Orient, Decide, Act [Boyd, 1976]



CSIRT-MU

CRUSOE Project

- Research of Tools for Cyber Situational Awareness and Decision Support of CSIRT Teams in Protection of Critical Infrastructures

- **Observe** – network and host monitoring
- **Orient** – visualization, incident handling dashboard
- **Decide** – impact assessment, attack countermeasure suggestion
- **Act** – dry-run of attack countermeasures

Contribution

- Summary of the **requirements** on a data model that could be used for capturing cyber situational awareness.
- Proposal of a **data model** that fulfills the requirements and describe in details its entities and relationships.
- Description of the **data sources** that can be utilized to fill the model in fully automated or semi-automated fashion.
- Illustration of how does the proposed data model enhance **incident response** in common scenarios.

Requirements

Interviews with Incident Handlers

Interviews

- CSIRT/CERT teams from EU countries
- *What do you lack in day-to-day operations and incident response?*

Common Answers

- Criticality estimation of attack target
- Vulnerability prioritization and dissemination
- Finding responsible person

Selected NATO Use Cases

NATO CDSA RFI

- Cyber Defense Situational Awareness Request for Information
- 35 use cases for cyber defence situational awareness system

- UC10 – Single authoritative data source
- UC12 – View connections of asset
- UC15 – Fuse data
- UC03 – Drill down / Roll up
- UC06 – View asset dependencies
- UC11 – View interconnectivity

Related Work

CyGraph

- System for improving cyber security posture
- Graph-based data model and database
- Layered design:
  - mission readiness
  - cyber threats
  - network infrastructure
  - cyber posture

Other Data Models

- M2D2, Virtual Terrain, CAMUS, . . .

Data Model

Proposed Data Model

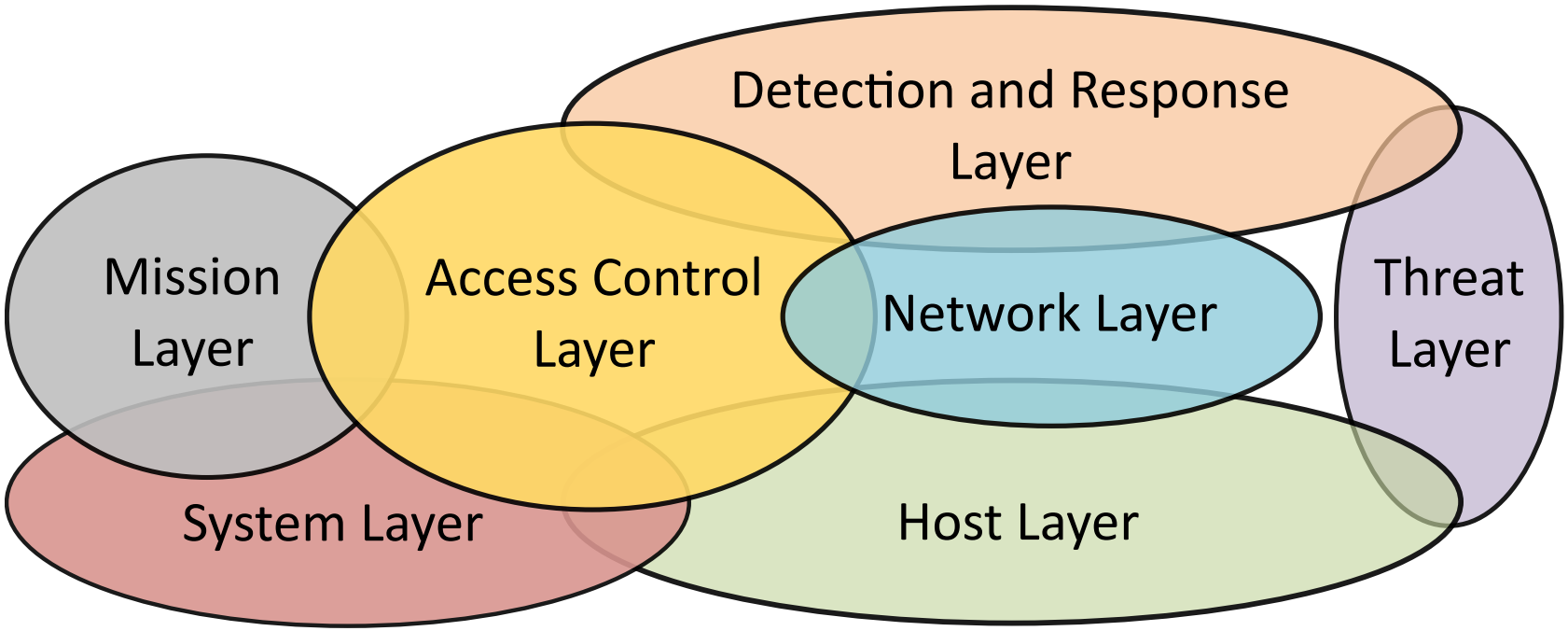
Key Characteristics

- All-embracing
- Comprehensive
- Attainable
- Sustainable
- Time-conscious
- Extensible

Novelties compared to related work

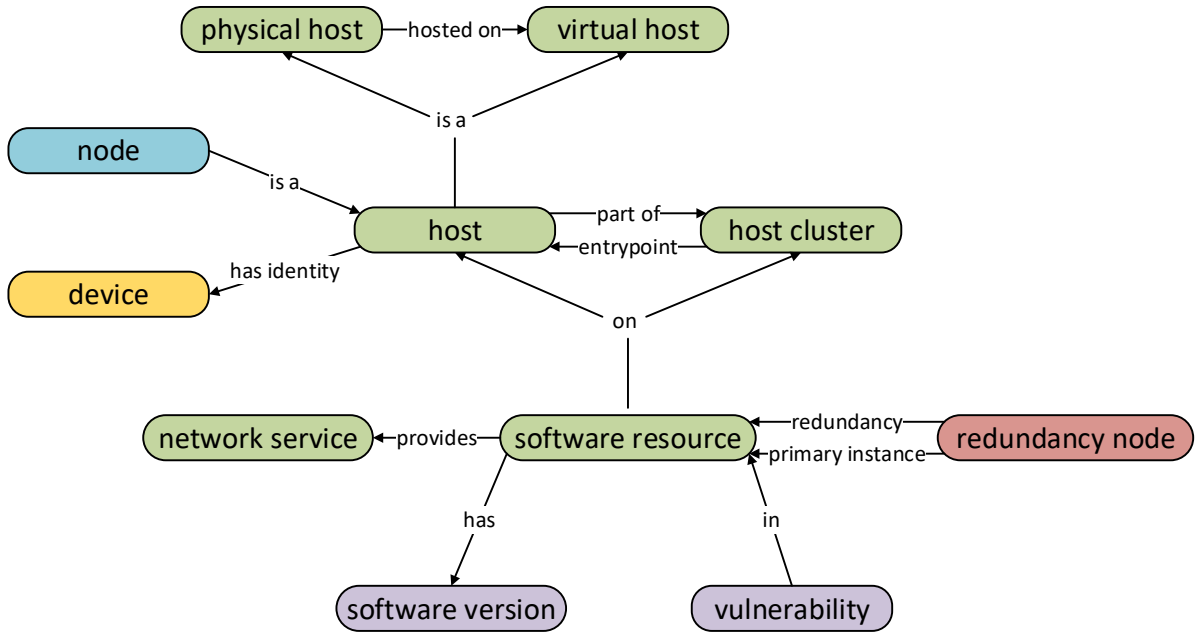
- Adherence to automatically aquirable content
- Inclusion of Access Control
- Grouping mechanisms – host clustering, etc.
- Dependancy and redundancy nodes

Layers



CSIRT-MU

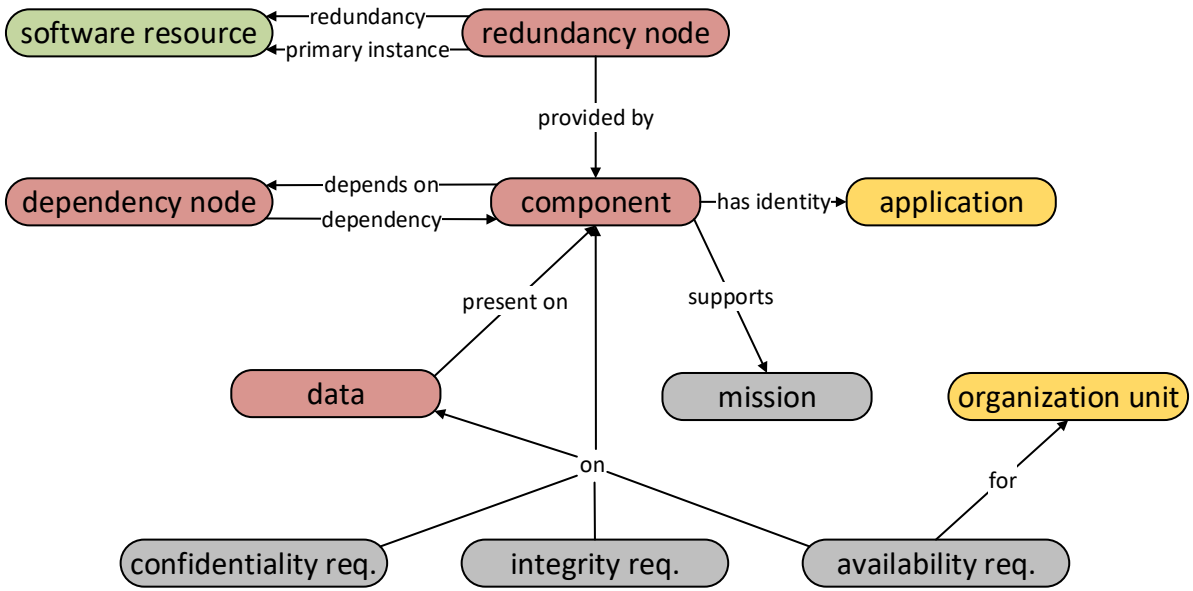
Host Layer



- Data mostly obtainable via network monitoring
- Clustering and virtualization information inserted manually

CSIRT-MU

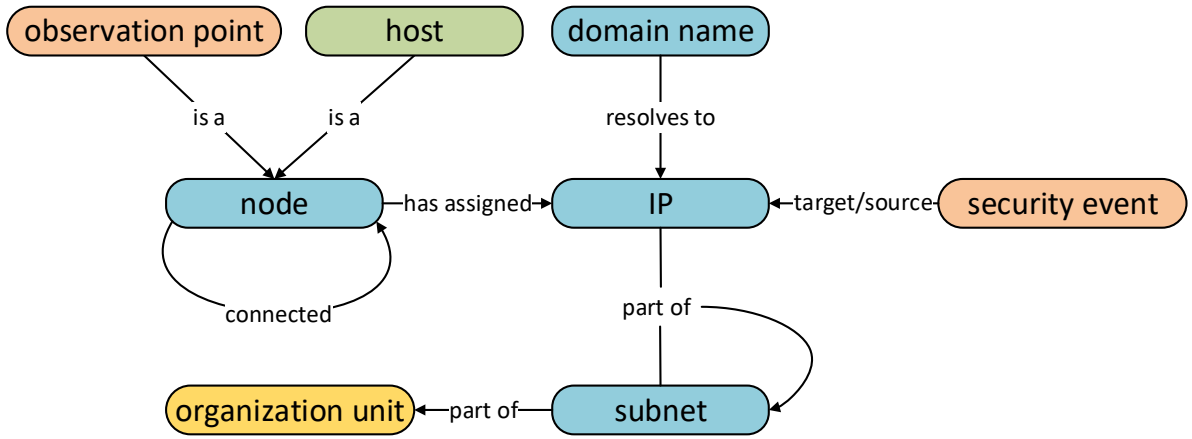
System Layer



- Connects network hosts with components of critical systems
- Describes distribution of sensitive data

CSIRT-MU

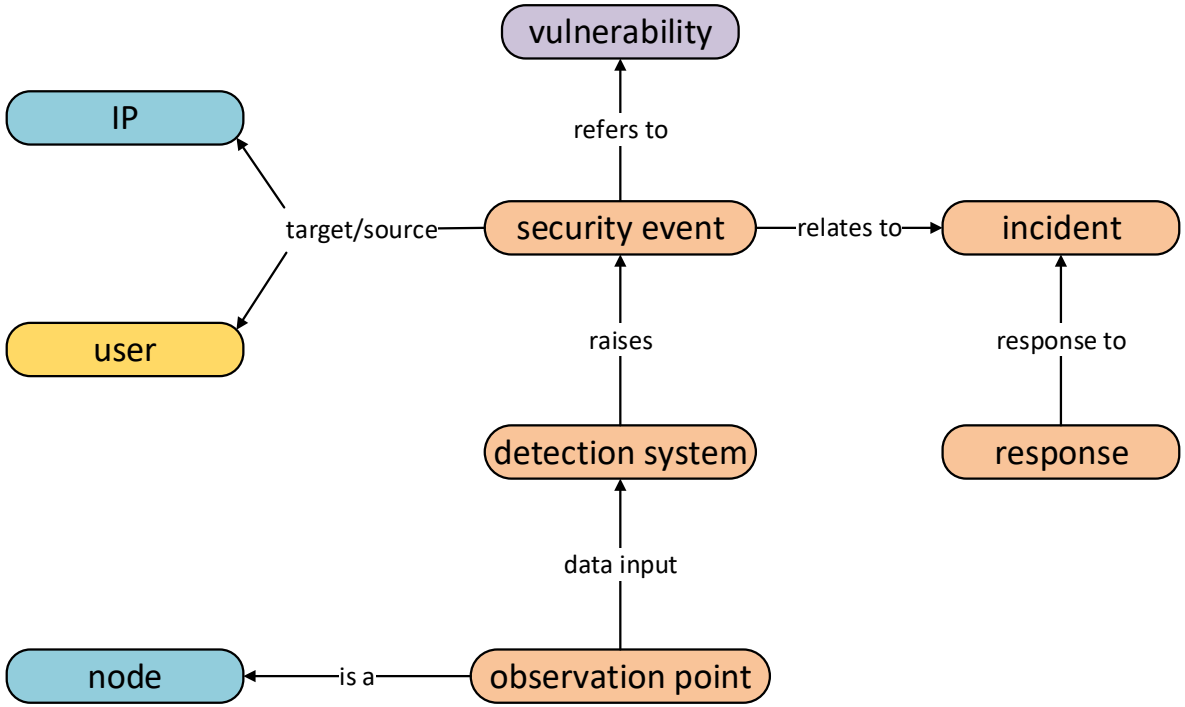
Network Layer



- Network topology, connections with organization units

CSIRT-MU

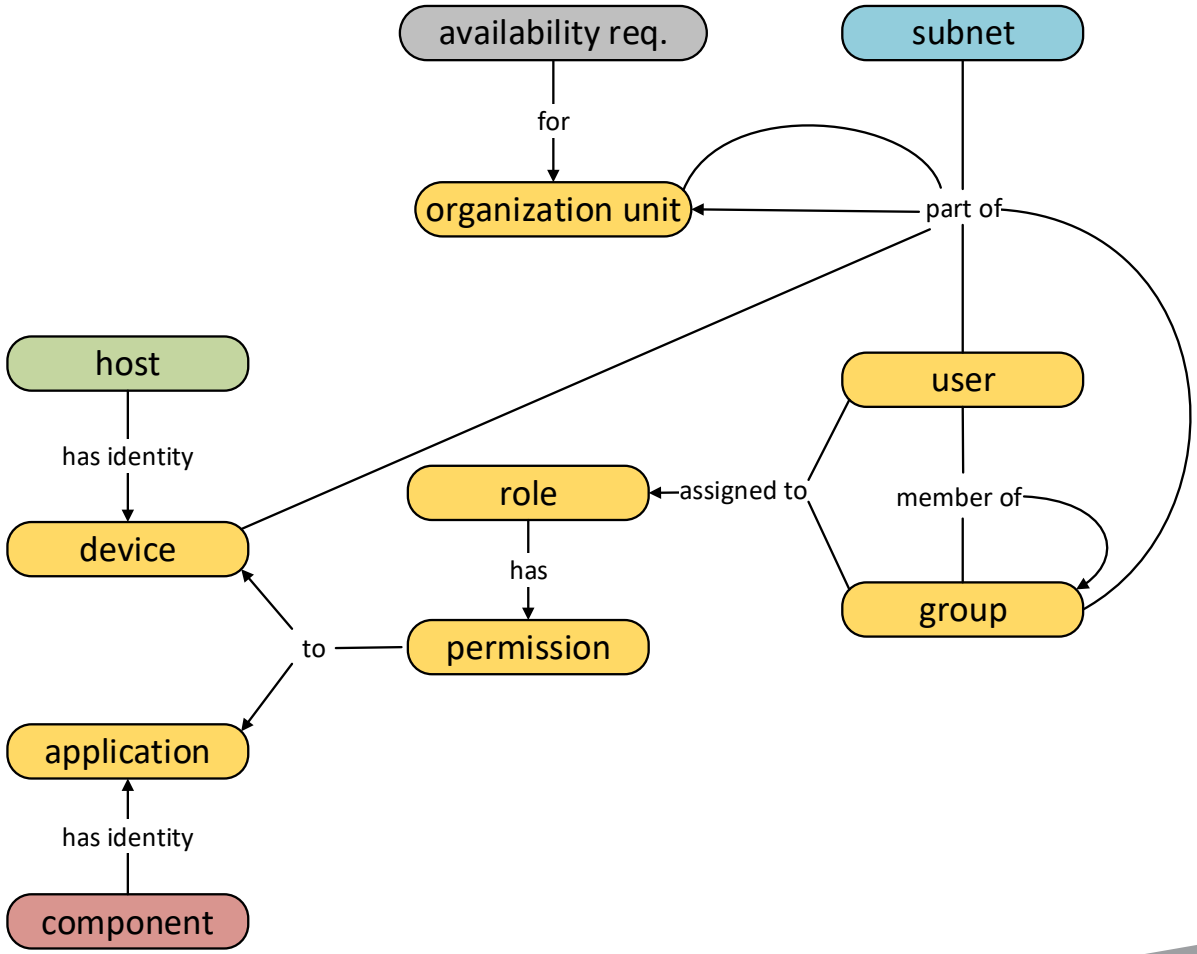
Detection and Response Layer



- Placement of intrusion detection systems
- History of security incidents

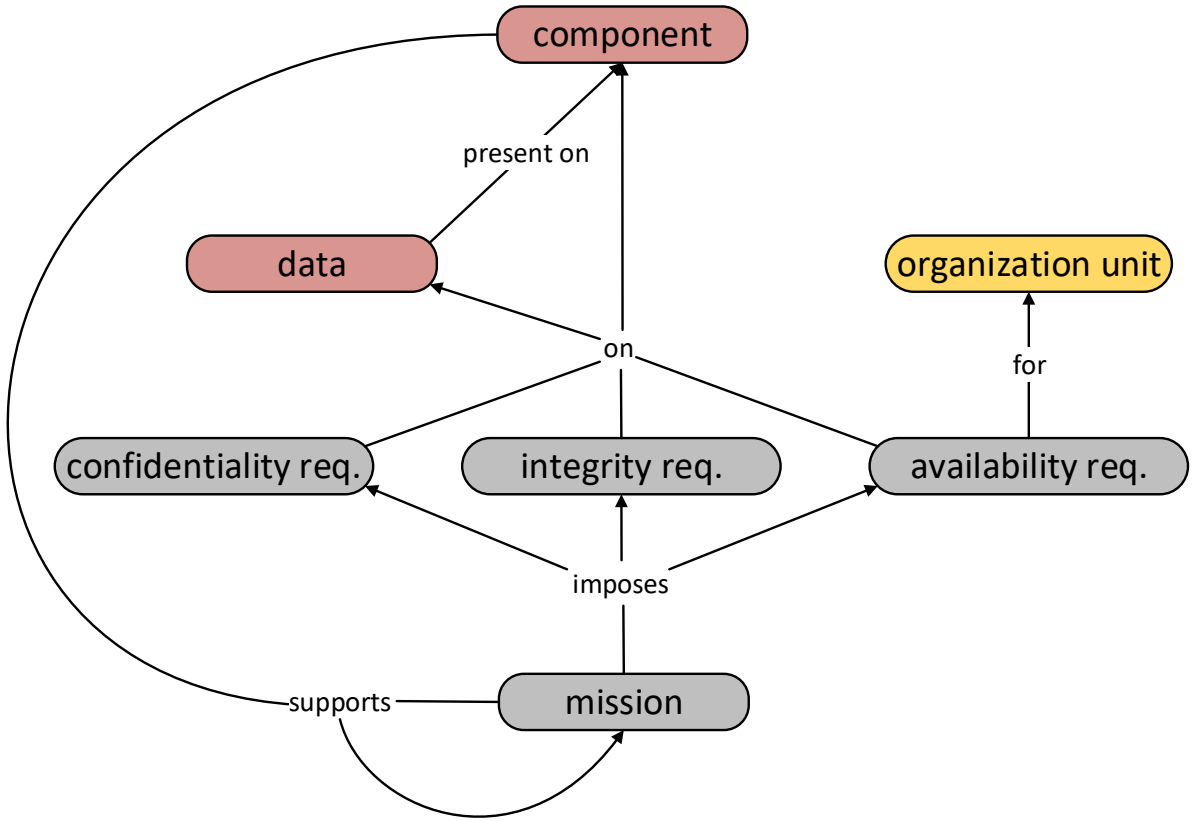
CSIRT-MU

Access Control Layer



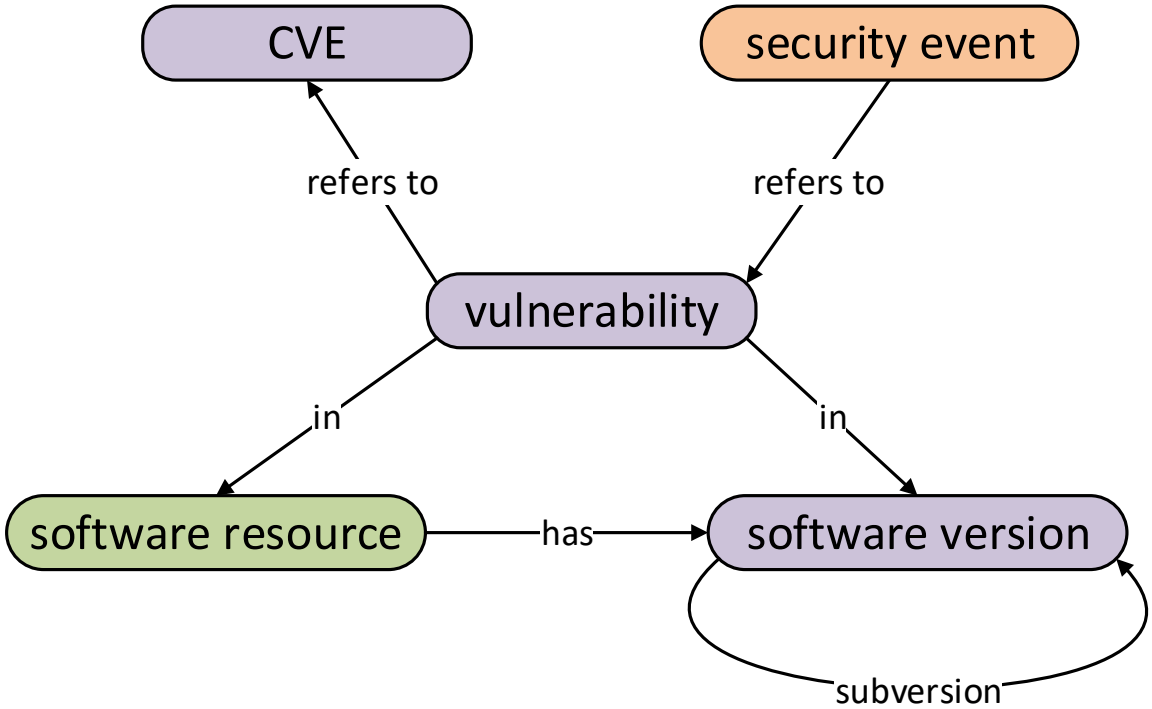
CSIRT-MU

Mission Layer



CSIRT-MU

Threat Layer



- Enumeration of vulnerabilities related to software resources

CSIRT-MU

Conclusion

Conclusion and Future Work

Conclusion

- Seven-layer model for cyber situational awareness,
- automation of obtaining data preferred,
- novel concepts included (access control, host clustering, etc.),
- evaluated through discussions with incident handlers.
- `https://github.com/CSIRT-MU/CRUSOE-Data-Model`

Future Work

- Implementation of cyber situational awareness system.
- Further examination of available data sources.

CSIRT-MU

THANK YOU FOR YOUR ATTENTION!

csirt.muni.cz

@csirtmu

Martin Husák

husakm@ics.muni.cz