INSTITUTE OF
COMPUTER SCIENCE
Masaryk University

# Situational Awareness: Detecting Critical Dependencies and Devices in a Network

**AIMS CONFERENCE**
13. 7. 2017

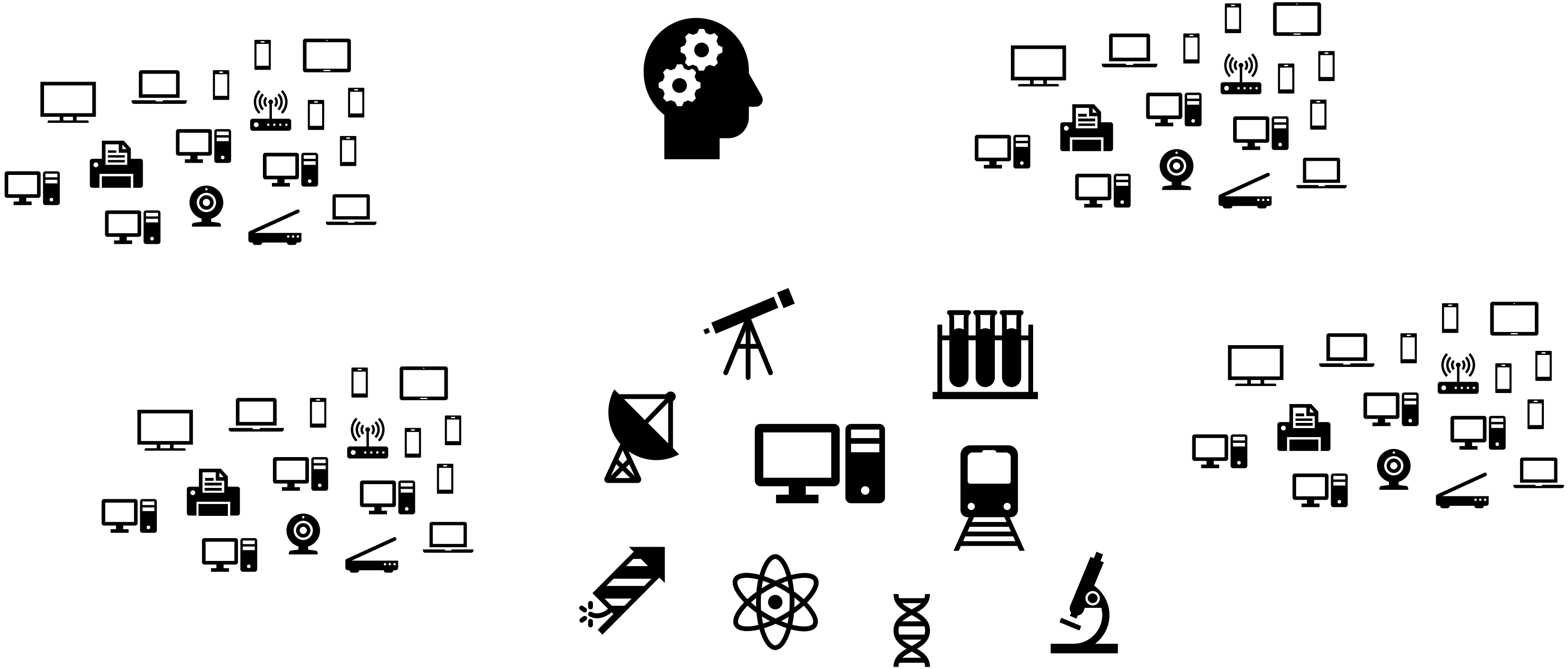
Martin Laštovička
lastovicka@ics.muni.cz

Brno **Ph.D.** Talent

# Situational Awareness

The knowledge and understanding of the current situation.

🧍 🖥️



# Motivation

- Automatic building of situational awareness
- Ever-evolving threat landscape and network threats
- Threat impact estimation with respect to current situation

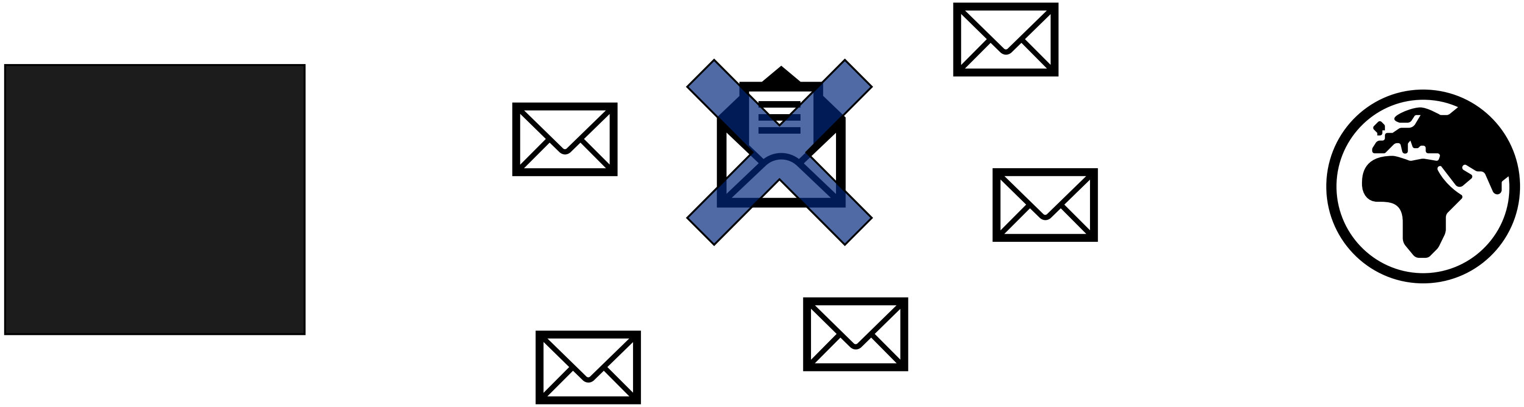
# Research Questions

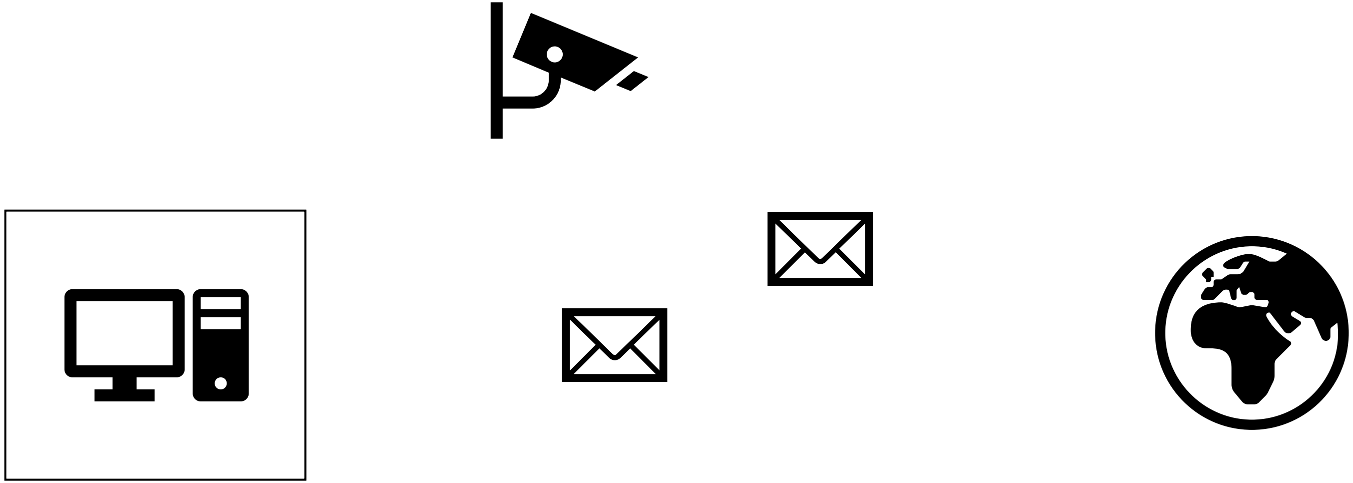
1. How can device and its services be identified in a complex network using passive network monitoring?

2. How can device dependencies be detected in a network?

3. How can device importance be estimated from the perspective of reaction to cyber threats?

# RQ1: Device and Service Identification





# How?

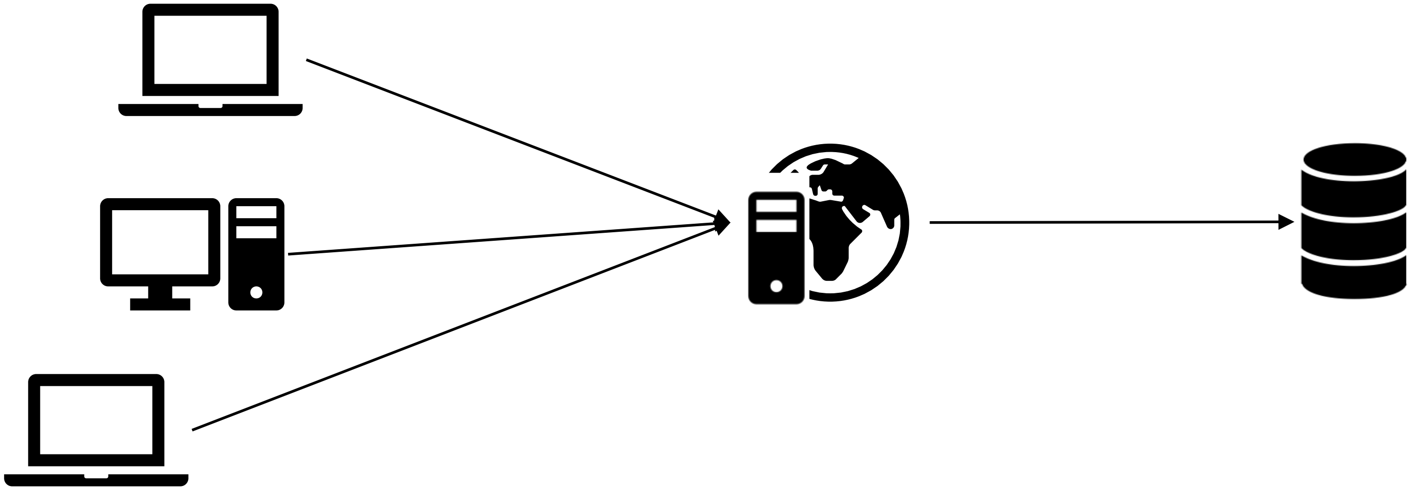
- TCP stack
- Specific domains
  - HTTP hostname
  - HTTPS SNI
- User-agent

- Service identifier
- Port
- Traffic characteristics

# Methods

- Extended flows – IPFIX
  - More information from L3, L4, L7 headers
  - How to update?
- Machine learning
  - Autonomous characteristics identification
  - How to scale?

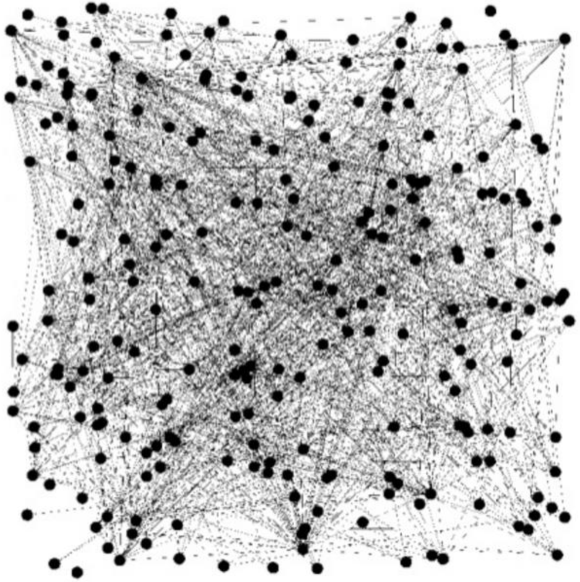
# RQ2: Detection of Device Dependencies

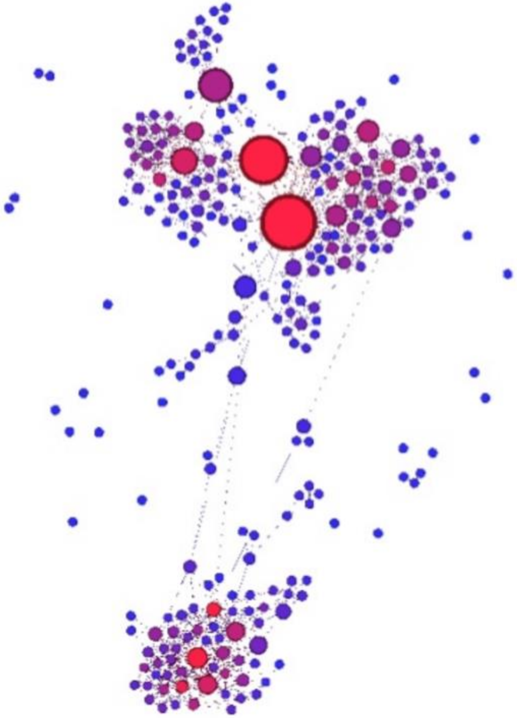


# How?

- Client-server communication
- Traffic characteristics

# RQ3: Importance Estimation





# How?

- Device identification
- Provided services
- Traffic statistics
- Number of dependencies
- Attack statistics

# Methods

- Graph algorithms
  - Graph centrality
  - Clique detection
- Analysis of attackers activities
  - Type of attack
  - Duration, repetition, number of targets

# Preliminary Results

- OS recognition in real network
  - Experiments with flow based passive identification
  - Encrypted traffic – ocsp protocol
- Graph-based data model
  - Machines and relations
  - Computations over data
- Attack targets analysis
  - Generic attacks (scans) on workstations/dynamic ranges
  - DoS, brute force attacks on servers

# Discussion

Martin Laštovička
lastovicka@ics.muni.cz

Brno Ph.D. Talent

Brno Ph.D. Talent Scholarship Holder – Funded by the Brno City Municipality