Decision Support for Mission-Centric Cyber Defence

ARES ’19,
August 26-29, 2019,
Canterbury, United Kingdom

Michal Javornik, Jana Komarkova, Martin Husak
Institute of Computer Science,
Masaryk University, Brno, Czech Republic

CSIRT-MU

Decision Support for Mission-Centric Cyber Defence

- **Introduction**
- **Motivating Use Case**
- **Mission Decomposition Model**
- **Analytical Framework**
  - Constraint Satisfaction/Optimization Problem
  - Attack Graph
  - Bayesian Network
  - Mission Resilience Metric
- **Summary**

Introduction

Mission

- System of **supportive processes**
- Established **functional requirements**

Process

- An **asset to be protected**
- Established **security requirements** – confidentiality, integrity, availability

Mission configuration

- Structure of supportive components (processes, IT services, cyber components) & their interactions
- Critical mission enables **more configuration alternatives**

Cyber environment

- Difficult/impossible to **protect all components**
- Difficult/impossible to **eliminate all vulnerabilities**

Introduction

The Goal

- **Keep the mission operational** as long as possible
- Selection of **the most resilient mission configuration**

Mission Decomposition Model

- A better **comprehension** of the mission
- **Communication** of decision-makers

Analytical Framework

- **Mathematical abstraction**
  - Rigorous thinking; integration tool
  - The statistical inference that reflects the situation

Mission Resilience Metric

How likely can a particular mission configuration be affected, i.e., the **probability of its successful disruption in terms of endangering established security requirements**.

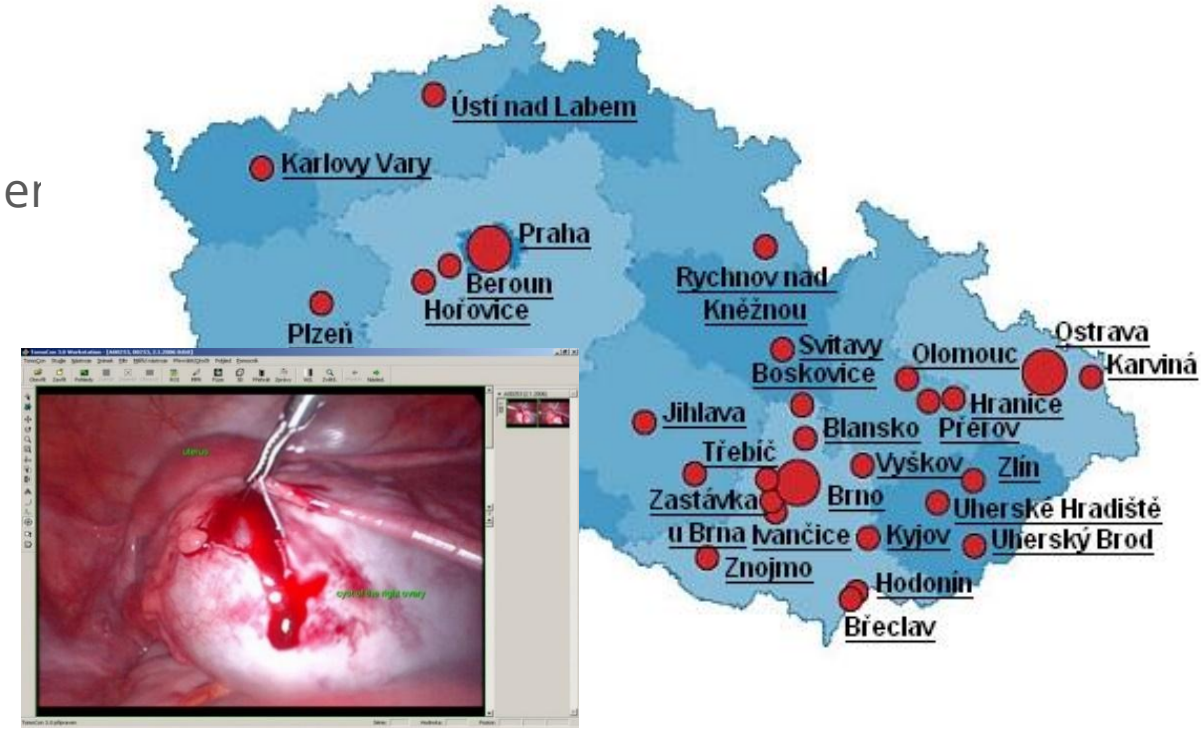
Motivating Use Case

Regional Medical Imaging

- Collaborative **processes across different** (healthcare) **service providers**
- Legal, ethical, contractual requirements (=> functional & security requirements)
- Life-threatening situations

The Mission

- Imaging assessment of the polytrauma patier



Mission Decomposition Model

Evaluation of the polytrauma patient

Mission Supportive Processes (Medical Domain)

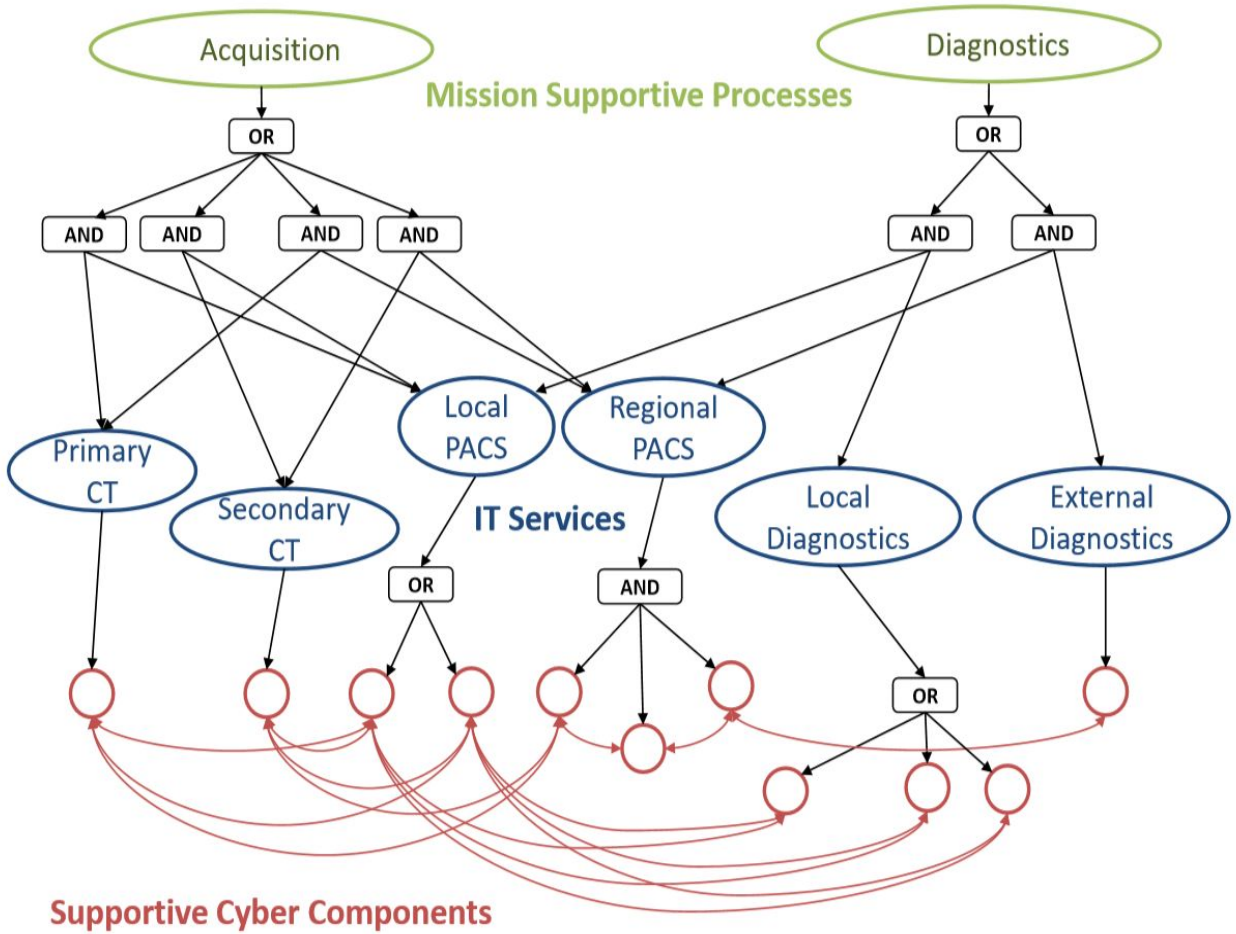
- Patient examinations (CT, MRI, MG screening, …)
- Emergency consultations (neurology, cardiology, …)
- Other consultations (oncology, mammography, …)

IT Services (SaaS)

- PACS (institutional, regional, …)
- Exchange/sharing of examinations

Supportive Cyber Components (Cyber Domain)

- Specific implementations of PACS
- The software of acquisition modalities
- Diagnostics software, CAD, visualization, …



Constraint Satisfaction/Optimization Problem

Constraint Satisfaction Problem $CSP = (X, D, C)$

- Set of variables $\{X_1, \dots, X_n\}$
- Associated domains $\{D_1, \dots, D_n\}$
- Related constraints $\{C_1, \dots, C_m\}$ (desired functional requirements)

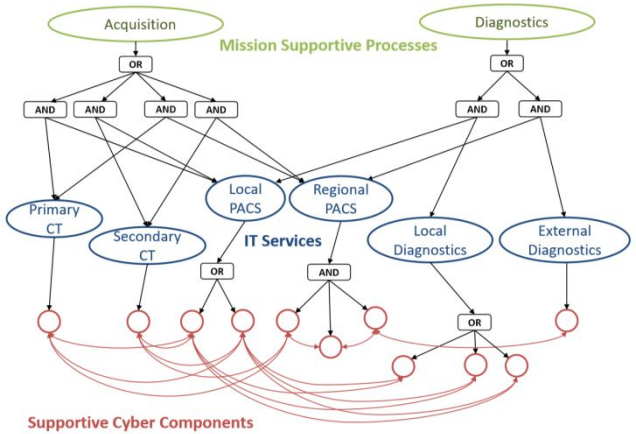
- Satisfactory solution – operational mission

Constraint Optimization Problem

- **Optimizing the security requirements** while **satisfying the required functionality** (keep the mission operational)

- Utility (objective) **real-valued function** (to be optimized)
- We calculate the **probability of an exploit endangering established security requirements**
- Searching for the best solution (the worst for the attacker)

Satysfying Mission Configuration



Valuation satisfying the constraints

- Constrained AND/OR tree abstraction
- Boolean Constraint System (Boolean formula, transformable to CNF

$$
\begin{aligned}
\varphi = & (TraumaCentre) \wedge \\
& (Acquisition \implies TraumaCentre) \wedge \\
& (Diagnostics \implies TraumaCentre) \wedge \\
& ((PrimaryCT \wedge LocalPACS \vee PrimaryCT \wedge RegionalPACS \vee SecondaryCT \wedge LocalPACS \vee SecondaryCT \wedge RegionalPACS) \\
& \implies Acquisition) \wedge \\
& ((LocalPACS \wedge LocalDiagnostics \vee RegionalPACS \wedge ExternalDiagnostics) \implies Diagnostics) \wedge \\
& (Acquisition\_PrimaryCT \implies PrimaryCT) \wedge (Acquisition\_SecondaryCT \implies SecondaryCT) \wedge \\
& ((PrimaryInstance\_LocalPACS \vee SecondaryInstance\_LocalPACS) \implies LocalPACS) \wedge \\
& ((LokalProxy\_RegionalPACS \wedge Server\_RegionalPACS \wedge RemoteProxy\_RegionalPACS) \implies RegionalPACS) \wedge \\
& ((PrimaryViewer\_LocalDiagnostics \vee SecondaryViewer\_LocalDiagnostics) \implies LocalDiagnostics) \wedge \\
& ((RemoteViewer\_ExternalDiagnostics) \implies ExternalDiagnostics).
\end{aligned}
$$

Attack Graph

Logical Attack Graph

- Related **vulnerabilities** and **interactions**
- Privileges related to attacker's target
  - **Pre-requisites** – allow exploitation
  - **Post-requisites** – result from a successful exploit
- Paths the attacker can follow to reach the desired target

Formal Description

$$(Exploits \cup Privileges, Prerequisities \cup Postrequisities)$$

where

$$Prerequisities \subseteq Privileges \times Exploits$$

$$Postrequisities \subseteq Exploits \times Privileges$$

Bayesian Network

Formal Description

$$BN = (DAG, Q)$$

DAG (Directed Acyclic Graph)

- Nodes – random variables
- Arcs – conditional (in)dependences among variables

Q (Quantification)

- Conditional probability distribution for each variable

Joint probability distribution (quantitative situational awareness)

$$P(X_1, \dots, X_n) = \prod_{i=1}^{n} P(X_i | parents(X_i))$$

Mission Resilience Metric

Attack Graph: input

- **Specific knowledge** – SW components, hosts, connectivity
- **Abstract knowledge** – vulnerability, exploit preconditions
- **Attacker's current position** – intrusion detection system
- **Target privileges** – CIA requirements, mission decomposition, the impact of a successful exploit

Attack Graph: output

- **Causality identification** – subgraph of privileges

Bayesian Network: input

- **Causality relationships**
- **Causality relationships quantification** (CPTs)
  - CVSS sub metrics – AC, E, ...
  - Other sources of uncertainty

Bayesian Network: output

- Probability of reaching the target privilege
- **Probability of disruption of a particular security requirement**

Mission Resilience Metric

Constraints Satisfaction

- **Functional requirements** of the mission **must be satisfied**
- Constellations of supportive processes & cyber components
- The set of **satisfying mission configurations**

Constraints Optimization (Utility Function Definition)

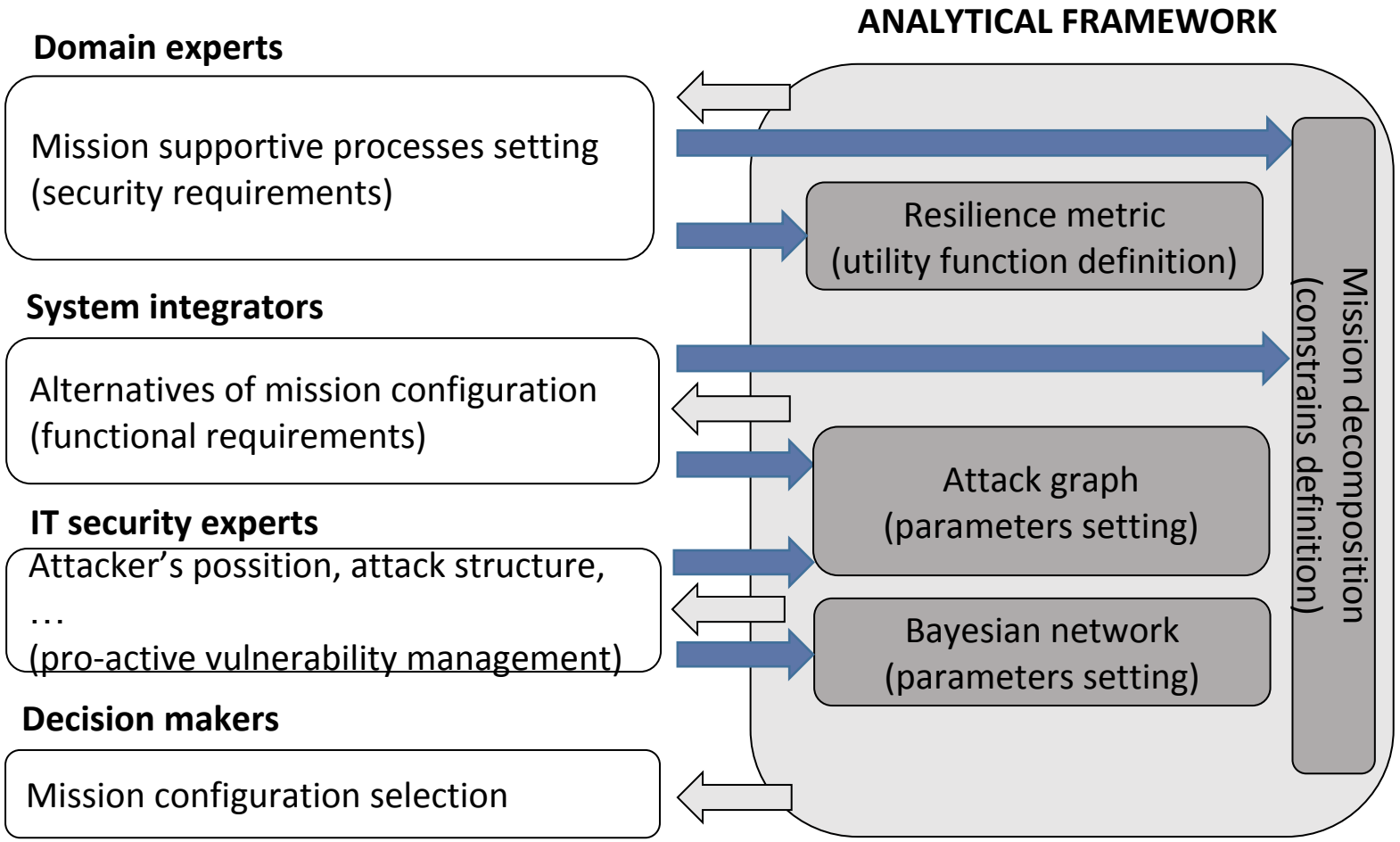
- **Security requirements** of the supportive processes **must be optimized**
- The most **resilient mission configuration**

- Considers **the ratio coefficients** among individual security requirements (multiple criteria)
- Calculates **the worst scenario** (the vulnerability) within an individual mission configuration
- Selects **the most optimistic configuration**

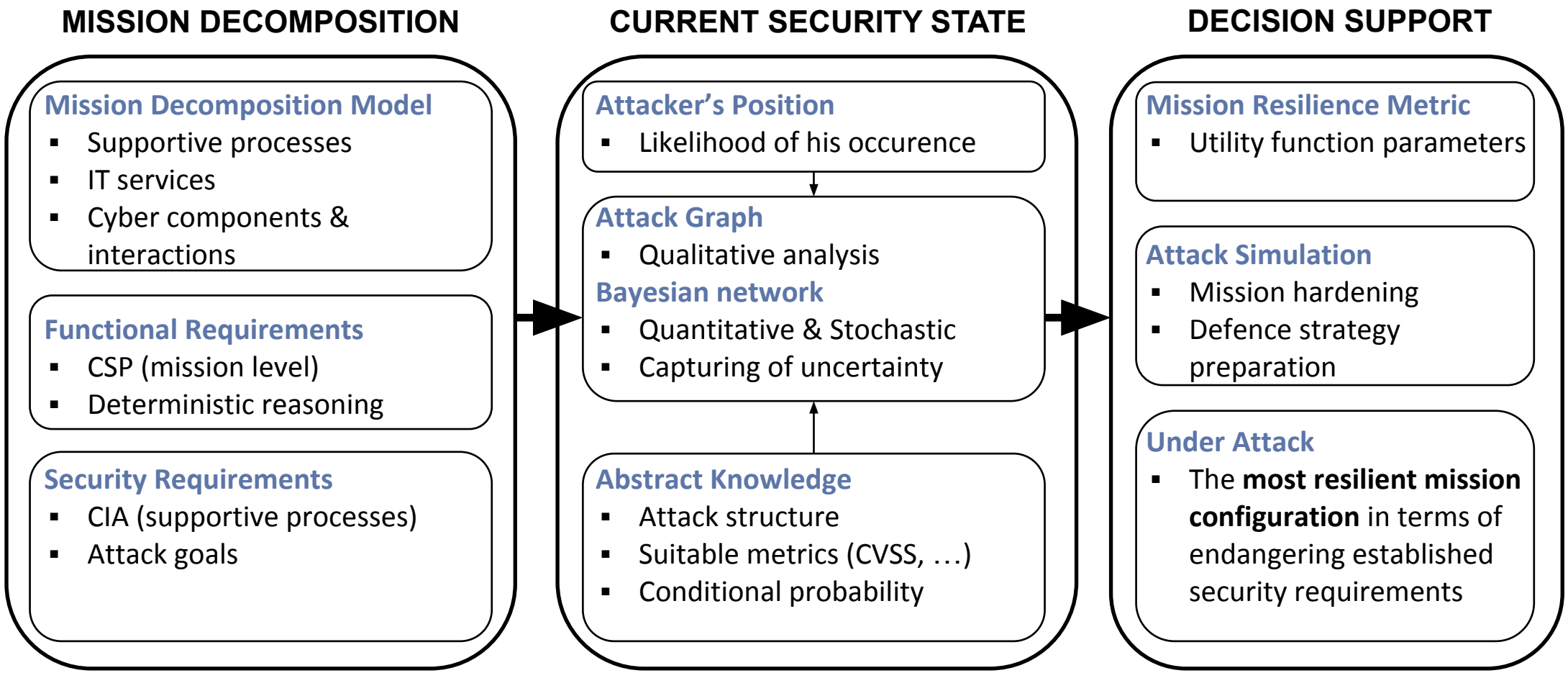
Stakeholders & Their Duties

Decision Making

- The joined effort of stakeholders
- Information provision
- Feedback



Summary


MISSION DECOMPOSITION
Mission Decomposition Model
Supportive processes
IT services
Cyber components & interactions
Functional Requirements
CSP (mission level)
Deterministic reasoning
Security Requirements
CIA (supportive processes)
Attack goals
CURRENT SECURITY STATE
Attacker's Position
Likelihood of his occurence
Attack Graph
Qualitative analysis
Bayesian network
Quantitative & Stochastic
Capturing of uncertainty
Abstract Knowledge
Attack structure
Suitable metrics (CVSS, …)
Conditional probability
DECISION SUPPORT
Mission Resilience Metric
Utility function parameters
Attack Simulation
Mission hardening
Defence strategy preparation
Under Attack
The most resilient mission configuration in terms of endangering established security requirements

QUESTIONS?

THANKS FOR YOUR ATTENTION!

https://csirt.muni.cz

@csirtmu

Michal Javornik

javor@ics.muni.cz

CSIRT-MU