Decision Support for Mission-Centric Network Security Management

NOMS 2020,

April 20-24, 2020,

Budapest, Hungary

Michal Javornik, Jana Komarkova, Lukas Sadlek, Martin Husak

Institute of Computer Science,
Masaryk University, Brno, Czech Republic

CSIRT-MU

Decision Support for Mission-Centric Network Security Management

- **Introduction**
- **Mission Decomposition Model**
- **Decision Support Process**
- **Process Implementation**
  - Attack Graph
  - Bayesian Network
  - Derivation of resilience metric
- **Evaluation in Operational Environment**
- **Summary**

Introduction

Mission-Centric Decision Support

- The goal: keep the mission **operational** as long as possible **in terms of established functional requirements**

Mission Resilience Metric

- The probability of its successful **disruption in terms of established security requirements**

Mitigation

- Difficult/impossible to **protect all components**
- Difficult/impossible to **eliminate all vulnerabilities**
- We compare the **resilience of possible mission configurations**

Decision Support Process

- Mathematical abstraction, statistical inference

Mission Decomposition Model

Graph-based model (understanding the complexity of security situation)

- Mission supportive processes, IT services, Cyber components, and their interactions
- Formal description of the mission

Mission supportive process

- An activity **delivered by people through cyber components**
- The main **asset to be protected**
- Establishment of **security requirements**: confidentiality, integrity, availability

Mission configuration

- An arrangement of mission-supportive processes & other entities
- Associated logical formula – formal expression of **functional requirements**

Satisfying mission configuration

- An assignment the logical formula evaluates to True
- Mission, if critical, should enable **more satisfying configurations**
- Mission: a **collection of satisfying mission configurations**

Decision Support Process

Environment description

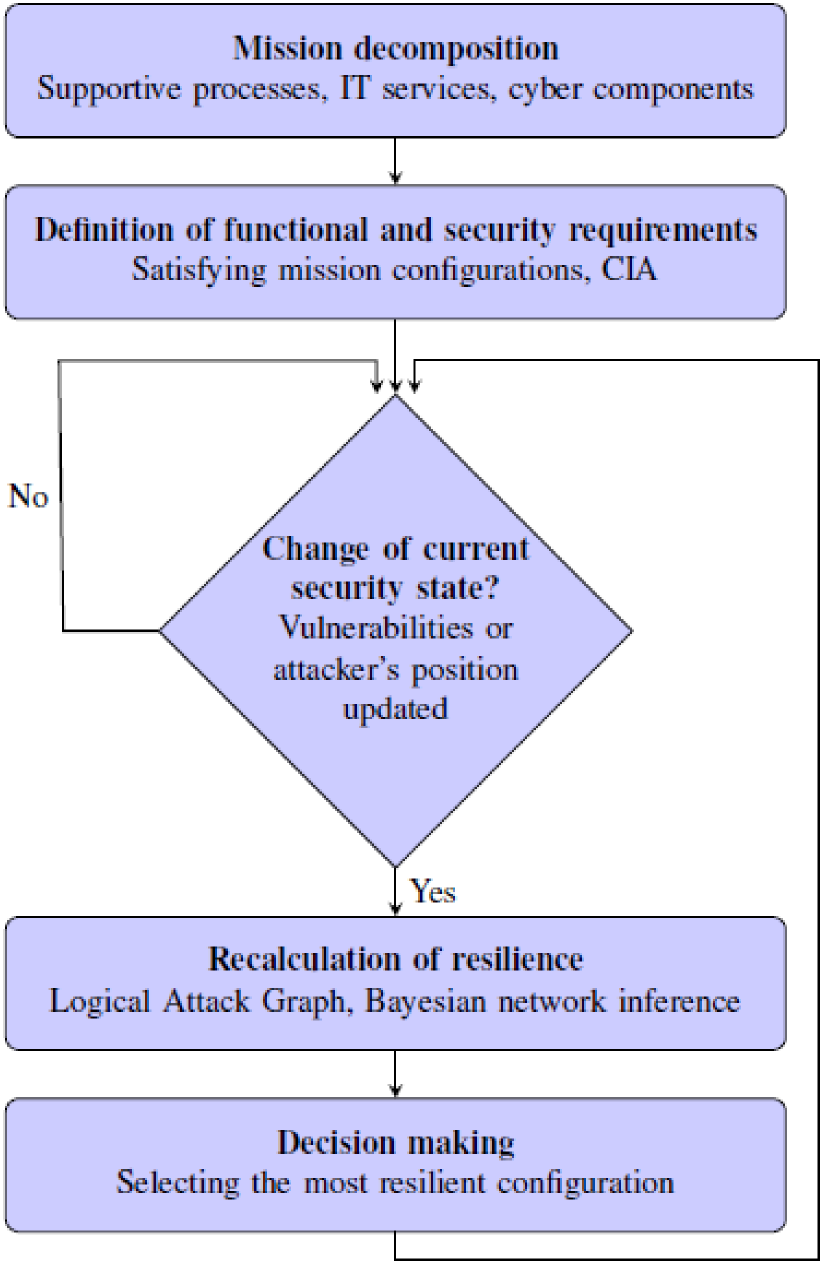
- Domain & IT experts responsibility

Checking of security state change

- Vulnerability scanners, IDS, …

Quantification of the security state

- The probability of disruption of established security requirements
- Inference mechanism of graphical probabilistic model


Mission decomposition
Supportive processes, IT services, cyber components
Definition of functional and security requirements
Satisfying mission configurations, CIA
No
Change of current security state? Vulnerabilities or attacker's position updated
Yes
Recalculation of resilience
Logical Attack Graph, Bayesian network inference
Decision making
Selecting the most resilient configuration

Attack Graph

Privilege-exploit Attack Graph

- Paths an attacker can follow to reach the desired target
- Bipartite graph

$$(\boldsymbol{Exploits} \cup \boldsymbol{Privileges}, \boldsymbol{Prerequisities} \cup \boldsymbol{Postrequisities})$$

where

$$\boldsymbol{Prerequisities} \subseteq \boldsymbol{Privileges} \times \boldsymbol{Exploits}$$

$$\boldsymbol{Postrequisities} \subseteq \boldsymbol{Exploits} \times \boldsymbol{Privileges}$$

- Privileges related to attacker’s target
  - Prerequisites – allow exploitation
  - Postrequisites – result from a successful exploit

Bayesian Network

Graphical probabilistic model

$$BN = (DAG, Q)$$

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)

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

Derivation of Resilience Metric

Model of the security state

- BN – representation of the desired distribution
- The probability an attacker reaches mission-critical privilege
- The probability of relevant exploit

CPD calculation

- AND relation of parent’s nodes

$$p(X_i|parents(X_i)) = \prod_E p(e_i)$$

- OR relation of parent’s nodes

$$p(X_i|parents(X_i)) = 1 - \prod_E (1 - p(e_i))$$

Desired quantity from the distribution

- Marginalization of random variables (critical privileges)

$$p(X_a) = \sum_{(X_1,\ldots,X_{a-1},X_{a+1},\ldots,X_n)} \prod_{i=1}^{n} p(X_i|parents(X_i))$$

Quantification of Security State - Input Data

MulVAL tool

- Enumeration of hosts – mission decomposition model
- Presence of vulnerabilities – common vulnerability scanners
- Attacker ‘s position – intrusion detection alerts
- Attack goals – mission security requirement

Bayesian inference

- Annotated vulnerabilities – NVD
- Conditional probability distributions - CVSS exploitability score

Evaluation in Operational Environment

Operational environment

- Protection of Masaryk University network
- 40,000 users, 25,000 unique IP addresses

Mission examples

- Network monitoring (Net-Flow monitoring)

  probes (building premises OR connection points) **AND**

  collectors (primary OR secondary)
- Incident handling

  collectors (primary OR secondary) **AND**

  request tracker (single service) **AND**

  attack mitigating services (AND/OR, specific/redundant)

Evaluation in Operational Environment

Experimental implementation

- MulVAL tool, Neo4j graph database
- VM: 8 cores, 32 GB RAM

Evaluation metrics

- **Timing information:** input/run MulVAL, creation of Bayesian model, inference calculation
- **Number of processed entities:** vulnerable hosts, nodes/edges in AG

Sample results

- Significant differences between missions
- Private /public network segment, homogeneous components
- **Feasible for operational needs:** number of vulnerabilities < 60
- Calculation involving **essential processes in the Masaryk University network in a reasonable time**

Summary

Description of the proposed algorithm

- Based on introduced mission decomposition model
- Probabilistic model, probability as a measure of resilience
- Description of the experimental implementation
- Preliminary estimates, identification of practical limitations
- Feasible for operational needs

Future work

- Generalizing the proposed approach
- Issues of computational complexity
- Visualization/justification of decisions (avoid the operator using it as a black box)
- Issues dealing with an automated response

QUESTIONS?

THANKS FOR YOUR ATTENTION!

https://csirt.muni.cz

@csirtmu

Michal Javornik

javor@ics.muni.cz

CSIRT-MU