# Decision Support for Mission-Centric Cyber Defence

Michal Javorník
Institute of Computer Science
Masaryk University
Brno, Czech Republic
javornik@ics.muni.cz

Jana Komárková
Institute of Computer Science
Masaryk University
Brno, Czech Republic
komarkova@ics.muni.cz

Martin Husák
Institute of Computer Science
Masaryk University
Brno, Czech Republic
husakm@ics.muni.cz

## ABSTRACT

In this paper, we propose a novel approach to enterprise mission modeling and mission-centric decision support for cybersecurity operations. The goal of the decision support analytical process is to suggest an effective response for an ongoing attack endangering established mission security requirements. First, we propose an enterprise mission decomposition model to represent the requirements of the missions' processes and components on their confidentiality, integrity, availability. The model is illustrated in a real-world scenario of a medical information system. Second, we propose an analytical process that calculates mission resilience metrics using the attack graphs and Bayesian network reasoning. The process is designed to help cybersecurity operations teams in understanding the complexity of a situation and decision making concerning requirements on enterprise missions.

## CCS CONCEPTS

• **Security and privacy** → **Formal security models**; • **Networks** → **Network security**;

## KEYWORDS

Cyber situational awareness, Decision support, Attack graph, Bayesian network, Mission resilience

**ACM Reference Format:**
Michal Javorník, Jana Komárková, and Martin Husák. 2019. Decision Support for Mission-Centric Cyber Defence. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3339252.3340522

## 1 INTRODUCTION

As the IT infrastructures grow larger, it is more and more complicated to protect them and all their components. The insufficient workforce in cyber security and the risks of misunderstanding between security operations and management further underline the problem. The security teams are not always aware of all the missions in an organization, nor knowing about missions' priorities. Under such circumstances, the risk of unwanted actions rises. For example, dropping network traffic of an infected system interrupts operations of a critical IT system or one of its dependencies, which was not known to the security team. Thus, we need to explore new ways of transferring information from management to security operations to relief the security operation teams and help both the parties in a correct and efficient decision making.

A specific problem to be resolved is how to take enterprise missions into account when taking decisions in cybersecurity operations, such as impact assessment and incident response, including restrictive countermeasures. There is a need to reflect the missions, their supportive processes (assets), and their dependencies; and to evaluate and capture the mission requirements in terms of the CIA triad (confidentiality, integrity, availability). The key question is how to quantify the mission resilience, i.e., how likely can a particular enterprise mission supportive process be affected and to what extent. To answer this question, we need to conduct mission decomposition and impact assessment so that we could provide necessary cyber situational awareness for the decision support process.

The mission decomposition, i.e., clarifying mappings of processes via services to cyber components, should take into account the current cybersecurity situation and events that appear in the network operation process. In addition, it should clearly communicate cybersecurity risks and mitigation measures between different groups of involved stakeholders and prioritize the measures while factoring their individual needs, e.g., its cost-effectiveness. Further, it should enable recalculation of current mission security attributes, i.e., the probability of successful mission disruption and its extent regarding the CIA triad. The decision making support should be built on mission's ability of successful adaptation (reconfiguration) in the face of actual adversary activities. Based on the current security information and events from network operation process, it should enable quantitative security assessment and comparison of the mission's available configurations and identification of the most secure one. It should also give a clear message to mission security administrators and administrators of employed cyber components.

The paper contributions to state of the art could be summarized as follows. First, we present an approach based on Constraint Satisfaction Problem (CSP) to model enterprise missions and supportive entities, which connects an organization's missions and requirements on them with IT infrastructure. As a part of this task, we performed a case study and an empirical evaluation of our approach to illustrate its capabilities in today's critical application domains and its supportive infrastructures. The case study deals with a medical information system for processing and sharing medical images and involves geographically distributed user groups and networking environments, strict requirements on confidentiality, integrity, and availability of the data, and other distinct features. The proposed methodology was empirically evaluated for the model of this system. Second, we use the mission decomposition model as

*ARES '19, August 26–29, 2019, Canterbury, United Kingdom*

an input, along with abstract knowledge gained from a vulnerability database and impact scoring system to construct a Bayesian network based on attack graph and formulate a CSP that express the mission resiliency needs. Calculations based on the CSP and the Bayesian network are used to gain quantitative and qualitative situational awareness, which can be used for decision support with regard to enterprise missions.

This paper is divided into six sections. Section 2 summarizes related work. Section 3 provides the necessary theoretical background. Section 4 introduces the approach to enterprise mission decomposition and modeling based on constraint satisfaction abstraction logic and illustrates it on a case study of a medical imaging information system. Section 5 describes the analytical process that uses the mission decomposition model and leads to decision support. Section 6 concludes the paper and outlines future work.

## 2 RELATED WORK

The problems of impact assessment, mission resiliency, and decision support in cyber security are often referenced as parts of cyber situational awareness [6, 10]. Cyber situational awareness consists of three levels, perception, comprehension, and projection [6]. First, we have to perceive the elements in the current situation, e.g., enumerating hosts and vulnerabilities in the network, locating critical infrastructure, etc. Once done, we may proceed to comprehension, e.g., understanding what threats are the network and critical infrastructure facing. Finally, when the second is reached, we may project which threats are the most likely to lead to compromise or how would that impact an organization's missions. Similarly, the OODA loop formalizes the decision process in four steps, Observe, Orient, Decide, and Act [10]. First, we have to observe the situation and orient in it. Based on the gained knowledge, one may adequately decide how to react to such a situation, and act in a way that was decided [10].

Impact assessment can be found in numerous publications, either as a stand-alone research topic or as a part of a larger work. Porras et al. [17] discuss M-Correlator, a mission-impact-based approach to alert prioritization and aggregation. The objective of mission impact analysis is to aggregate related alerts into incidents and rank them based on the threat each incident poses to the operational mission. Their approach relies on expert knowledge of critical systems and of most concerning attacks classes to those assets. The attack impact assessment is very simple; for each alert, it takes into account the criticality of the target asset and whether the alert is of a type with a high threat to the asset. Valeur et al. [21] introduce a comprehensive alert correlation system that also contains an impact analysis component. To assess the impact, they require a service asset database, service heartbeat monitors, service dependencies, and service importance concerning the whole network. They determine the immediate impact of an attack by monitoring the services dependent on the attacks service, searching for those, that were negatively affected by the attack and computing the overall damage to the mission. They use the assessed impacts to prioritize the attacks for remediation. Their approach is very reactive as they do not consider the possible continuation of the attack as we intend to. Virtual Terrain Assisted Impact Assessment for Cyber Attacks (VTAC) [1] proposes an algorithm for impact assessment. It utilizes the Virtual Terrain model of the network and considers four impact types: host impact (the potential damage done to a host with respect to its services and their importance to the host), service impact (how potentially compromised a particular service is over a given network), user impact (how potentially damaged the hosts are that a particular user has accounts on), and network impact (how potentially damaged the entire network is with respect to the alerts received per its machines). It utilizes basic calculations to estimate the impact of the network. The disadvantages of the approach are that it heavily depends on the estimation of importance, and the calculations express more overall risk exposure to a network than the impact of an actual attack. Future Situation and Impact Awareness framework (FuSIA) [3] is a framework for estimating the impact based on plausible futures. The plausible futures are defined in terms of states of hosts in the network (normal, attacked, discovered, partially compromised, compromised). The current situation in the network can evolve into a plausible future by event happening (attacks). Several algorithms are proposed to search for plausible futures and combine the results into a single set of futures with re-computed plausibility scores. The two presented algorithms determine plausible futures based on an attacker's capability and based on a possibility to attack. Recently, Huang et al. [4] proposed a framework for assessing the impacts of cyber attacks in cyber-physical systems. The risk assessment is based on predicting cyber attack from conditional probabilities captured in a Bayesian network. The paper provides a solid theoretical foundation, although a presented case study is limited to a simulated industrial system.

Two works are of special importance for us as they focus on mission resiliency. Lewis et al. [12] focused on an assessment of the impact on mission resulting from cyber attacks. The authors introduce a reference model for impact assessment and situation projection, looks at the issue as a constraint satisfaction problem depicted as a constraint network. It incorporates apparatus from certainty factors theory as an alternative to Bayesian reasoning. Jakobson [7] gives a detailed description of the mission resiliency modeling issue. The mission resiliency system is modeled as two interacting processes: the process of mission operation situation management and the process of mission cyber defense situation management. The resilient cyber defense system is based on adaptable resilient mission-centric architecture, and mission adaptation policies.

Related work on decision logic focuses on finding optimal response actions to attack. They are meant as a base for automated defense. However, much of the reasoning behind optimal response action selection could be applied to assessing a response benefit. Lee at al. [11] explore the relevant cost factors, cost models, and cost metrics. The authors separate the cost into five categories: false negative cost (the damage cost due to successful intrusion by undetected attack), true positive cost (the disruption of the service caused by the response), false positive cost (the disruption of service and availability due to falsely detected legal traffic), true negative cost (always 0), and misclassified hit cost (the cost of reaction to a wrong type of attack). The categories are closely based on detection scenarios. Their approach points out the need to deal with uncertainty with input parameters. The Adaptive intrusion response using attack graphs (ADEPTS) [2] utilizes an I-Graph, the representation of possible attack graphs that captures the exploits, exploit

preconditions, and channels required for intrusion spreading. The optimal mitigation is the way to cut the channels that stops the attacker from gaining the goal and minimizes the cost of unavailability and the disruption of dependencies. However, to construct the I-Graph, the authors need a complete database of vulnerabilities, their descriptions, and complete system service description, including the dependencies. The model for response selection by Strasburg et al. [19] together with their previous work [20] focus on cost estimation of a response. They propose a structured and comprehensive methodology for estimating response cost. They divide the cost into three parts: response operational cost, response goodness and response impact on the system and provide a method how to compute the partial costs and combine the partial costs into the overall cost. Their approach requires a lot of human input and is not scalable. For common usage, their methodology should be extended by automated estimation of input parameters. Kheir et al. [9] describe the service dependency model and provide a complete methodology to use this model in order to evaluate intrusion and response costs. The authors search for responses with best Return-on-Response-Investment, which compares the benefit of the response with relation to the cost of its implementation. They state several propagation patterns in which they consider not only the damage caused by the propagation of dependency's functionality loss but also other types of propagation, such as the propagation of positive effects and propagation of the dependent service's compromise on its dependencies. The response selection model (REASSESS) [13] allows mitigating network-based attacks by incorporating a response selection process that evaluates negative and positive impacts associated with each countermeasure. The considered negative effects are the disturbance of the service caused by the action, which takes into account the importance of the service and the level of disturbance. The considered positive effects are the response success rate for a given response and alert. The concept of response success rate is interesting, because it does not require any deep theoretical analysis of dependencies and is based purely on the experience, however very imprecise in practice since networks change too often to derive any meaningful historical data.

# 3 THEORETICAL BACKGROUND

In this section, we provide the necessary theoretical background for our work. First, we introduce the constraint satisfaction problem. Second, we introduce attack graphs and their extensions based on Bayesian networks.

## 3.1 Constraint Satisfaction Problem

We use the constraint atisfaction abstraction modeling technique, i.e., finding values of involved variables satisfying relevant constraints, for representation (correct description of mission configuration knowledge, details for problem visualization, etc.) as well as for reasoning support, e.g., to provide explanations. Constraint Satisfaction Problem (CSP) is supposed to be expressed via three types of entities: variables, their associated domains, and constraints relating to them.

Formally speaking, CSP is defined as a triple $[X, D, C]$, where $X$ is a set of variables, $X_1, ..., X_n$; $D$ is a set of associated nonempty domains, $D_1, ..., D_n$; and $C$ is a set of constraints, $C_1, ..., C_m$. A set of possible values that can be assigned to variable defines the associated domain. The constraint specifies allowable combinations of variables' values. Every constraint $C_j$ consists of constraint scope, a subset of the variables, and a constraint relation over these variables, a subset of the Cartesian product of involved variables' domains. A state of the problem is defined as an assignment of values to some of the variables. So, searching for a problem solution corresponds to searching in the space of states. An assignment of values to all of the variables satisfying all of the constraints is called the solution of CSP. The issue of finding a solution is referred to as satisfiability of CSP.

Assuming that all the variables can be either true or false, then we are dealing with the so-called Boolean Constraint System. A Boolean CSP can be expressed as a Boolean formula. A Boolean formula is composed of Boolean variables and the operators: and, or, implication, bi-implication, not. Underlying mathematics says that any propositional logic formula can be transformed into so-called conjunctive normal form formula (conjunction of clauses, a clause is a disjunction of literals, literal is a variable or its negation, a variable can have a value of true or false).

## 3.2 Attack Graphs and Bayesian Networks

There are two formal models that we incorporated into our decision support process, attack graphs and Bayesian networks. Herein, we provide a necessary introduction into these two formalisms before we start with the description of our proposed process.

Attack graph is a graphical representation of an attack scenario that was introduced in 1998 by Phillips and Swiler [15] and quickly became a popular method of formal representation of cyber attacks and cybersecurity situation. Formally, an attack graph is a tuple $G = (S, r, S_0, S_s)$, where $S$ is a set of states, $r \subseteq S \times S$ is a transition relation, $S_0 \subseteq S$ is a set of initial states, and $S_s \subseteq S$ is a set of success states [18]. The initial state represents the state before the attack starts. Transition relations represent possible actions of an attacker. These are usually weighted, e.g., by the probability that the attacker will choose the action. If an attacker takes all the actions to transition from an initial state to any of the success states, the attack is successful, as the success states represent a system compromise [5]. A recent comprehensive taxonomy of attack graph generation and usage was proposed by Kaynar [8].

From a practical perspective, the overview of attack graph tools was given by Yi et al. [22]. The authors provide a comparison and analysis of both open source and commercial tools. The most convenient tool for our needs is MulVAL (Multihost, multistage, Vulnerability Analysis) [14], a framework conducting vulnerability analysis on a network. It comprises of scanners, that run on each host, and an analyzer that processes the scan results and the information about the vulnerability. Its main advantages are that it can process vulnerability specification from publicly available sources automatically, and the complexity of the algorithm for building an attack graph is polynomial. The information about vulnerability effects was taken from ICAT database that categorized the vulnerability impact into four categories: confidentiality loss, availability loss, integrity loss, and privilege escalation. From those categories, only

availability loss and privilege escalation are considered in the framework. The vulnerabilities are detected by running OVAL-scanner on each host in the network. To achieve a polynomial complexity of attack graph generation, logic programming and reasoning rules are used to express the compromise propagation, the exploitability of host, and network access.

While attack graphs serve well in describing the attack scenarios and state transitions comprehensively, they miss the aspect of probability and conditional variables. For this purpose, researchers adopted Bayesian networks, probabilistic graph models that represent the variables and the relationships between them in the form of an acyclic graph with nodes as the discrete or continuous random variables and edges as the relationships between them. The nodes maintain the states of the random variables and conditional probability form.

There are several equivalent definitions of a Bayesian network. Bayesian network is usually represented as a directed acyclic graph (DAG). Each node represents a variable that has a certain set of states. The edges represent the causal relationships between the nodes. Formally, let $G = (V, E)$ be a DAG, and let $X = (X_v)_{v \in V}$ be a set of random variables indexed by $V$. A Bayesian Network consists of a set of variables and a set of direct edges between variables. Each variable has a finite set of mutually exclusive states. The variable and direct edge form a DAG. To each variable $A$ with parents $B_1, B_2 ... B_n$, there is attached a conditional probability table $P(A|B_1, B_2 ... B_n)$.

Bayesian networks can be constructed from attack graphs. The so-called Bayesian attack graphs were investigated in details by Poolsappasit et al. [16]. The authors proposed a method to estimate an organization's security risks using the metrics defined in CVSS and an attack graph extended by likelihoods of exploiting relationships between the attack graph's nodes. The processes of static and dynamic risk assessment are proposed, along with a generation of security risk mitigation plans.

## 4 MISSION DECOMPOSITION

In this section, we introduce our approach to enterprise mission decomposition and modeling based on constraint satisfaction abstraction logic. First, we introduce the constraint satisfaction problem as a theoretical background for our work. Subsequently, we discuss modeling of the enterprise mission based on CSP. Finally, we illustrate the concept in a case study of a medical imaging information system.

### 4.1 Mission Decomposition Model

We have decided to model mission's configurations and related reasoning as a CSP or specifically as a Boolean CSP. An enterprise mission can be decomposed into relevant supportive processes. Mission supportive processes are considered as key assets to be protected. Individual supportive processes can be mapped into relevant supportive IT services, and they can consequently be mapped into supportive cyber components and their specific interactions. We assume that enterprise missions can be accomplished in many ways, i.e., reflecting current mission goals (functional and security requirements), we are considering more alternatives to enterprise mission configuration. Communication needs of a particular mission configuration are posed to the communication requirements of employed cyber components and expressed in cyber terms. Mission decomposition rules are expressed via special AND/OR nodes and relevant edges in the graph representation. The AND/OR notation is inspired by the work of Jakobson [7]. The model especially enables expression of initial confidentiality, integrity, and availability (CIA) requirements for every individual mission supportive process as well as mapping of those requirements to relevant cyber components.

Enterprise missions are considered in four dimensions: mission functional requirements, mission security requirements, mission operational configuration, and mission resilience. An enterprise mission can be formally described as a system of functional requirements. Desired functionalities are based on individual mission supportive processes and consequently on individual IT services and cyber components, respectively. Regarding the security, an enterprise mission can be formally described as a system of security requirements (expressed as desired levels of confidentiality, integrity, and availability) based on individual mission supportive processes and consequently on individual IT services and cyber components, respectively. Mission operational configuration must be in line with actual mission functional and security requirements and be expressed as a specific configuration of mission supportive entities and their specific interactions. Mission configuration alternatives are expressed via special AND/OR nodes and controlled by AND/OR logic. AND-node in a particular mission configuration requires the presence of all of its children nodes representing its supportive IT services and cyber components, respectively. OR-nodes express the options of mission reconfiguration as it requires the presence of at least one of its children nodes representing its supportive IT services and cyber components, respectively. Mission resilience is its ability to continue to operate while maintaining the required operational capabilities (desired functional and security requirements) in the face of current adversary activities, its ability to achieve the mission's current objectives. Mission resilience depends upon the resilience of its supportive cyber components.

An example of a system modeled using our proposed approach can be seen on Figure 1. Further information on the modeled system and the process of modeling it can be found in the following subsection. The resulting logical formula representing the satisfying configurations for the model in a given use case is presented in Figure 2. The usage of the formula is described in Section 5.

### 4.2 Case Study: Regional Medical Imaging

To illustrate our proposed approach, we describe a case study of mission decomposition model of a part of a regional medical imaging system that enables region-wide collaboration of healthcare service providers. First, we briefly describe the domain and the system. Subsequently, we describe a mission decomposition model of the system based on the approach presented previously.

The medical imaging domain consists of a spectrum of mutually interconnected activities, the spectrum of individual collaborative processes across many healthcare service providers. The supportive IT environment is composed of domain-specific applications running on specially configured computer networks. Predefined rules

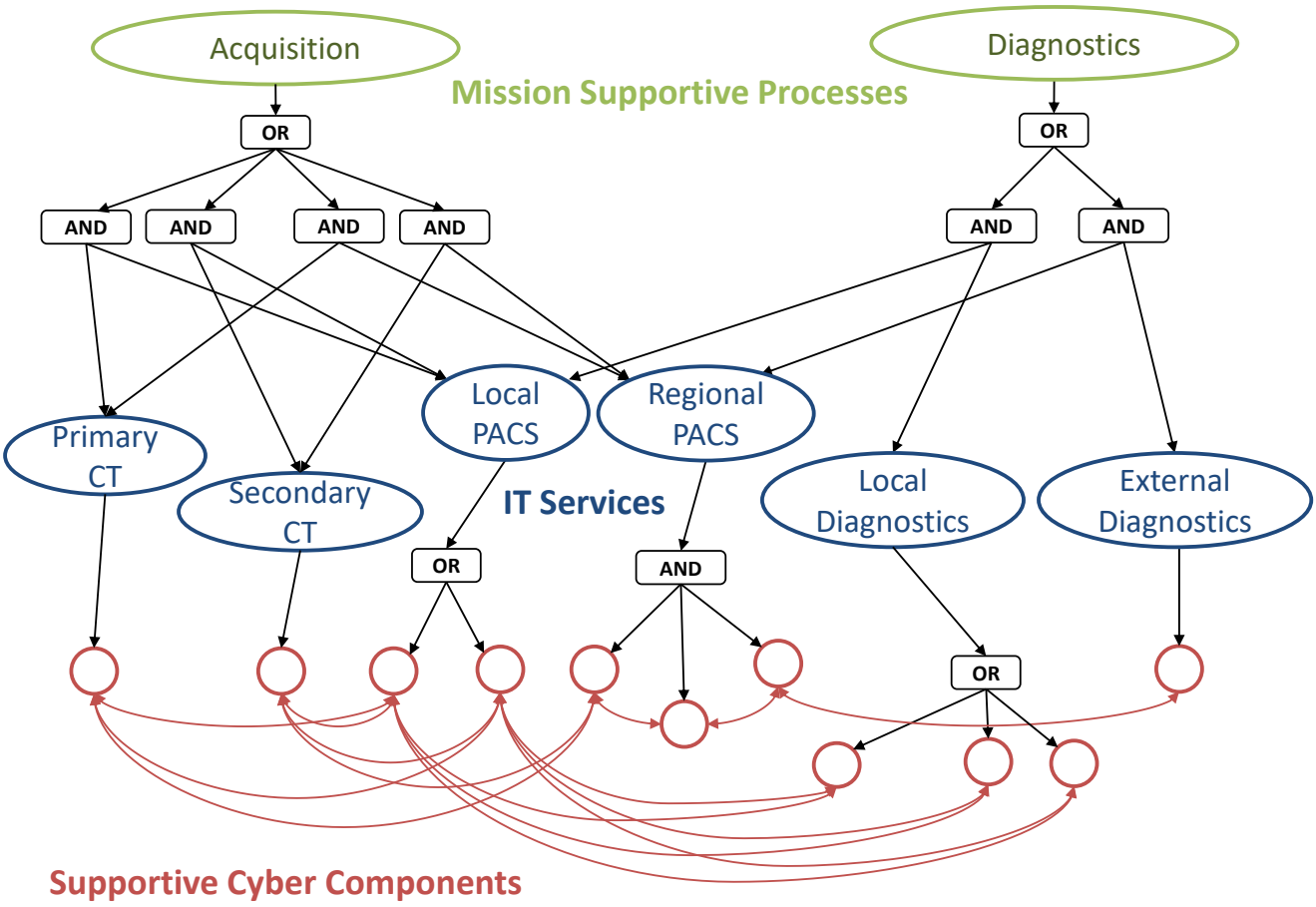


**Figure 1: Example of mission decomposition model.**

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

**Figure 2: Logical formula representing the satisfying mission configurations.**

describing all possible operational constellations of the mission in line with functional and security requirements posed to individual supportive processes constitute the basis of the model. The security requirements posed to individual processes reflect the legal, ethical, contractual or other issues. They are expressed as required levels of confidentiality, integrity, and availability.

The core mission supportive processes in the area of medical imaging are especially processes of patient examinations (specific CT, MRI, roentgen examinations, mammography screening, etc.), emergency consultations (neurology, cardiology, etc.), daily routine of hospital's departments dependent on image information, expert consultations (oncology, mammography, etc.), and others. Supportive processes are being built on domain-specific IT services like services of medical image data acquisition, institutional or regional Picture Archiving and Communication System (PACS), services for exchange and sharing of image data between individual hospital departments and other cooperating healthcare institutions, services necessary for medical image examinations' diagnostics, etc. The subsystem of supportive cyber components consists of a spectrum of domain-specific products of many vendors: particular implementations of PACS, software components for controlling of acquisition modalities, software for special medical image data processing, software for specific diagnostic purposes, etc. Cyber components communicate via a spectrum of medical domain-specific communication protocols reflecting the functional requirements of the mission.

Next, we describe the scene of a trauma center. The center is equipped with two computed tomography (CT) scanners placed in the CT control room. CT-scanner is generally considered as mandatory equipment of trauma centers, especially for patients who had suffered from multiple traumas. The image examinations are mostly diagnosed locally, but there is also a possibility the examinations to be diagnosed remotely, so a radiologist to perform an image analysis does not need to be present at a trauma center. Trauma center's critical processes are based on supportive services alternatively provided by other institutions.

Two critical processes are forming the trauma center's mission. The first one is the acquisition process, labeled *Acquisition*, consisting of performing CT examinations and pushing the acquired image datasets to the communication system PACS to be accessible for additional processing. The second one is the diagnostics process, labeled *Diagnostics*, consisting of querying and retrieving medical image examinations from archiving and communication system PACS and performing desired diagnostics.

The two processes are based on the following supportive IT services: services of medical image data acquisition, labeled *PrimaryCT* and *SecondaryCT*, services for secure image data communication within trauma center or between distant healthcare institutions in the region, labeled *LocalPACS* and *RegionalPACS*, and services of local and external diagnostics of CT examinations, labeled *LocalDiagnostics* and *ExternalDiagnostics*. The IT services are based on the following software components: software controlling the image acquisition and forwarding the acquired data to PACS, labeled *Acquisition_PrimaryCT* and *Acquisition_SecondaryCT*, software implementations of primary and secondary instances of LocalPACS service, labeled *PrimaryInstance_LocalPACS* and *SecondaryInstance_LocalPACS*, software components implementing local or remote proxies of RegionalPACS service, labeled *LocalProxy_RegionalPACS* and *RemoteProxy_RegionalPACS*, software components implementing central node of RegionalPACS service, labeled *CentralNode_RegionalPACS*, software components implementing primary or secondary local diagnostic viewers, labeled *PrimaryViewer_LocalDiagnostics* and *SecondaryViewer_LocalDiagnostics*, software component implementing remote diagnostic viewer, labeled *RemoteViewer_ExternalDiagnostics*.

## 5 DECISION SUPPORT PROCESS

In this section, we describe the concept of an analytical process that utilizes the mission decomposition model and leads to decision support. The basic starting point is the determination of a set of constraints defining potential solutions and the determination of utility functions expressing the interests of decision makers. We are searching for a (semi)optimal solution of complex decision-making problem. The goal is to propose mitigating steps and give an explanation of the steps to network security administrators and other relevant decision makers.

The continuous decision support process is depicted in Figure 3 and consists of three phases:

(1) The first phase is the construction of the mission decomposition model described in Section 4 and is executed only once. The formal description of satisfying mission configurations forms the basis for additional mathematical modeling. See Figures 1 and 2 for examples. The model and formula are used in the following phases as static information.
(2) The second phase deals with representing the current security situation. It uses the mission decomposition model along with mathematically expressed constraints defining satisfying mission configurations; it employs the techniques of attack graphs and Bayesian networks as well as the abstract knowledge on cyber threats and the attacker's position to generate resulting Bayesian attack graphs.
(3) The third phase integrates the static output of the first phase and the dynamic output of the second phase. It identifies the resulting optimal reconfigurations of the cyber components with respect to mission resilience and countermeasures against cyber threats.

The recommendation of a configuration of the system that reflects the current security situation and mission constraints is the output of the whole process. The recommended configuration should then be set up manually or automatically. However, the change of configuration changes the current situations, which returns the process into the second phase. The backward arrow in the schema in Figure 3 depicts the undertaken decision that caused changes in the mission's supportive computer networks configuration. As a result, the second and third phases can be iterated indefinitely.

### 5.1 Representation of the Current State

Representation of the current state represents the second phase of the process. It consists of generating a Bayesian attack graph (BAG)

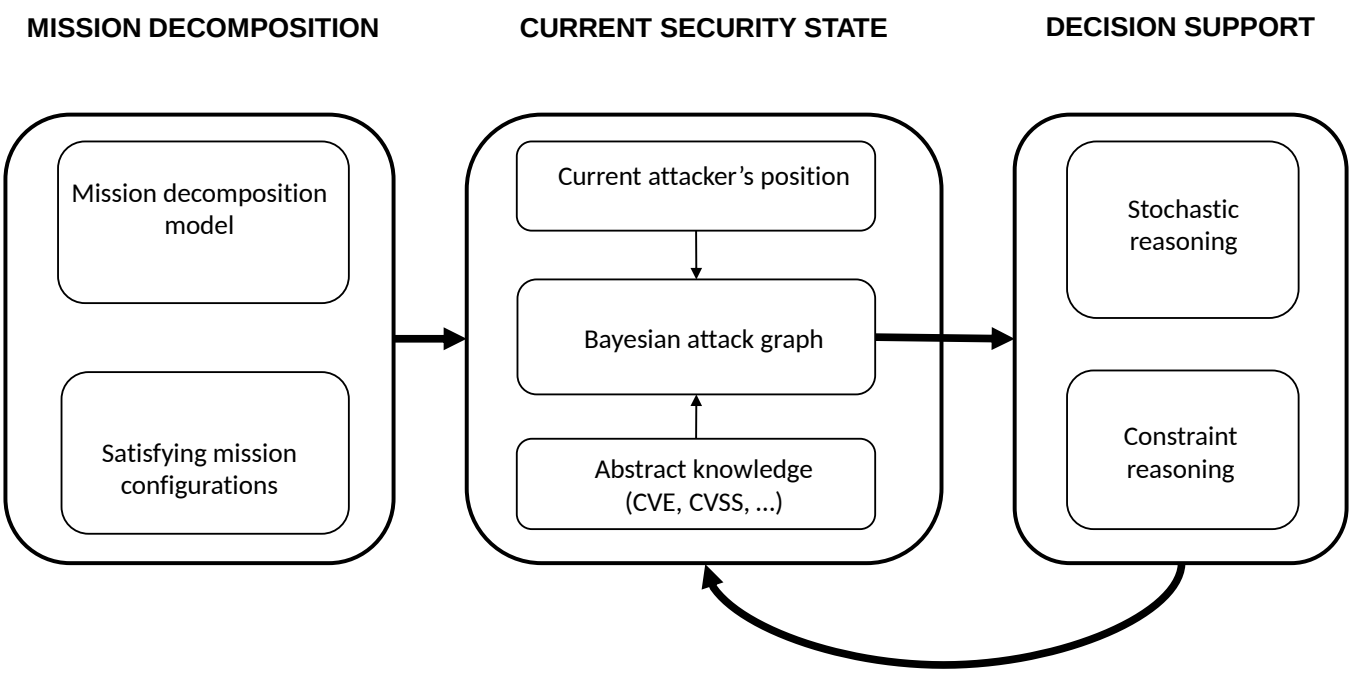


**Figure 3: Phases of the analytical process for decision support.**

from the static mission decomposition model provided by the first phase (see Section 4) and dynamic abstract knowledge consisting of information on threat vectors and the attacker's position. Integrating the attacker's position into the process requires collaboration with intrusion detection systems and corresponds to the position of an attacker in the attack graph and the procedure of actions the attacker already executed.

The abstract knowledge of threats can be represented in numerous ways and obtained from various sources. Herein, we propose using the information on vulnerabilities from publicly available sources, such as NVD[1], a de facto standard library of vulnerabilities in CVE format, or various vulnerability databases maintained by software vendors or security specialists. Vulnerabilities in CVE are accompanied by CVSS[2], a scoring system that characterizes the attack complexity and impact of vulnerabilities in terms of confidentiality, integrity, and availability (CIA triad). CVSS database, as publicly accessible trusted information source, provides us with quantitative characteristics necessary for attack graph building and Bayesian network reasoning. Especially Attack Complexity as specific security metric and Impact Metrics referring potential impact (regarding CIA consequences for given cyber component) of a successful exploit of a given vulnerability, i.e., privileges an attacker will obtain as a consequence of a successful exploit. So, employing CVSS Attack Complexity security metric (interpreted as the conditional probability of successful exploit) enables computation of unconditional probabilities of successful multi-step attack and exploits of mission-critical vulnerabilities.

To sum up the second phase, the particular steps goes as follows. First, we generate the attack graph from available data, mission decomposition model, and abstract knowledge. Mission decomposition model provides a list of IT systems for which we find vulnerabilities and weaknesses in NVD. The generation of the attack graph could be achieved by MulVal [14]. Second, we take the attack graph generated by MulVal and convert it into the Bayesian attack graphs. The process will create an attack graph where leafs corresponding to vulnerabilities have a probability equal to exploitability score from CVSS. The structure of the attack graph is not changed in this step; only the probabilities are updated. As a result of the two steps, we have a model of the static security situation, including mission view. If appropriate data are available, we can insert the attacker's position into the attack graph. This could be achieved in cooperation with an intrusion detection system or similar tool that can report exploitation of a vulnerability or similar event. The attack graph and Bayesian attack graphs should be recalculated if needed. As an output, we have a Bayesian attack graph that represents the current security situation. The evaluation is performed in the third phase.

## 5.2 Decision Support

In the third phase, we take the outputs of previous phases and choose the optimal (the most resilient) mission configuration using the sound mathematical grounding of constraint satisfaction problem and Bayesian networks. More mathematically formulated: "considering the stochastic nature of the issue and the explicitly formulated mission's configuration constraints, we optimize utility function expressing the interests of decision makers." Bayesian networks allow us to quantify the desired likelihood of successful exploit of vulnerabilities of the given cyber component in the network. In other words, they allow us to calculate the unconditional

[1]National Vulnerability Database, https://nvd.nist.gov/
[2]Common Vulnerability Scoring System, https://nvd.nist.gov/vuln-metrics/cvss

probability of an adversary exploits the system. The constraint reasoning uses the logical expression to check which configurations of the system preserve its functionality if countermeasures are taken to mitigate the threats calculated by the stochastic reasoning.

The proposed approach helps us to understand and measure the vulnerability of an enterprise mission as the likelihood of successful exploit of those left vulnerabilities which are critical for our mission. Nevertheless, the final decision on countermeasures and reconfigurations of the system are in the hands of human operators.

## 6 CONCLUSION

In this paper, we proposed a novel approach to decision support for cyber defense that takes enterprise missions into account. First, we proposed an enterprise mission decomposition model employing constraint satisfaction mathematical abstraction formally describing mission requirements as well as complex relationships between mission supportive entities. The model was supported by a case study of a regional medical imaging system for which we created the model. Subsequently, we proposed an analytical process that takes the mission decomposition model and abstract knowledge of cyber attacks to generate the stochastic model of the security situation that can be used to provide decision support to security operations. The combination of the mission decomposition model and analytical process allows for making decisions, such as system reconfiguration and access restriction, with respect to the importance and requirements of the underlying IT systems to enterprise missions. Proposed analytical framework (especially underlying stochastic model) covers the complex relationships of a real-world situation which are necessary for quantification of the situation. It enables to count useful quantitative characteristics: the unconditional probability of mission disruption (successful exploit of critical vulnerabilities of mission operational configurations), prioritization of security-related steps, dynamic categorization of cyber components, etc.

In our future work, we are going to implement the tools to perform the proposed decision support process. Subsequently, we want to evaluate our approach on a real-world IT system, such as the medical information system that we already used for mission decomposition, as well as in a simulated scenario. In the first case, we want to evaluate the feasibility of our approach in practice. In the second case, we want to create a benchmark for further optimization. Further, we want to evaluate the feasibility of automated decision making in cyber defense, so that we may relief human operators in their duties even more.

## ACKNOWLEDGMENTS

This research was supported by the Security Research Programme of the Czech Republic 2015 - 2020 (BV III / 1 VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20172020070 Research of Tools for Cyber Situational Awareness and Decision Support of CSIRT Teams in Protection of Critical Infrastructure.

## REFERENCES

[1] Brian Argauer and Shanchieh Jay Yang. 2008. VTAC: virtual terrain assisted impact assessment for cyber attacks. In *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security*.
[2] Bingrui Foo, Y-S Wu, Y-C Mao, Saurabh Bagchi, and Eugene Spafford. 2005. ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*. IEEE, 508–517.
[3] Jared Holsopple and Shanchieh Jay Yang. 2008. FuSIA: Future situation and impact awareness. In *Information Fusion, 2008 11th International Conference on*. IEEE, 1–8.
[4] Kaixing Huang, Chunjie Zhou, Yu-Chu Tian, Shuanghua Yang, and Yuanqing Qin. 2018. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems. *IEEE Transactions on Industrial Electronics* 65, 10 (Oct 2018), 8153–8162.
[5] Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda. 2019. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Communications Surveys Tutorials* 21, 1 (Firstquarter 2019), 640–660.
[6] Sushil Jajodia, Peng Liu, Vipin Swarup, and Cliff Wang. 2010. *Cyber situational awareness*. Vol. 14. Springer.
[7] Gabriel Jakobson. 2014. *Mission Resilience*. Springer International Publishing, Cham, 297–322.
[8] Kerem Kaynar. 2016. A taxonomy for attack graph generation and usage in network security. *Journal of Information Security and Applications* 29 (2016), 27–56.
[9] Nizar Kheir, Nora Cuppens-Boulahia, Frédéric Cuppens, and Hervé Debar. 2010. A Service Dependency Model for Cost-Sensitive Intrusion Response. In *Computer Security – ESORICS 2010*. Springer Berlin Heidelberg, Berlin, Heidelberg, 626–642.
[10] Alexander Kott, Cliff Wang, and Robert F. Erbacher. 2015. *Cyber defense and situational awareness*. Vol. 62. Springer.
[11] Wenke Lee, Wei Fan, Matthew Miller, Salvatore J. Stolfo, and Erez Zadok. 2002. Toward cost-sensitive modeling for intrusion detection and response. *Journal of computer security* 10, 1-2 (2002), 5–22.
[12] Lundy Lewis, Gabriel Jakobson, and John Buford. 2008. Enabling cyber situation awareness, impact assessment, and situation projection. In *MILCOM 2008 - 2008 IEEE Military Communications Conference*.
[13] Sven Ossenbühl, Jessica Steinberger, and Harald Baier. 2015. Towards automated incident handling: How to select an appropriate response against a network-based attack?. In *IT Security Incident Management & IT Forensics (IMF), 2015 Ninth International Conference on*. IEEE, 51–67.
[14] Xinming Ou, Sudhakar Govindavajhala, and Andrew W Appel. 2005. MulVAL: A Logic-based Network Security Analyzer. In *USENIX Security Symposium*. Baltimore, MD, 8–8.
[15] Cynthia Phillips and Laura Painton Swiler. 1998. A Graph-based System for Network-vulnerability Analysis. In *Proceedings of the 1998 Workshop on New Security Paradigms (NSPW '98)*. ACM, New York, NY, USA, 71–79.
[16] Nayot Poolsappasit, Rinku Dewri, and Indrajit Ray. 2012. Dynamic Security Risk Management Using Bayesian Attack Graphs. *IEEE Transactions on Dependable and Secure Computing* 9, 1 (Jan 2012), 61–74.
[17] Phillip A. Porras, Martin W. Fong, and Alfonso Valdes. 2002. A mission-impact-based approach to INFOSEC alarm correlation. In *International Workshop on Recent Advances in Intrusion Detection*. Springer, 95–114.
[18] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M. Wing. 2002. Automated generation and analysis of attack graphs. In *Security and privacy, 2002. Proceedings. 2002 IEEE Symposium on*. IEEE, 273–284.
[19] Chris Strasburg, Natalia Stakhanova, Samik Basu, and Johnny S. Wong. 2009. A framework for cost sensitive assessment of intrusion response selection. In *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International*, Vol. 1. IEEE, 355–360.
[20] Christopher Roy Strasburg, Natalia Stakhanova, Samik Basu, and Johnny S. Wong. 2008. The methodology for evaluating response cost for intrusion response systems. *Computer Science Technical Reports* 199 (2008).
[21] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Richard A. Kemmerer. 2004. Comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on dependable and secure computing* 1, 3 (2004), 146–169.
[22] Shengwei Yi, Yong Peng, Qi Xiong, Ting Wang, Zhonghua Dai, Haihui Gao, Junfeng Xu, Jiteng Wang, and Lijuan Xu. 2013. Overview on attack graph generation and visualization technology. In *Anti-counterfeiting, security and identification (asid), 2013 ieee international conference on*. IEEE, 1–6.