Received: 13 December 2021 | Revised: 12 May 2022 | Accepted: 15 May 2022

DOI: 10.1002/eng2.12538

RESEARCH ARTICLE

Engineering Reports Open Access WILEY

Mission-centric decision support in cybersecurity via Bayesian Privilege Attack Graph

Michal Javorník | **Martin Husák**

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

Correspondence
Martin Husák, Institute of Computer Science, Masaryk University, Šumavská 416/15, 602 00 Brno, Czech Republic.
Email: husakm@ics.muni.cz

Funding information
European Regional Development Fund, Grant/Award Number: CZ.02.1.01/0.0/0.0/16_019/0000822

Abstract

We present an approach to decision support in cybersecurity with respect to cyber threats and stakeholders' requirements. We approach situations in which cybersecurity experts need to take actions to mitigate the risks, such as temporarily putting an IT system out of operation, but need to consult them with other stakeholders. We propose a decision support system that uses a mission decomposition model representing the organization's functional and security requirements on its IT infrastructure. Based on the cybersecurity state assessment, that is, discovery of vulnerabilities and attacker's position, the decision support system calculates the resilience metrics for each IT infrastructure's configuration, that is, how likely are they to not be disrupted. The calculation is enabled by two novel formal models, Privilege-Exploit Attack Graph and Bayesian Privilege Attack Graph, which reduce complex attack graphs into a comprehensible bipartite graph. Moreover, they illustrate the impact of exploiting the vulnerabilities and attackers gaining the privileges. The system recommends the most resilient mission configurations that are comprehensible to both cybersecurity experts and non-technical stakeholders, who may then choose which configuration to apply. Our approach is illustrated in a case study of a real-world medical information system.

KEYWORDS

attack graph, Bayesian network, cybersecurity, decision support, enterprise mission

JEL CLASSIFICATION

Computer and software engineering

1 | INTRODUCTION

With the IT infrastructures growing larger and more complex, it becomes increasingly complicated to protect them, eliminate all their vulnerabilities, react to every new threat, and be prepared to face every possible attack scenario, especially with the scarce workforce in cybersecurity nowadays. Such circumstances create a need for automation and support in decision-making.[1,2] Moreover, cybersecurity incident response teams and security operations centers

(CSIRT/CERT/SOC) are not always aware of the priorities of the organization they protect. In other words, they lack so-called cyber situational awareness, that is, the perception of the elements in the cyber environment, the comprehension of their meaning, and the projection of their status.[3] For example, a security team may, in good faith, put an infected machine out of operation and, thus, unwillingly interrupt operations of a critical system or its dependency. Cybersecurity operators would benefit from systems that would increase their cyber situation awareness.[2] However, collaboration with other stakeholders in the organization is essential. The cybersecurity experts need to come to an understanding with the organization's management and users and administrators of critical IT infrastructure.[4]

In our work, we assume two prerequisites. First, the organization operating an IT infrastructure has its mission or business objectives, which put functional requirements on the IT infrastructure. Second, there are multiple alternative configurations of the infrastructure that fulfill the requirements. For example, the organization relies on an information system that exists in two instances, and at least one of the instances needs to be running. Under such assumptions, we approach two specific problems. The first is the decision support of cybersecurity experts in terms of selecting the most resilient configuration of the IT infrastructure so that they can mitigate threats and reduce the risks. The second is the need to involve other stakeholders in the decision-making and select the option that is effective in mitigating cyber threats and does not disrupt the enterprise mission and related requirements. In a typical scenario that we consider in our work, the cybersecurity experts discover a major vulnerability that requires some IT services to be put out of operation before a patch is available. However, disconnecting all such services would disrupt the organization's mission because the services are essential to the organization. If possible, alternative services without the vulnerability could be used instead of the vulnerable ones; otherwise, it may be worth taking the risk and continuing using the vulnerable services instead of disrupting the mission. While the cybersecurity experts may quantify the risks, it is usually up to the other stakeholders, such as management or users of critical systems, to make the final decision. Thus, there is a need to involve both cybersecurity experts and non-technical stakeholders in the decision-making process and consider both cyber risk and impacts on enterprise mission in the calculation of the infrastructure's resilience. More formally, the key research question for this article is how to transparently quantify the resilience of an enterprise mission (with respect to an ongoing or potential attack) and determine optimal mitigation measures in the presence of multiple critical targets and incomplete information about the current position of the attacker.

To resolve the outlined issues, we propose a mission-centric decision support system for cybersecurity operations that also facilitates understanding between the cybersecurity experts and other stakeholders. We use a mission decomposition model from our previous work[4] that represents the enterprise mission, its supporting IT services, and their components, thus enumerating the services the organization depends on and stating the objectives that must be achieved despite the presence of threats.[5] Moreover, the mission's security requirements are included, representing the impact of a successful compromise or disruption in terms of loss of confidentiality, integrity, and availability (CIA).[4] The decision support system also relies on cybersecurity state assessment processes that enrich the mission decomposition model with the information on vulnerabilities found in the network and enumerate the hosts and services that are or are suspected to be under the control of an attacker. Common tools, such as vulnerability scanners and intrusion detection systems, can be used for this purpose, and our proposed approach is independent of the tools in use. The decision support system reacts to changes in cybersecurity state assessment and calculates the resiliency metrics for all possible configurations of the IT infrastructure that enable the enterprise mission with respect to current vulnerabilities and the attacker's position. The most currently resilient configurations are recommended to the users, that is, cybersecurity experts and other stakeholders, who may then choose the optimal configuration to implement.

Let us briefly introduce the main concepts and theoretical background of our approach. We formalize the concept of multi-step and multi-target attacks by introducing the auxiliary structure of the Complex Privilege-Exploit Attack Graph and the resulting structure of the Bayesian Privilege Attack Graph. The resulting structure is a standard Bayesian network that models the causal relationships among trust levels over the set of mission-related privileges. Its semantics, where nodes represent the level of trust to the legitimate users of the mission, is well understood by the decision-makers. It is up to them whether they apply the recommended defense strategy or use the calculated resilience values of alternative mission configurations to apply a different strategy. By analogy, the model allows us to determine the most effective defense (compute the most resilient configuration) for an arbitrarily chosen subset of critical targets. To understand the mathematics behind the model, a deeper background in probability theory is necessary. The resulting Bayesian network compactly represents the joint probability distribution of random variables of interest, quantifying the mission security state. To do this, that is, to quantify the resilience of a given mission configuration, we need to recalculate the posterior distribution of desired variables representing the critical privileges using the prior distribution and having the probability distribution of the variables representing the current (observed or estimated) position of the attacker.

The use of our proposed decision support system is illustrated in a real-world case study of a medical information system, which uses a combination of local and remote IT services to support medical image data acquisition and diagnostics. We show how a vulnerability of a local machine or a reported breach of a remote service jeopardizes the resilience of the whole infrastructure. The requirements for confidentiality, integrity, and availability in medical information systems are high, but so are the operational requirements posed by the medical staff.[6] Thus, we may illustrate the issues of decision-making in scenarios in which the most resilient configuration (from the cybersecurity perspective) is incompatible with the demands of the users.

This article is divided into five sections. Section 2 summarizes the related work and highlights the main differences from our approach. Section 3 outlines the decision support system, including the mission decomposition model, cybersecurity state assessment, calculation of mission resilience, and final decision making. Section 4 presents a case study of the experimental deployment of the proposed system in an operational setting of a regional medical imaging system. Section 5 concludes the article and outlines the directions for future work.

2 | RELATED WORK

In this section, we summarize related work on the main topics of this article. First, we discuss the mission-centric approach to cybersecurity and its two crucial tasks, mapping assets to the mission and mission-centric impact assessment. Second, we discuss related work using attack graphs and Bayesian networks, two fundamental models used in this work. Finally, we provide an overview of related work on decision support in cybersecurity. In each subsection, we provide a commentary on the main differences between our approach and related work.

2.1 | Mission-centric cybersecurity

Mission-centric cybersecurity consists of two main tasks, mapping mission-supportive cyber assets to enterprise mission or business processes and assessing the impact of a cyber attack on a mission. Such a mapping allows assessing risk or impact to the mission, not only the cyber assets, as it is traditionally perceived.[5] There is a need to enumerate the cyber assets that support a mission and describe its dependencies. The impact assessment has been the subject of cybersecurity research for a long time and can be found in a plethora of publications as a stand-alone research topic or part of a broader work.

Earlier works on this topic emerged from alert correlation. For example, Porras et al.[7] presented M-Correlator, a mission-impact-based approach to prioritize and aggregate alerts. The objective of their work is to aggregate related alerts into incidents and rank them by the threat they pose to the mission. Such an approach relies on the detailed knowledge of the protected systems and most critical threats. The impact assessment is straightforward; an alert is ranked higher if the target asset has high criticality and if the threat associated with the alert type is high. Valeur et al.[8] introduced a comprehensive system for alert correlation that contains an impact analysis component. The immediate impact of an attack is determined by observing the services dependent on the attacked service and estimating the mission disruption.

The Cyber Assets, Missions, and Users (CAMUS)[9] is a proof of concept system that allows for automatic mapping of cyber assets to the missions and users. The entities of users, missions, cyber assets, and cyber capabilities are extended by detailed information about them, such as the user's role in the organization or a workstation the user often uses. The detailed structure of the model was described by Buchanan,[10] and further developments were presented at the Mission Impact Workshop.[11]

In other related works, Musman et al.[12] investigated an approach to a cyber mission impact assessment on the example of military missions. The authors used a business process modeling notation to model the missions. Their model captures the dynamic, temporal, and sequential nature of a mission. They measured the impact as a change to the mission's measure of effectiveness, which is caused by the effects of a cyber attack on information technology. Sun et al.[13] presented a mission-task-asset (MTA) map, which is used to associate the mission and tasks with assets, and a system object dependency graph (SODG) that captures intrusion propagation at the operating system level. The authors used a Bayesian network to leverage the data from the SODG and quantify the impact on the mission represented in MTA. Lei[14] discussed the role of cyber situational awareness in achieving mission resilience and proposed a framework in which the cyber terrain must ensure the continuity of a mission before, during, and after an attack. The impact dependency graph is used for mission impact assessment. Similarly, Guion and Reith[15] discussed mapping the missions to cyber terrain consisting of systems, devices, data, software, processes, personas, and other entities. The control of such entities is considered an advantage for the attacker or defender, and the authors propose to leverage it in impact assessment. Silva and Jacob[16] pointed out the need to switch from threat-centric and vulnerability-centric to mission-centric approaches and proposed a mission-centric risk assessment methodology. First, they model the enterprise missions and assets and relations between them and specify risk measurement criteria. Subsequently, they identify threats and their impact on the assets to estimate the risk of mission violation.

The work of Gabriel Jakobson and his colleagues is the direct inspiration for our work. First, Jakobson and Buford[17] focused on an assessment of the impact on the mission resulting from cyber attacks and the projection of possible attacks. The authors introduced a reference model for impact assessment and situation projection and approached the issue as a constraint satisfaction problem in a constraint network. Their work incorporates apparatus from the certainty factors theory as an alternative to the Bayesian reasoning used in our work. Later, a conceptual graph was introduced to capture the relationship between cyber attacks and the mission impact.[18] The conceptual graph was used to infer plausible future cybersecurity situations.[19] Both works consider a model of a cyber terrain that has the capacity to support a mission. The capacity is decreased by cyber attacks. Another paper discusses the shift from IT-centric to mission-centric cybersecurity and proposes fundamental principles and architectures.[5] The research was summarized in a book chapter on mission resilience and enabling technologies.[20]

In recent years, cyber resilience aligning cybersecurity with business continuity is becoming a new cybersecurity paradigm. Based on the information about the system and the attacker's footprint, Huang et al.[21] presented a response mechanism that includes the design of optimal resilience strategies and security reconfiguration of the cyber system to minimize the further risk of attack while maintaining critical functions and performances. Similarly, Hutschenreuter et al.[22] presented a resilience strategy that guarantees business continuity even during cyber incidents. They introduced a resilience framework combining a cyber attack detection system with ontologies and an inference system that automates not only the detection of cyber incidents but also the response and recovery phases. Zhang and Malaccaria[23] provided a strong mathematical foundation for analyzing an organization's time resilience to cyber attacks. They introduced a mathematical framework combining Markov chains with attack graphs to help an organization determine a security plan, that is, to select the optimal portfolio of security controls to mitigate an optimal attacker.

We were inspired by these works in the creation of our own mission decomposition model presented in our earlier paper.[4] The model used in our work uses the AND/OR notation and is based on the constraint satisfaction problem.[17,20,24,25] The difference between our approach and the related work is that we do not consider mission capacity; functional requirements, that is, constraints, are a binary matter. The logic of the model used in our work allows selecting the most resilient configuration among all feasible ones, that is, to derive a Bayesian network of associated privileges including both critical targets and likely attacker positions and to calculate the resilience of the configuration.

2.2 | Attack graphs and Bayesian networks in cybersecurity

This work builds upon two theoretical models commonly used in cybersecurity analyses and elsewhere, attack graphs and Bayesian networks. Although the approaches based on these two models appeared in the literature for about a decade and the models themselves are even older, the quantitative security risk assessment modeling, which builds on principles of Attack Graphs and Bayesian networks to capture the probabilistic nature of this issue successfully is a highly promising approach even today.

Attack graphs have become popular models of representing cyber attacks. They date back to 1998, when they were proposed by Philips and Swiler.[26] The Bayesian networks allow the extension of the attack graphs as a probabilistic model, which is advantageous for many applications. The first mention of such extended models, often referred to as Bayesian attack graphs, dates back to 2008 in the work of Lie and Man.[27] The attack graph and Bayesian attack graphs were then used frequently. For example, Poolsappasit et al.[28] proposed a method to estimate the risks to an organization's security using the attack graph and the CVSS metrics[*]. The attack graph is extended by the probability of exploiting the attack graph's nodes. The authors further proposed the procedures of static and dynamic risk assessment and generating risk mitigation plans. Shin et al.[29] developed a risk model to represent the probability of cyber attacks and how an organization complies with security policies. Augessy et al.[30] proposed an approach to model ongoing and possible future attacks. Khosravi-Farhad et al.[31,32] proposed the use of the Bayesian decision networks to measure the impact of vulnerabilities and to find minimum-cost security measures.

An overarching analysis of the use of standard Bayesian network models in cybersecurity and research gaps can be found in the work of Chockalingam et al.[33] A strategic advantage of Bayesian networks in cybersecurity modeling is their ability to combine heterogeneous sources of knowledge and also deal with limited data availability. First, it highlights the irreplaceability of probabilistic modeling in the field of cybersecurity, in particular, the potential of standard Bayesian networks to formally express the nature of the problem. Second, the models (variables used in Bayesian networks) are primarily technology-oriented, with little focus on the human element, such as the level of trust associated with legitimate users.

In recent works, He et al.[34] surveyed the use of graph models, including attack graphs and Bayesian networks, to assess risks associated with unknown vulnerabilities. Zimba et al.[35] proposed a technique of Bayesian network-based weighted attack path modeling, including the quantitative characterization of possible attack paths, to capture interlinked attack paths generated by advanced persistent threats upon the exploitation of vulnerabilities of cloud components. Ibne Hossain et al.[36] illustrated the efficacy of Bayesian networks in addressing a range of possible cyber risks, offering possible mitigation options, and assessing and enhancing the overall cyber resilience of a smart grid. Wang et al.[37] proposed a dynamic risk assessment model that uses the Bayesian attack graph to infer the system risk status. Network system vulnerabilities are analyzed using the CVSS metrics in both static and dynamic ways. The model can automatically infer an attacker's capability and estimate each node's risk status by incorporating the obtained attack evidence. Wang et al.[38] extended FAIR (Factor Analysis of Information Risk), one of the most popular models for quantitative cybersecurity risk assessment based on quantifiable risk factors. The FAIR model was implemented using the Bayesian networks, which provided a more flexible and extensible solution for risk assessment and decision-making in cybersecurity. Li et al.[39] approached the complexity of attack graphs and proposed DeepAG, a system that makes a prediction of which attack path in the graph is more likely to be taken by an attacker.

The work of Khouzani et al.[40] is one of the closest to our work in approaching the multipath attack problem, considering a large number of attack paths, each involving the exploitation of different vulnerabilities, as a multi-objective optimization problem for cybersecurity defense. It measures the overall security risk as the expected damage inflicted by the most effective attack paths in a probabilistic attack graph. It presents a sound mathematical framework that transforms the defender problem into a highly efficient mixed-integer linear programming problem. To illustrate more clearly the probabilistic nature of the problem and, in particular, to increase the overall clarity for the decision-maker, it shows how the problem can be solved using probabilistic graphical methods instead. As a defense, it selects an optimal portfolio of security countermeasures that minimizes the overall security risk. The effectiveness of the security countermeasures is specified using the probability of intrusion success.

The application of game theory in cybersecurity risk analysis has received much attention recently. Many of such approaches use the Bayesian networks and their derivates. Particularly successful and highly relevant are game theory approaches based on Stackelberg games. In a Stackelberg game, the leading player (in our case, the defender) moves first, and all other players (attackers) move after him. The so-called Bayesian Stackelberg games, in which the leading player is unsure and has incomplete information about the adversary, play an important role in the cybersecurity domain. Paruchuri et al.[41] focused on finding an efficient technique for choosing the leader's optimal strategy in such games since, in general, this problem is NP-hard. To counteract multistage cyber attacks, Zhang and Malacaria[42] use a Bayesian Stackelberg game and select the optimal portfolio of security controls. Incomplete information about the current state of the attacker, represented by a probability distribution, plays a key role in the cyber-defense mechanism and its mathematical framework behind. Online optimization solves over probabilistic attack graphs. Wang and Neil[43] present a comprehensive decision analytic framework that uses hybrid Bayesian networks (a mixture of discrete and continuous variables representing a security state) to solve the decision problem from a game theory perspective. It implements influence diagrams in a game model of defender and attacker and provides detailed insight into the process of modeling the interaction between defenders and attackers, managing cyber security risk, and identifying the optimal decision strategy for defenders.

There is also a number of works proposing the application of the above-mentioned techniques in specific environments. For example, Huang et al.[44] applied the impact assessment based on Bayesian networks to cyber-physical systems.

Sakib et al.[45] presented a Bayesian network model and its analytical capabilities to predict and assess disasters in the oil and gas supply chain. Spanakis et al.[46] introduced a multi-layer model of attack and threat identification and analysis for connected health services. The model focuses on specific cyber risks in delivering health services and the identification of domain-specific requirements. The work extends the attack graph generation techniques to represent humans, processes, and policies. Ivanov et al.[47] presented automated security management of smart infrastructures (e.g., smart cities) with the aim to minimize risk by eliminating the most critical vulnerabilities. Doynikova et al.[48] proposed a variation of the attack graph to provide security decision support in control systems. Stergiopoulos et al.[49] explored the options of automatic analysis of attack graphs for the needs of risk prioritization and mitigation in large-scale and complex networks used in Industry 4.0.

The literature review shows that using attack graphs and Bayesian networks, including their variations and combinations, is popular and abiding in cybersecurity with a plethora of use cases. However, analytical tools and approaches combining attack graphs with mission-centric perspectives are rare; the approaches using such inputs and models to quantify cyber resilience and threats to privilege holders are missing completely. Our approach brings novel perspectives that enrich previous works by providing additional use cases. Further, there is one fundamental difference between our and related work in the way in which we convert attack graphs into Bayesian networks. Related work mostly aims at exactness and aims at expert users and, thus, keeps as much information in the graphs as possible. On the contrary, in our approach, we reduce the attack graph into a bipartite graph, including only privileges and exploits. The bipartite graph is more comprehensible than the complex attack graph, not only for experts but also for non-technical stakeholders, which is advantageous in decision making.

2.3 | Decision support in cybersecurity

The related work on decision support in cybersecurity is mostly focused on finding optimal response actions to an attack[50,51] or recommending a countermeasure to prevent a predicted cyber attack.[52] Other examples of decision support and recommender systems applied to the cybersecurity domain can be found in the recent literature review by Pawlicka et al..[1] Nevertheless, the reasoning behind optimal response selection overlaps with or can be applied to increasing resilience. Other trends in decision support for cybersecurity focus on visualization and provenance.[53] Still, it is not uncommon to rely solely on expert judgment.[54] Recently, Murenin et al.[55] provided an overview and comparison of the most prominent systems and approaches to design decision-making systems and their application in heterogeneous distributed information systems, although with very wide conclusions. Emerging issues in this domain seem to be privacy risk management[56] and the use of distributed ledger technologies (e.g., blockchain) that would enable privacy-preserving countermeasure selection.[57]

A survey on reaction framework and optimal selection of countermeasures against cyber attacks was presented by Nespoli et al.[51] Recent related work includes the work by Zhang et al.,[24] who presented a constraint optimization model that could be used as a decision support system for the allocation of security controls. However, the paper's main contribution is a proposed stochastic optimization model to handle uncertainties in breach probability estimation. Correa et al.[25] optimized the selection of countermeasures at runtime, formalized the attack mitigation search task as a constraint optimization problem, and proposed an autonomic computing architecture including a precise set of technologies for each of its components to mitigate suspected ongoing cyber attacks.

Recently, Schmitz and Pape[58] proposed LiSRA, a lightweight security risk assessment framework for smaller organizations that lack data or knowledge. In LiSRA, the experts fill in the risks for a specific domain, while users specify security practices and organization characteristics. LiSRA recommends security activities and provides insights into the mitigation effects of the recommendations. Li et al.[59] in 2020 encountered countermeasures selection for multipath attacks formulated as an optimization problem and proved the problem to be NP-hard. Gonzalez-Granadillo et al.[60] proposed a countermeasure selection using hypergraph, a concept defined in the author's previous work.[61]

Kotenko and Doynikova[62] outlined the uncertainty of attacker behavior and the complexity of interconnections between resources in modern distributed systems. The authors propose a model-driven approach to the security assessment and countermeasure selection that is based on integration with security information and event management systems, namely the open standards and databases. A common feature of this work with our proposal is modeling the uncertainty of the attacker's behavior, which, in our case, is done via the probabilistic attacker's position.

Deterministic and stochastic models presented by Schmidt et al.[63] provided a structured approach to the composition of a portfolio of security controls that is effective concerning the costs and multiple objectives related to risk reduction. The goal is to reduce the overall risk and increase the expected difficulty of completing any of the attacks. As the objectives can be conflicting, the paper demonstrates the importance of the optimization-based approach, that is, finding the right balance across multiple criteria. The method is supposed to be used as a managerial decision-making tool in supply chain risk management.

In our recent work,[2] we presented a decision support component into the CRUSOE toolset, which aims to improve cyber situational awareness in incident handling. The CRUSOE toolset uses a continuous collection of data on the network and their visualization to guide a user through the procedures of incident handling and response. A preliminary, simplified version of the approach presented in this article is implemented in the toolset. The toolset is publicly available[†], and the implemented algorithms were presented in another previous work.[64] Otherwise, our previous work presents only the basic ideas[64] and places particular tools into context.[2] In this article, we provide a detailed description of our approach in a generic context, not specifically for the incident handling support.

The main difference between our work and related work in terms of decision support is the motivation and task to resolve. The related work, in most cases, discusses either preemptive tasks of risk analysis without the involvement of dynamic changes in the protected systems or recommending the optimal strategy in responding to an attack. While there is common ground with our work, there are substantial differences in motivation. While our approach could be used for risk management, it allows for dynamic assessment of the situation and reacts to the attacker's position. Similarly, reconfiguration is also an effective measure to mitigate a cyber thread. However, there are other options, and selecting the optimal response typically chooses between them if considering reconfiguration at all. Further, the related work is mostly aimed at cybersecurity experts and does not reflect the need to consult the action plan between technical and non-technical stakeholders, which is one of the goals of our work.

3 | PROPOSED DECISION SUPPORT SYSTEM

The decision support system proposed in this work is based on the mission decomposition model and the security state assessment and recommends the most resilient configuration of the IT infrastructure. Herein, we outline the system and the four phases of the decision-making process, which are discussed in detail in the following subsections. The workflow of our proposed decision support system is depicted in Figure 1. Throughout this section, we use the notation summarized in Table 1.

The proposed approach stands on three assumptions. First, the critical mission commonly allows multiple satisfying configurations, that is, different combinations of supportive processes, IT services, and cyber components that meet all functional requirements. Having multiple satisfying configurations is a natural outcome of avoiding a single point of failure in critical systems.[4] The alternative mission configurations are derived from the AND/OR relations between the mission and its dependencies.[20] Second, the mission-supportive processes are regarded as critical assets to be protected. We concentrate on mission-supportive processes instead of vulnerabilities or cyber components.[5,16] Third, the decision support exploits the mission's ability to adapt and reconfigure in the face of adversarial activities. All the functional requirements have to be satisfied in order to keep the mission operational.[64]

The first phase of the decision support system consists of the decomposition of the mission and the definition of its functional and security requirements. An enterprise mission is decomposed into one or more *mission-supportive processes*, mission-related activities delivered by people through IT services and cyber components. The security requirements (requirements on CIA) are assigned to individual mission-supportive processes. The mission-supportive processes are mapped to one or more *IT services*, the abstract representations of their components. IT services are mapped to hosts and services in the network, referred to as *cyber components*. We approach the mission as a set of possible arrangements of mission-supportive processes, IT services, and cyber components. Any arrangement of mission-supportive processes delivering all the required mission's functionalities is called the *satisfying mission configuration*. The first phase was suggested in our previous work[4] and is discussed in detail in Section 3.1.

The second phase consists of a continuous security state assessment. The decision support system continuously updates information on the security situation, that is, vulnerabilities of the cyber components and the attacker's position

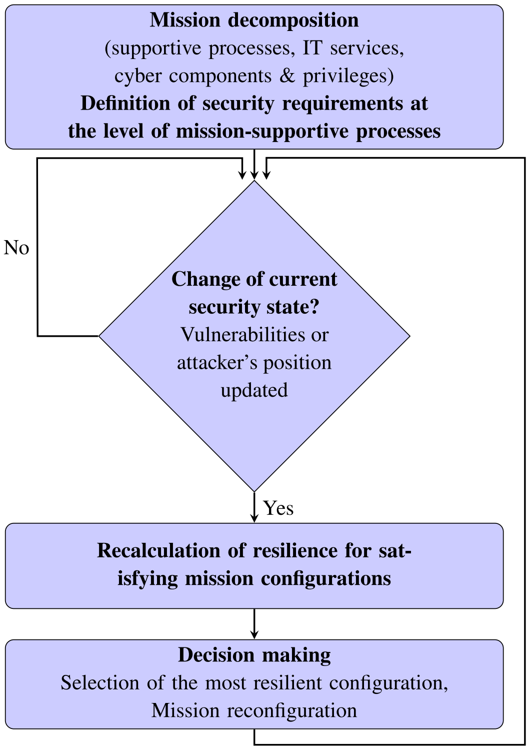
Mission decomposition
(supportive processes, IT services,
cyber components & privileges)
Definition of security requirements at
the level of mission-supportive processes
No
Change of current
security state?
Vulnerabilities or
attacker's position
updated
Yes
Recalculation of resilience for satisfying mission configurations
Decision making
Selection of the most resilient configuration,
Mission reconfiguration

FIGURE 1 Overview of the decision support process in the proposed decision support system.

TABLE 1 Summary of notation.

Variable	Meaning
P	Set of privileges associated with the mission configuration
E	Set of exploits associated with the mission configuration
I, G	Subset of initial privileges (positions gained by the attacker)
C	Subset of critical privileges
X_i	Bernoulli random variables corresponding to certain privileges
$PreReq$	Set of prerequisites
$PostReq$	Set of postrequisites
$CPEAG$	Complex Privilege-Exploit Attack Graph
$BPAG$	Bayesian Privilege Attack Graph corresponding to $CPEAG$
$parent(X_i)$	Parent node of node X_i in $BPAG$
E_j	An intermediary exploit node in the corresponding $CPEAG$
$p(E_j)_{parent(X_i)}$	The probability of a successful exploit E_j assuming the attacker has privilege $parent(X_i)$

and held privileges. The security situation changes if, for example, a new vulnerability is discovered on a cyber component or an attacker gains a privilege, such as control over a cyber component. The attacker's position also implies the set of cyber components that are threatened. The attacker's privileges are the privileges held by the attacker on a controlled system. The security state assessment was partially proposed in our previous work[64] and is discussed in detail in Section 3.2.

The third phase, mission resilience recalculation, is triggered by a change in the security situation. Mission resilience is the probability of a successful violation of the established security requirements of its most resilient satisfying mission configuration. Mathematical probability is used as a measure; the probability function assigns a real number from the interval $\langle 0,1\rangle$ to each mission configuration. A logical attack graph is employed to represent the current security situation (i.e., the attacker's position and held privileges and the list of cyber components and their vulnerabilities) using the parameters derived from the mission decomposition model. The inference mechanism of a Bayesian network is then employed to reflect the situation. The resulting model then allows for calculating the probability that an attacker reaches the target privilege, that is, the probability that the security requirements are violated. The third phase was partially proposed in our previous work[64] and is discussed in detail in Section 3.3.

The fourth phase is decision-making. There is a need to select the most resilient mission configuration based on the risks calculated in the third phase. For each satisfying mission configuration, we consider the calculated amount of effort (probability value) that the attacker must expend to compromise the specified level of mission security successfully. The configuration with the lowest computed probability is selected as the most resilient and is recommended to be set. However, the stakeholders acknowledge the recommendation and make the final decision. It is then up to the operators to acknowledge the recommendation and apply the changes in mission configuration to protect the IT infrastructure. The details of the fourth phase are presented in Section 3.4.

3.1 | Mission decomposition

Herein, we discuss the first phase of our decision support system, which includes mission decomposition and modeling. We use a mission decomposition model proposed in our previous work,[4] which is inspired by Lewis et al.[17] and uses the AND/OR notation proposed by Jakobson.[20]

Mission decomposition stands on the following premises. A mission is decomposed into mission-supportive processes that are mapped to IT services that are consequently mapped to cyber components. Moreover, the mission is formally described as a system of *mission functional requirements* and *mission security requirements*. The functional requirements are posed on IT services by the mission-supportive processes and on cyber components by the IT services. The security requirements are expressed as desired levels of the CIA (e.g., *None*, *Low*, or *High*) posed on mission-supportive processes, IT services, and cyber components. A *satisfying mission configuration* is a subset of mission-supportive processes, IT services, and cyber components that align with the mission's functional requirements. Finally, *mission resilience* is the mission's ability to continue its operations while maintaining all the required functional and security requirements.

The mission decomposition model[4] is a graph structure with the mission-supportive processes, IT services, and cyber components as nodes. The functional requirements are represented as edges between mission-supportive processes and IT services or between IT services and cyber components. The alternative mission configurations are expressed via the AND/OR nodes.[20] An AND node in a mission configuration poses a requirement for the presence of all of its child nodes. The child nodes represent either the supportive IT services or the cyber components. An OR node expresses a mission configuration option since it poses a requirement for the presence of at least one of its child nodes. For example, let us consider a mission-supportive process dependent on two IT services. In such a situation, an AND node is added to the model, the mission-supportive process is connected to the AND node, and the AND node is connected to the two IT services. The OR nodes or combinations of AND/OR nodes are used similarly. A mission-supportive process may be satisfied by more mission configurations, that is, combinations of IT services and cyber components. For example, a mission-supportive process dependent on one of the two IT services produces three satisfying mission configurations, one with the first IT service, one with the second IT service, and one with both. Finally, the edges between cyber components indicate network visibility of the components, that is, a situation in which the two components can reach each other and interact.[4]

An example of a mission decomposition model and its entities can be found in Figure 2. Mission-supportive processes are drawn in green, IT services in blue, and cyber components and their associated privileges in red. Full arrows and AND/OR nodes in the graphical structure visualize the dependencies between the supportive components and the logic that determines satisfying mission configurations. The dashed arrows between cyber components represent open communication channels when the component is used in a mission configuration. An example of a model of a real-world system is described in Section 4. Examples of a mission decomposition model and a logical formula representing its satisfying configuration are presented in Figures 4 and 5.

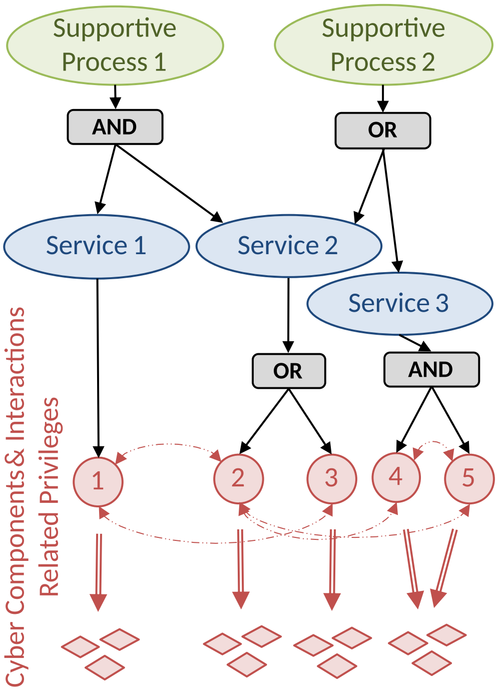

FIGURE 2 A simple mission decomposition model.

3.2 Security state assessment

In this section, we discuss the second phase of the decision-making, the security state assessment. The goal of the security state assessment phase is to represent the current security situation and observe its changes in time. If a change in the security state occurs, the recalculation of mission resilience is triggered. Herein, we first present the representation of the network security situation, that is, obtaining and representing information on vulnerabilities and the attacker's position in the network. Second, we comment on implementation issues, such as viable data sources.

The representation of the current security state complements the mission decomposition model and provides the remaining pieces of information required to calculate the resilience of the mission. Contrary to the mission decomposition model, which is static, the security state needs to be continuously updated. The mission decomposition model enumerates the supportive cyber components, that is, hosts and services in the network that enable the mission. Mission resilience reflects a risk of the disruption of its supportive cyber components and, thus, there is a need to estimate and represent this risk. Further, the risk depends on the attacker's current position, which should also be considered. Security state assessment consists of three tasks:

(i) Discovering the vulnerabilities of the hosts in the network via vulnerability scanners or similar tools.
(ii) Disclosing the attacker's position via intrusion detection systems or similar tools.
(iii) Formal representation of the security state for the following phases of the decision support process.

Vulnerabilities can be discovered with a plethora of available tools including the Nessus[‡] vulnerability scanner, host-based tool Pakiti[§], or third-party tools like Shodan[¶]. However, it is often impossible to have access to all assessed hosts in the network, including the ones supporting a mission, and the options of remote vulnerability assessment are limited. Readers interested in technical details are kindly referred to the work of Laštovička et al.[65] on network-wide vulnerability discovery. Nevertheless, the information on vulnerabilities is well structured in vulnerability databases, such as NVD[#], a de facto standard library of vulnerabilities in the CVE format[||]. CVE records are accompanied by CVSS[**], a scoring system that provides security metrics for vulnerabilities. An example of using CVE, CPE, and CVSS for cybersecurity risk management can be found in the work of Ushakov et al..[66] The remotely exploitable vulnerabilities are marked by the *Network* attack vector in CVSS. The *Impact Metrics* refer to the potential impact of a successful exploit on CIA and have the values of *None*, *Low*, and *High*. The *Attack Complexity* metric (interpreted as the conditional probability that the attacker successfully exploits the vulnerability given that the attacker already holds the necessary privileges) enables the mission resilience calculation as discussed in Section 3.3.

An attacker's position is an abstract term that, in the context of this article, corresponds to the privileges held by an attacker. An attacker may gain a wide scale of privileges, such as reading access to sensitive data or full control over a machine. The attacker's position is an enumeration of such privileges mapped on cyber components. In the initial state, we assume the attacker is located outside the network and has the same privileges as any remote entity accessing the cyber components via the Internet. The attacker's position can be updated if their activity has been observed or assumed. We may use various intrusion detection systems or forensic tools to detect compromised hosts and services. If an attacker is found to have gained some privileges or full control over a cyber component, the list of the attacker's positions is extended with the exploited privileges on the cyber component. Alternatively, the attacker's position can be adjusted manually, namely, in the case of remote cyber components. If a component is operated in a remote network and its operators inform us that the remote network is under attack, we may manually set the attacker's position at the remote component. A probability as a number between 0 and 1 may represent that we are not sure if the attacker holds the privileges or set a level of trust in remote services.

The security state is represented as a list of hosts and services in the network that poses as cyber components in the mission decomposition model. In an implementation, the hosts and services can be identified by their IP address, port number, domain name, or URL. Each host and service also have two lists assigned to them, one with the vulnerabilities and one for the attacker's position. The vulnerabilities are identified by their CVE number, and the CVSS scores are attached. All the details and details can be looked up in NVD. Naturally, the list has to be updated every time a new vulnerability is found or patched. The attacker's position is a real value in the interval $[0, 1]$ attached to a host or service. An example is attached in the case study in Section 4.3. The implementation uses JSON format, as displayed in Figure 6.

3.3 | Mission resilience calculation

In the third phase, presented in this section, the decision support system reacts to changes in the security situation and recalculates the resilience of mission configurations. Our proposed approach is based on attack graphs and their extensions. First, we provide an outline of the methods. Subsequently, we introduce the Complex Privilege-Exploit Attack Graph, a formal representation of exploits and privileges and a stepping stone for further calculations, and the Bayesian Privilege Attack Graph, a fundamental model for the mission resilience calculation. Finally, we present the algorithm of the resilience calculation that uses both graph models. Our approach to this phase was partially presented in our previous work[64] and is extended here.

3.3.1 | Method description

The proposed method, depicted in Figure 3, calculates the resilience of the mission configuration in terms of the probability of violating the security requirements. Its inputs are the mission decomposition model and a set of security requirements, presented in Section 3.1, and information on vulnerabilities and the attacker's position provided by the security state assessment presented in Section 3.2. The mission decomposition model is enriched with a system of privileges associated with the cyber components employed in a particular mission configuration. The security state of the mission is quantified via these privileges and the probability that they are already in the attacker's hands.

The calculation goes as follows. For each satisfying mission configuration, that is, an alternative mission configuration that meets the functional requirements, the following four steps are performed:

(i) *Identification of critical privileges.* Critical privileges would allow the established security requirements of the mission to be violated if gained by an attacker. They can be gained as a consequence of the successful exploitation of vulnerabilities related to cyber components used in a respective mission configuration. The *Impact Metrics* in CVSS link the successful exploitation of a given vulnerability to its consequences in terms of breaches of CIA. Having the vulnerabilities of relevant cyber components, the mission decomposition model gives us a mapping of individual security requirements (determined at the level of individual mission-supportive processes) to cyber components and desired privileges.

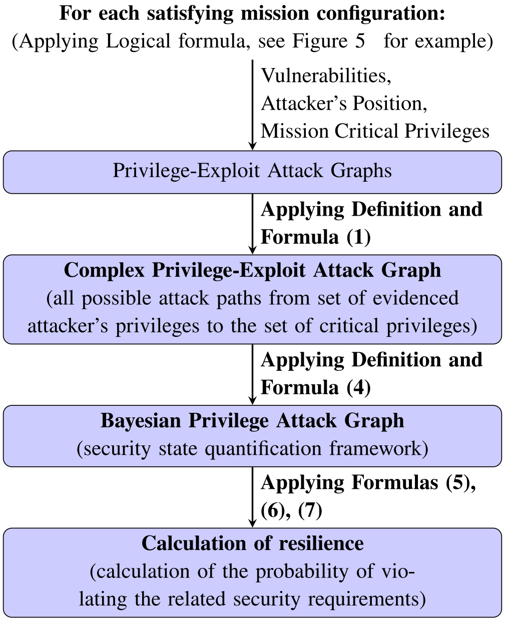
For each satisfying mission configuration:
(Applying Logical formula, see Figure 5 for example)
Vulnerabilities,
Attacker's Position,
Mission Critical Privileges
Privilege-Exploit Attack Graphs
Applying Definition and Formula (1)
Complex Privilege-Exploit Attack Graph
(all possible attack paths from set of evidenced attacker's privileges to the set of critical privileges)
Applying Definition and Formula (4)
Bayesian Privilege Attack Graph
(security state quantification framework)
Applying Formulas (5), (6), (7)
Calculation of resilience
(calculation of the probability of violating the related security requirements)

FIGURE 3 Recalculation of resilience for satisfying mission configurations.

(ii) *Complex Privilege-Exploit Attack Graph generation.* Knowing the involved cyber components and their interaction specified in the mission decomposition model, we can create a bipartite graph (comprising privileges relevant to a given mission configuration and exploits relevant to the cyber components' configuration) showing all possible attack paths from the set of evidenced attacker's privileges to the set of identified critical privileges.

(iii) *Bayesian Privilege Attack Graph generation.* Having precisely specified relationships between exploits and privileges, we derive the Bayesian network of privileges, that is, a mathematical model providing necessary inference mechanisms.

(iv) *Calculation of resilience for individual mission configurations.* Considering the current attacker's position (probabilities assigned to the privileges representing the attacker's presence in the system), we use the inference mechanisms of the Bayesian network to quantify the resilience (the probability that the attacker will gain critical privileges) of the given mission configuration.

3.3.2 | Complex Privilege-Exploit Attack Graph

Attack graphs[26] are a popular method of formal representation of cyber attacks. An attack graph represents all paths through a system that end in a state where an intruder has violated a security policy. Attack graphs provide an efficient way to summarize the threats to a network and are widely recognized tools for analyzing the progress of an attack. 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.[67] The initial state represents the state before the attack starts. Transition relations represent the possible actions of an attacker. These are often weighted, for example, by the probability that the attacker will choose the action. Nowadays, there are a plethora of tools for attack graph generation; a comprehensive taxonomy was proposed by Kaynar,[68] and an overview of the attack graph tools was given by Yi et al.[69]

In our work, we use a variation of the attack graph named (Complex) Privilege-Exploit Attack Graph. The *Privilege-Exploit Attack Graph* is a directed bipartite graph ($Exploits \cup Privileges, Prerequisites \cup Postrequisites$) representing dependencies between exploits and relevant privileges in the form of prerequisites and postrequisites of an exploit. The exploits, together with privileges, constitute a set of nodes, and the prerequisites, together with the postrequisites, constitute a set of directed edges. Prerequisites represent privileges allowing exploitation of the relevant vulnerability. Postrequisites represent privileges resulting from a successful exploit of the relevant vulnerability. More formally, they can be expressed as subsets of Cartesian products $Prerequisites \subseteq Privileges \times Exploits$ and $Postrequisites \subseteq Exploits \times Privileges$.

We consider a set of evidenced initial privileges and, by analogy, a set of privileges as possible targets of the attacker. Therefore, we introduce the *Complex Privilege-Exploit Attack Graph* (CPEAG), which covers all identified attack paths leading from a set of attacker's positions (privileges probably gained by an attacker) to a set of possible targets, that is, privileges we consider critical in the context of the mission. We introduce the *Boolean feasibility function* over the set of privileges that form the exploit's prerequisites in the CPEAG as a logical expression over the exploit's prerequisites describing the necessary conditions enabling an exploit. Let us have a satisfying mission configuration and an algorithm that generates a Privilege-Exploit Attack Graph. Then, CPEAG is a tuple:

$$CPEAG = (P, E, I, C, PreReq, PostReq, F), \tag{1}$$

where P denotes the set of privileges associated with the mission configuration, $I \subseteq P$ denotes the set of initial privileges (attacker's position), $C \subseteq P$ denotes the set of critical privileges, E denotes the set of exploits, which includes exploits from all possible attack paths generated by the algorithm and leading from any privilege from I to any privilege from C. $PreReq \subseteq P \times E$ denotes the set of prerequisites, where the edges leading to a given exploit identify the privileges that make up the prerequisites of an exploit (feasibility function attributed to the exploit specifies their relevance). $PostReq \subseteq E \times P$ denotes the set of postrequisites, where the edges leading from the exploit identify the privileges possibly gained by an attacker when the exploit is successful (feasibility function attributed to the privilege specifies their relevance). F denotes the set of Boolean feasibility functions comprising of:

(i) Feasibility functions attributed to the exploits.
This function is defined as a logical condition over the privileges that form the exploit's prerequisites in the CPEAG. The logical condition must be met for an exploit to be possible.

(ii) Feasibility functions attributed to the privileges.
This function is defined as a logical condition over the exploits for which the privilege forms postrequisites. The logical condition must be met for the privilege to be gained by an attacker.

The tuple $(E \cup P, PreReq \cup PostReq)$ forms a directed bipartite graph. This structure provides information on the causality relationships among the security entities involved. This qualitative information is necessary for the subsequent quantification of a given security state.

3.3.3 | Bayesian Privilege Attack Graph

Bayesian networks are another widely used tool in cybersecurity, often as a probabilistic extension of attack graphs, the so-called Bayesian attack graphs.[27] Bayesian networks are usually represented as directed acyclic graphs. The nodes represent random variables, and the edges represent their conditional dependencies. Each node is assigned a conditional probability distribution based on the values of its parent nodes in the graph. Formally, let $G = (V, E)$ be a directed acyclic graph, 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 variables and the direct edges form a directed acyclic graph. To each variable A with parents $B_1, B_2 ... B_n$, a conditional probability table $P(A|B_1, B_2 ... B_n)$ is attached.

In our work, we propose our custom version of attack graphs and Bayesian networks based on exploits and privileges. We propose the *Bayesian Privilege Attack Graph* (BPAG) as an analytical framework representing the mission configuration in the form of a Bayesian network of related privileges and their relationships. The nodes of the BPAG are random variables representing the probability that an attacker holds the privilege. The edges represent an opportunity for an attacker to extend their privileges further. The BPAG depicts how an attacker can extend his influence over the mission security goals. We can especially quantify the threat exposure to mission-critical assets. The strong arguments for the BPAG are, in particular, its compactness, the availability of a range of efficient inference mechanisms (due to its Bayesian network structure), and clear interpretation of derived results within the context of the mission decomposition model.

BPAG is derived from CPEAG, which describes the security situation. The relationship between the exploit node and the privilege nodes representing the relevant preconditions of the exploit (the condition necessary to launch an attack, potentially leading to a successful exploit and the probability of success) must be expressed exactly.

Let X_i *for* $i = 1, \dots, n$ represent the prerequisites of an exploit E_0, that is, there are oriented edges leading from X_i to E_0 in the corresponding CPEAG. Let $p(e_i)$ *for* $i = 1, \dots, n$ represent the probability that an attacker succeeds given that he holds the privilege X_i. Let X_0 represent the postrequisite of an exploit E_0, that is, the privilege gained by an attacker when an exploit E_0 is successful. In the context of this exploit, we can consider the privileges X_i as parents of the privilege X_0.

Just to recall the relevant fundamentals of the probability theory, two basic situations result from the Privilege-Exploit Attack Graph for an exploit to be possible. The corresponding privilege nodes are in a logical AND relationship, that is, all prerequisites for the exploit to be successful must be met, or the corresponding privilege nodes are in a logical OR relationship. that is, at least one of the prerequisites for the exploit to be successful must be met.

The calculation of the probability of success (an attacker gains the privilege X_0 given that he already holds parent privileges) corresponding to the logical AND is formally expressed as:

$$p(X_0|parents(X_0)) = \prod_{i=1,\dots,n} p(e_i), \tag{2}$$

in the case of all the prerequisites $X_i = True$; the probability is equal to 0, otherwise.

The calculation of the probability of success corresponding to the logical OR is formally expressed as:

$$p(X_0|parents(X_0)) = 1 - \prod_{i=1,\dots,n} (1 - p(e_i)), \tag{3}$$

in the case of at least one of the prerequisites $X_i = True$; the probability is equal to 0, otherwise.

In general, considering the possible relationships among the privileges that make up the prerequisites of a given exploit, the condition necessary to carry out an attack (the feasibility of an exploit) can be expressed as a Boolean formula. We need to quantify the probability of success for all assignments that satisfy this formula, that is, assignments that evaluate the formula to *True*. Each Boolean formula can alternatively be notated (while maintaining the truth values) in a conjunctive normal form.

Let $CPEAG = (P, E, I, C, PreReq, PostReq, F)$ be a CPEAG. A BPAG corresponding to this CPEAG is a Bayesian network $BPAG = (DAG, Q)$, where DAG denotes a directed acyclic graph. Nodes X_i *for* $i = 1, \dots, n$ are Bernoulli random variables corresponding to the set of privileges P. The edges represent their conditional dependencies. An edge leads from the node $parent(X_i)$ into node X_i if and only if there is an intermediary exploit node E_j from E in the corresponding bipartite graph $(E \cup P, PreReq \cup PostReq)$, for whom the $parent(X_i)$ is in a position of prerequisites of the exploit and X_i in a position of postrequisites of the exploit. Q denotes the set of local conditional probability distributions. Let E_j be an intermediary exploit for the nodes X_i and $parent(X_i)$. Let $p(E_j)_{parent(X_i)}$ represent the probability that the attacker succeeds given that he holds the privilege $parent(X_i)$. Let the resulting logical formula created by substituting the feasibility functions of the intermediary exploits into the feasibility function of the privilege X_i be expressed in conjunctive normal form.

The individual entries in the conditional probability distributions are calculated as follows:

$$p(X_i, |parents(X_i)) = \prod_C \left(1 - \sum_L (1 - p(E_j)_{parent(X_i)}) \right), \tag{4}$$

where C represents the set of clauses in the formula, and L represents the set of literals in the respective clause.

3.3.4 | Calculation

The joint probability distribution of random variables representing possession of privileges relevant to a particular mission configuration provides a useful analytical framework with an important insight into the mission security situation. Having a joint probability distribution of random variables, we can derive the probability distributions over their subsets. Concerning the attacker's position, we can quantify the security state of the mission configuration and then compare the resilience of individual configuration alternatives. The Bayesian network provides an efficient way to quantify the joint probability of a specific state of variables representing critical privileges given the state of variables representing the attacker's presence in the system.

Let the set of random variables X_i *for* $i = 1, \dots, n$ of the Bernoulli distribution represent the nodes from the BPAG corresponding to the given mission configuration. Let us define three subsets of it:

- The subset of *gained privileges* represents the attacker's position, that is, a subset of k observed random variables $X_G = X_{g_1}, \dots, X_{g_k}$. We can assign them a value in the form of unconditional probability.
- The subset of *critical privileges* was derived from the mission decomposition model, that is, a subset of l queried random variables $X_C = X_{c_1}, \dots, X_{c_l}$. We need to calculate the probability of their specific states.
- The subset of *remaining privileges* represents all other nodes from the BPAG, that is, a subset of m random variables $X_R = X_{r_1}, \dots, X_{r_m}$. They constitute the rest of the Bayesian network and must be taken into calculation.

We deal with the set of observed variables, the set of queried variables, and the set of remaining variables that make up the entire joint probability distribution behind the scene. The set of local conditional probability distributions expresses all the necessary dependencies among the random variables in the network.

Following the mathematical terminology, we must calculate the probability of specific assignments of a subset of random variables representing the critical privileges given the probability of assignments of a subset of the random variables representing the evidenced privileges.

The resilience of a mission configuration is quantified as the probability that an attacker will fail to achieve any of the critical privileges, provided that he has already obtained the evidenced ones. The higher the probability, the more resilient the mission configuration is. We have to calculate the conditional probability $P(X_C|X_G)$. Applying the definition of conditional probability, we calculate as follows:

$$P(X_C = \bar{c}|X_G = \bar{g}) = \frac{P(X_C = \bar{c}, X_G = \bar{g})}{P(X_G = \bar{g})}, \tag{5}$$

where $\bar{c} = False$ represents the required security state (the probability an attacker fails), and $\bar{g} = True$ represents the evidenced attacker's position.

Using the Bayesian network representation of the joint probability distribution and marginalizing over the variables representing the remaining privileges $X_{r_1}, \dots, X_{r_m}$, the numerator of Formula (5) can be expressed as follows:

$$\begin{aligned} &P(X_C = \bar{c}, X_G = \bar{g}), \\ &= \sum_{X_{r_i}} \dots \sum_{X_{r_m}} \prod_{i=1}^{n} P(X_i, |parents(X_i))_{X_C=\bar{c}, X_G=\bar{g}}. \end{aligned} \tag{6}$$

The denominator (normalization constant) of Formula (5) is to ensure that the formula for all possible values of X_C sums to 1. We need to calculate the numerator of the formula for each possible value of X_C. The denominator of the formula can then be expressed as follows:

$$P(X_G = \bar{g}) = \sum_{X_{c_1}} \dots \sum_{X_{c_l}} P(X_C, X_G = \bar{g}). \tag{7}$$

3.4 | Decision making

In the fourth and last phase of the decision support process, we take the outputs of the previous phase, that is, a list of satisfying mission configurations and their resilience scores. The goal of this phase is to select the most resilient configuration and make the final decision. First, we comment on selecting the most resilient mission configuration. Second, we discuss the decision-making, including filtering the results and taking the previous configuration into consideration.

Selecting the most resilient configuration is a straightforward task. However, additional filtering may be applied to prevent making unnecessary recommendations and reconfigurations. For each satisfying mission configuration, we consider the calculated amount of effort that the attacker must expend to compromise the mission security. The configuration with the lowest computed probability is selected as the most resilient. If no postprocessing is applied, this configuration is recommended to be set.

In practice, however, it might not be feasible to change configurations too often, or the reasoning behind the recommended reconfiguration might not be strong enough to justify it. For example, if the resilience of the newly recommended configuration is only slightly higher than the resilience of the current configuration, the reconfiguration might not be worth it. The reconfiguration takes time and effort, and frequent changes might decrease the comfort of users. Thus, we may apply a threshold and recommend only those newly calculated most resilient configurations that significantly improve the mission resilience.

Selecting the most resilient configuration terminates the decision support process. However, it is up to the stakeholders to either follow the recommendation and set the recommended configuration or not. The final decision-making is usually an issue of mission management. The supportive roles, that is, IT experts, security experts, and domain experts, are primarily responsible for the correctness of the mission decomposition model and other partial parameters entering the calculation. They do not have to understand the situation in a broader context. The values of resilience computed for satisfying mission configurations must be considered relative and in the broader context of other factors, such as the cost of the reconfiguration and the changes in economic efficiency, redundancy of critical components, or user comfort. It is out of the scope of this article to formalize and include these factors in the decision-making process. The automation of infrastructure reconfiguration is also out of the scope of this work. Human involvement in the operations is still required, at least in the form of supervision.

4 | CASE STUDY

To evaluate our proposed approach, we conducted a case study using our proposed decision support system in a medical information system. Herein, we first briefly describe the environment of a regional medical imaging system. Subsequently, we illustrate the use of the decision support system in four subsections, one for each phase as described in Section 3. Finally, we discuss the evaluation and findings.

It is important to state at the beginning that to validate the presented approach in all its aspects, we combined the following two methods: a real-world case study and an expert evaluation. More comments on the evaluation methodology and possible alternatives are presented in the discussion. The principles of our proposed approach were evaluated by experts from CSIRT-MU, the cybersecurity incident response team of Masaryk University[††], in collaboration with the administrators of the regional medical imaging system and the experts from the radiology department of The University Hospital Brno[‡‡].

It is also worth noting that the medical domain is distinctive in terms of cybersecurity risk assessment as it often favors reliability and usability over security. We kindly refer the readers interested in this topic to a survey by Malamas et al.[6]

4.1 | Regional medical imaging

Medical imaging involves a plethora of mutually interconnected activities and collaborative processes across many providers of healthcare services. Its supportive IT infrastructure composes of many domain-specific applications running both locally and remotely. The core mission-supportive processes in medical imaging are the processes of patient examinations via a number of methods (e.g., computed tomography (CT), magnetic resonance imaging, roentgen examinations, mammography screening), emergency and expert consultations (e.g., with the specialists in neurology, cardiology, oncology), and daily routines of hospital's departments dependent on image information. Mission-supportive processes are built around two IT services. The first is image data acquisition via local or regional Picture Archiving and Communication System (PACS), a service for exchanging and sharing image data between hospital departments and other cooperating healthcare institutions. The second are services necessary for medical image examination and diagnostics. The cyber components contain a plethora of domain-specific devices and pieces of software, such as PACS's particular implementations, software components for controlling acquisition modalities, software for special medical image data processing, and software for specific diagnostic purposes. Cyber components communicate via a spectrum of domain-specific communication protocols.

In the case study, we model a trauma center equipped with two CT scanners. CT scanners are generally considered mandatory pieces of equipment in trauma centers, especially for patients with multiple traumas. Typically, a diagnosis based on an image examination is performed locally. However, it is also possible to conduct the image examination remotely; a radiologist does not need to be physically present at the trauma center. The trauma center's critical processes can be supported by IT services provided by other institutions.

4.2 | Mission decomposition

The mission decomposition of the considered trauma center is displayed in Figure 4. Further, the logical formula representing the satisfying mission configurations is presented in Figure 5. The formula represents satisfying mission configurations, that is, allowable combinations of Boolean variables representing the inclusion (*True*) or exclusion (*False*) of each cyber component and IT service in the configuration.[4] The trauma center's mission is formed by two mission-supportive processes, acquisition, and diagnostics. The *Acquisition* involves CT examinations and sending the acquired images to PACS to make them accessible for further analysis. The *Diagnostics* involves the retrieval of medical images from PACS and conducting the diagnostics.

The two mission-supportive processes are enabled by six IT services: medical image data acquisition services (*PrimaryCT* and *SecondaryCT*), services of secure image data transfer within the trauma center or between regional institutions

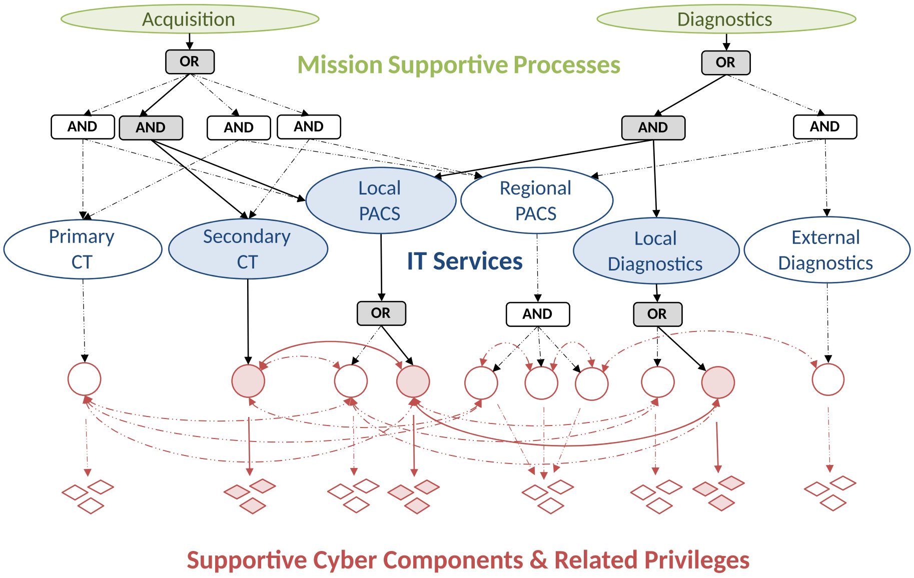

FIGURE 4 Mission decomposition model of a regional medical imaging system. The most resilient mission configuration is highlighted.

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

FIGURE 5 Logical formula representing the satisfying mission configurations.

(*LocalPACS* and *RegionalPACS*), and local and external diagnostics services (*LocalDiagnostics* and *ExternalDiagnostics*). The *Acquisition* process requires at least one CT and one PACS to run. This requirement is represented by the OR node over the four AND nodes over the pairs of CT and PACS. The *Diagnostics* process requires either local PACS with local diagnostics or external PACS with external diagnostics. The AND/OR representation is similar to the previous case.

The IT services are enabled by numerous cyber components. *PrimaryCT* and *SecondaryCT* are supported by *Acquisition_PrimaryCT* and *Acquisition_SecondaryCT*, two instances of software controlling the image acquisition and forwarding the acquired data to PACS. *LocalPACS* is supported by at least one of the two local instances of PACS (*PrimaryLocalPACS* and *SecondaryLocalPACS*). This is represented by the OR node. *RegionalPACS* has to be supported by the regional instance of PACS (*Server_RegionalPACS*), and local and remote proxies (*LocalProxy_RegionalPACS* and *RemoteProxy_RegionalPACS*). All three components need to be running, which is represented by the AND node. *LocalDiagnostics* is supported by two local diagnostic viewers (*PrimaryViewer_LocalDiagnostics* and *SecondaryViewer_LocalDiagnostics*) connected via the OR node. *ExternalDiagnostics* is supported by a remote diagnostic viewer (*RemoteViewer_ExternalDiagnostics*). Each cyber component has three related privileges depicted as red squares beneath them. Finally, the red edges between the pairs of cyber components illustrate their network visibility. Each edge connects two components that can reach and interact with each other. Two components are not connected if they cannot reach each other, for example, if there is a firewall dropping connections between the components, or the two components are located in different local networks.

The security requirements for the critical processes in the case study scenario should be set by the trauma center management. Consistent protection of the CIA of processes in the healthcare environment is generally considered essential. However, if the healthcare system has to face a long-term attack, priority can be given to protecting the availability and integrity of these processes to save a patient's health and life. In a general scenario, all three security requirements are assigned the value *High* as default to both processes. The confidentiality requirement can be set to *Low* under severe cybersecurity conditions.

4.3 | Security state assessment

Security state assessment in the medical imaging system is conducted continuously. Local administrators use a plethora of vulnerability scanners and intrusion detection systems to disclose vulnerabilities on cyber components in their constituency, attacks against them, and their compromises. Further, if the local infrastructure uses services provided by remote organizations, the remote organization may report attacks on their infrastructure to the local cybersecurity personnel. Under such circumstances, let us assume two changes in the current security situation that illustrate common scenarios of the security state assessment.

First, a vulnerability scanner disclosed two distinct vulnerabilities on machines that control *PrimaryCT* and *SecondaryCT*. The vulnerabilities are publicly known and have their CVE records. Thus, their CVSS scores are looked up in NVD. The *Impact Metrics* and *Attack Complexity* metrics are saved for later calculation. It is worth mentioning that a vulnerable component may still be a part of the most resilient configuration. For example, a vulnerable component may be irreplaceable, or the calculated resilience of other configurations with other vulnerable components might be lower.

Second, trust in an institution providing IT service *RegionalPACS* has decreased in reaction to the cyber attack on that institution. There is a chance that some privileges, for example, control over remote cyber components, are already in the hands of an attacker. The probability of the random variables' positiveness, expressing the fact that an attacker already gained the privileges associated with the corresponding supportive cyber components, was increased from 0 to 0.5. It can be increased to 1 if we have indications that the attacker has obtained the privilege.

The resulting cybersecurity state assessment is formatted for use by the decision support system. See Figure 6 for an example of JSON-formatted output of state assessment containing both vulnerable CT systems (*PrimaryCT* and *SecondaryCT*) and the *RegionalPACS* with the attacker's position set to 0.5, indicating the potential breach.

4.4 | Resilience calculation

The change in the security state assessment triggers a resilience calculation procedure. For each satisfying mission configuration, a set of Privilege-Exploit Attack Graphs is constructed using the enumeration of cyber components and their

```
{ "PrimaryCT": {
    "Attackers_position": 0.0,
    "Vulnerabilities": {
      "CVE–20xx–xxxx": {
        "Attack_complexity": "Low",
        "Confidentiality": "High", "Integrity": "High", "Availability": "High"
      }
    }
  },
  "SecondaryCT": {
    "Attackers_position": 0.0,
    "Vulnerabilities": {
      "CVE–20yy–yyyy": {
        "Attack_complexity": "Low",
        "Confidentiality": "Medium", "Integrity": "Medium", "Availability": "Medium"
      }
    }
  },
  "RegionalPACS":{
    "Attackers_position": 0.5,
    "Vulnerabilities": {}
  }}
```

FIGURE 6 The output of security state assessment with two vulnerable hosts and one host probably controlled by an attacker.

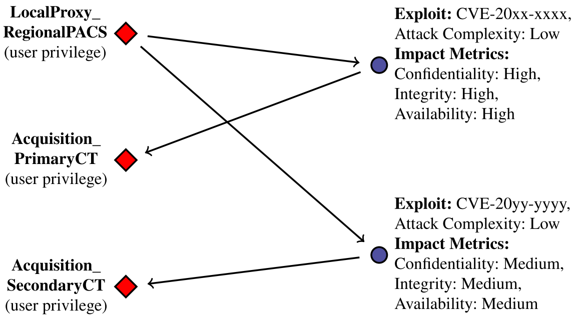

FIGURE 7 Excerpt from the Complex Privilege-Exploit Attack Graph.

network visibility, enumeration of components' vulnerabilities, anticipated attacker's position, and critical privileges. The critical privileges can be used to violate mission security requirements and are set as the attacker's goals in the attack graphs. The set of Privilege-Exploit Attack Graphs is then merged into a CPEAG. All the paths leading to the compromise of the mission's security requirements are known at the moment. An excerpt from the CPEAG is depicted in Figure 7, where we can see three privileges and two exploits. Holding a user privilege on *LocalProxy_RegionalPACS* enables the attacker to reach *Acquisition_PrimaryCT* and *Acquisition_SecondaryCT* components, exploit them via the vulnerabilities, and obtain new privileges.

Subsequently, the BPAG corresponding to CPEAG is constructed. An excerpt from the graph for the configuration with the services of *PrimaryCT*, *RegionalPACS*, and *External Diagnostics* is depicted in Figure 8. The attacker's position in the excerpt includes the privileges to the three components supporting the *RegionalPACS* that are suspected to be under the attacker's control. These privileges are included in the attacker's position, and their level of trust is set to 0.5. In this configuration, the attacker may use *LocalProxy_RegionalPACS* to reach and exploit *Acquisition_PrimaryCT*. In alternate configurations, the *Acquisition_PrimaryCT* may be replaced with *Acquisition_SecondaryCT* with a different exploit.

Having defined the joint probability distribution representing the current security state and following the procedure presented in Section 3.3.4, we calculate the resilience of a mission configuration as the conditional probability that an attacker will fail to obtain any of the critical privileges. After the recalculation, the current mission configuration's resilience proved to be approximately half that of the previous most resilient configuration. Figure 4 depicts an example of the most resilient, fully operational mission configuration, corresponding to the declared change of trust and change of vulnerabilities.

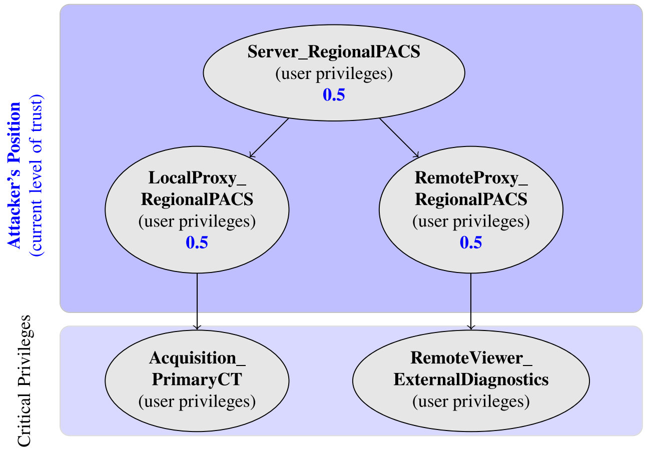

FIGURE 8 Excerpt from the Bayesian Privilege Attack Graph.

4.5 | Decision making

Figure 4 shows all the mission-supportive processes, IT services, and cyber components and highlights the most resilient mission configuration, that is, the configuration with the lowest probability of violation of the mission security requirements. The entities that constitute the most resilient configuration are colored and are recommended to be running to satisfy the mission's functional requirements. As we can see, the decision support system recommended a configuration relying on IT services of *Secondary CT*, *Local PACS*, and *Local Diagnostics*. The IT services of *Local PACS* and *Local Diagnostics* are recommended to rely on one of their supporting cyber components. The IT services of *PrimaryCT*, *Regional PACS*, and *External Diagnostics* and their supportive cyber components are not included in the configuration and can be turned off without interrupting the mission-supportive processes. If such services and components contain a vulnerability or are not trustworthy, they are recommended to be turned off or disconnected until the vulnerability is patched or the trust is regained, which is the case of cyber components discussed in the security state assessment. For practical reasons, there is no need to turn off or disconnect components that are trustworthy or not vulnerable. For example, there is no need to turn off *PrimaryLocalPACS* even though the configuration with *SecondaryLocalPACS* was recommended because there are no security issues with both components. On the contrary, the *Acquisition_SecondaryCT* is left running even with the vulnerability, at least until the more severe vulnerability on the *Acquisition_PrimaryCT* is patched or the security state changes.

The decision support system makes a recommendation, and the decision-maker has to make the final decision. If the stakeholders decide to follow the recommendation, the most resilient mission configuration is applied, and the network operators have to turn on all of its components and turn off or disconnect others. Before the decision is made and the configuration changes are executed, the decision-maker must realize the consequences of the unavailability of IT services and components. For example, the involved personnel will have to be present to use the *LocalPACS* without the possibility of remote consultations via *RegionalPACS*. Such configuration may cause a decrease in the quality of treatment. If such limitations are acceptable, the vulnerable components are turned off, and untrusted remote IT services are disconnected to increase local resilience. In general, if we have two mission configurations equally resilient, we should prefer the more comprehensive one that includes more IT services and cyber components. A more comprehensive satisfying mission configuration can enable higher quality diagnostics, greater patient and physician comfort, greater cost-effectiveness, or other benefits.

4.6 | Discussion

The presented case study illustrated that the proposed approach, while still being at the prototype stage, is effectively applicable even in specific areas such as the healthcare information system. The system provides comprehensible support to the decision-making of all involved stakeholders, not only the cybersecurity experts. Nevertheless, the role of experts in the systematization of relevant knowledge is irreplaceable throughout the life cycle of the proposed model, that is, in the phases of model construction, the initial setting of its parameters, continuous updating of parameters according to the changing security situation, and especially in the phase of evaluation based on domain knowledge, mathematical theory and experience with mostly non-repeatable real security situations. The mathematics behind the non-deterministic scenario model derives the difficulty of potential courses of action of the attackers trying to achieve any of the critical objectives under alternative mission configurations, that is, something that is unverifiable in practice. As well as expert assessment of threat severity, the probability of the attacker's initial position is crucial for the following stochastic inference.

A major issue determining the practical applicability of the system has emerged during its evaluation. The correct determination of the probability that the privileges under consideration are or will be held by legitimate users in the context of potential cyber threats is absolutely crucial. To gain a clearer insight into the security situation and to make the most of the possibilities offered by the model, it is a matter of training and fine-tuning the model structure and its parameters for each specific application domain. However, by simulating different scenarios, the model becomes a highly effective tool for self-education of security roles and discovering the mission's security weaknesses at different levels.

From a scientific perspective, there is a need to conduct a more formal evaluation of the proposed system. However, such a task is challenging, with many obstacles mentioned in the literature. As of now, there are not many other choices than case studies and expert or user evaluations. The preliminary steps towards evaluating such systems were investigated very recently, for example, in the work of Rodriguez-Bermejo et al.,[70] who propose an evaluation methodology for mission-centric cyber situational awareness capabilities covering correct technical implementation, core functionality, and user acceptance. In another example, Happa et al.[71] conducted a user evaluation study of decision support tools for SOC analysts. A recent complex decision support system for cybersecurity incident handling proposed by Husák et al.[2] also resorted to case study and user evaluation. These examples from the past two years illustrate the issues of evaluation of expert systems in cybersecurity caused by many specifics of this particular field of application. Evaluation of such and similar tools before 2020 was nearly non-existent, as noted by Gutzwiller et al.[72]

The situation is not much clearer in terms of evaluating Bayesian network-based models and their application in cybersecurity. As discussed by Chockalingam et al.,[33] who survey such models, there are several options to validate them, but none that would be widely used. We found it difficult to validate otherwise than via the expert evaluation and a case study, especially for the decision-making phase, and we came to the conclusion that it would not be beneficial to conduct other evaluations. For example, one of the used approaches is the Monte Carlo simulation. Using such an approach would be simple, but its results would not be meaningful given the motivation of our work and the highly situational nature of cybersecurity.

There are possibilities of setting up a testbed for the evaluation of our proposed system and even for the comparison to other works. Using the cyber infrastructure simulators or cyber ranges, one can set up a sample environment or a digital twin of a real-world environment to conduct experiments on. However, given the variety of infrastructure in related work (e.g., oil supply chain,[45] Industry 4.0,[49] or health services[46]) and their particular issues, this would be laborious with unclear outcomes.

5 | CONCLUSION

In this article, we proposed a novel mission-centric decision support system that helps the cybersecurity experts, in collaboration with other stakeholders, select the most resilient configuration of an IT infrastructure in the light of a current cybersecurity situation. Our goal was to give cybersecurity experts a tool that would autonomously recommend the most resilient alternatives of IT infrastructure and then facilitate the decision-making in which other stakeholders are involved. Our proposed system calculates the resilience metrics of all configurations satisfying predefined requirements. However, the decision on which configuration to apply is left to the stakeholders, who may consider arbitrary additional criteria, such as user comfort or economic losses given by the reconfiguration, which are influenced by the field of application.[6] Nevertheless, the recommendation considers the cybersecurity perspective comprehensively, even for non-technical decision-makers.

The proposed decision support system uses a mission decomposition model to map enterprise missions to hosts and services in the network and sets its functional and security requirements. The decision support system reacts to changes in the security situation, such as the discovery of a vulnerability or take-over of an asset by an attacker. Because a cybersecurity breach often cannot be confirmed, the probability that an attacker has access to certain privileges is used in the calculation. Further, the system then uses two novel graph models, Complex Privilege-Exploit Attack Graphs and Bayesian Privilege Attack Graphs, to calculate the resilience of each mission configuration that fulfills the functional requirements. The complex attack graphs and other structures used in related work[39,49] are difficult for non-technical decision-makers to grasp because of many technical details and the lack of domain-specific content. Thus, our novel graph structures reduce the complex attack graph into a comprehensible bipartite graph illustrating the impact of exploiting a vulnerability on the privileges in the infrastructure. The proposed approach makes it possible to link different perspectives on the state of security, to abstract the decision problem into a more understandable form, and, given that the key assets to be protected are critical domain-specific processes, in particular, to involve domain experts in the decision-making process. The intuitiveness and explanatory capabilities of the initial mission decomposition model, as well as the resulting Bayesian network depicting the level of trust that mission-related privileges are still held by legitimate users, brings a good understanding by decision-makers which is essential for discussions with domain experts when discussing and justifying optimal decisions.

The proposed approach was evaluated in a real-world case study of a medical information system. However, there are limitations to the proposed approach. Namely, the model lacks precise initial probabilities. The interpretation of the CVSS metrics might not be accurate and may lead to an imperfect accuracy of the initial conditional probability distribution. The initial marginal probability distributions, such as the position of the attacker, are also estimated imperfectly. Further, the non-trivial task of weighing the remaining advantages and disadvantages alongside calculated resilience in selecting the best configuration is still up to the decision-makers. The system takes into consideration neither the cost of reconfiguration nor the impact on user comfort or economic efficiency. Although we facilitated the decision-making for both cybersecurity experts and non-technical stakeholders, there is still the need to keep humans involved and consider the opinions of various stakeholders.

In our future work, we are going to improve the implementation of the decision support system and publish the full implementation. At the moment, only a partial implementation is publicly available as a part of a more complex system.[2] Further, the evaluations shall continue. A testbed could be set up to create a benchmark for the evaluation of the system in a controlled environment. However, field trials and more interactions with potential users shall give more insights than formal evaluation or performance analysis.[70-72] We plan to extend the number of modeled missions and circle of their stakeholders to collect feedback on the decision support system and its features. For example, it would be interesting to find a balance between the level of details in the mission decomposition model and the cost to maintain it. Guidelines on mission modeling and setting mission requirements, graphical user interfaces, and visualizations would facilitate work with the system even further.

ACKNOWLEDGMENT

This research was supported by ERDF “CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence” (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

PEER REVIEW

The peer review history for this article is available at https://publons.com/publon/10.1002/eng2.12538.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

CONFLICT OF INTEREST

The authors declare no potential conflict of interest.

AUTHOR CONTRIBUTIONS

Michal Javorník: conceptualization (equal); investigation (lead); methodology (lead); validation (lead); writing – original draft (supporting). **Martin Husák:** conceptualization (equal); methodology (supporting); validation (supporting); writing – original draft (lead).

ENDNOTES

[*] See Section 3.2 for detailed information on CVSS.

[†] https://github.com/CSIRT-MU/CRUSOE

[‡] https://www.tenable.com/products/nessus

[§] https://github.com/CESNET/pakiti-server
[¶] https://www.shodan.io/
[#] National Vulnerability Database, https://nvd.nist.gov/
[‖] Common Vulnerabilities and Exposures, https://cve.mitre.org/
[**] Common Vulnerability Scoring System, https://nvd.nist.gov/vuln-metrics/cvss
[††] https://csirt.muni.cz/?lang=en
[‡‡] https://www.fnbrno.cz/en/the-university-hospital-brno/t1000

ORCID

Michal Javorník https://orcid.org/0000-0003-1076-7005
Martin Husák https://orcid.org/0000-0001-7249-9881

REFERENCES

1. Pawlicka A, Pawlicki M, Kozik R, Choraś RS. A systematic review of recommender systems and their applications in cybersecurity. *Sensors*. 2021;21(15):18.1-6.
2. Husák M, Sadlek L, Špaček S, Laštovička M, Javorník M, Komárková J. CRUSOE: a toolset for cyber situational awareness and decision support in incident handling. *Comput Secur*. 2022;115:102609.
3. Kott A, Wang C, Erbacher RF. *Cyber defense and Situational Awareness*. Springer; 2014.
4. Javorník M, Komárková J, Husák M. Decision support for mission-centric cyber defence. Proceedings of the 14th International Conference on Availability, Reliability and Security; 2019:34:1-34:8; ACM, New York, NY.
5. Jakobson G. Mission-centricity in cyber security: architecting cyber attack resilient missions. Proceedings of the 2013 5th International Conference on Cyber Conflict (CYCON 2013); 2013.
6. Malamas V, Chantzis F, Dasaklis TK, Stergiopoulos G, Kotzanikolaou P, Douligeris C. Risk assessment methodologies for the internet of medical things: a survey and comparative appraisal. *IEEE Access*. 2021;9:40049-40075.
7. Porras PA, Fong MW, Valdes A. A mission-impact-based approach to INFOSEC alarm correlation. Proceedings of the International Workshop on Recent Advances in Intrusion Detection; 2002:95-114; Springer.
8. Valeur F, Vigna G, Kruegel C, Kemmerer RA. Comprehensive approach to intrusion detection alert correlation. *IEEE Trans Depend Secure Comput*. 2004;1(3):146-169.
9. Goodall JR, D'Amico A, Kopylec JK. Camus: automatically mapping cyber assets to missions and users. Proceedings of the Military Communications Conference, 2009. MILCOM 2009; 2009:1-7; IEEE.
10. Buchanan L, Larkin M, D'Amico A. Mission assurance proof-of-concept: mapping dependencies among cyber assets, missions, and users. Proceedings of the 2012 IEEE Conference on Technologies for IEEE Homeland Security (HST); 2012:298-304; IEEE.
11. D'Amico A, Buchanan L, Goodall J, Walczak P. Mission impact of cyber events: scenarios and ontology to express the relationships between cyber assets, missions and users. Proceedings of the International Conference on Cyber Warfare and Security Academic Conferences International Limited; 2010:388.
12. Musman S, Tanner M, Temin A, Elsaesser E, Loren L. Computing the impact of cyber attacks on complex missions. Proceedings of the 2011 IEEE International Systems Conference; 2011:46-51; IEEE.
13. Sun X, Singhal A, Liu P. Who touched my mission: towards probabilistic mission impact assessment. Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense; 2015:21-26; ACM.
14. Lei J. Cyber situational awareness and mission-centric resilient cyber defense. Proceedings of the 2015 4th International Conference on Computer Science and Network Technology (ICCSNT); Vol. 01, 2015:1218-1225.
15. Guion J, Reith M. Cyber terrain mission mapping: tools and methodologies. Proceedings of the 2017 International Conference on Cyber Conflict (CyCon US); 2017:105-111; IEEE.
16. Silva FRL, Jacob P. Mission-centric risk assessment to improve cyber situational awareness. Proceedings of the 13th International Conference on Availability, Reliability and Security; 2018:56; ACM.
17. Lewis L, Jakobson G, Buford J. Enabling cyber situation awareness, impact assessment, and situation projection. Proceedings of the MILCOM 2008 - 2008 IEEE Military Communications Conference; 2008.
18. Jakobson G. Mission cyber security situation assessment using impact dependency graphs. Proceedings of the 14th International Conference on Information Fusion; 2011:1-8; IEEE.
19. Jakobson G. Extending situation modeling with inference of plausible future cyber situations. Proceedings of the 2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA); 2011:48-55.
20. Jakobson G. *Mission Resilience*. Springer International Publishing; 2014:297-322.
21. Huang Y, Huang L, Zhu Q. Reinforcement learning for feedback-enabled cyber resilience. *Annu Rev Control*. 2022;18.1-6.
22. Hutschenreuter H, Çakmakçi SD, Maeder C, Kemmerich T. Ontology-based cybersecurity and resilience framework. Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021) SCITEPRESS; 2021:458-466.
23. Zhang Y, Malacaria P. Optimization-time analysis for cybersecurity. *IEEE Trans Depend Secure Comput*. 2021.
24. Zhang H, Chari K, Agrawal M. Decision support for the optimal allocation of security controls. *Decis Support Syst*. 2018;115:92-104.

25. Correa C, Robin J, Mazo R, Abreu S. Intelligent decision support for cybersecurity incident response teams: autonomic architecture and mitigation search. In: Luo B, Mosbah M, Cuppens F, Othmane L.B, Cuppens N, Kallel S. (Eds.) *Risks and Security of Internet and Systems*. Springer International Publishing; 2022:91-107.
26. Phillips C, Swiler LP. A graph-based system for network-vulnerability analysis. Proceedings of the 1998 Workshop on New Security Paradigms; 1998:71-79; ACM, New York, NY.
27. Liu Y, Man H. Network vulnerability assessment using Bayesian networks. In: Dasarathy, B. V. (Ed.), *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005*. Vol 5812. International Society for Optics and Photonics; 2005:61-71.
28. Poolsappasit N, Dewri R, Ray I. Dynamic security risk management using Bayesian attack graphs. *IEEE Trans Depend Secure Comput*. 2012;9(1):61-74.
29. Shin J, Son H, ur Rahman K, Heo G. Development of a cyber security risk model using Bayesian networks. *Reliab Eng Syst Saf*. 2015;134:208-217.
30. Aguessy F-X, Bettan O, Blanc G, Conan V, Debar H. Hybrid risk assessment model based on Bayesian networks. In: Ogawa K, Yoshioka K. (Eds.) *Advances in Information and Computer Security*. Springer International Publishing; 2016:21-40.
31. Khosravi-Farmad M, Rezaee R, Harati A, Bafghi AG. Network security risk mitigation using Bayesian decision networks. Proceedings of the 2014 4th International Conference on Computer and Knowledge Engineering (ICCKE); 2014:267-272.
32. Khosravi-Farmad M, Ghaemi-Bafghi A. Bayesian decision network-based security risk management framework. *J Netw Syst Manag*. 2020;1794-1819.
33. Chockalingam S, Pieters W, Teixeira A, Gelder P. Bayesian network models in cyber security: a systematic review. In: Lipmaa H, Mitrokotsa A, Matulevičius R (Eds.), *Secure IT Systems*. Springer International Publishing; 2017:105-122.
34. He W, Li H, Li J. Unknown vulnerability risk assessment based on directed graph models: a survey. *IEEE Access*. 2019;7:168201-168225.
35. Zimba A, Chen H, Wang Z. Bayesian network based weighted APT attack paths modeling in cloud computing. *Futur Gener Comput Syst*. 2019;96:525-537.
36. Ibne Hossain Niamat U, Nagahi M, Jaradat R, Shah C, Buchanan R, Hamilton M. Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem. *J Comput Des Eng*. 2020;7(3):352-366.
37. Wang T, Lv Q, Hu B, Sun D. CVSS-based multi-factor dynamic risk assessment model for network system. Proceedings of the 2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC); 2020:289-294.
38. Wang J, Neil M, Fenton N. A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Comput Secur*. 2020;89:101659.
39. Li T, Jiang Y, Lin C, Obaidat M, Shen Y, Ma J. DeepAG: attack graph construction and threats prediction with bi-directional deep learning. *IEEE Trans Depend Sec Comput*. 2022;1-28.
40. Khouzani MHR, Liu Z, Malacaria P. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *Eur J Oper Res*. 2019;278(3):894-903.
41. Paruchuri P, Pearce JP, Marecki J, Tambe M, Ordonez F, Kraus S. Playing games for security: an efficient exact algorithm for solving Bayesian stackelberg games. Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems; Vol. 2, 2008:895-902.
42. Zhang Y, Malacaria P. Bayesian stackelberg games for cyber-security decision support. *Decis Support Syst*. 2021;148:113599.
43. Wang J, Neil M. A Bayesian-network-based cybersecurity adversarial risk analysis framework with numerical examples. arXiv preprint arXiv:2106.00471. 2021.
44. Huang K, Zhou C, Tian YC, Yang S, Qin Y. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Trans Ind Electron*. 2018;65(10):8153-8162.
45. Sakib N, Ibne HNU, Nur F, Talluri S, Jaradat R, Lawrence JM. An assessment of probabilistic disaster in the oil and gas supply chain leveraging Bayesian belief network. *Int J Product Econ*. 2021;235:108107.
46. Spanakis EG, Bonomi S, Sfakianakis S, et al. Cyber-attacks and threats for healthcare – a multi-layer thread analysis. Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC); 2020:5705-5708.
47. Ivanov D, Kalinin M, Krundyshev V, Orel E. Automatic security management of smart infrastructures using attack graph and risk analysis. Proceedings of the 2020 4th World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4); 2020:295-300.
48. Doynikova EV, Fedorchenko AV, Novikova ES, U shakov Igor A., Krasov AV. Security decision support in the control systems based on graph models. Proceedings of the 2021 IV International Conference on Control in Technical Systems (CTS); 2021:224-227.
49. Stergiopoulos G, Dedousis P, Gritzalis D. Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0. *Int J Inf Secur*. 2022;21(1):37-59.
50. Fielder A, Panaousis E, Malacaria P, Hankin C, Smeraldi F. Decision support approaches for cyber security investment. *Decis Support Syst*. 2016;86:13-23.
51. Nespoli P, Papamartzivanos D, Mármol FG, Kambourakis G. Optimal countermeasures selection against cyber attacks: a comprehensive survey on reaction frameworks. *IEEE Commun Surv Tutor*. 2018;20(2):1361-1396.
52. Polatidis N, Pimenidis E, Pavlidis M, Mouratidis H. Recommender systems meeting security: from product recommendation to cyber-attack prediction. In Boracchi G, Iliadis L, Jayne C, Likas A. (Eds.) *Engineering Applications of Neural Networks*. Springer International Publishing; 2017:508-519.
53. Garae J, Ko RKL. *Visualization and Data Provenance Trends in Decision Support for Cybersecurity*. Springer International Publishing; 2017:243-270.

54. Krisper M, Dobaj J, Macher G. Assessing risk estimations for cyber-security using expert judgment. In Yilmaz M, Niemann J, Clarke P, Messnarz R. (Eds.), *Systems, Software and Services Process Improvement*. Springer International Publishing; 2020:120-134.
55. Murenin I, Doynikova E, Kotenko I. Towards security decision support for large-scale heterogeneous distributed information systems. Proceedings of the 2021 14th International Conference on Security of Information and Networks (SIN); Vol. 1, 2021.
56. Gonzalez-Granadillo G, Menesidou SA, Papamartzivanos D, et al. Automated cyber and privacy risk management toolkit. *Sensors*. 2021;21(16):1-28.
57. Khemaissia R, Derdour M, Ferrag MA, Djeddai A. Network countermeasure selection under blockchain based privacy preserving. Proceedings of the 2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI); 2021.
58. Schmitz C, Pape S. LiSRA: lightweight security risk assessment for decision support in information security. *Comput Secur*. 2020;90:101656.
59. Li F, Li Y, Leng S, et al. Dynamic countermeasures selection for multi-path attacks. *Comput Secur*. 2020;97:101927.
60. Gonzalez-Granadillo G, Doynikova E, Garcia-Alfaro J, Kotenko I, Fedorchenko A. Stateful RORI-based countermeasure selection using hypergraphs. *J Inf Secur Appl*. 2020;54:102562.
61. Gonzalez-Granadillo G, Doynikova E, Kotenko I, Garcia-Alfaro J. Hypergraph-driven mitigation of cyberattacks. *Internet Technol Lett*. 2018;1(3):e38.
62. Kotenko I, Doynikova E. Selection of countermeasures against network attacks based on dynamical calculation of security metrics. *J Defense Model Simul*. 2018;15(2):181-204.
63. Schmidt A, Albert LA, Zheng K. Risk management for cyber-infrastructure protection: a bi-objective integer programming approach. *Reliab Eng Syst Saf*. 2021;205:107093.
64. Javorník M, Komárková J, Sadlek L, Husák M. Decision support for mission-centric network security management. Proceedings of the 2020 IEEE/IFIP Network Operations and Management Symposium (NOMS 2020); 2020.
65. Laštovička M, Husák M, Sadlek L. Network monitoring and enumerating vulnerabilities in large heterogeneous networks. Proceedings of the NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium; 2020.
66. Ushakov R, Doynikova E, Novikova E, Kotenko I. CPE and CVE based technique for software security risk assessment; Vol. 1, 2021:353-356.
67. Sheyner O, Haines J, Jha S, Lippmann R, Wing Jeannette M. Automated generation and analysis of attack graphs. Proceedings of the 2002 IEEE Symposium on Security and Privacy; 2002:273-284; IEEE.
68. Kaynar K. A taxonomy for attack graph generation and usage in network security. *J Inf Sec Appl*. 2016;29:27-56.
69. Yi S, Peng Y, Xiong Q, et al. Overview on attack graph generation and visualization technology. Proceedings of the 2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID); 2013:1-6.
70. Rodriguez-Bermejo DS, Medenou RD, Riquelme RP, Vidal JM, Torelli F, Sánchez SL. Evaluation methodology for mission-centric cyber situational awareness capabilities. Proceedings of the 15th International Conference on Availability, Reliability and SecurityAssociation for Computing Machinery; 2020; New York, NY.
71. Happa J, Agrafiotis I, Helmhout M, Bashford RT, Goldsmith M, Creese S. Assessing a decision support tool for SOC analysts. *Digital Threats Res Pract*. 2021;22(3):1-35.
72. Gutzwiller R, Dykstra J, Payne B. Gaps and opportunities in situational awareness for cybersecurity. *Digital Threats Res Pract*. 2020;1(3):18;1-6.

How to cite this article: Javorník M, Husák M. Mission-centric decision support in cybersecurity via Bayesian Privilege Attack Graph. *Engineering Reports*. 2022;e12538. doi: 10.1002/eng2.12538