Lightweight Impact Assessment and Projection of Lateral Movement and Malware Infection

Martin Husák*‡, Michal Javorník*,
*Institute of Computer Science, Masaryk University, Czech Republic
†Cyber Center for Security and Analytics, The University of Texas at San Antonio, USA
husakm@ics.muni.cz, javor@ics.muni.cz

***Abstract*—Resilient IT infrastructures must maintain the required service level even when faced with adversarial activity. Not only should we aim at minimizing the attack surface by hardening our cyber assets, but we should also elaborate on how to respond to running cyber attacks and immediate threats in situations where there is not enough time to patch vulnerabilities or other harden the infrastructures. In this work, we propose a lightweight approach to increasing resilience by projecting the attacker's lateral movement or the spread of malware. While related work builds on elaborate vulnerability assessment and analysis of complex attack paths, we were inspired by recent advances in rapid incident response, namely the recommendation of similar devices close to those already exploited. Using this approach, we can provide prompt recommendations using only the easily obtainable data on the cyber assets, such as device fingerprints. We prioritize promptness and applicability over precision, which complements the existing approaches.**

***Index Terms*—cybersecurity, resilience, lateral movement**

I. Introduction

Resilient information systems and computer networks have become vital due to the reliance of today's society on such systems. Cyber attacks may debilitate organizations, communities, or even societies. Ensuring the continuation of IT services, namely in critical infrastructures, is often of utmost importance, even when facing a cyber attack or malware infection. Various approaches to increasing the resilience of IT infrastructures were proposed in related works [1], [2]. Researchers conducted elaborated vulnerability scans and dependency detection and modeling to conduct attack impact assessment [3]–[5]. Moreover, they proposed attack projection and prediction methods to estimate the upcoming attacks or the continuation of a running one [3], [6]. Recently, recommender systems were employed for the cybersecurity needs to help address the cyber attacks at the right place at the right time [3], [7], [8]. However, the cybersecurity teams are often understaffed or overloaded with work to successfully deploy all the tools proposed in recent research, namely in situations when the tools require non-trivial amounts of high-quality data or other inputs that are hard to collect [6], [9].

We are aiming to resolve two problems not or only partially addressed in related work. First, the existing approaches to model and project the attacks, assess risks, and estimate the next targets, are usually heavily dependent on high-quality data on the protected network [2], [3], [10], [11]. A detailed vulnerability assessment and scoring or dependency detection between the assets in the network are time and resource-consuming and might not be feasible on a large scale or with a sufficient level of precision or at all in many environments [12]. Moreover, the threat landscape and cybersecurity situation are dynamic and constantly changing. The related works often rely on static analysis of a snapshot of the current situation, while the situation may change dramatically in a short time.

In this paper, we propose an approach to increasing network resilience by estimating the next possible targets of the attacker's lateral movement or spread of malware. Our approach builds upon the risk score calculated from the similarity and proximity of devices in the network [6], [13]. Contrary to previous works, our work utilizes much simpler measurements and data collection; instead of running deep vulnerability scans and dependency assessments, we only require device fingerprints and network topology. Moreover, our approach is reactive and considers a currently running attack, lateral movement, and malware infection spread. Our contribution is a proposal of a system that is much easier to implement, deploy, and use in practice while providing novel features.

This paper is structured into five sections. Section II summarizes related work. Section III defines the similarity and distance metrics used for the risk score calculation. Projection of the attacker's lateral movement or malware infection spread is discussed in Section IV. Section V concludes the paper.

II. Background and Related Work

This work builds on top of several research directions and continuous research and development efforts that often intertwine and complement each other. Namely, we extend the research into decision support and recommender systems in cybersecurity [6], [8] and the use of Bayesian networks for such purposes [2], [14].

A. Decision support in cybersecurity

Decision support and recommender systems are interesting area of cybersecurity research with promising application, even though they are not widely used in practice yet [7], [8], [15]. Nevertheless, there is a plethora of ongoing research on decision support in cybersecurity. The existing works aim at a rather static recommendations like optimal investment in cyber defences, placement of sensors and defense mechanisms [7], [15]. However, not many works are dedicated to incident

response and taking prompt actions [8], where a poor decision-making is a an issue of paramount importance [9].

A prime example of decision support in cybersecurity is the work of Polatidis et al. [3], who proposed their application for attack prediction and selection of the most probable path the attacker will take in an attack graph. A common task for decision support tools in cybersecurity research is finding an optimal countermeasure to a cyber attack. Such works were surveyed by Nespoli et al. [16]. Other noteworthy works include the combined intrusion detection and recommender system proposed by Katherine B. Lyons [17]. Such a system recommends an action at the time of the incident detection. Sayan et al. [18] went even further and proposed making recommendation of countermeasure combined with attack prediction. Nisioti et al. [19] proposed a decision support system that aims at reducing the duration of digital forensics investigation. Recently, Husák and Bouček [6], [13] proposed a tool that recommends similar devices in close proximity of an already infected devices, which is aiming directly at incident response and attack mitigation.

B. Application of Bayesian networks in cybersecurity

This work employs the concept of Bayesian networks, which is well-known to cybersecurity research community; they are namely known as a popular extension of the attack graphs, enabling stochastic reasoning over the representations of cyber assets and their vulnerabilities [14].

In recent years, Khosravi-Farhad et al. [4] proposed the use of the Bayesian decision networks to measure the impact of vulnerabilities and to find minimum-cost security measures. Khouzani et al. [5] approached 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. A similar approach was taken by Javorník and Husák [2] to select the most resilient configuration of an IT infrastructure under adversarial activity. Zimba et al. [20] 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. [1] 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. [10] proposed a dynamic risk assessment model that uses the Bayesian attack graph to infer the system risk status. Li et al. [21] approached the complexity of attack graphs and proposed a system that makes a prediction of which attack path in the graph is more likely to be taken by an attacker. Wang et al. [22] extended FAIR (Factor Analysis of Information Risk) model for quantitative cybersecurity risk assessment based on quantifiable risk factors.

In a very recent and closely related work, Sharmin et al. [11] proposed the use of Bayesian belief networks to infer the targets of the attacks based on the passive reconnaissance data, including OS fingerprints.

Apart from approaching generic cybersecurity problems, researchers also delved into specific use cases and deployment environment using the techniques discussed in other related works. The examples include impact assessment in cyber-physical systems [23], prediction and assessment of disasters in the oil and gas supply chain [24], health service [25], smart cities [26], or Industry 4.0 [27].

It is also worth noting that Howland [28] argued the CVSS scores, which are widely used in the afore-mentioned works [2], [10], [11], are not suitable metrics for assessing severity and risk of the vulnerabilities.

III. Modeling IT Infrastructures

Modeling the IT infrastructures is a hard task due to their complexity and the large number of actors and factors to consider [29]. Often, there is a need to balance the complexity, richness, and precision of information with practical abilities to collect and update them in reasonable time and use them effectively [29]. In this work, we are inspired by the CRUSOE data model [30], which aims at balancing data precision with their feasibility. We provide a simplified model to illustrate our approach that does fully conform to the data model. Nevertheless, we then highlight how to enhance our model towards accepting more features into consideration for further calculations.

The remainder of this work considers two concepts, similarity and proximity, which are subsequently used to calculate the risk score. We set up a simple model to capture the data required to calculate them. Both can be derived from multiple features and their combination and thus, we highlight a few features as examples.

A. Similarity Metrics

First, the similarity metrics designate how similar are the two hosts to each other regardless of their location. Potential features include the hardware and software equipment or the number and variety of provided network services.

The similarity can be derived from the fingerprint of an operating system of the machine. The fingerprints are easy to collect via active network scanning (e.g., using Nmap [31]). Exporting fingerprints into the CPE format allows for processing by the machine since it is structured. The OS fingerprint suggest not only the OS of the machine but also its type and role in the network – Windows and MacOS hosts suggest workstations, Unix/Linux suggests servers, while Android or iOS suggests a mobile device. This is not exact, but gives a rough idea, which is sufficient for the probabilistic assessment discussed in this paper. It is worth noting that even such a simplistic approach can be sufficient for large-scale vulnerability assessment [12].

B. Proximity Metrics

Second, the proximity of the two hosts in the network may be determined by a plethora of features. A natural one is a

physical distance, which may play a role in the case of mobile devices. In the remainder of this work, however, we focus on metrics of logical distance or, more precisely, node distance in various graph-based representations, such as network topology. We derive multiple tree-like representations of the network hosts and their belonging to the same subnet or IP address range or organization's department. We emphasize models that can be constructed using simple network measurements and asset management.

Our main source of inspiration is the CRUSOE toolset [30], which successfully employed graph representation of all the entities and relationships in the infrastructure. Let the nodes in the graph represent the hosts in the network, subnets, departments, fingerprints, and other relevant entities. The relations indicate whether the fingerprint was taken from the host or the host belongs to the subnet or department. Even if not all the data sources are used or available, the CRUSOE toolset shows it is possible to collect and aggregate such data using mostly non-specialized tools.

An example of proximity metrics represented in the graph is displayed in Figure 1. Let's comment on three examples of proximity metrics motivated by three distinct attack vectors. First, let's consider a self-spreading malware, such as a worm. Worms typically scan their surrounding networks to find hosts to exploit further. Thus, the hosts in the same IP address range or subnet are threatened. Second, the malware can spread via infected USB sticks, malicious files, or email attachments. In such cases, it will most likely spread to devices used by the same user as the already infected one. If a centralized authentication system is used, we may assess which users logged in to which devices and, thus, are users of such systems. Alternatively, in the working environment, the users in the same office may share the USB sticks or malicious emails can be forwarded among colleagues. In such cases, we may employ asset management and model how each device belongs to a certain employee or department and fall under the organization's divisions.

C. Risk Score: Estimating the Probability of Attack Spread

Related works approach the cybersecurity situation assessment via a rather static vulnerability assessment that would include the construction of highly detailed attack graphs [2], [3]. In our work, we chose a more speculative approach since, during the incident response, cybersecurity teams need to act promptly but do not have enough information on the present vulnerabilities and details on the malware or attacker. The main question in this section, inspired by related work [6], is: *if one device in the infrastructure is exploited, what is the probability of the spread of infection on another device?*

The fundamental concepts of our approach are based on the proximity and similarity of the devices in the network, as proposed by Husák [6]. For each pair of devices, a *risk score* (R) can be calculated. R a quotient of *similarity* (S) and *distance* (D) of the two devices. It is calculated as follows [6]:

$$R = \frac{S}{D} = \frac{s_1 * s_2 * ...s_n}{min\{d_1, d_2, ..., d_n\}} \quad (1)$$

In practice, weights are assigned to partial similarities ($s_1...s_n$) and distances ($d_1...d_n$).

The similarity is calculated as a product of all considered partial similarities, each having a value in the range $< 0, 1 >$. For simplicity, let's consider only the similarity of the OS fingerprints. CPE strings are widely used to represent a piece of software, including the operating systems, and can be provided by network scanning software, such as Nmap [31]. Thus, the assumed similarity is the similarity of the two CPE strings. Since CPE are character strings, a Levenshtein distance can be used. However, related work [6] leverages the fact that each part of a CPE string has a different value and adds more points for the same vendor or major version, fewer points for the same minor version or patch, and so on.

The distance leverages the graph-based representation of data originally proposed for the CRUSOE data model [30]. Formally, the distance stands for the shortest path between the two nodes representing devices in the network over the nodes of certain types. The node types depend on the chosen metric. Reminding Figure 1, we may see two features: organizational hierarchy (top, yellow) and network topology (orange, bottom). Let's say we calculate the distance between the two Linux servers. They are in the same subnet, so the metric of network topology gives a distance of 2, but they are in different departments, which gives the distance in the organizational hierarchy of 6. The final distance for the risk score calculation is the minimal distance of all, in this case, 2 from the network topology.

Recently, a tool was created to recommend similar devices in close proximity to an infected one using the risk score [13]. Before the recommendations can be made, there is a need to collect data on the infrastructure. The discussed tool uses the CRUSOE toolset [30] for this purpose. The toolset provides rich, heterogeneous data on network assets and their relationships. The richer the data are, the more features can be included in the risk score calculation, and the more precise the recommendations can be. However, simple data can be used as well; the minimal dataset could consist of network topology, device enumeration, and fingerprints of the devices. Such data can be obtained with common tools, such as Nmap, and can be frequently updated. The physical location of devices (e.g., building, room), belonging of device or subnet to the organization's department, or authentication logs indicating who uses which device are other sources of valuable data for the recommendations. Readers are kindly referred to the related works [6], [13], [30] and GitHub repository[1] for implementation details.

[1]https://github.com/CSIRT-MU/recommender-system-for-network-security-management

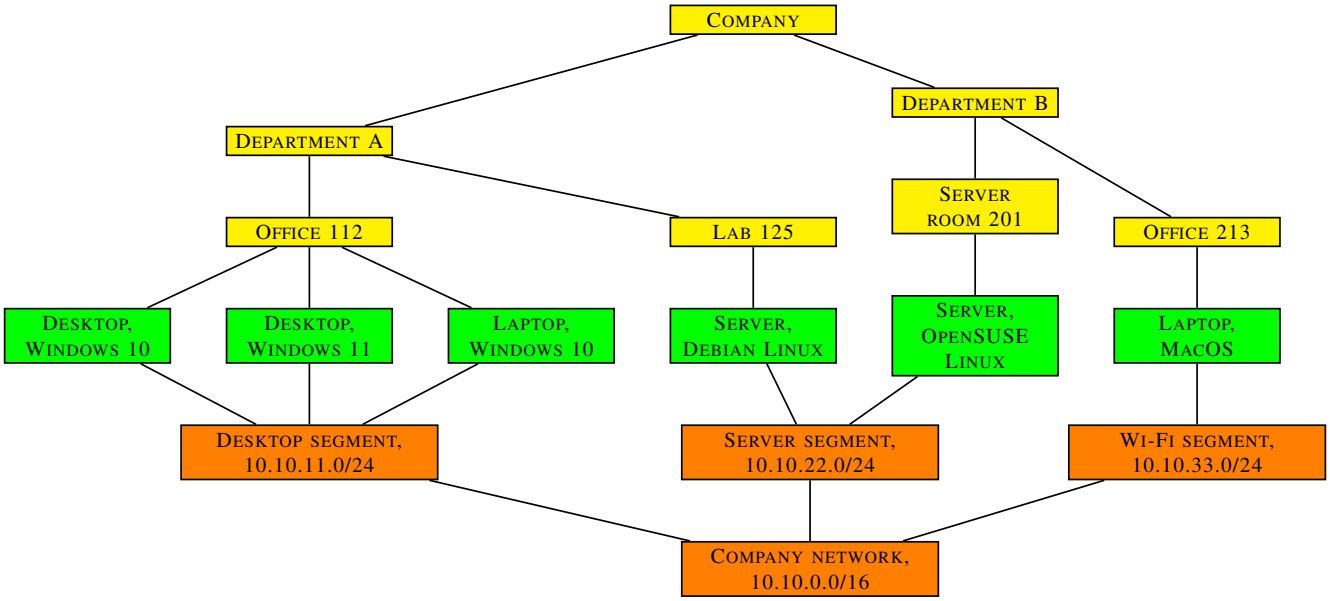

Fig. 1. A simple IT infrastructure model with network hosts (middle, green) organized in organization's hierarchy (top, yellow) and network topology (bottom, orange).

IV. Attack and Malware Spread Projection using Bayesian Network

In the previous, we illustrated how to model the assets in the IT infrastructure and formalized the *risk score* calculation that estimates the probability of malware spread or attacker's lateral movement from one host to another. Herein, we extend the *risk score* towards the whole network to model the attack or infection spread on a larger scale. We propose an approach to model lateral movement or attack spread in the network using Bayesian network and inference, which we describe in the first subsection. Subsequently, we propose several additions to the base model, which reflect practical needs and use cases.

Let's have a set of hosts in the network. Each host has a set of features, belongs to certain groups, or has relationships with other entities, which all allow for calculating the risk score between all pairs of hosts in the network. To begin with, we construct a graph with nodes only, no edges. The nodes represent the hosts in the network. Adding the edges requires caution because before we can convert the graph into a Bayesian network (BN), we need to ensure the graph is acyclic. Moreover, we need to define how to fill the Conditional Probability Tables (CPTs) in nodes with multiple incoming nodes.

We propose an algorithm to construct the BN to help in our calculations. The BN is constructed just in time when an attack is detected or suspected. For each host, we assign a number $(0, 1>$, where 0 means no adversarial control of the host, 1 means confirmed attacker's control over the host, and values in between represent the probability of the attacker's control over that host.

The construction of the BN is formalized in Algorithm 1 and works as follows. The initial graph contains a node for each

Algorithm 1 The construction of the Bayesian network.

```
▷ Inputs
H ← list of hosts in the network
h ← already exploited host
t ← risk score threshold value
▷ Variables
G ← new empty directed graph
P ← empty list          ▷ nodes added in previous iteration
C ← empty list          ▷ nodes added in current iteration
G ← h
P ← h
▷ Further iterations
while no edge can be added do
    for i in P do
        for j in H do
            if (i,j) would not create cycle in G then
                if (riskScore(i, j) > t) then
                    G ← j
                    G ← (i,j)
                    C ← j
                end if
            end if
        end for
    end for
    ▷ Updating and clearing the lists of newly added hosts for the next iteration
    P ← C
    C ← empty list
end while
return G
```

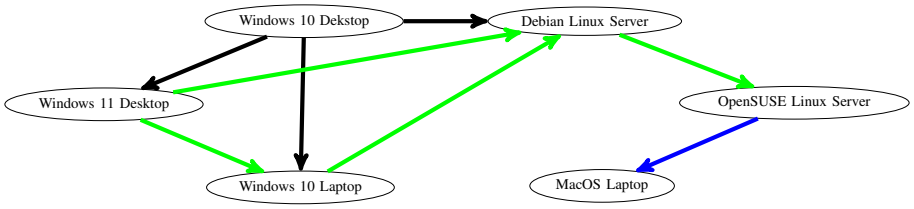

Fig. 2. An example of the construction of a Bayesian network starting with the Windows 10 Desktop. Black arrows are added in the first iteration, green arrows in the second iteration, and blue arrow in the final iteration.

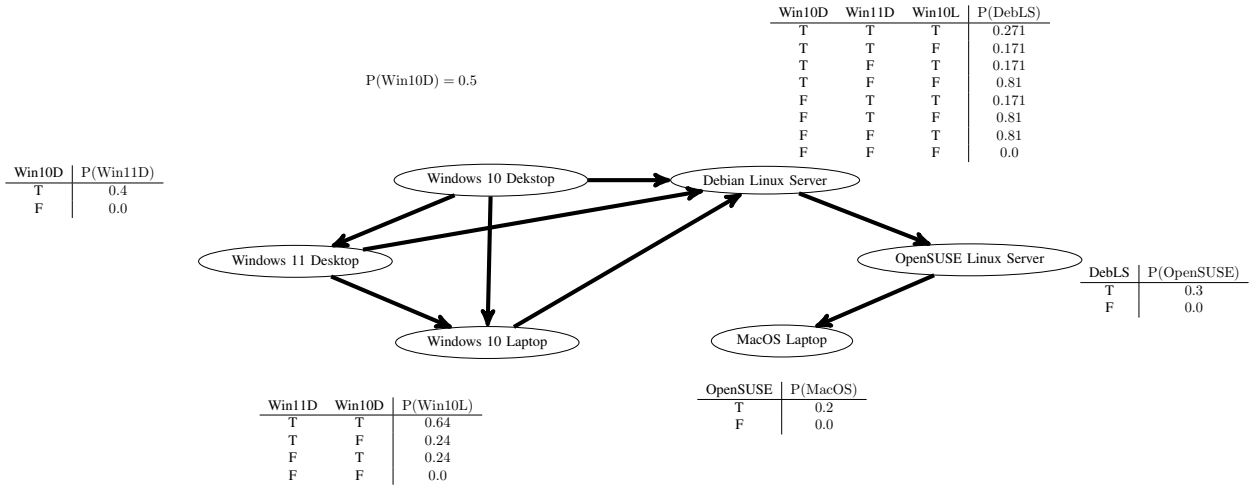

Fig. 3. A sample Bayesian network for the attack spread estimation - final stage with CPTs.

host and no edges. The edges are added one by one so that the graph remains directed and acyclic. Only those edges for which the Risk Score is bigger than a pre-defined threshold can be added to the graph. The construction starts from the already infected node (as reported by other tools or observations). In random order, we process the nodes added to the graph in the previous step. The processing of a node means adding the directed edges from that node to the node of the initial graph that were not yet processed. The edges are weighted with the risk score between the two nodes and added to the BN. The step processing of nodes is repeated until it it not possible to add another edge or there are no isolated nodes in the original graph. Figure 2 illustrates the process of constructing the BN in three iterations, where in each iteration, the nodes added in the previous iteration are processed. No edge is added if the associated risk score is below threshold or the graph would become cyclic.

When the graph is constructed, we need to add CPTs. Our assumption is that the attacker may advance simultaneously in all possible ways. The risk scores, which are used as the weights of the directed edges, are used to represent independent events. Thus, all the incoming edges of a node are independent events. We construct the CPT of a node using the risk scores of the incoming edges. All the probabilities can now be calculated. Figure 3 illustrates the final stage of the BN construction with the CPTs added.

The described algorithm leads to the construction of a BN representing the joint probability distribution of the considered cybersecurity risks over a given network of cyber components. Given a joint probability distribution defined this factorized form, we can efficiently calculate the risk of an individual or even of the group of desired cyber components. A fundamental feature of the inference mechanism is its ability to recalculate the so-called posterior distribution of unobserved desired variables using the so-called prior distribution and the distribution of the observed variables.

The output of the calculation is the probability of exploitation of all the devices in the infrastructure. The users can sort the devices in the network by this probability to locate devices that are threatened the most by the current attack. Naturally, the imminent threat is faced by the devices that are similar and close to those already exploited. Nevertheless, the attack may propagate in the infrastructure and exploit other devices that are farther or less similar. If such devices support the critical infrastructure or critical organization's mission, the users may be alerted of this fact and plan their protection ahead of the attack spread.

V. Conclusion

In this paper, we proposed a novel approach to selecting the most resilient configuration of the IT infrastructure. Instead of relying on elaborate asset and vulnerability assessment, we propose using a more lightweight approach based on the

projection of the attacker's lateral movement and malware infection spread based on the similarity and closeness of devices in the network [6]. The data required to support our approach are easily obtainable with common tools, and the novel techniques are partially implemented in related work [13], which makes our approach easily implementable and quickly usable in practice. Moreover, it aligns well with current incident response practices and procedures [8], which further facilitates potential deployment and usage.

In our future work, we are going to provide a functional sample or reference implementation of our approach, as well as an artificial or well-anonymized data sample for evaluation and experimentation. We plan on further intertwining the cybersecurity tools and approaches to maximize the usability of particular procedures and find novel uses for them that would increase the capabilities of security teams without inflating their toolsets and further overwhelming the incident handlers.

ACKNOWLEDGMENT

This research was supported by project "MSCAfellow5_ MUNI" (No. CZ.02.01.01/00/22_010/0003229).

REFERENCES

[1] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using bayesian network-based approach: a system of systems problem," *Journal of Computational Design and Engineering*, vol. 7, no. 3, pp. 352–366, 2020.

[2] M. Javorník and M. Husák, "Mission-centric decision support in cybersecurity via bayesian privilege attack graph," *Engineering Reports*, vol. 4, no. 12, p. e12538, 2022.

[3] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks," *Evolving Systems*, vol. 11, no. 3, pp. 479–490, 2020.

[4] M. Khosravi-Farmad and A. Ghaemi-Bafghi, "Bayesian decision network-based security risk management framework," *Journal of Network and Systems Management*, vol. 28, pp. 1794–1819, 2020.

[5] M. Khouzani, Z. Liu, and P. Malacaria, "Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs," *European Journal of Operational Research*, vol. 278, no. 3, pp. 894–903, 2019.

[6] M. Husák, "Towards a data-driven recommender system for handling ransomware and similar incidents," in *2021 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2021.

[7] A. Pawlicka, M. Pawlicki, R. Kozik, and R. S. Choraś, "A systematic review of recommender systems and their applications in cybersecurity," *Sensors*, vol. 21, no. 15, 2021.

[8] M. Husák and M. Čermák, "SoK: Applications and Challenges of Using Recommender Systems in Cybersecurity Incident Handling and Response," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: ACM, 2022.

[9] J. Happa, I. Agrafiotis, M. Helmhout, T. Bashford-Rogers, M. Goldsmith, and S. Creese, "Assessing a decision support tool for soc analysts," *Digital Threats: Research and Practice*, vol. 2, no. 3, 6 2021.

[10] T. Wang, Q. Lv, B. Hu, and D. Sun, "CVSS-based Multi-Factor Dynamic Risk Assessment Model for Network System," in *2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, 2020, pp. 289–294.

[11] N. Sharmin, S. Roy, A. Laszka, J. Acosta, and C. Kiekintveld, "Bayesian models for node-based inference techniques," in *2023 IEEE International Systems Conference (SysCon)*, 2023.

[12] M. Laštovička, M. Husák, and L. Sadlek, "Network monitoring and enumerating vulnerabilities in large heterogeneous networks," in *IEEE/IFIP Network Operations and Management Symposium*, 2020.

[13] V. Bouček and M. Husák, "Recommending similar devices in close proximity for network security management," in *2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2023, pp. 481–484.

[14] S. Chockalingam, W. Pieters, A. Teixeira, and P. van Gelder, "Bayesian network models in cyber security: A systematic review," in *Secure IT Systems*. Cham: Springer International Publishing, 2017, pp. 105–122.

[15] L. Ferreira, D. C. Silva, and M. U. Itzazelaia, "Recommender systems in cybersecurity," *Knowledge and Information Systems*, pp. 1–37, 2023.

[16] P. Nespoli, D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1361–1396, Secondquarter 2018.

[17] K. B. Lyons, "A recommender system in the cyber defense domain," Master's thesis, Air Force Institute of Technology, 2014.

[18] C. Sayan, S. Hariri, and G. Ball, "Cyber security assistant: Design overview," in *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS*W)*. New York, NY, USA: IEEE, 2017, pp. 313–317.

[19] A. Nisioti, G. Loukas, A. Laszka, and E. Panaousis, "Data-driven decision support for optimizing cyber forensic investigations," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2397–2412, 2021.

[20] A. Zimba, H. Chen, and Z. Wang, "Bayesian network based weighted apt attack paths modeling in cloud computing," *Future Generation Computer Systems*, vol. 96, pp. 525–537, 2019.

[21] T. Li, Y. Jiang, C. Lin, M. Obaidat, Y. Shen, and J. Ma, "Deepag: Attack graph construction and threats prediction with bi-directional deep learning," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[22] J. Wang, M. Neil, and N. Fenton, "A bayesian network approach for cybersecurity risk assessment implementing and extending the fair model," *Computers & Security*, vol. 89, p. 101659, 2020.

[23] K. Huang, C. Zhou, Y. C. Tian, S. Yang, and Y. Qin, "Assessing the physical impact of cyberattacks on industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 8153–8162, Oct 2018.

[24] N. Sakib, N. U. Ibne Hossain, F. Nur, S. Talluri, R. Jaradat, and J. M. Lawrence, "An assessment of probabilistic disaster in the oil and gas supply chain leveraging bayesian belief network," *International Journal of Production Economics*, vol. 235, p. 108107, 2021.

[25] E. G. Spanakis, S. Bonomi, S. Sfakianakis, G. Santucci, S. Lenti, M. Sorella, F. D. Tanasache, A. Palleschi, C. Ciccotelli, V. Sakkalis, and S. Magalini, "Cyber-attacks and threats for healthcare – a multi-layer thread analysis," in *2020 42nd Annual International Conference of the IEEE Engineering in Medicine Biology Society (EMBC)*. IEEE, 2020, pp. 5705–5708.

[26] D. Ivanov, M. Kalinin, V. Krundyshev, and E. Orel, "Automatic security management of smart infrastructures using attack graph and risk analysis," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 295–300.

[27] G. Stergiopoulos, P. Dedousis, and D. Gritzalis, "Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in industry 4.0," *International Journal of Information Security*, vol. 21, no. 1, pp. 37–59, 2022.

[28] H. Howland, "CVSS: Ubiquitous and Broken," *Digital Threats*, vol. 4, no. 1, feb 2022.

[29] M. Husák, T. Jirsík, and S. J. Yang, "SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: ACM, 2020.

[30] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, and J. Komárková, "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling," *Computers & Security*, vol. 115, p. 102609, 2022.

[31] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.Org, 2008.