2023 IEEE International Carnahan Conference on Security Technology (ICCST) | 979-8-3503-1587-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCST59048.2023.10726853

Enhancing Cybersecurity Proactive Decision-Making through Attack Tree Analysis and MITRE Framework

Anas Husseis
Industrial Cybersecurity
Ikerlan
Mondragon/Arrasate, Spain
ahusseis@ikerlan.es

Jose Luis Flores
Industrial Cybersecurity
Ikerlan
Mondragon/Arrasate, Spain
jlflores@ikerlan.es

Andrej Bregar
Cybersecurity
Informatika d.o.o
Maribor, Slovenija
andrej.bregar@informatika.si

Giovanni Mazzeo
Department of Economics, Law, Cybersecurity, and Sports Sciences
University of Naples 'Parthenope'
Napoli, Italy
giovanni.mazzeo@uniparthenope.it

Luigi Coppolino
Department of Engineering
University of Naples 'Parthenope'
Napoli, Italy
luigi.coppolino@uniparthenope.it

***Abstract*—In today's increasingly complex and dynamic cybersecurity landscape, organizations face the constant challenge of identifying and addressing security requirements effectively. This article proposes a comprehensive approach aimed at enhancing the process of cybersecurity decision-making and streamlining security analysis. This is achieved by leveraging attack tree analysis, the MITRE framework - particularly ATT&CK and D3FEND, as well as the Gordon-Loeb cost-benefit model. Attack trees provide a structured representation of potential vulnerabilities and attack paths, while the MITRE framework offers a robust knowledge base of real-world attack methods and corresponding mitigations. Moreover, analysing the financial cost and benefits coming from implementing a remediation strategy provides significant input for the decision maker. By integrating these approaches, organizations gain valuable insights into their security posture, prioritize security measures, and allocate resources more effectively. This article explores the methodology of mapping attack tree nodes to specific MITRE attack techniques and the corresponding mitigations and applies Gordon-Loeb cost-benefit model so that organizations optimize their security strategy and bolster their overall cybersecurity resilience.**

***Index Terms*—Proactive Cybersecurity, MITRE, Decision Making, Cost-Benefit, Attack Trees**

I. Introduction

In the context of cybersecurity, organizations continuously strive to identify and address security requirements in a proactive and systematic manner. With the evolving threat landscape and increasing sophistication of cyber-attacks, there is a pressing need for comprehensive approaches that aid in cybersecurity decision-making and facilitate the analysis of security requirements. This article introduces a methodology designed to streamline the process of identifying vulnerabilities and determining appropriate mitigation strategies. The approach involves a fusion of attack tree analysis and the MITRE framework, with specific emphasis on leveraging ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [1] and D3FEND (Detection, Denial, and Disruption Framework Empowering Network Defense) [2]. Additionally, we integrate the Gordon-Loeb (GL) cost-benefit model [3] in the attack tree aiming to provide directives for the decision maker such that the potential loss resulting from cyber attacks and the benefits of implementing a set of mitigation actions are taken into account.

Attack trees provide a structured representation of the steps an attacker may take to exploit weaknesses in a system or network. By decomposing an attack into its constituent parts, attack trees enable a systematic understanding of potential threats and aid in prioritizing security measures [4]. Previous research has acknowledged the importance of attack trees as effective instruments for the analysis and visualization of potential attack paths and vulnerabilities. Within this domain, Xie et al. proposed a methodology for risk assessment that utilizes attack trees to establish an integrated risk model, encompassing both the cyber and physical layers of a system [5]. Additionally, Xu et al. incorporated attack trees into an approach aimed at evaluating attack identification for the security management of Software-Defined Networking [6]. Moreover, a recent study employed attack trees in the development of a software application that automates and formalizes the assessment of information security for system assets while identifying security weaknesses within the system [7]. In the electric sector, the National Electric Sector Cybersecurity Organization Resource (NESCOR) reported various examples of complex attack trees targeting the Electric Power and Energy Sector (EPES) [8].

While attack trees serve to model diverse ways for executing cyber attacks, it is valuable to consolidate existing knowledge and frameworks, such as the MITRE framework, in order to

979-8-3503-1587-5/23/$31.00 ©2023 European Union

establish a comprehensive and integrated approach to modelling threats and countermeasures. MITRE framework, widely regarded as a leading resource in the cybersecurity community, offers valuable insights into real-world attack methods and corresponding mitigations. ATT&CK provides a knowledge base of adversary tactics, techniques, and procedures (TTPs) [1], while D3FEND complements it by focusing on defensive cyber foundations [9]. In order to characterize the financial impact and measure the costs of the selected mitigations and the benefit they provide to the organization, GL model presents a suitable framework to perform cost benefit analysis in the cybersecurity.

Building upon these foundations, this article introduces a methodology for enriching attack trees by mapping attack tree nodes to specific techniques and sub-techniques from ATT&CK and then assigning the required values on the tree in order to perform the cost benefit analysis; this is explained in detail in section IV. By doing so, security practitioners can easily identify the relevant mitigations provided by the MITRE framework, enabling a more streamlined and informed decision-making process.

II. Modeling Cyber-Threats Using Attack Trees: A Use Case on EPES

When organizations embark on the assessment of security requirements and the evaluation of their preparedness against cyber security threats, a crucial initial step involves defining the infrastructure assets and conducting a comprehensive risk assessment. Various standards, such as IEC 62443, ISO 27001, and Magerit [10], offer explicit directives and recommendations for conducting effective risk assessments. In this article, our focus is centered specifically on the guidance provided by the IEC 62443 standard.

According to the IEC 62443 standard, specifically IEC 62443-3-2 Clause 4 depicts the workflow that outlines the primary steps required to establish zones and conduits as well as the risk assessment. These steps can be summarized as the following Zones & Conduit Requirements (ZCRs):

- ZCR 1. Identify the System Under Consideration (SUC).
  - Input: Initial system architecture diagrams and inventory. Company policies, regulations, tolerable risk guidelines, etc.
  - Output: Updated system architecture diagrams and inventory with IACS external services and support identified.
- ZCR 2. Perform and initial cyber security risk assessment.
  - Input: Existing PHAs and other relevant risk assessment and corporate risk matrix.
  - Output: Initial evaluation of risk.
- ZCR 3. Partition the SUC into zones and conduits.
  - Input: Standards and best practices, policies, supplier guidelines, critically assessments, data flows, functional specifications, etc.
  - Output: Initial or revised zone and conduit diagram.
- ZCR 4. Initial risk exceeds tolerable risk?
  - YES → ZCR 5. A detailed cyber security risk assessment must be performed.
    - Output: Residual cyber security risk and Target Security Levels (SL-Ts) for each zone and conduit.
  - NO → ZCR 6. Document cyber security requirements, assumptions and constraints.
    - Input: Company policies, regulations, tolerable risk guidelines, etc.
    - Output: Cyber security requirement specification (CRS).
- ZCR 7. Asset Owner Approval

The concept of attack trees aligns seamlessly with this risk assessment process, as cyber security experts engage in a meticulous examination of potential threats and their associated impacts. Concurrently, they calculate the actual security level, known as the Achieved Security Level (SL-A), for each individual zone. It is imperative for these experts to delineate the appropriate security measures that ensure $SL-\mathrm{A} \geq SL-\mathrm{T}$, effectively aligning with the desired security objectives.

A. Practical Use Case: Analyzing Attack Tree at EPES Watt Hour Meter

This sub-section presents a practical use case in the EPES sector, demonstrating the application of attack trees and their mapping to the ATT&CK framework. Specifically, we analyse the vulnerabilities within the customer zone, focusing on the threat actor targeting the client's watt-hour meter (Figure 1). The objective of the attacker in this scenario is to manipulate the meter measurements, posing potential risks such as fraudulent billing or unauthorized access to electricity.

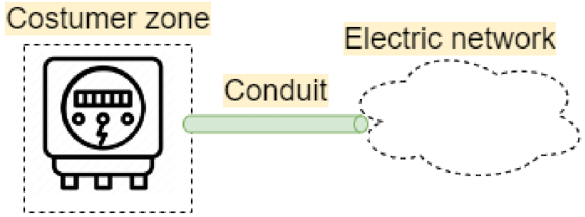


Fig. 1. Electric sub-infrastructure at the customer side.

Figure 2 illustrates the attack tree structure, where the first leaf on the top represents the initial requirement of the threat agent obtaining physical access to the meter. This requirement serves as a foundation for the subsequent attack attempts. Moving to the second level of the tree, we delve into the primary methods that the attacker can employ, including hardware manipulation, targeting communication channels, and compromising the software component/s. Finally, the last layer of the tree outlines the specific techniques and sub-techniques that can be employed to exploit existing vulnerabilities.

The two layers in the bottom of the tree represent the consequences in case those attacks were successful, specifically: bill manipulation, unauthorized access, and denial of service.

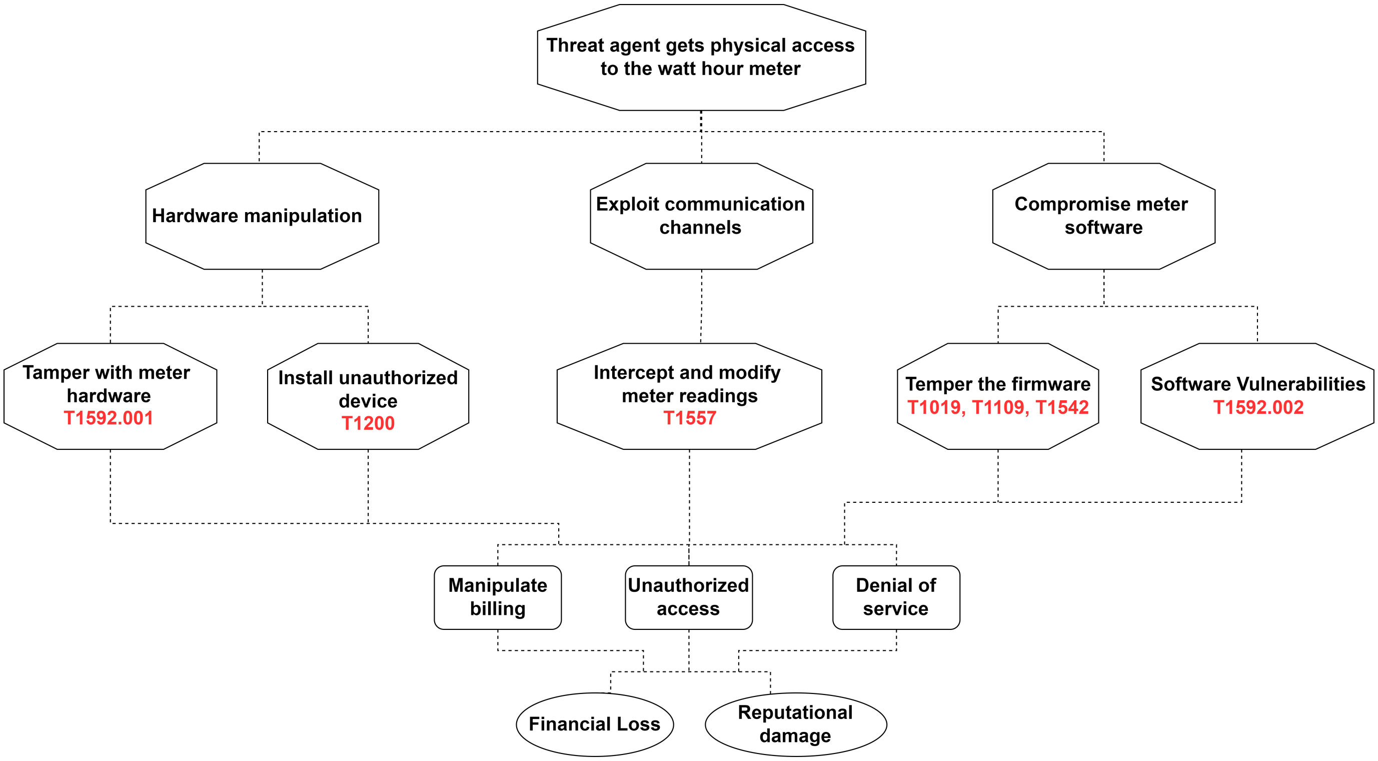

Threat agent gets physical access to the watt hour meter
Hardware manipulation
Exploit communication channels
Compromise meter software
Tamper with meter hardware
T1592.001
Install unauthorized device
T1200
Intercept and modify meter readings
T1557
Temper the firmware
T1019, T1109, T1542
Software Vulnerabilities
T1592.002
Manipulate billing
Unauthorized access
Denial of service
Financial Loss
Reputational damage

Fig. 2. Attack tree on the customer zone.

The impact of these consequences will result in financial loss as well as reputational damage.

For the purposes of this example, our focal point centers exclusively on the customer zone and the encompassed hardware and software assets. To broaden the scope and encompass additional components within the electric network, such as the billing system, the methodology can be expanded to introduce one or more supplementary attack trees. This expansion results in the creation of an attack forest which models more sophisticated cyber attacks.

Importantly, it should be noted that the attack tree is constructed independently of any existing security measures already implemented within the zone. Its purpose lies in deriving security requirements and assessing whether additional measures are necessary.

III. DEFINING SECURITY REQUIREMENTS AND MITIGATION MEASURES

Translating the intricate details of an attack tree into actionable security requirements necessitates the extraction of overarching security needs through a meticulous analysis of the attack tree. This endeavour demands specialized expertise within the relevant domain. In this section, this exact process is undertaken, involving the comprehensive examination of the attack nodes within the attack tree to deduce and formulate high-level security requirements.

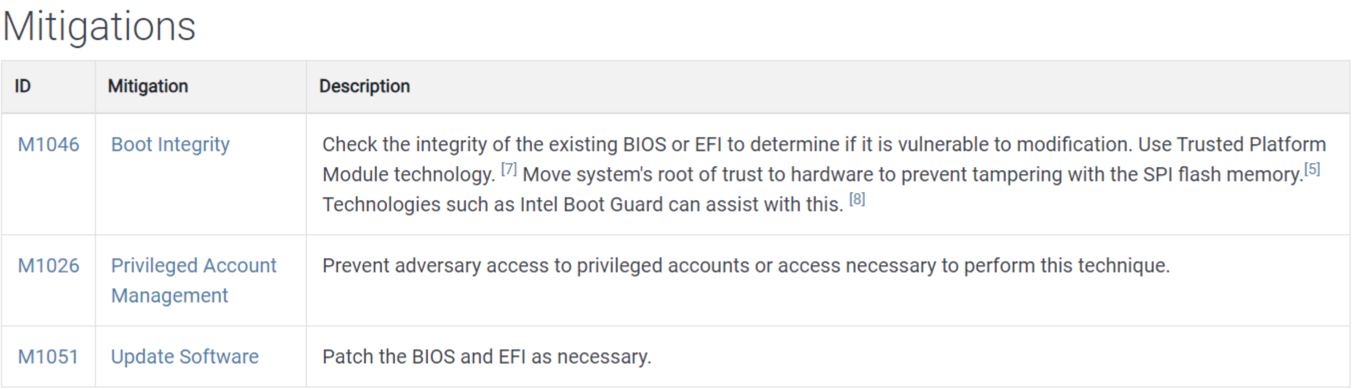
Based on the attack tree presented in Figure 2, we can derive the following high-level security requirements:

- Detection of hardware manipulation.
- Verification of hardware integrity.
- Implementation of a secure communication protocol.
- Integrity validation of software installation and updates.

These requirements can undergo further analysis by security experts to refine them into more specific functional and non-functional requirements, tailored to the unique characteristics of the infrastructure.

To effectively address these requirements, the utilization of the MITRE ATT&CK and D3FEND frameworks proves to be instrumental. During this stage, attention is directed towards exploring attack technique 1542-Pre-OS Boot: System Firmware, specifically its sub-technique 001- System Firmware, which involves tampering with system firmware, as depicted in the corresponding leaf of the attack tree.

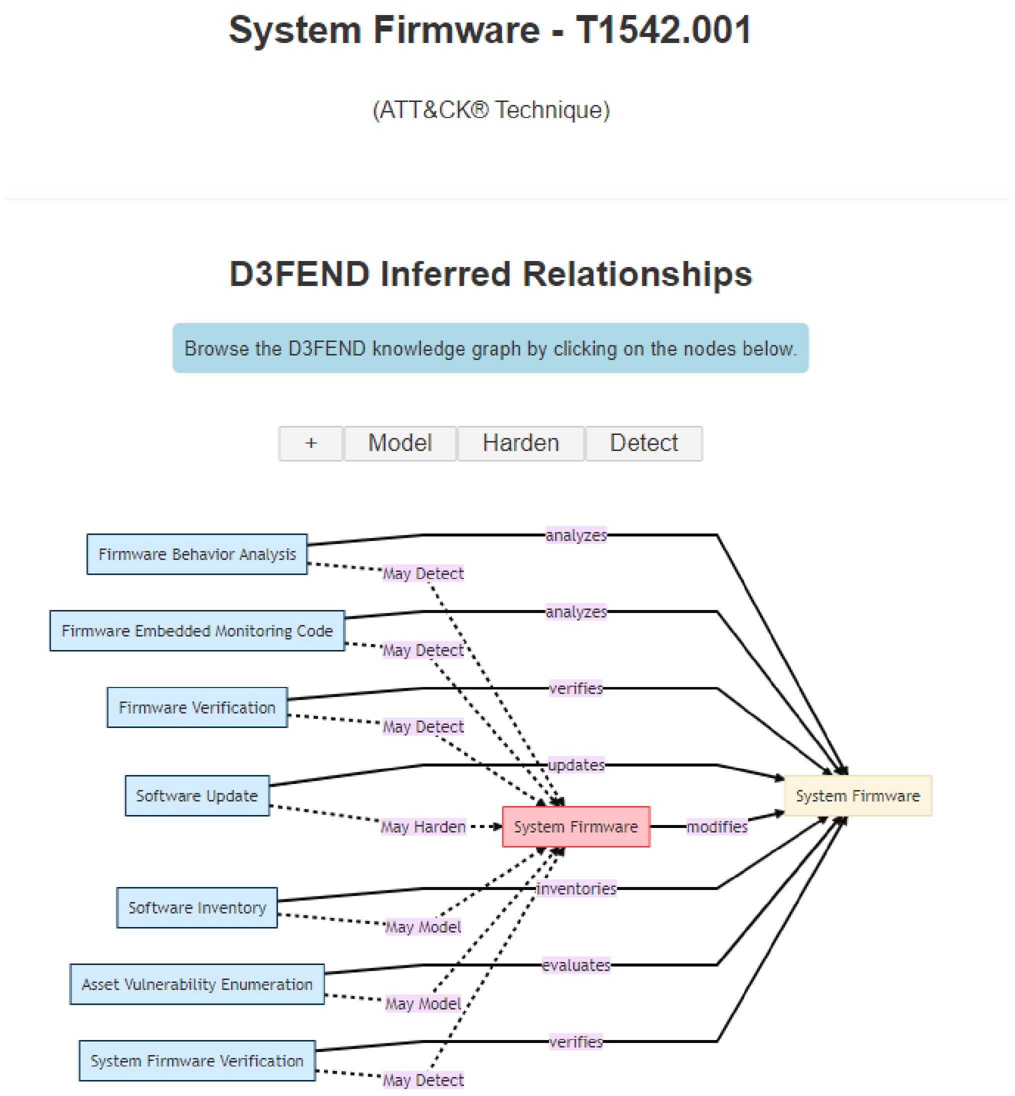
Figure 3 presents the suggested mitigations offered by the ATT&CK framework, while Figure 4 from D3FEND visually depicts the associated threat, the corresponding mitigations, and the targeted artifact. The set of mitigations provided within ATT&CK offers overarching guidelines, necessitating further exploration to pinpoint precise solutions. In contrast, the D3FEND framework categorizes these mitigations based on their alignment with potential threat responses and their contributions to protecting the organization's assets. Although the selection of the security solutions also requires further analysis, the value of a more nuanced approach that D3FEND provides enables a comprehensive understanding of how different mitigation strategies interplay with diverse threats and bolster overall organizational resilience.



Mitigations

ID	Mitigation	Description
M1046	Boot Integrity	Check the integrity of the existing BIOS or EFI to determine if it is vulnerable to modification. Use Trusted Platform Module technology. [7] Move system's root of trust to hardware to prevent tampering with the SPI flash memory.[5] Technologies such as Intel Boot Guard can assist with this. [8]
M1026	Privileged Account Management	Prevent adversary access to privileged accounts or access necessary to perform this technique.
M1051	Update Software	Patch the BIOS and EFI as necessary.

Fig. 3. ATT&CK recommended mitigations for T1542.001.



System Firmware - T1542.001

(ATT&CK® Technique)

D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.

Fig. 4. D3FEND recommended mitigations for T1542.001.

IV. Cost-Benefit Analysis

This section presents a method to apply a cost-benefit analysis, specifically based on the well-known Gordon-Loeb (GL) model, and establishes its connection to the attack tree introduced in Section 2. The GL model provides a structured approach for evaluating the potential costs and benefits associated with cybersecurity investments. To implement the GL model effectively, analysts should adhere to four key steps:

1) Estimate the value of tangible and intangible assets being protected, which represents the potential loss (L).
2) Estimate the probability that the cybersecurity event will be successfully executed (v).
3) Derive the expected loss by multiplying the values obtained from the previous steps, i.e., $v \times L$.
4) Based on the productivity (p) and cost of potential countermeasures (C), allocating investments to protect the organization's assets.

Delving into the decision-making essence of the fourth step, the balance between $p \times C$ and $v \times L$ is vital. The former provides a measure of the cost-effectiveness of a countermeasure, while the latter estimates the prospective loss from a security incident. If $p \times C$ is less than $v \times L$, the countermeasure is seen as a sound investment. Conversely, if it exceeds $v \times L$, the solution might be cost-prohibitive. This comparison is foundational in guiding organizations towards optimal cybersecurity decisions.

In the context of the attack tree, which provides a detailed representation of potential attack paths, it is possible to assign different values to the nodes in order to serve the target analysis model (Figure 5).

To apply the cost-benefit analysis to the tree, it is necessary to assign values of L and v to the nodes that represent malicious actions within the attack tree. This allows for the quantification of the expected loss in case the technique or subtechnique is successfully executed. By analyzing the output of the cost-benefit analysis, organizations can justify their cybersecurity investment decisions and determine the most effective allocation of resources to protect critical assets.

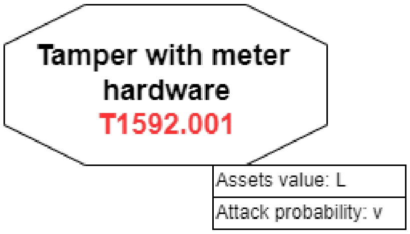


Fig. 5. Tagging values to the tree nodes.

Note that we have not provided numerical examples in this article as the values are infrastructure specific. Additionally, in more complex trees the analyst should consider "and" and "or" relationships in the tree to calculate the final probability and cost.

V. Conclusion

This article presents a comprehensive approach that combines attack tree analysis and GL cost-benefit model with the MITRE framework to enhance cybersecurity decision-making and streamline the analysis of security requirements. By leveraging the structured representation of attack trees and the wealth of knowledge in the MITRE framework, informed decisions can be taken in a systematic way such that organizations optimize their security strategies and bolster their overall cybersecurity resilience. A practical use case from EPES sector has been investigated showcasing the application of this methodology and elucidating the advantages of integrating the MITRE framework for deriving effective mitigation measures.

Acknowledgment

This work was supported by the European Union's Horizon 2020 for Research and Innovation Program under Grant 101020560 (CyberSEAS).

References

[1] "MITRE ATT&CK®." https://attack.mitre.org/ (accessed Jun. 25, 2023).

[2] "D3FEND Matrix — MITRE D3FENDTM." https://d3fend.mitre.org/ (accessed Jun. 25, 2023).

[3] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," J Cybersecur, vol. 6, no. 1, Jan. 2020, doi: 10.1093/CYBSEC/TYAA005.

[4] Terrance R Ingoldsby, "Attack Tree-based Threat Risk Analysis," Alberta, 2021.

[5] F. Xie, T. Lu, X. Guo, J. Liu, Y. Peng, and Y. Gao, "Security analysis on cyber-physical system using attack tree," Proceedings - 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2013, pp. 429–432, 2013, doi: 10.1109/IIH-MSP.2013.113.

[6] H. Xu, J. Su, X. Zong, and L. Yan, "Attack identification for software-defined networking based on attack trees and extension innovation methods," Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, vol. 1, pp. 485–489, Nov. 2017, doi: 10.1109/IDAACS.2017.8095128.

[7] U. Kuzmina, O. Kazakov, and B. Erushev, "Building an Attack Tree for Analysis of Information Security Risks," Proceedings - 2023 International Russian Smart Industry Conference, SmartIndustryCon 2023, pp. 164–168, 2023, doi: 10.1109/SMARTINDUSTRYCON57312.2023.10110738.

[8] A. Lee, "Attack Trees for Selected Electric Sector High Risk Failure Scenarios NESCOR Version 2.0," 2015.

[9] P. E. Kaloroumakis and M. J. Smith, "Toward a Knowledge Graph of Cybersecurity Countermeasures," The MITRE Corporation, 2021.

[10] "PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información." https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html (accessed Aug. 18, 2023).