Toward Risk-driven Cybersecurity Management for Virtual Networks

Toward Risk-driven Cybersecurity Management for Virtual Networks

Francesca Coriale, Daniele Bringhenti, Fulvio Valenza
Dip. Automatica e Informatica
Politecnico di Torino
Torino, Italy
Emails: {first.last}@polito.it

***Abstract*—In recent years, virtualization paradigms have significantly increased the complexity of network infrastructures, making systematic risk assessment a central pillar for modern cybersecurity management. However, existing methodologies are largely static, do not adequately incorporate risk assessment, and fail to account for the strategic nature of modern adversaries. In this context, my doctoral research aims to advance network security by integrating risk assessment into two complementary fields: threat modeling and network security configuration. The primary advancement in threat modeling lies in integrating complex dynamic interactions between attackers and defenders through game-theoretic strategies to quantify risk in adversarial scenarios. Meanwhile, in network security configuration, the goal is to natively integrate these risk metrics into automated logic to optimize the deployment and reconfiguration of security functions. In this paper, I present the research questions and methodological directions that will guide my PhD activity in developing these integrated, risk-driven solutions.**

***Index Terms*—virtual network security, risk assessment, threat modeling, security automation**

I. Introduction

Evaluating security risks and mitigating potential threats are essential operations for sustaining a resilient computer network. In particular, risk assessment represents the analytical backbone of cybersecurity management, as it provides a structured methodology for identifying, evaluating, and prioritizing threats to organizational assets. At its core, the process seeks to quantify the relationship between the probability of a threat occurrence and the resulting impact. By transforming qualitative evaluations into quantitative metrics, risk assessment enables stakeholders to make informed decisions regarding resource allocation and mitigation strategies. In an era where network virtualization has dramatically increased complexity and dynamism, systematic risk assessment is no longer merely a manual compliance task, but an indispensable prerequisite for protecting digital infrastructure. In particular, it should serve as the basis for two closely correlated security operations: threat modeling and network security configuration.

On the one hand, threat modeling is the proactive process of identifying and analyzing potential threats and the attack paths that enable attackers to reach critical resources. While traditional methodologies have increasingly integrated risk metrics to prioritize vulnerabilities based on their exploitability and impact, creating a comprehensive risk analysis of threats that considers not only impact but also the probability of each event is still a work in progress. Furthermore, the efficacy of traditional threat models is often undermined by their static nature, leading to rapid obsolescence and a failure to account for the dynamic, interdependent strategies of both attack and defense.

On the other hand, network security configuration consists of the operations required to provide protection against identified threats. Traditional manual strategies are no longer feasible in modern virtual networks, as they lead to frequent, risky misconfigurations across interconnected systems. To address these challenges, substantial research has focused on network security configuration automation, aiming to reduce the burden on security administrators and minimize the likelihood of human-induced vulnerabilities. Furthermore, automation enhances access to advanced security services for smaller companies, which might otherwise be excluded due to the high cost of specialized personnel. It also accelerates incident response, reducing recovery costs: statistical analysis [1] reveals that in 2025, the global average cost of a data breach has decreased by 9% over last year, thanks to fast detection and control of breaches. However, automation without contextual correlation may be either too permissive or disruptively rigid. Integrating risk assessment into automated workflows would provide the decision logic necessary for dynamic attack responses. By leveraging real-time risk scores, automated systems could adjust security postures proportionately to the current threat level. This synergy would ensure that automated triggers are proportionate to the severity of the threat, effectively preventing service disruptions caused by overly aggressive security policies.

In view of these observations, the goal of my PhD research is to advance the state of the art in integrating risk assessment processes into cybersecurity, with a special emphasis on protecting virtual networks. The objective in integrating risk assessment with threat modeling is to quantify the influence of these risk variables within frameworks that account for the strategic interactions between attackers and defenders. By incorporating probability and impact metrics into game-theoretic models, it would be possible to analyze the equilibrium of security investments and offensive strategies. Instead, the goal of enriching network security configuration with risk-aware intelligence is to design new automated approaches that can optimize the configuration of functions such as firewalls, based

on the risks posed by the threats against which protection is required.

The remainder of this paper is organized as follows. Section II analyzes the related literature. Section III summarizes the work carried out so far, while outlining future research directions. Section IV presents the conclusions.

II. State of the art

A. Threat Modeling

Threat modeling has been a prominent topic in the literature for many years and on which great steps forward have been made. The most studied methodology in this research area is the use of attack graphs for threat description. Even when attempts are made to include risk assessment parameters or goals in attack graphs, the proposed models remain limited.

A first group of studies takes into consideration only the point of view of the defender, who must understand and prevent the possible actions of the attacker, and rarely analyzes dynamic situations with multiple perspectives. In this perspective, [2]–[9] propose various techniques for defenders to identify potential threats and assess associated risks. The first one proposes the Attack-Countermeasure Tree paradigm, which includes both attack and defense mechanisms, in the form of detection and mitigation events at any position in the tree. That model computes the probability of a successful attack, taking into account whether the vector remains undetected or unmitigated, but it does not provide an optimization strategy under budget constraints. Then, [3] proposes an attack graph extended with countermeasure nodes as graph leaves, and some additional factors to characterize the internal nodes, such as feasibility. Even though the risk assessment of the system is declared as the main objective, the evaluation remains qualitative, focusing only on the consequence nodes and not on all intermediate stages. Instead, [4] formalizes attack trees to compute the minimum exploitation cost of an attack in order to support defensive investment decisions, but it does not address countermeasure optimization under budget constraints. Other studies [5], [6] assess the system's risk level without evaluating security measures. In particular, [5] focuses on risk assessment in power system networks, whereas [6] exploits Bayesian networks to dynamically calculate the daily risk for each attack path. Finally, [7]–[9] provide security hardening strategies based on the criticality evaluation of the present vulnerabilities, ignoring crucial factors such as the value of the asset at risk and the success probability of each threat.

A second group of studies has investigated the interactions between the attacker and the defender, but only to a limited extent [10]–[12]. In [10], game theory is used to determine attack and defense actions based on countermeasures and vulnerabilities in the Defense graph, to find the best action for each player in response to the other's action. Similarly, [11] implements a game theory approach with Attack-Defense Diagrams, which incorporate aspects of time, probability, and cost to reflect timing of attack steps and countermeasures, their success chances, as well as skills and knowledge of the players that may increase over time with lessons learned from previous attack steps. Instead, the work carried out in [12] extracts possible behaviors of rational actors from an Attack-Defense graph to obtain the optimal selection of countermoves for each actor. However, these approaches share an important limitation: they focus only on scenarios with one player from each category, ignoring possible strength imbalances if one league is larger or more powerful than the other.

The most feature-complete approach integrating risk assessment within threat modeling is the one presented in [13]. The risk management model proposed there is based on Bayesian networks that allow quantifying the possibilities of system compromise dynamically during the deployed phase of the network. Furthermore, with the suggested multi-objective optimization, it is possible to account for an economic budget constraint and thus provide the necessary information to make a trade-off between the costs of threat mitigation and the potential negative consequences of an overly permissive approach. Even though this technique marks a milestone in the field, the attacker's abilities and behavior are not considered, and the relationship between the actions of the attacker and defender has not been thoroughly explored.

B. Network Security Configuration Automation

The function for which security configuration automation has been the most investigated for many years is the distributed firewall. This research activity is mainly driven by the topic's relevance to virtual network protection and the complexity of the problem, which involves two tasks: firewall allocation and filtering rule computation. However, the studies that address these two sub-problems simultaneously, i.e., [14]–[21], still have limitations that could be overcome by integrating risk assessment into the configuration process.

Some of them [14]–[17] have intrinsic shortcomings: [14], [15] are limited to linear service chains, [16] ignores the presence of middleboxes in its configuration process, [17] is not applicable to virtual networks. Moreover, they pursue infrastructure-related optimization objectives rather than prioritizing threat mitigation based on their risk, i.e., resource usage minimization [14], performance metric improvement [15], firewall rule set reduction [16], and energy efficiency [17]. Unlike them, the approach presented in [18], [19] is more feature-rich, combining automation and formal verification with optimization, and offers a variant specifically tailored to reactive reconfiguration [20]. Still, its optimization scope remains restricted to minimizing firewall deployment and rule-set size. Furthermore, the security policies on which the approach works focus primarily on isolation rather than threat mitigation, and operational budget constraints are not considered. Finally, [21] tackles the firewall reconfiguration problem from a different perspective by establishing the optimal scheduling of updates for multiple virtual firewall instances. However, also in this case, the scheduling computation does not account for threat impact on the network.

Beyond firewall configuration, two studies in the research area of network security automation that contemplate threat risks are [22], [23]. [22] leverages a risk assessment model

to determine mitigation actions based on the risk posed by exposed vulnerabilities. However, its application is restricted to triggering predefined reactive actions via static threshold rules, and remains entirely decoupled from firewall configuration, preventing a truly integrated, risk-aware optimization process. Finally, [23] proposes a heuristic approach to selecting an optimal countermeasure deployment that minimizes the system's risk within budget constraints. Also this work remains incomplete due to dynamic security considerations, as it relies on a static attacker assumption and fails to account for how an adversary might strategically adapt to deployed defenses. Moreover, it assumes unrealistic uniform asset importance, and relies on limited CVSS-based likelihood metrics, failing to capture realistic risk variations and evolving attacker capabilities.

III. Research Methodology

As illustrated by the literature analysis in Section II, the research to date on integrating risk assessment into virtual network security management approaches has significant gaps that need to be addressed. In view of this problem, the main objectives of my PhD research are to investigate the potential synergy between risk-aware threat models and strategic game-theoretic interplay between attackers and defenders, and also to design novel automatic network security configuration approaches that account for threat risk in their reasoning.

In order to structure my research activity and outline the planned workflow of its methodology, as shown in Fig. 1, the following research questions have been formulated:

- $RQ_{1.1}$: What are the best-suited game theory strategies to enhance risk-based threat modeling processes?
- $RQ_{1.2}$: How far can the ratio between the number of attackers and defenders be pushed without compromising the system defensibility?
- $RQ_{2.1}$: How can automatic network (re)configuration logic be modeled to natively integrate risk metrics and respond to risk assessment evaluations?
- $RQ_{2.2}$: How can risk assessment models guide resilience and network segmentation methodologies?

Specifically, the research questions $RQ_{1.1}$ and $RQ_{1.2}$ are related to threat modeling, whereas $RQ_{2.1}$ and $RQ_{2.2}$ concern network security configuration.

The first research question $RQ_{1.1}$ may seem straightforward, but it may lead to many different paths depending on whether the information obtained from the players is accurate. Selecting the appropriate strategy is crucial to effectively address the problem of balancing different points of view with different risk evaluations, and it will also serve as the foundation for subsequent research directions. Among the possible candidate models to achieve this goal, I am currently analyzing the potential of Bayesian Games, which are particularly suited to addressing the information asymmetry inherent in cyber defense, where the defender's knowledge of the attacker's motives or capabilities is often partial. Bayesian Games are a fundamental class of strategic games with imperfect information, in which players are unsure about the payoffs,

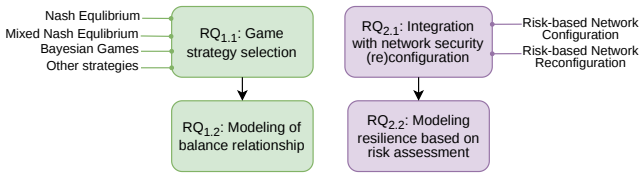

Fig. 1. Research design and workflow

actions, or characteristics of their opponents. Another class of candidates is represented by the Nash Equilibrium and the Mixed Nash Equilibrium, which define a state in which no player can increase their expected payoff by unilaterally changing their strategy, assuming that all other players keep their strategies unchanged. They provide a formal basis for identifying defensive configurations that remain robust against rational exploitation.

Based on the selection of game strategies in the previous research question, a possible further research related to the question $RQ_{1.2}$ may investigate how the numerical balance between attackers and defenders affects system stability. The idea is to explore how varying the player ratio can alter the equilibrium of game-theoretic strategies and influence the overall defensibility of the infrastructure. The final objective is to determine the limit to which this ratio can be pushed before the defensive posture is critically compromised. By analyzing these scaling dynamics, the study aims to identify the critical points at which the attackers' collective advantage overcomes the defenders' resource allocation.

The research question $RQ_{2.1}$ addresses the challenge of integrating risk assessment techniques with automated network security configuration and reconfiguration models to obtain risk-aware decision methodologies. Within this research line, I have already designed two complementary risk-aware security configuration approaches tailored for distributed packet-filtering firewalls used to protect virtual networks.

The first approach consists in a formal methodology that, after evaluating the risk level of threats present within the network based on a risk assessment model accounting for both threat impact and likelihood, automatically computes the optimal set of firewall configuration operations (i.e., firewall allocation and filtering rule creation) required to minimize the overall network risk, while adhering to economic constraints. Such a solution can guide network administrators in determining an optimal trade-off between security expenses and acceptable residual risk. Instead, the second approach consists in a decision-support methodology that computes the optimal ordering of firewall updates to prioritize blocking the most impactful attacks, in order to address the problem of firewall reconfiguration transient management effectively[1]. This solution was defined to address the high complexity and multi-vector nature of modern cyberattacks, which necessitate frequent distributed firewall reconfigurations, introducing a

[1]A demo paper related to this work has been submitted to the IEEE NetSoft 2026 conference.

transient period that might include vulnerable stages, if not properly scheduled. Both designed approaches integrate a risk assessment model with a constraint-based optimization formulated as a partial weighted Maximum Satisfiability Modulo Theories (MaxSMT) problem. Thanks to this formulation, they can jointly combine automation, formal verification, and optimization, ensuring their outputs are formally proven correct and contribute to maximizing network protection against the most critical threats. In the future, significant efforts will be dedicated to enhancing these two solutions further and to researching other possible integration strategies, for which tailored evaluation criteria will be established to assess their performance and effectiveness.

Finally, addressing the research question $RQ_{2.2}$ may involve investigating how risk assessment models can guide the design of resilient network segmentation architectures to improve overall resilience. For instance, one possible strategy would involve risk-driven partitioning logic, where the segmentation granularity is proportional to the detected vulnerability surface across different subnetworks. Such an approach would enable the system to isolate riskier threat vectors and prevent lateral movement, effectively enhancing overall resilience against cascading failures. Another possible strategy may involve using risk levels to prioritize the deployment of redundant resources in the most critical network segments, ensuring that core operational functions are maintained even under adversarial conditions. Future work will focus on defining how risk-guided architectures can bridge the gap effectively between high-level risk evaluation and concrete security hardening.

IV. Conclusions

This paper presents an overview of the state of the art in integrating risk assessment across different fields of virtual network security management, highlighting the main challenges and opportunities. It also outlines the research directions I am pursuing during my PhD program, which aim to explore how game theory can improve the integration between risk assessment and threat modeling processes and to enhance configuration automation with strategies that minimize risk and maximize system resilience. In line with these goals, the resolution of the discussed research questions will guide my research, ensuring a clear structure and focus throughout my PhD program.

Acknowledgment

This project has received funding from the European Union's Horizon Europe Research and Innovation Programme under grant agreement No. 101168144 (MIRANDA).

References

[1] IBM. (2025) Cost of a data breach report 2025. [Online]. Available: https://www.ibm.com/reports/data-breach

[2] A. Roy, D. S. Kim, and K. S. Trivedi, "Attack countermeasure trees (ACT): towards unifying the constructs of attack and defense trees," *Secur. Commun. Networks*, vol. 5, no. 8, pp. 929–943, 2012.

[3] S. Unger, E. Arzoglou, M. Heinrich, D. Scheuermann, and S. Katzenbeisser, "Risk assessment graphs: Utilizing attack graphs for risk assessment," *CoRR*, vol. abs/2307.14114, 2023.

[4] A. Simpson, M. Dellago, and D. W. Woods, "Formalizing attack trees to support economic analysis," *Comput. J.*, vol. 67, no. 1, pp. 220–235, 2024.

[5] I. Semertzis, V. S. Rajkumar, A. Ştefanov, F. Fransen, and P. Palensky, "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs," in *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, 2022, pp. 1–6.

[6] P. Cheimonidis and K. Rantos, "A bayesian-markov framework for proactive and dynamic cyber risk assessment driven by EPSS," in *IEEE International Conference on Cyber Security and Resilience, CSR 2025, Chania, Crete, Greece, August 4-6, 2025*. IEEE, 2025, pp. 281–286.

[7] 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.

[8] J. Zhang, W. Wang, and E. Zio, "Study on the application of graph theory algorithms and attack graphs in cybersecurity assessment," in *7th International Conference on System Reliability and Safety, ICSRS 2023, Bologna, Italy, November 22-24, 2023*. IEEE, 2023, pp. 558–564.

[9] U. Bansal, G. Sikka, L. K. Awasthi, and B. K. Bhargava, "Quantitative evaluation of extensive vulnerability set using cost benefit analysis," *IEEE Trans. Dependable Secur. Comput.*, vol. 21, no. 1, pp. 298–308, 2024.

[10] S. Bistarelli, M. Dall'Aglio, and P. Peretti, "Strategic games on defense trees," in *Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Ontario, Canada, August 26-27, 2006*, ser. Lecture Notes in Computer Science, vol. 4691. Springer, 2006, pp. 1–15.

[11] H. Hermanns, J. Krämer, J. Krcál, and M. Stoelinga, in *Principles of Security and Trust - 5th International Conference, POST 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*, ser. Lecture Notes in Computer Science, vol. 9635. Springer, 2016, pp. 163–185.

[12] B. Fila and W. Widel, "Exploiting attack-defense trees to find an optimal set of countermeasures," in *33rd IEEE Computer Security Foundations Symposium, CSF 2020, Boston, MA, USA, June 22-26, 2020*. IEEE, 2020, pp. 395–410.

[13] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," *IEEE Trans. Dependable Secur. Comput.*, vol. 9, no. 1, pp. 61–74, 2012.

[14] N. Schnepf, R. Badonnel, A. Lahmadi, and S. Merz, "Rule-based synthesis of chains of security functions for software-defined networks," *Electron. Commun. Eur. Assoc. Softw. Sci. Technol.*, vol. 76, 2018.

[15] C. Yang, X. Mi, Y. Ouyang, R. Dong, J. Guo, and M. Guizani, "SMART intent-driven network management," *IEEE Commun. Mag.*, vol. 61, no. 1, pp. 106–112, 2023.

[16] M. Yoon, S. Chen, and Z. Zhang, "Minimizing the maximum firewall rule set in a network with multiple firewalls," *IEEE Trans. Computers*, vol. 59, no. 2, 2010.

[17] D. Bringhenti and F. Valenza, "Greenshield: Optimizing firewall configuration for sustainable networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 6, pp. 6909–6923, 2024.

[18] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Automated firewall configuration in virtual networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 2, pp. 1559–1576, 2023.

[19] D. Bringhenti, S. Bussa, R. Sisto, and F. Valenza, "A two-fold traffic flow model for network security management," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 4, pp. 3740–3758, 2024.

[20] F. Pizzato, D. Bringhenti, R. Sisto, and F. Valenza, "Automatic and optimized firewall reconfiguration," in *NOMS 2024 - IEEE Network Operations and Management Symposium, Seoul, Republic of Korea, May 6-10, 2024*. IEEE, 2024, pp. 1–9.

[21] D. Bringhenti and F. Valenza, "Optimizing distributed firewall reconfiguration transients," *Comput. Networks*, vol. 215, p. 109183, 2022.

[22] N. Wintering, E. Lanfer, and N. Aschenbruck, "Automating network perimeter threat prevention for decentralized network administration," in *20th International Conference on Network and Service Management, Prague, Czech Republic, October 28-31, 2024*. IEEE, 2024, pp. 1–7.

[23] O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, Y. Ohta, T. Yagyu, Y. Elovici, and A. Shabtai, "Heuristic approach for countermeasure selection using attack graphs," in *34th IEEE Computer Security Foundations Symposium, CSF 2021, Dubrovnik, Croatia, June 21-25, 2021*. IEEE, 2021, pp. 1–16.