Adaptive, Agile and Automated Cybersecurity Management

Adaptive, Agile and Automated Cybersecurity Management

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

***Abstract*—In recent years, the network paradigms of Software Defined Networking and Network Function Virtualization have gained significant traction, leading to the emergence of new network architectures that emphasize flexibility and adaptability. However, the rapid evolution of these paradigms has outpaced the development of effective cybersecurity management solutions, which remain largely reliant on traditional, manual processes. In this context, my doctoral research aims to advance network security automation by integrating Artificial Intelligence and formal methods into hybrid approaches for automating the configuration of network security functions. These approaches seek to combine the strengths of both fields,which are formal correctness, optimization, and computational efficiency. In this paper, I present the research questions and directions that will guide my PhD activity in developing such hybrid approaches.**

***Index Terms*—security automation, formal methods, artficial intelligence**

I. Introduction

Cybersecurity management is a critical aspect of every modern organization, as it goes beyond merely protecting assets and ensuring business continuity. It also plays a pivotal role in maintaining the trust of customers and stakeholders. Under the umbrella of cybersecurity management, various activities are conducted, including risk and vulnerability assessment, incident response, as well as the orchestration, allocation, and configuration of security services.

However, the current landscape of security management remains as turbulent as ever, mainly because the shift from traditional to virtualized networks has not been accompanied by a corresponding evolution in security management processes, which remain primarily rooted in manual approaches. As attackers grow more skilled and aware of potential vulnerabilities to exploit, security administrators must keep pace with the evolving nature of virtualized networks, handling ever more intricate topologies and security configurations. This has resulted in security administrators being frequently overwhelmed by the vast volume of data to analyze, the multitude of security services to configure, and the increasing complexity of network management. The manual configuration of security systems such as NAT, IDS, firewalls, and VPNs can be particularly time-consuming, even in small to medium-sized business networks. Ultimately, when considering also the high risk of misconfiguring these critical systems, the balance inevitably shifts in favor of attackers.

To address these challenges, substantial research efforts have been dedicated to cybersecurity automation, with the aim of reducing the burden on security administrators and diminishing the likelihood of human-induced vulnerabilities. Furthermore, automation offers additional advantages, including enhanced accessibility to advanced security services for smaller companies, which might otherwise be precluded by the high costs of specialized personnel. Automation also enables more rapid incident response, thereby reducing potential damage and recovery expenses. Statistical analysis [1] reveals that in 2024, companies implementing extensive automation experienced average savings of 1.88 million dollars.

In view of these observations, the goal of my PhD research is to advance the state of the art in the automation of cybersecurity management processes. In the extensive range of activities that could be researched within cybersecurity management, I have identified the specific area of interest to concentrate on during my PhD program: the automation of the configuration of Network Security Functions (NSFs). The critical role of NSFs (e.g., firewalls, VPNs, and IDSs) in organizational security strategies, coupled with the complexities of manual configuration, makes this area a prime candidate for automation. In particular, I aim to explore the use of Artificial Intelligence (AI) to automate configuration processes, investigating the range of AI techniques applicable to this task and evaluating their effective integration with formal methods-based approaches, with the ultimate goal of establishing a unified framework that seamlessly combines the strengths of both domains.

The remainder of this paper is structured as follows. Section II reviews the literature related to my research field. Section III summarizes my prior and ongoing work, while outlining future research direction. Section IV presents the conclusions.

II. State of the art

The automated configuration of NSFs has gained increasing attention from the research community over the past few decades, following the growing recognition of cybersecurity's critical importance. However, the existing literature on this topic is fragmented, as it encompasses a wide range of approaches, each tailored to specific types of NSFs, such as firewalls, VPNs, and IDSs. Moreover, some NSFs have been explored more extensively than others, either due to their

more straightforward nature or their synergy with AI-based approaches, which are currently trending and particularly well-suited for automation.

A prime example of a well-studied NSF is the firewall, which has been the focus of extensive research efforts to automate various aspects of its management. Related to the configuration of firewalls, a first group of studies is [2]–[4]. The paper [2] is one of the earliest works to propose a tool for assisting security administrators by automatically generating and analyzing firewall configurations: once the feasibility of the desired policies is established based on the network configuration and administrator-defined trust assumptions, the tool iteratively generates the policies. The work [3] takes a different approach, leveraging static analysis based on formal specifications to detect potential inconsistencies (e.g., shadowing, correlation, generalization, and redundancy) in firewall policies expressed in low-level language before their deployment and enforcement. The approach discussed in [4] employs formal argumentation and preference reasoning for analyzing and automatically generating firewall policies, improving policy comprehensibility for administrators through its declarative nature. However, these approaches share multiple similar limitations. First, they focus exclusively on traditional computer networks, while modern networks increasingly rely on Software Defined Network (SDN) and Network Function Virtualization (NFV) paradigms. Second, the challenge of optimizing the configuration of firewalls is not addressed.

Regarding the first shortcoming, it was later overcome by some other approaches in the literature. For instance, [5] introduces a semantic-based tool for the Linux-integrated Netfilter firewall, allowing users to specify firewall configurations independently of rule order, which is a key limitation of traditional Netfilter. Another example of work targeting virtual networks is [6], where the authors propose a network configuration synthesis tool that leverages stratified Datalog to model network behavior and express routing requirements as constraints, effectively reducing the synthesis problem to a constraint satisfaction problem. Nevertheless, none of these approaches still prioritize optimization, which represents a crucial gap in the literature, especially considering the increasingly stricter requirements for maximized efficiency and resource consumption of modern networks.

Similar shortcomings can be found in the literature on VPNs, a situation further exacerbated by the significantly lower volume of research compared to firewalls. In traditional networks, early studies on the automated configuration of VPNs can be found in [7]–[10]. The work [7] is notable for being among the first to recognize the necessity of automating VPN configuration through technology abstraction and the importance of maximizing resource availability. However, the proposed approach was not mature for practical implementation, as it relied on a brute-force algorithm that struggled to scale with network size. The following papers [8], [9] successfully proposed algorithms for automating the configuration of VPNs, marking a milestone in the field. On the one hand, [8] introduced two different algorithms for the achievement of the task: the Bundle Approach, based on the given requirements, groups traffic flows into disjoint bundles and guarantees completeness and correctness; the Direct Approach instead generates policies directly from the requirements, prioritizing efficiency and scalability over completeness. On the other hand, [9] expands on the previous study by introducing the Ordered-Split Approach, a third algorithm designed to mitigate the scalability and redundancy limitations of the prior two, eliminating the need for security administrators to make trade-offs. Finally, [10] presents a framework designed for inter-domain security policy management, addressing the challenge of enforcing policies in distributed architectures.

On softwarized and virtualized networks the lack of research is evident, with only a few works [11] [12] [13] addressing the topic. Specifically, [11] introduces a method that integrates SDN with IPsec to streamline VPN management, leveraging OpenFlow switches (acting as VPN clients) and controllers to distribute IPsec configuration parameters to the clients. The work [12] adopts a similar SDN-based approach for managing IPsec Security Associations but introduces the novelty of supporting both IKE and IKE-less setups while simplifying network resource orchestration through centralized key management in the SDN controller. Finally, the paper [13] proposes an interesting cross-over between DevOps and VPNs management, in which the concepts of the former (continuous communication, collaboration, integration) are applied to the resolution of the automated configuration problem by allowing the deployment of VPN tunnels via a web-based graphical interface to enhance usability and manageability.

On the other end of the spectrum, the literature on Intrusion Detection Systems (IDS) is significantly more extensive, including works that specifically address SDN environments. This disparity in research can be attributed to the nature of IDS technology, which primarily involves network traffic analysis. This task naturally aligns with AI-based approaches for classification and regression. For this reason, scientists have focused on developing solutions for IDS based on many different AI techniques, including Long short-term memory combined with Convolutional Neural Networks [14], Deep Ensemble Learning [15] and Federated Deep Learning [16]. As a result, IDSs have benefited from rapid advancements in AI, leading to a wealth of solutions that far outpace those available for firewalls and VPNs, whose configuration challenges are not as quickly addressed by current Machine Learning algorithms – or at least not in ways that have been thoroughly explored.

III. Research Directions

As illustrated by the literature analysis of Section II, the research carried out so far on network security automation lacks approaches that (i) leverage formal methods to ensure configuration correctness and to confer soundness and stability to the resulting solutions, (ii) incorporate process optimization as a core objective, and (iii) address scalability challenges through the adoption of AI-based solutions.

The first two shortcomings have been recently addressed successfully by VEREFOO, a constraint programming-based

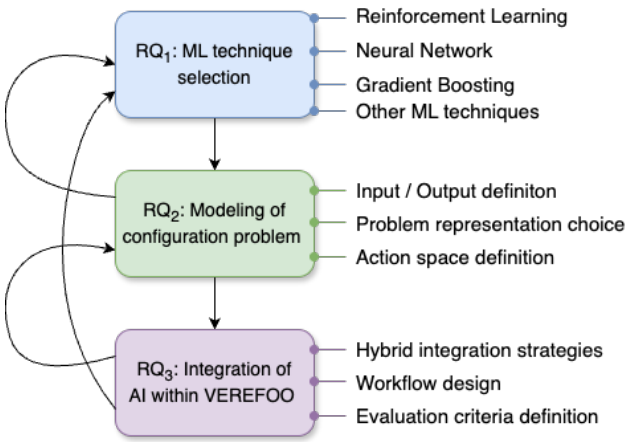

Fig. 1. Research design and workflow

approach that fully automates the configuration of NSFs while ensuring formal correctness by construction and aiming to optimize the resulting configurations. The approach has been developed for both firewalls [17] [18] [19] and VPNs [20] [21]. Specifically, during my Master's Degree thesis and the initial months of my PhD program, I contributed to the VEREFOO project, focusing on further enhancing the optimization capabilities of the approach in the context of VPNs. However, the current implementation of VEREFOO does not incorporate any AI-based strategies, relying exclusively on the resolution of a Maximum Satisfiability Modulo Theories (MaxSMT) problem to model and solve the configuration task.

In light of these considerations, the objective of my PhD research is to investigate the potential synergy between Artificial Intelligence and formal methods in the context of network security automation, and to develop a hybrid approach that combines the strengths and methodologies of VEREFOO with AI-based techniques, addressing the inherent scalability and performance limitations associated with a solely formal methods-based approach.

In order to structure my research activity, the following research questions have been formulated:

- RQ_1: What is the best-suited Machine Learning technique to automate network security configuration?
- RQ_2: How can the configuration problem be modeled to leverage the selected Machine Learning technique?
- RQ_3: How can AI techniques be integrated within network security automation frameworks, such as VEREFOO, based on formal methods?

Figure 1 illustrates the research design, outlining the planned workflow of the future research activity structured around the previously discussed research questions. The first research question, while straightforward, is fundamentally relevant. Selecting the appropriate Machine Learning technique is critical to address the automatic configuration problem in an effective way, and it will also serve as the foundation of the subsequent research directions. Therefore, I am currently exploring the potential of Reinforcement Learning as a promising candidate for this task. Unlike other Machine Learning techniques such as Neural Networks or Gradient Boosting, which have demonstrated strong performance in classification and regression tasks, Reinforcement Learning is particularly well-suited to decision-making problems, where the goal is to learn a policy that maximizes a defined reward function. Another strong candidate for this task is the use of supervised learning techniques, which can be employed to learn a model that predicts the optimal configuration based on a set of input features. However, this approach may not be as effective as Reinforcement Learning in capturing the dynamic nature of the configuration task, where the context and requirements may change over time. Additionally, the use of supervised learning would require a large amount of labeled data to train the model, which may not be readily available in practice.

The second research question investigates the modeling of the configuration task in accordance with the characteristics and requirements of the selected Machine Learning technique. Continuing with the example of Reinforcement Learning, this involves choosing between a model-free or model-based approach, each associated with different algorithms (e.g., Q-Learning, SARSA, Dyna-Q), and carefully defining the state and action spaces, along with an appropriate reward function.

I expect the process of addressing the first two research questions to be highly iterative, as early results may prompt a reevaluation of initial choices regarding algorithm selection, model design, or problem representation. Consistently with this perspective, I recently started working on the definition of an approach aimed at the automation of a specific task belonging to the configuration of firewalls: the reordering of firewall rules. This work is motivated by two main reasons: (i) the order of firewall policies significantly influences network performance, as suboptimal rule arrangements may cause redundant look-ups and increased latency; and (ii) the task of reordering firewall rules is a well-defined problem that can be naturally formulated with Reinforcement Learning, enabling us to assess the viability of this approach without confronting the full complexity of the broader configuration process. Moreover, it offers an opportunity to gain practical experience with Reinforcement Learning, thereby accelerating the resolution of the first two research questions when extending the investigation to the full scope of the automated configuration problem. Otherwhise, if the results of this initial work are not satisfactory for the long-term research, I will consider the possibility of employing supervised learning techniques such as Random Forests or Graph Neural networks by modeling the configuration task as a classification problem, where the goal is to predict through a binary decision wheter a firewall should be placed on a specific position or not.

Finally, the third research question addresses the challenge of integrating AI techniques with tools like VEREFOO, leveraging formal methods, to obtain a hybrid framework. Many different integration strategies can be envisioned to address this question. For instance, one possible strategy involves leveraging AI to generate a candidate configuration, which is subsequently validated by VEREFOO to ensure compliance

with the specified security properties. This schema would effectively delegate the optimization workload to the AI, while entrusting VEREFOO with the task of verifying the formal correctness of the resulting solution. Another possible strategy could involve using AI to generate a partial draft of the configuration, which is then completed by VEREFOO, using this partial solution as a starting point. This approach would enable VEREFOO to focus on the most complex aspects of the configuration task, while AI handles simpler parts, significantly reducing the overall solution space and improving the performance of VEREFOO. Significant efforts will be dedicated to exploring these and many other possible integration strategies, for which clearly defined evaluation criteria must be established to assess their performance and effectiveness.

IV. Conclusions

This paper presents an overview of the state of the art on automated network security management, highligthing the main challenges and opportunities in the field. It also outlines the research directions I am pursuing during my PhD program, which aims to explore the potential synergy between AI and formal methods, with the goal of developing a hybrid approach that combines the strengths of both methodologies: computational efficiency, formal correctness and optimality. In line with this goal, the resolution of the discussed research questions will guide my research activity, ensuring a clear structure and focus throughout the course of my PhD program.

Acknowledgment

This work was supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the EU - NextGenerationEU.

References

[1] IBM. (2024) Cost of a data breach report 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[2] P. Verma and A. Prakash, "FACE: A firewall analysis and configuration engine," in *2005 IEEE/IPSJ International Symposium on Applications and the Internet (SAINT 2005), 31 January - 4 February 2005, Trento, Italy*. IEEE Computer Society, 2005, pp. 74–81. [Online]. Available: https://doi.org/10.1109/SAINT.2005.28

[3] J. Wu, X. Chen, Y. Zhao, and J. Ni, "A flexible policy-based firewall management framework," in *International Conference on Cyberworlds 2008, Hangzhou, China, 22-24 September 2008, Proceedings*. IEEE Computer Society, 2008, pp. 192–194. [Online]. Available: https://doi.org/10.1109/CW.2008.134

[4] A. K. Bandara, A. C. Kakas, E. C. Lupu, and A. Russo, "Using argumentation logic for firewall configuration management," in *Integrated Network Management, IM 2009. 11th IFIP/IEEE International Symposium on Integrated Network Management, Hofstra University, Long Island, NY, USA, June 1-5, 2009*. IEEE, 2009, pp. 180–187. [Online]. Available: https://doi.org/10.1109/INM.2009.5188808

[5] P. Adão, C. Bozzato, G. D. Rossi, R. Focardi, and F. L. Luccio, "Mignis: A semantic based tool for firewall configuration," in *IEEE 27th Computer Security Foundations Symposium, CSF 2014, Vienna, Austria, 19-22 July, 2014*. IEEE Computer Society, 2014, pp. 351–365. [Online]. Available: https://doi.org/10.1109/CSF.2014.32

[6] A. El-Hassany, P. Tsankov, L. Vanbever, and M. T. Vechev, "Network-wide configuration synthesis," *CoRR*, vol. abs/1611.02537, 2016. [Online]. Available: http://arxiv.org/abs/1611.02537

[7] R. Isaacs, "Lightweight, dynamic and programmable virtual private networks," in *Proc. of the 2000 IEEE Third Conference on Open Architectures and Network Programming*, 2000, pp. 3–12. [Online]. Available: https://doi.org/10.1109/OPNARC.2000.828128

[8] Z. Fu and S. F. Wu, "Automatic generation of ipsec/vpn security policies in an intra-domain environment," in *Proc. of the Operations & Management, 12th International Workshop on Distributed Systems, DSOM 2001, Nancy, France, October 15-17, 2001*, O. Festor and A. Pras, Eds., 2001, pp. 279–290. [Online]. Available: http://www.simpleweb.org/ifip/Conferences/DSOM/2001/DSOM2001/proceedings/S8-3.pdf

[9] Y. Yang, C. U. Martel, and S. F. Wu, "On building the minimum number of tunnels: an ordered-split approach to manage ipsec/vpn policies," in *Proc. of Managing Next Generation Convergence Networks and Services, IEEE/IFIP Network Operations and Management Symposium, NOMS 2004, Seoul, Korea, 19-23 April 2004*, 2004, pp. 277–290. [Online]. Available: https://doi.org/10.1109/NOMS.2004.1317665

[10] Y. Yang, Z. J. Fu, and S. F. Wu, "BANDS: an inter-domain internet security policy management system for ipsec/vpn," in *Proc. of Integrated Network Management VII, Managing It All, IFIP/IEEE Eighth International Symposium on Integrated Network Management (IM 2003), March 24-28, 2003, Colorado Springs, USA*, vol. 246, 2003, pp. 231–244. [Online]. Available: https://doi.org/10.1109/INM.2003.1194183

[11] Y. Li and J. Mao, "Sdn-based access authentication and automatic configuration for ipsec," in *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*, vol. 01, 2015, pp. 996–999. [Online]. Available: https://doi.org/10.1109/ICCSNT.2015.7490904

[12] G. L. Millán, R. M. López, and F. Pereñíguez-Garcia, "Towards a standard sdn-based ipsec management framework," *Comput. Stand. Interfaces*, vol. 66, 2019. [Online]. Available: https://doi.org/10.1016/j.csi.2019.103357

[13] L. Firdaouss, A. Bahnasse, B. Manal, and Y. Ikrame, "Automated VPN configuration using devops," in *Proc. of the 12th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2021) / the 11th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2021), Leuven, Belgium, November 1-4, 2021*, ser. Procedia Computer Science, vol. 198. Elsevier, 2021, pp. 632–637. [Online]. Available: https://doi.org/10.1016/j.procs.2021.12.298

[14] J. Malik, A. Akhunzada, I. Bibi, M. Imran, A. Musaddiq, and S. W. Kim, "Hybrid deep learning: An efficient reconnaissance and surveillance detection mechanism in sdn," *IEEE Access*, vol. 8, pp. 134 695–134 706, 2020.

[15] S. Haider, A. Akhunzada, I. Mustafa, T. B. Patel, A. Fernandez, K.-K. R. Choo, and J. Iqbal, "A deep cnn ensemble framework for efficient ddos attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 53 972–53 983, 2020.

[16] J. Cui, H. Sun, H. Zhong, J. Zhang, L. Wei, I. Bolodurina, and D. He, "Collaborative intrusion detection system for sdvn: A fairness federated deep learning approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 34, no. 9, pp. 2512–2528, 2023.

[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. [Online]. Available: https://doi.org/10.1109/TNSM.2024.3452150

[18] D. Bringhenti, G. Marchetto, R. Sisto, F. Valenza, and J. Yusupov, "Introducing programmability and automation in the synthesis of virtual firewall rules," in *Proc. of the 6th IEEE Conference on Network Softwarization, NetSoft 2020, Ghent, Belgium, June 29 - July 3, 2020*, 2020, pp. 473–478. [Online]. Available: https://doi.org/10.1109/NetSoft48620.2020.9165434

[19] D. Bringhenti, S. Bussa, R. Sisto, and F. Valenza, "Atomizing firewall policies for anomaly analysis and resolution," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 3, pp. 2308–2325, 2025. [Online]. Available: https://doi.org/10.1109/TDSC.2024.3495230

[20] D. Bringhenti, R. Sisto, and F. Valenza, "Automating VPN configuration in computer networks," *IEEE Trans. Dependable Secur. Comput.*, vol. 22, no. 1, pp. 561–578, 2025. [Online]. Available: https://doi.org/10.1109/TDSC.2024.3409073

[21] D. Bringhenti, G. Marchetto, R. Sisto, and F. Valenza, "Short paper: Automatic configuration for an optimal channel protection in virtualized networks," in *Proc. of CYSARM@CCS '20: the 2nd Workshop on Cyber-Security Arms Race, Virtual Event, USA, November, 2020*. ACM, 2020, pp. 25–30. [Online]. Available: https://doi.org/10.1145/3411505.3418439