Intent-Based Attack Mitigation through Opportunistic Synchronization of Microservices

Do Duc Anh Nguyen, Fabien Autrel, Ahmed Bouabdallah, Jérôme François, Pierre Alain, Guillaume Doyen

Intent-Based Attack Mitigation through Opportunistic Synchronization of Microservices

Do Duc Anh Nguyen*, Fabien Autrel*, Ahmed Bouabdallah*, Jérôme François†, Pierre Alain‡ and Guillaume Doyen*
*SOTERN - IRISA (UMR CNRS 6074), IMT Atlantique, firstname.lastname@imt-atlantique.fr
†SnT, University of Luxembourg and Inria Nancy Grand Est, jerome.francois@uni.lu
‡SOTERN - IRISA (UMR CNRS 6074), Université de Rennes, pierre.alain@irisa.fr

***Abstract*—Malware threats to digital infrastructure demand prompt and accurate countermeasures due to their rapid propagation across entire networks. Addressing this challenge requires security automation, and Intent-Based Networking (IBN) provides a promising solution by expressing intents, standing for dynamic countermeasure, without specifying operations. However, a challenge lies in the delayed reaction of IBN systems due to intrinsic costly operations (e.g., translation, deployment, and assurance) compared to the fast propagation mechanisms of malware. As a candidate solution, we consider two mechanisms to accelerate reaction time. First, we explore to what extent security functions, functioning as Policy Enforcement Points (PEPs), can be implemented through microservices, which bring flexibility and scalability to support dynamic features. Second, we consider opportunistic synchronization between PEPs to react, at least partially but autonomously to promptly halt ongoing malware propagation. This paper discusses related works, outlines our approach, and presents the current status of this research.**

***Index Terms*—Mitigation, IBN, Microservices, Opportunistic synchronization**

I. Introduction

Digital architectures are susceptible to a wide range of malware attacks (5.5 billion reported in 2022[1]). Malware may possess self-propagation abilities to spread across entire networks after their successful initial infection, intensifying the challenge of responding promptly and accurately in complex systems. To address it, security automation is required and Intent-Based Networking (IBN), a technology that enables users to express network outcomes, known as intents, without specifying detailed operations, can be leveraged. IBN can be employed to facilitate the dynamic deployment of security functions (e.g., firewalls) based on intents, allowing reactions to security alerts (e.g., blocking propagation traffic). However, ensuring accurate countermeasures derived from intents in complex infrastructures is challenging, as a single misconfiguration may increase the exposure to vulnerabilities. Also, automatically modifying deployed intents in response to attacks and provisioning suitable security policies and functions, among a multitude of others, add to the computational and validation complexity of the full set of network functions. As a result, IBN systems may become slow and unscalable, leading to delays in preventing malware attacks with fast propagation mechanisms. To address this issue, we propose to explore two possible solutions. First, since security functions acting as Policy Enforcement Points (PEPs) are expected to be flexible and scalable, we consider microservices, which are decomposed from large applications that enhance system agility by allowing the deployment and scaling of functions independently, reducing the risk of system-wide failures. Second, we propose to empower PEPs to autonomously adjust their behavior or security policies while awaiting the computation of accurate responses from a central IBN controller. Synchronization mechanisms are necessary for PEPs to cooperate and explore appropriate capabilities due to their differences. To achieve fast synchronization, the opportunistic approach can be employed to allow PEPs to quickly and autonomously synchronize their responses whenever an alert is raised.

The rest of the paper is structured as follows: Section II provides the state of the art in the IBN area, microservices, and signaling methodologies; Section III presents our contribution in the IBN area; Section IV discusses our current status, and finally, Section V contains the remarks of the paper.

[1]Source: 2023 SonicWall Cyber Threat Report.https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf

II. State of the Art

In this section, we highlight some related works in IBN, microservices, and signaling methods for security reaction.

A. Recent Advances in Intent-based Security

An IBN system [1] performs three main tasks: (1) translating intents into configurations or policies; (2) providing necessary PEPs; and (3) ensuring intent compliance. In [2], the authors propose to implement the Interface to Network Security Functions (I2NSF) framework, which uses automata theory to extract information from YANG policies and converts it into device-level data for NSF provisioning. However, redundant and conflicting policies may arise. This problem is solved in [3] with a formal approach. Maximum Satisfiability Modulo Theory (MaxSMT) is employed to compute optimal firewall rules in response to DDoS alerts.

B. Microservices

Microservices [4] involve breaking down complex applications into small, independent services. Virtualized Intrusion Detection Systems (IDSs) proposed in [5] are microservices with adaptable policies that ensure balanced workloads in high traffic. In [6], microservices serve as API gateways that provide security management (e.g., authentication) in communication between IoT devices and clients. In considering a

more general case, the framework of [7] can automate the selection of microservices to secure specific web services by expressing high-level requirements.

C. Signaling Methodologies

To synchronize PEPs, effective signaling is essential for sharing information during attacks. In [8], the authors propose a strategy using rings of Intrusion Prevention Systems (IPSs) around client hosts for DDoS mitigation. Hop-by-hop communication within the same ring is triggered by an IPS alert, and mitigation methods are activated when the total rate exceeds a threshold. Instead of focusing solely on individual client hosts, the authors in [9] explore IPS communication across multiple domains. An IPS can signal other IPSs in different domains to collectively filter traffic upon detecting an attack.

Proposed IBN systems, although offering reliable protection, face latency and scalability challenges, potentially delaying responses to malware attacks. To our knowledge, while many contributions utilize microservices for enforcing security policies, few address reaction intents. Moreover, the integration of microservices and signaling methods for synchronized reactions remains an open question.

III. Contribution

To avoid the computational burden of IBN reactions, we consider opportunistic synchronization for rapid responses in security functions. The approach consists of leveraging existing data packets as an opportunity to share reaction information and synchronize their responses. Concretely, for fast synchronization between microservices, we can utilize dataplane programmability to embed reaction decisions into packets. This enables on-the-path microservices with appropriate capabilities to promptly apply countermeasures. Since the attack paths can be various, a microservice can randomly signal (or propagate) modified packets to its neighbors. This process can continues in an epidemic-like approach until those with the appropriate security capabilities (e.g., packet filtering) can generate and enforce new security policies. This ensures the immediate deployment of countermeasures upon detecting an attack, eliminating the need for extensive consideration of network topology or waiting for IBN computation. Additionally, updated security policies may need conversion to intents for reporting or high-level conflict checking. Therefore, this approach holds potential for mitigating the malware impact, especially given the varied and rapid nature of its propagation mechanisms.

IV. Work in Progress

We selected a use case focusing on malware attacks due to their varied and rapid propagation mechanisms, which pose a challenge to our model. For malware selection, we consult recent top malware reports from 2020–2023 by CIS [10]. The 2023 report reveals that old malware (e.g., Ursnif variants from 2000) remains a threat, while most of the recent malware from 2021–2023 lacks detailed analysis. As a good trade-off between freshness and availability of technical materials, a set of samples for 2010–2020 is considered. Currently, 13 out of 46 selected samples have self-propagation capabilities (the fast propagation criterion), while others require attackers' commands. Among these, brute-force password attacks and vulnerability exploration stand out as faster mechanisms than spamming emails, USB, or drive-by downloads. On that shortlist, three malwares (Wannacry, NotPetya, and Bad Rabbit) propagate through the EternalBlue vulnerability identified in 2017. With a clear understanding of EternalBlue and their propagation traffic, these malware samples can be suitable candidates for our use case. Our future steps involve experimenting with conventional IBN systems to highlight their limitations in prompt reactions. Two potential candidates for experimentation are I2NSF [2] and the MaxSMT-based system [3] due to their applicability in security management and available implementations.

V. Conclusion

Prompt and accurate responses to malware attacks are crucial to limit their impact. The proposed opportunistic approach aims to empower microservices for autonomous and rapid reactions. Our current work involves a thorough assessment of scalability challenges within the standard IBN architecture. Subsequently, we plan to design a first opportunistic mechanism to synchronize microservices in enforcing autonomous reaction policies and compare its performance and reliability with that of the standard IBN architecture.

Acknowledgment

This work has been partially supported by the French National Research Agency under the France 2030 label (Superviz ANR-22-PECY-0008). The views reflected herein do not necessarily reflect the opinion of the French government.

References

[1] A. Leivadeas and M. Falkner, "A survey on intent-based networking," *IEEE Communications Surveys Tutorials*, vol. 25, no. 1, pp. 625–655, 2023.

[2] J. Kim, E. Kim, J. Yang, J. Jeong, H. Kim, S. Hyun, H. Yang, J. Oh, Y. Kim, S. Hares, and L. Dunbar, "Ibcs: Intent-based cloud services for security applications," *IEEE Communications Magazine*, vol. 58, no. 4, pp. 45–51, 2020.

[3] D. Bringhenti, J. Yusupov, A. M. Zarca, F. Valenza, R. Sisto, J. B. Bernabe, and A. Skarmeta, "Automatic, verifiable and optimized policy-based security enforcement for sdn-aware iot networks," *Computer Networks*, vol. 213, p. 109123, 2022.

[4] I. Nadareishvili, R. Mitra, M. McLarty, and M. Amundsen, *Microservice architecture: aligning principles, practices, and culture*. " O'Reilly Media, Inc.", 2016.

[5] N. Zhang, H. Li, H. Hu, and Y. Park, "Towards effective virtualization of intrusion detection systems," in *Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, 2017, pp. 47–50.

[6] D. Lu, D. Huang, A. Walenstein, and D. Medhi, "A secure microservice framework for iot," in *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2017, pp. 9–18.

[7] S. Abidi, M. Essafi, C. G. Guegan, M. Fakhri, H. Witti, and H. H. B. Ghezala, "A web service security governance approach based on dedicated micro-services," *Procedia Computer Science*, vol. 159, pp. 372–386, 2019.

[8] J. François, I. Aib, and R. Boutaba, "Firecol: a collaborative protection network for the detection of flooding ddos attacks," *IEEE/ACM Transactions on networking*, vol. 20, no. 6, pp. 1828–1841, 2012.

[9] B. Rashidi and C. Fung, "Cofence: A collaborative ddos defence using network function virtualization," in *2016 12th international conference on network and service management (CNSM)*. IEEE, 2016, pp. 160–166.

[10] (2023) Top 10 malware q3 2023. [Online]. Available: https://www.cisecurity.org/insights/blog/top-10-malware-q3-2023