Intent-Based Attack Mitigation through Opportunistic Synchronization of Microservices

Do Duc Anh Nguyen[*†1], Fabien Autrel[‡1], Ahmed Bouabdallah[§1], Jérôme François[¶2], Pierre Alain[‖1], and Guillaume Doyen[**1]

[1]Self-prOtecting The futurE inteRNet – IMT Atlantique, RÉSEAUX, TÉLÉCOMMUNICATION ET SERVICES – France

[2]Interdisciplinary Centre for Security, Reliability and Trust – Luxembourg

Résumé

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 (eg, 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 propagation. This paper discusses related works, outlines our approach, and presents the current status of this research.

[*]Intervenant

[†]Auteur correspondant: do-duc-anh.nguyen@imt-atlantique.fr

[‡]Auteur correspondant: fabien.autrel@imt-atlantique.fr

[§]Auteur correspondant: ahmed.bouabdallah@imt-atlantique.fr

[¶]Auteur correspondant: jerome.francois@uni.lu

[‖]Auteur correspondant: pierre.alain@irisa.fr

[**]Auteur correspondant: guillaume.doyen@imt-atlantique.fr