جامعة محمد الخامس بالرباط
Université Mohammed V de Rabat

École Nationale Supérieure d'Informatique et d'Analyse des Systèmes
Centre d'Études Doctorales en Sciences des Technologies de l'Information et de l'Ingénieur

AVIS DE SOUTENANCE DE THESE DE DOCTORAT

Monsieur Anass SEBBAR

soutiendra publiquement sa thèse de Doctorat en Informatique

Le Mardi 01 Mars 2022 à 10H au Grand amphi à l'ENSIAS

Intitulé de la thèse

Advanced detection and prevention technique to mitigate threats in multi-domain Software-Defined Networking using supervised machine learning techniques

UNIVERSITE MOHAMMED V - RABAT
ENSIAS

Devant le Jury composé de :

Président :
Pr. Mahmoud NASSAR, PES, ENSIAS, Université Mohammed V de Rabat
Directeur de thèse :
Pr. Mohamed Dafir ECH-CHERIF EL KETTANI, PES, ENSIAS, UM5 de Rabat
Co-Directeur de thèse :
Pr. Mohammed BOULMALF, PES, UIR, Rabat
Rapporteurs :
Pr. Mostafa BELLAFKIH, PES, INPT, Rabat
Pr. El Mamoun SOUIDI, PES, FSR, Université Mohammed V de Rabat
Pr. Rahal ROMADI, PES, ENSIAS, Université Mohammed V de Rabat
Examinateur :
Pr. Abderrahim BENSLIMANE, Professeur des universités, Université d'Avignon, France

Advanced detection and prevention technique to mitigate threats in multi-domain Software-Defined Networking using supervised machine learning techniques

Abstract: Software-defined networks (SDN) is a new flexible, automated, and dynamic network architecture that manages network services by abstraction and provides more networking capabilities. Indeed, SDN's centralized architecture provides better control, programmability, and orchestration over network resources. In addition, SDN solves the issues that stem from the archaic and hard-to-scale design of traditional networks. SDN brings also new protocols such as OpenFlow, new devices (e.g., Controllers and the OF-Switches), and new abstractions layers, which require significant expertise and specific engineering knowledge. The idea behind using an SDN architecture relies on separating the control plane from the data plane and logically centralizing it under a single/distributed controller. Due to its centralized architecture and the lack of intelligence on the data plane, SDN suffers from many security issues that slow down its deployment. On the other hand, centralizing the control plane brings new security threats such as having a single point of failure, on top of inheriting most of the known threats that traditional networks suffer from. Furthermore, traditional security methods are no longer able to protect this type of network as the complexity of attacks increases as quickly as innovation grows. To deal with these issues, we propose in this thesis a new robust and flexible security framework, "–1– key pool generator for mitigation threats 'KPG-MT' –2– context-based node acceptance based on the random forest model 'CBNA-RF' –3– multi-domain detection anomaly for SDN based on ML models 'MDDA-SDN'", the main objective is to guarantee nodes authentication and data confidentiality while preserving performance and guaranteeing a better quality of service. The main contributions of this thesis concern the development of a multi-defense mechanism for SDN architecture (single/distributed) while using the most appropriate machine learning technique for each attacks type. To do so, we build a real SDN dataset based on different simulations and scenarios (stress tests by using multiple flows and SDN nodes). Performing and modeling SDN levels-based attacks will also be made using a BlackBox approach to extract their main features and build a local dataset for further data analysis. The results obtained from the implementations and evaluations of our models demonstrate the effectiveness of our methodology frameworks against SDN levels-based attacks.

Keywords: SDN, OpenFlow, OpenDaylight Controller, Multi-Domain SDN, Advanced persistent Attacks, Machine learning, Ensemble Learning.

Résumé : Les réseaux définis par logiciel (SDN) représentent une nouvelle architecture de réseau flexible, automatisée et dynamique qui gère les services de réseau par abstraction et fournit davantage de capacités de mise en réseau. En effet, l'architecture centralisée du SDN permet un meilleur contrôle, une meilleure programmabilité et une meilleure orchestration des ressources du réseau. En outre, le SDN résout les problèmes qui découlent de la conception archaïque et difficile à dimensionner des réseaux traditionnels. Le SDN apporte également de nouveaux protocoles tels que OpenFlow, de nouveaux dispositifs (par exemple, les contrôleurs et les commutateurs OF) et de nouvelles couches d'abstraction, ce qui nécessite une grande expertise et des connaissances techniques spécifiques. L'idée derrière l'utilisation d'une architecture SDN repose sur la séparation du plan de contrôle du plan de données et sur la centralisation logique de ce dernier sous un contrôleur unique ou distribué. En raison de son architecture centralisée et du manque d'intelligence sur le plan des données, le SDN souffre de nombreux problèmes de sécurité qui ralentissent son déploiement. D'autre part, la centralisation du plan de contrôle apporte de nouvelles menaces de sécurité telles que le fait d'avoir un seul point de défaillance, en plus d'hériter de la plupart des menaces connues dont souffrent les réseaux traditionnels. En outre, les méthodes de sécurité traditionnelles ne sont plus en mesure de protéger ce type de réseaux, car la complexité des attaques augmente aussi vite que l'innovation. Pour faire face à ces problèmes, nous proposons dans cette thèse un nouveau cadre de sécurité robuste et flexible, « –1– key pool generator for mitigation threats 'KPG-MT' –2– context-based node acceptance based on the random forest model 'CBNA-RF' –3– multi domain detection anomaly for SDN based on ML models 'MDDA-SDN' », l'objectif principal étant de garantir l'authentification des noeuds et la confidentialité des données tout en préservant les performances et en garantissant une meilleure qualité de service. Les principales contributions de cette thèse concernent le développement d'un mécanisme de défense multiple pour l'architecture des SDN (simple/distribuée), tout en utilisant la technique d'apprentissage machine la plus appropriée pour chaque type d'attaque. Pour ce faire, nous construisons un ensemble de données SDN réel basé sur différentes simulations et scénarios (tests de stress en utilisant des flux multiples et des nœuds SDN). La réalisation et la modélisation d'attaques basées sur les niveaux SDN seront également effectuées en utilisant une approche de boîte noire pour extraire leurs principales caractéristiques et pour construire un ensemble de données locales pour une analyse plus approfondie des données. Les résultats obtenus à partir des mises en œuvre et des évaluations de nos modèles démontrent l'efficacité de nos cadres méthodologiques contre les attaques basées sur les niveaux de SDN.

Mots-clés : SDN, OpenFlow, OpenDaylight Controller, Multi-Domain SDN, Advanced persistent Attacks, Machine learning, Ensemble Learning.