Angers, le 7 juillet 2021

AVIS DE SOUTENANCE DE THÈSE

DOCTORAT (Arrêté du 25 mai 2016)

Monsieur Abdel Karim KASSEM

candidat au diplôme de Doctorat de l'Université d'Angers, est autorisé à soutenir publiquement sa thèse

le 23/07/2021 à 11h00
UCO
Learning Lab
Bâtiment scientifique
44, rue Rabelais
49000 ANGERS

sur le sujet suivant :

Système intelligent basé sur des techniques de l'apprentissage automatique pour l'évaluation de la sécurité et la détection des cyber-intrusions

Directeur de thèse : **Monsieur Pierre CHAUVET**

Composition du jury :
Monsieur Abd El Salam ALHAJJAR, Professeur Université Libanaise, Liban, Examinateur
Monsieur Olivier BARTHEYE, Maître de Conférence Ecole de l'Air, Salon-de-Provence, Examinateur
Monsieur Pierre CHAUVET, Professeur UCO Université Catholique de l'Ouest, Directeur de thèse
Monsieur Bassam DAYA, Professeur Université Libanaise, Liban, Co-directeur de thèse et Examinateur
Madame Michaela GEIERHOS, Professeur Université de la Bundeswehr, Allemagne, Rapporteur
Monsieur Mohammad HAJJAR, Professeur Université Libanaise, Liban, Rapporteur

Résumé de la thèse

L'apprentissage automatique est devenu une technologie décisive pour la cyber sécurité dans le but de protéger les réseaux et systèmes informatiques contre les cybercriminels. En conséquence, l'objectif de cette thèse est d'améliorer le mécanisme de sécurité appliquée, et proposer un système intelligent basé sur des techniques d'apprentissage automatique pour la détection des cyber-intrusions. Nous avons donc appliqué la technique de test de pénétration permettant de découvrir les vulnérabilités concernant les attaques les plus courantes. Plus tard, nous avons fourni des suggestions de sécurité et des solutions concernant ces cyber-attaques risqués. De plus, nous avons appliqué les techniques de web mining pour identifier plusieurs approches en termes de comportement des visiteurs et d'évaluation de la cyber sécurité. Par la suite, nous avons parvenu à détecter l'activité des visiteurs, leur comportement, le contrôle des ressources d'accès et les menaces qui peuvent affronter le serveur web. Ensuite, un système intelligent de détection d'intrusion hôte (HIDS : Host-based Intrusion Detection System) a été développé en utilisant les techniques de text mining. Pour cela, nous avons construit un ensemble de données de classification de texte fiables comprenant 6000 enregistrements d'URL malveillantes. Ce type de données nous a amené à proposer le modèle DOC2VEC comme méthode de représentation de caractéristiques dans notre HIDS. De plus, nous avons appliqué plusieurs techniques d'apprentissage automatique. Par conséquent, le perceptron multicouche (multilayer perceptron MLP) s'est avéré être le modèle le plus précis à 90,67% pour détecter les attaques SQLi, XSS ainsi que les attaques par traversée de répertoires. En outre, nous avons développé un nouveau système intelligent de sécurité appelé SIS-ID adopté pour détecter les dernières URL malveillantes et étendu aux attaques par déni de service distribuées (DDoS). De plus, notre système qui est basé sur plusieurs techniques d'apprentissage automatique a été examiné via deux bases de données configurées qui sont les DB-MALCURL et DB-DDOS extraites de l'institut canadien de cybersécurité (CIC). Ensuite, nous avons évolué les performances du système en utilisant nos méthodes d'optimisation d'apprentissage proposées. Ainsi, le SIS-ID a atteint la meilleure précision (98,52%) basé sur le modèle de vote qui détecte l'attaque d'URL malveillantes. D'autre part, le modèle stacking a enregistré la précision maximale (77,04 %) pour détecter l'attaque DDOS. Finalement, nous avons validé notre proposition de SIS-ID à l'aide d'un matériel basé sur la simulation en temps réel au sein de l'université libanaise. Par conséquent, le matériel a été configuré sur la base du modèle facteur de valeur aberrante locale (LOF) qui a atteint l'efficacité d'éviter une attaque par déni de service (DOS) effectuée sur une scène en temps réel.