Modélisation et Détection des Cyberattaques Assistées par l'IA

Contexte

Les cyberattaques dynamiques, caractérisées par leur adaptabilité et leur sophistication, représentent un défi évolutif en cybersécurité. Contrairement aux menaces traditionnelles, qui s'appuient souvent sur des modèles ou des vulnérabilités prédéfinis, les attaques dynamiques peuvent changer de tactique à la volée dans le but d'échapper aux mécanismes de détection. Cette évolution signifie le passage d'une orchestration manuelle des menaces vers un système d'attaque plus automatisé et intelligent, ce qui les rend de plus en plus difficile à prévoir et à atténuer.

L'intégration de l'intelligence artificielle (IA) dans la réalisation des cyberattaques permet aux attaquants d'automatiser leurs processus décisionnels, et même d'adapter leurs stratégies d'attaque en temps réel en fonction des mesures défensives qu'ils rencontrent. Cela augmente non seulement la vitesse et l'ampleur des attaques, mais permet également un niveau de personnalisation qui était auparavant inaccessible, faisant des cyberattaques assistées par l'IA un défi important, même pour les solutions de défenses les plus avancées.

Ce projet de doctorat en cotutelle entre l'Université de Lorraine, France, et l'Université Internationale de Rabat, Maroc, est un projet collaboratif qui a pour ambition de développer une analyse approfondie des cyberattaques dynamiques et assistées par l'IA, et de développer des approches de détection et de mitigation de celles-ci.

Objectifs

Les objectifs de cette thèse sont :

- **L'analyse des comportements des attaquants** : Comprendre les tactiques, techniques et procédures des attaquants en analysant les données des attaques passées et en cours. Cela inclut l'étude des mécanismes utilisés dans les attaques basées sur l'IA.
- **Le développement de modèles prédictifs** : Concevoir des modèles prédictifs avancés utilisant l'apprentissage automatique (e.g., réseaux de neurones de graphes spatio-temporels dynamiques) pour identifier les schémas et les signatures des attaques dynamiques et basées sur l'IA. Ces modèles aideront à anticiper ce type d'attaques et améliorer les systèmes de détection en quasi-temps réel.
- **La construction de contre-mesures et de stratégies de mitigation** : Élaborer et tester des stratégies de réponse et de mitigation pour neutraliser les attaques dynamiques, minimisant ainsi les dommages potentiels.
- **Le développement de modèles basés sur la théorie des jeux** : Explorez l'utilisation de modèles de théorie des jeux, tels que les jeux dynamiques markoviens, pour évaluer l'efficacité des méthodes défensives contre les attaquants assistés par l'IA. Cela implique de quantifier les valeurs du modèle de jeu pour la prise de décision dans des scénarios dans lesquels les attaquants utilisent des techniques d'IA pour lancer des attaques avancées.

Profil recherché et procédure de candidature

Le candidat doit justifier d'une expérience en apprentissage automatique (ML) et idéalement des connaissances en cyber sécurité. Pour candidater :

- CV détaillé
- Lettres de recommandations
- Relevés de notes de master ou école d'ingénieur

Vous adressez votre candidature à Abdelkader Lahmadi (lahmadi@loria.fr) et Mehdi Zakroum (mehdi.zakroum@uir.ac.ma)

Environnement de travail

Ce projet de thèse est en cotutelle entre l'Université de Lorraine (UL), Nancy, France, et l'Université Internationale de Rabat (UIR), Rabat, Maroc. Les laboratoires d'accueil sont le TICLab (UIR) et le LORIA (UL). La thèse s'étale sur 36 mois. Le doctorant passera idéalement 18 mois à l'UIR et 18 mois à l'UL, au total.

Rémunération et avantages

Le doctorant bénéficiera d'une bourse d'excellence LUE "Lorraine Université d'Excellence". Les frais de déplacement entre les deux pays sont couverts. Le doctorant bénéficiera de plusieurs facilités dans les deux campus (piscine, salle de sports, restauration, etc.).