Apprentissage par renforcement pour l'évaluation automatisée du risque dans les systèmes en réseau

Contexte :
Les systèmes en réseaux OT (Operational Technology) et IoT sont devenus omniprésents dans notre quotidien et notre environnement pour réaliser différentes tâches allant de la mesure et de la surveillance, de la santé, de la domotique, jusqu'à leur intégration dans des systèmes sensibles et critiques. Il a été démontré par plusieurs travaux de recherche et de développement que ces systèmes et leurs équipements présentent différentes vulnérabilités et ils peuvent être utilisés par des attaquants pour réaliser des attaques complexes et ciblées avec des dégâts conséquentes au niveau matériel, financier et même humain. Il est ainsi devenu indispensable d'étudier et analyser le niveau de présence des vulnérabilités et les possibilités des attaques sur ces systèmes. Dans le laboratoire LORIA – Inria Nancy Grand Est, nous développons des techniques basées sur l'apprentissage automatique pour étudier la sécurité de ces équipements et ces objets dans différents environnements aussi industriels que domotique.
L'analyse de la sécurité de ces système se traduit notamment par une analyse des risques potentiels d'une attaque. Cette analyse est actuellement très manuel et nécessite un effort humain important.

Sujet :
Dans cette thèse, nous proposons d'explorer les méthodes d'apprentissage par renforcement profond (Deep Reinforcement Learning) [1,2] pour l'évaluation automatisée de la sécurité d'un environnement cible simulé/émulé sous forme d'un jumeau numérique. Notre approche s'appuie sur des agents RL (Reinforcement Learning) pour cartographier automatiquement les chemins d'attaque dans un système simulé ou émulé. Ces agents simulent les comportements des attaquants et des utilisateurs pour construire des chemins d'attaque complexes et identifier leurs conséquences, voire leurs effets cascade. Le rôle d'un agent RL attaquant est d'exploiter artificiellement des vulnérabilités pour construire son chemin vers une cible [3]. En revanche, les agents utilisateurs mènent des actions légitimes pour installer des logiciels, ouvrir un PDF, cliquer sur un lien dans un mail, déployer un objet connecté, etc.
Les applications de test de notre approche, sont notamment un système industriel d'un micro-réseau électrique (microgrid) [4] en format jumeau numérique haute-fidélité et des objets connectés en format honeypot IoT pour évaluer les performances de cette approche en termes de scénarios d'attaque détectés, et son passage à l'échelle.
Cette thèse apporte une technique et un prototype d'une solution capable d'automatiser l'évaluation du risque dans des infrastructures critiques en identifiant a priori les chemins d'attaque potentiels. Cette approche s'appuie sur des jumeaux numériques pour valider les résultats dans des environnements assez fidèle à la réalité. Les deux cas d'usage (jumeau numérique et honeypot IoT) étudiés et testés dans ce travail seront hébergés et déployés sur la plateforme LHS de Nancy [5].

Références
[1] Richard S. Sutton, Reinforcement Learning: A Introduction, http://incompleteideas.net/book/the-book.html
[2] Mohamed Said Frikha, Sonia Mettali Gammar, Abdelkader Lahmadi, Laurent Andrey. Reinforcement and deep reinforcement learning for wireless Internet of Things: A survey. *Computer Communications*, 2021, 178, pp.98-113.
[3] https://github.com/microsoft/CyberBattleSim
[4] Mingxiao Ma, Abdelkader Lahmadi, Isabelle Chrisment. Detecting a Stealthy Attack in Distributed Control for Microgrids using Machine Learning Algorithms. *3rd IEEE International Conference on Industrial Cyber-Physical Systems (ICPS)*, Jun 2020, Tampere (online), Finland.

[5] Frédéric Beck, Abdelkader Lahmadi, Jérôme François. HSL: a Cyber Security Research Facility for Sensitive Data Experiments. *DISSECT - 7th IEEE/IFIP Workshop on Security for Emerging Distributed Network Technologies*, May 2021, Bordeaux, France

Qualifications requises

- Diplôme d'ingénieur ou Master en informatique
- Connaissances : réseau, web, sécurité informatique
- Langages de programmation : Python, shells et autres sont appréciés
- Environnement de programmation : préférable d'être familier avec des librairies comme scikit learn, pandas, dask, numpy, cuda (et autres librairies/outils de ML), environnement de développement collaboratif (github)
- Langues : français, anglais

Cadre du travail :

L'équipe RESIST (https://team.inria.fr/resist/) de l'Inria Nancy Grand Est est spécialisée dans la mise à l'échelle et la sécurité des systèmes en réseau à travers trois axes principaux : le monitoring, l'analyse de données et l'orchestration. Elle a une grande expertise dans la définition de nouvelles méthodes et le développement d'outils à base d'algorithmes d'apprentissage pour la gestion des systèmes en réseaux et en particulier leur sécurité. Cette expertise a donné lieu à des travaux publiés et reconnus dans de nombreux domaines et notamment l'analyse de trafic (chiffré), le fingerprinting d'actions IoT, la détection d'attaques, etc. L'équipe se compose actuellement d'une trentaine de membres mélangeant chercheurs, professeurs, maîtres de conférence, doctorants, post-doctorants et ingénieurs. Elle est intégrée au LORIA, un laboratoire commun entre l'Inria, l'Université de Lorraine et le CNRS, qui compte environ 400 personnes au total.

Informations complémentaires :

Localisation : Nancy
Encadrants : Abdelkader Lahmadi (Loria), Isabelle Chrisment (Inria)
Durée : 36 mois (à partir du 01/10/2023)

Pour postuler :

Envoyer les documents suivants à abdelkader.lahmadi@loria.fr
avant le 15/07/2023 :

- CV
- Lettre de motivation
- Copie des diplômes universitaires et relevés de notes
- Thèse de master si achevée ou description du sujet
- Au moins une lettre de recommandation d'une personne qui vous a encadré par le passé (avec ses informations de contact)
- Toute autre information utile (publication scientifique par exemple)