Thèse dispositifs de leurrage reconfigurables et à haute interactivité pour les systèmes de contrôle industriels

Stéphane Mocanu stephane.mocanu@inria.fr, Julien Francq julien.francq@naval-group.com, Jean Leneutre jean.leneutre@telecom-paris.fr

Localisations possibles : Grenoble ou Région Parisienne (Palaiseau)

Contexte

Ce sujet de thèse fait partie du projet SuperviZ (https://files.inria.fr/superviz/) financé par le Programme et équipements prioritaires de recherche (PEPR) Cybersécurité (https://www.pepr-cybersecurite.fr/). Le projet SuperviZ contribue au domaine de la « sécurité des systèmes, des logiciels et des réseaux ». Plus précisément, il cible la détection, la réponse et la remédiation aux attaques informatiques, sujets regroupés sous l'appellation de « supervision de sécurité ».

La supervision de la sécurité fait face à des défis importants, avec l'augmentation du nombre de composants à surveiller et la croissante hétérogénéité des capacités de ces composants (serveurs, ordinateurs personnels, tablettes, téléphones, objets divers) en termes de communication, stockage et calcul.

Au sein du projet SuperviZ, le lot « Détecter les attaques » s'intéresse à l'amélioration des techniques de détection comportementale. Actuellement, la détection comportementale est challengée par la difficulté à obtenir des modèles fiables, que ce soit par l'apprentissage – technique largement majoritaire – ou par d'autres moyens (spécifications, politique de sécurité, etc.). De plus, les alertes proposées par ces détecteurs comportementaux manquent de capacité à expliquer la source du problème et à proposer des mécanismes de remédiation. Le lot se focalise d'une part sur l'amélioration des capacités de détection, d'autre part sur leur robustesse, et finalement sur leur utilisation dans des environnements très spécifiques (mobile, immersif).

Objectifs

Dans le cadre de la « mesure de la Force Cyber » des attaquants, il faut pouvoir comprendre leurs moyens d'attaques, aussi appelés TTPs (Tactiques, Techniques et Procédures). Dans le monde de l'IT, c'est-à-dire des systèmes d'information classiques, il existe des produits du commerce fournissant ce type de renseignements. Dans le monde des systèmes industriels et de l'OT (Operational Technology), les informations sont en revanche plus difficiles à récolter car elles concernent des attaques ultra-spécialisées, s'activant de manière rare et intempestive, et dépendantes des architectures visées. Or, l'historique des attaques récentes nous montre que des attaques sur des systèmes OT peuvent avoir des conséquences catastrophiques pour les intérêts vitaux d'un Etat, preuve en est l'attaque sur Colonial Pipeline, ou bien l'intrusion d'un réseau de traitement de l'eau potable en Floride.

Verrous technologiques :

Afin de surveiller les activités de ce type d'attaquant, une possibilité est d'utiliser un « pot de miel » ou « honeypot ». Ce dispositif de leurrage imitant une infrastructure réseau fictive incite les attaquants potentiels à s'y connecter pour y réaliser des opérations frauduleuses (« indolores » car réalisées sur une infrastructure maîtrisée). L'avantage de ce dispositif est que l'attaquant y laisse des « traces » donnant des informations sur les TTPs utilisés : protocoles visés, dates de première connexion, adresses IP se connectant, pays d'origine, etc. C'est ce que produit typiquement le honeypot « CONPOT » : bien que hautement configurable, la palette de protocoles industriels (Modbus, http, SNMP, s7comm) et de composants industriels émulés est limitée. Les expérimentations menées montrent que quelques heures seulement après la mise en service de l'honeypot, ce dernier enregistre plusieurs dizaines de tentatives de connexions, préalables à une attaque potentielle. Malheureusement, bien qu'intéressantes, ces premières informations récoltées ne permettent pas d'avoir une vue complète des TTPs des attaquants. Impression renforcée par le fait que l'architecture émulée est très simple, et que donc les capacités de propagation d'un attaquant dans un réseau réaliste plus complexe ne sont pas jaugeables. Par ailleurs, ces informations peuvent être elles-mêmes modifiées malicieusement (ex. : masquage des adresses IP). Enfin, l'architecture visée étant statique, l'attaquant, une fois connecté à

l'architecture, a tendance à ne plus y revenir n'y voyant plus aucun intérêt : l'attaquant échappe ainsi à toute surveillance.

Objectifs et moyens techniques :

L'objectif de cette thèse est de proposer un honeypot reconfigurable fournissant une haute interactivité avec les attaquants. Il devra être reconfigurable dynamiquement afin de conserver son attractivité, tout en restant « plausible », c'est-à-dire représentatif d'un système industriel réel, et donc ne pas trop s'en écarter : cela constitue donc un premier verrou. A ce titre, l'étude de la notion de jumeau numérique (Digital Twin) OT pourrait être utile. Ce dispositif de leurrage sera également reconfigurable avec à chaque nouvelle itération une nouvelle difficulté à contourner : par exemple, une nouvelle ségrégation réseau, une nouvelle règle d'IDS, etc. Ceci afin de constater à quel point les attaques sont automatiques et adaptables. Cette intrication autonome et adaptative attaque/défense pourra être réalisée le cas échéant à l'aide d'un apprentissage par renforcement profond (Deep Reinforcement Learning, DeepRL), par un réseau antagoniste génératif (Generative Adversarial Network, GAN), voire même par des agents autonomes basés sur de l'IA générative.

Un volet attribution sera également développé dans la thèse : en effet, il faudra à terme connecter la récolte d'informations du dispositif de leurrage à des outils existants de Cyber Threat Intelligence (CTI) afin de pouvoir tenter d'identifier des groupes d'attaquants via les TTPs employés.

Profil recherché

Le profil privilégié est celui d'informaticien avec un parcours sécurité informatique architecture et systèmes. Profil automaticien avec des très bonnes connaissances en informatique et programmation est également possible.

Deux localisations sont possibles :

- l'équipe mixte LIG/INRIA Ctrl-A (https://team.inria.fr/ctrl-a/fr/).
- l'équipe ACES (Autonomous Critical Embedded Systems), laboratoire LTCI, Télécom Paris, Institut Polytechnique de Paris (https://www.telecom-paris.fr/en/research/labs/information-processing-ltci/teams/autonomous-critical-embedded-systems).

Le niveau de salaire est celui d'un contrat doctoral de l'Université Grenoble-Alpes (https://doctorat.univ-grenoble-alpes.fr/preparer-un-doctorat-/sujets-et-financements/).

Références.

[1] S. Tricaud, « CONPOT : l'art de faire mûrir ses pommes en simulant un système de contrôle industriel (ICS) », MISC n°97, mai/juin 2018.
[2] J. Franco, A. Aris, B. Canberk, A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems", IEEE Commun. Surv. Tutorials 23(4): 2351-2383, 2021.
[3] M. Abbas, H. Debar, J. Gouy, « Leurrage et Jumeau Numérique », C&esar 2021, "Automatisation en Cybersécurité", 2021.
[4] R. S. Sutton, A. G. Barto, "Reinforcement Learning, 2nd Edition", The MIT Press, 2018.
[5] H. Chen, L. Jiang, "Efficient GAN-based Method for Cyber-Intrusion Detection", arXiv:1904.02426, 2019.
[6] T. D. Wagner, K. Mahbub, E. Palomar, A. E. Abdallah, "Cyber threat intelligence sharing: Survey and research directions", Comput. Secur. 87, 2019