TH 2.2 Détection des scénarios d'attaque avancés dans les systèmes industriels par une approche mixte IDS/Supervision industrielle

Stéphane Mocanu stephane.mocanu@inria.fr Equipe CTRL-A, Laboratoire LIG, Centre de recherche Inria Rhône-Alpes, Minatec Campus, 17 rue des Martyrs, 38054

Contact : stephane.mocanu@inria.fr

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).

Dans le contexte d'amélioration des modèles de détection et explicabilité des alertes nous nous intéressons à la détection des attaques dans les systèmes industriels en couplant les alertes des moniteurs de comportement du trafic réseau (NIDS – Networks Intrusion Detection System) avec le log des événements du système de contrôle/commande/supervision du processus physique (SCADA – Supervisory Control and Data Acquisition). Ce sujet de recherche vise à étendre une approche existante (détection réseau « comportementale » développée dans la thèse de Oualid Koucham) en corroborant les alertes avec l'analyse de l'historique du comportement du système industriel tel qu'enregistré par le SCADA (la salle de contrôle).

Objectifs

Nous souhaitons trouver des liens entre les évènements de sécurité alertés par le NIDS et une trajectoire particulière du processus physique reconstituée à partir de l'historique du SCADA. Bien qu'il ne s'agisse pas d'une corrélation dans le sens de la « corrélation des alertes », car l'historique du SCADA comprend l'évolution (les trajectoires) des variables du processus, les objectifs de la démarche sont les mêmes à savoir la réduction des faux positifs et la compréhension des alertes. En particulier cette approche pourrait mettre en évidence le lien entre des évènements de sécurité

et les changements de comportement du processus à long terme mais aussi permettra, dans certains cas, discriminer les défaillances des attaques. Par exemple si un actionneur présente des signes de fatigue dans l'historique du SCADA en absence des évènements cyber, un évènement cyber corrélé à un comportement inattendu de l'actionneur pourrait être diagnostiqué plutôt comme une défaillance qu'une attaque.

Approche envisagée

Pour le partie détection comportementale on va se baser comportementale on se base sur des travaux existants. La corrélation des informations dans les logs du SCADA avec le trafic réseau nécessitera un enrichissement des entrées des logs avec des informations réseau. La reconnaissance des tendances du processus et des modes de comportement sera basée sur des algorithmes de machine learning. La méthodologie et les outils seront validés sur la plateforme expérimentale G-ICS. (http://lig-g-ics.imag.fr/)

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. La personne retenue intégrera l'équipe mixte LIG/INRIA Ctrl-A (https://team.inria.fr/ctrl-a/fr/) et participera activement au projet SuperviZ (participation aux réunions de projet, réseaux de doctorants and animations scientifiques).

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.

Oualid Koucham. Intrusion detection for industrial control systems. Automatic. Université Grenoble Alpes, 2018. English. ⟨NNT : 2018GREAT090⟩. ⟨tel-02108208⟩

Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, Frédéric Majorczyk. Cross-domain Alert Correlation methodology for Industrial Control Systems. *Computers and Security*, 2022, 118 (July), pp.102723. ⟨10.1016/j.cose.2022.102723⟩. ⟨hal-03636549⟩