TH 2.3 Détection des intrusions orientée hôte dans les systèmes industriels

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

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 possibilité d'embarquer une systèmes de détection d'intrusions sur un équipement de contrôle industriel. . Traditionnellement, en raison des ressources de calcul limitées des équipements de contrôle/commande industriels mais aussi de l'utilisation des systèmes d'exploitation propriétaires, la détection des intrusions dans les systèmes industriels est limitée aux approchés orientées réseaux. Les nouvelles générations d'équipement sont, d'une part, basées sur des plateformes de calcul plus puissantes et, d'une autre part, embarquent des systèmes d'exploitation ouverts (typiquement Windows CE LTS). Cette thèse s'intéresse au prototypage d'un HIDS (Host Intrusion Détection System) pour la détection des attaques dans les SCADA sur une plateforme ouverte (ODK Siemens et/ou Soft PLC) basée sur le monitoring temps-réel des tâches embarquées.

Objectifs

Ce sujet vise à étendre le déploiement de systèmes de détection des intrusions basé sur les approches comportementale dans les systèmes industriels jusqu'aux équipements terminaux (automates programmables industriels). Plus précisément on étudie le déploiement d'un IDS comportemental sur un automate programmable industriel et l'impact sur la performance temps-réel de la commande.

Approche envisagée

Nous allons nous appuyer sur l'analyse des programmes embarqués et des spécifications sorties des normes pour la synthèse des moniteurs. Le principal défi est l'évaluation de l'impact de l'IDS sur la performance temps réel de l'automate programmable. La minimisation du nombre des propriétés de sécurité à surveiller ainsi que de leur complexité sera déterminante pour la performance de la solution. Un second aspect étudié sera la comparaison des types d'attaques orientées processus détectés par le HIDS versus la capacité de détection d'un NIDS. Cette comparaison permettra permettre de réduire encore plus le nombre des propriétés de sécurité surveilles. Néanmoins, il est connu que l'état interne d'un contrôleur embarqué est partiellement observable par un NIDS à partir du trafic réseau. Une approche de corrélation entre les alertes des NIDS et celles du HIDS permettra d'évaluer la valeur ajoutée du HIDS dans un système de détection distribué hybride (HIDs/NIDS). 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 ou systèmes embarquées. 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⟩

L. Garcia, S. Zonouz, Dong Wei and L. P. de Aguiar, "Detecting PLC control corruption via on-device runtime verification," 2016 Resilience Week (RWS), Chicago, IL, USA, 2016, pp. 67-72, doi: 10.1109/RWEEK.2016.7573309 https://ws.engr.illinois.edu/sitemanager/getfile.asp?id=2344

Josh Hilke, Runtime Monitoring of PLCs In Critical Real-Time Systems, Master Thesis, https://dspace.mit.edu/bitstream/handle/1721.1/139377/Hilke-jrhilke-meng-eecs-2021-thesis.pdf

.