# TH 3.2 Auto-reconfiguration des systèmes industriels. Etude de la résilience face aux cyber-attaques

Stéphane Mocanu stephane.mocanu@inria.fr, Eric Rutten Eric.Rutten@inrialpes.fr , Gwenaël Delaval gwenael.delaval@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).

## Objectifs

Nous nous intéressons aux mécanismes de réaction en cas d'attaque dans les systèmes industriels. Plus particulièrement nous sommes intéressés par les mécanismes d'auto-reconfiguration du système en cas d'attaque. L'approche traditionnelle se limite à une reconfiguration du réseau de communication visant à isoler les équipements compromis. Ce mécanisme est peu adapté aux systèmes industriels car l'isolation d'un contrôleur compromis laisse une partie du processus physique en évolution libre ce que peut engendrer des situations dangereuses.

L'objectif de l'étude vise la synthèse d'une méthodologie de reconfiguration du système en cas d'attaque. Basé sur les alertes levées par des IDS un mécanisme de décision va identifier les équipements compromis. La reconfiguration du réseau de communication permettre l'isolation des équipements compromis. En utilisant les contrôleurs restants la reconfiguration de la commande va charger de nouveau programmes de contrôle afin d'assurer l'intégrité et la sécurité fonctionnelle du processus piloté.

Nous allons utiliser la méthodologie de synthèse de contrôleurs discrets pour la reconfiguration du système. On va s'appuyer sur les outils de modélisation des systèmes synchrones tel que Heptagone (extension de Lustre) qui permet de formuler le problème de reconfiguration sous la forme d'un contrat qui renforce la satisfaction des fonctions de sécurité du système physique. Un outil de synthèse des contrôleurs tel que BZR ou Reax permettra la synthèse de l'algorithme de reconfiguration.

## Approche envisagée

Une méthodologie d'auto reconfiguration du système basée sur une boucle autonomique sera réalisée. Nous allons nous baser sur des IDS existants pour le monitoring et l'analyse. L'exécution des actions concerne la reconfiguration de l'architecture réseau et des programmes de commande des automates. La politique de reconfiguration (Plan) sera basée sur une synthèse des contrôleurs à évènements discrets renforçant les propriétés de sécurité du système physique en cas d'attaque. 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.

Gwenaël Delaval, Ayan Hore, Stéphane Mocanu, Lucie Muller, Eric Rutten. Discrete Control of Response for Cybersecurity in Industrial Control. IFAC 2020 - IFAC World Congress 2020, Jul 2020, Berlin, Germany. pp.1-8. ⟨hal-02569406⟩