Nouvelles vulnérabilités, nouvelles menaces, nouvelles solutions

Grenoble mardi et mercredi 30 et 31 janvier 2018

Approche par filtre basée sur la distance aux états critiques pour la sécurisation des systèmes cyber-physiques face aux cyberattaques

Franck Sicard

Doctorant – Laboratoire G-SCOP

Tel : 33 4 76 57 50 82 – franck.sicard@grenoble-inp.fr

Mots clés : *Cybersécurité, sûreté, détection d'intrusion, contrôle-commande, approche par filtre, models based*

Résumé :

Conçus à l'origine pour assurer la productivité et la sûreté de fonctionnement, les systèmes de contrôle-commande (*ou Industrial Control System, ICS*) sont présents dans de nombreuses infrastructures critiques (production et distribution d'Energie, transports, défense…) et sont de nos jours la cible de cyberattaques. Du ver informatique Stuxnet (2010) aux attaques par rançongiciels (2016-2017) en passant par l'attaque sur le réseau électrique ukrainien (2015), les ICS présentent de nombreuses vulnérabilités qui permettent de générer de grandes surfaces d'attaques. De plus, comme ils pilotent des systèmes physiques (Systèmes Cyber-Physiques), les impacts en cas d'attaque sont extrêmement importants (pertes humaines, financières, dégâts environnementaux, arrêts de production…).

Afin de protéger les ICS, une approche basée sur des filtres a été développée pour détecter des intrusions pouvant amener le système dans des états critiques. Les mécanismes de détection mis en œuvre reposent sur la localisation de ces filtres dans l'architecture matérielle mais également sur des modèles du procédé et de commande. Ces modèles permettent de connaître, sans compromission possible de la part d'un attaquant, l'état du système et donc de calculer un éloignement à des zones critiques. En fonction de la détection, les filtres peuvent alerter les opérateurs d'une dérive, bloquer des actions pouvant amener le système dans des états critiques ou mettre le système en replis.

La présentation permettra de détailler l'approche et la méthodologie de conception des filtres (de l'analyse de risques aux algorithmes de détection). Des exemples d'applications illustrant diverses attaques possibles seront mis en avant ainsi que les différents mécanismes de détection engagés pour les repousser.