Nouvelles vulnérabilités, nouvelles menaces, nouvelles solutions

Grenoble mardi et mercredi 30 et 31 janvier 2018

Revue des différentes approches pour les systèmes de détection d'intrusion (IDS) pour les systèmes de contrôle industriels : des approches classiques aux approches par machine learning

Pr Jean-Marie Flaus

Professeur – Laboratoire G-SCOP

Tel : 33 4 76 82 62 29 – jm.flaus@gmail.com

Mots clés : *Cybersécurité, Intrusion Detection System (IDS), système cyber physique, machine learning*

Résumé :

La cybersécurité des installations industrielles est une question qui préoccupe fortement les pouvoirs publics. De nouvelles réglementations et guides ont été proposés ces dernières années pour mettre en place une démarche de défense en profondeur permettant de maîtriser le cyber-risque.

Dans le cadre de cette démarche, les systèmes de détection d'intrusion constituent un élément important. Ils ont pour objectif d'alerter en cas d'intrusion et toute la difficulté est d'avoir un bon taux de détection sauf pour autant générer de fausses alertes. Pour les installations industrielles dites à risque, la mise en place de tels dispositifs fait partie des recommandations des principaux guides, notamment celui de l'ANSSI.

De nombreuses approches ont été proposées pour la détection d'intrusion depuis les années 80. On distingue classiquement les IDS à base de signature et les IDS détectant les anomalies de comportement. Ces algorithmes ont été conçus pour les systèmes informatiques. Pour les systèmes industriels, les contraintes sont différentes : il est particulièrement important de ne pas avoir de faux positifs et les aspects temps réel sont très importants. Cependant, il peut être envisageable de s'appuyer sur un modèle du comportement du système physique et le débit est souvent moins important.

L'objectif de cette présentation est de faire un tour d'horizon des principales méthodes pour la conception des IDS pour les systèmes industriels en y incluant les dernières approches à base d'apprentissage (*machine learning*).