Nouvelles vulnérabilités, nouvelles menaces, nouvelles solutions

Grenoble mardi et mercredi 30 et 31 janvier 2018

Génération de scénarios d'attaque contre les systèmes industriels

Maxime Puys

Doctorant VERIMAG, Université Grenoble Alpes

Tel : 33 4 57 42 22 46 – maxime.puys@univ-grenoble-alpes.fr

Mots clés : *SCADA, sécurité, sûreté, scénario d'attaque, méthodes formelles, protocoles*

Résumé :

Les systèmes industriels (SCADA) sont la cible d'attaques informatiques depuis Stuxnet en 2010. De part leur interaction avec le monde physique, leur protection est devenue une priorité pour les agences gouvernementales. Dans cet exposé, nous présentons plusieurs travaux ayant pour objectif de vérifier formellement la sécurité des systèmes industriels. Dans un premier temps, nous vérifions des propriétés de sécurité telles que la confidentialité ou l'authentification sur les protocoles OPC-UA et MODBUS. Nous modélisons pour cela les messages envoyés par ces protocoles à l'aide d'outils simulant toutes les actions possibles d'un attaquant. Nous étendons par ailleurs les propriétés vérifiées par ces outils à des propriétés sur le flux des messages. Dans un second temps, nous cherchons à vérifier si un attaquant, une fois entré dans le système (par exemple par la compromission d'un composant), peut violer des propriétés de sûreté de fonctionnement. Les propriétés visées dans ce cas sont des propriétés liées au procédé et jugées comme critiques (par exemple, vérifier qu'un sectionneur électrique n'est jamais ouvert en charge). Nous modélisons pour cela le système à vérifier ainsi que des attaquants caractérisés par leurs positions et leurs capacités de nuisance, résultant par exemple d'une analyse de risque.