Etude des vulnérabilités des IHM de supervision industrielle

Référence du stage : SEF-2019-LA-11
Encadrant : Soraya Kesraoui (Soraya.KESRAOUI@segula.fr)
Compétances requises : cyber-sécurité.
Mots clés : Cyber-sécurité, Vulnérabilités, IHM industrielles, SCADA
Equipe : R&I de Lanester (Segula Technologies)

1. Présentation de l'entreprise

SEGULA Technologies est un groupe d'ingénierie présent mondialement, au service de la compétitivité de tous les grands secteurs industriels : automobile, aéronautique, énergie, ferroviaire, naval, pharmacie et pétrochimie. Présent dans 26 pays, fort de ses 100 implantations dans le monde, le Groupe privilégie une relation de proximité avec ses clients grâce aux compétences de ses 11 000 collaborateurs. Ingénieriste de premier plan plaçant l'innovation au coeur de sa stratégie, SEGULA Technologies mène des projets d'envergure, allant des études jusqu'à l'industrialisation et la production.

2. Contexte

Les systèmes industriels se différencient des systèmes informatiques standards par leur capacité à piloter des procédés physiques, tels que les installations d'eau ou d'électricité. Sur le plan fonctionnel, ces systèmes sont régis par un ensemble de contraintes (métier, temps réel, sûreté de fonctionnement et disponibilité) et ont une durée de vie entre 10 et 40 ans. Un système de contrôle-commande permet le pilotage d'un procédé industriel physique au travers des fonctions de commande, de surveillance et de supervision. La commande a un rôle opérationnel qui consiste à faire exécuter un ensemble d'opérations pour agir sur le procédé physique (Niel et Craye 2002). La surveillance a un rôle informationnel qui porte sur le recueil des signaux provenant du procédé et de la commande, reconstituer l'état du système, dresser des historiques et le traitement de défaillance. La supervision a un rôle décisionnel qui permet d'optimiser, en présence ou non de défaillances, le fonctionnement du système.
Les systèmes industriels actuels intègrent de plus en plus les technologies de l'information sans tenir compte des vulnérabilités qu'elles peuvent introduire (ANSSI, 2012). De plus, la conception de ces systèmes se focalise plus sur la sûreté de fonctionnement, laissant de côté les aspects liés à la cyber-sécurité. Notons aussi que contrairement aux systèmes informatiques standards qui parviennent à corriger les vulnérabilités par l'application de correctifs, les systèmes industriels, par leur contraintes de disponibilité et de sûreté, ne peuvent pas adopter les mêmes correctifs ce qui constitue un vrai risque pour les systèmes industriels (ANSSI, 2012). Il devient alors nécessaire de renforcer la sécurité des systèmes industriels contre les cyber-attaques d'autant que ces dernières peuvent avoir des conséquences très lourdes (pertes financières, impact sur l'environnement, vol de données, responsabilité civile/pénale, image et notoriété,…).
La sécurité des systèmes industriels repose sur trois piliers fondamentaux qui sont la disponibilité, l'intégrité et la confidentialité. La disponibilité est la possibilité des éléments constitutifs du système d'être accessibles et utilisables à chaque demande (Zhu et al. 2011). L'intégrité signifie que les produits et services fournis sont complets et conformes aux réglementations (ANSSI, 2012) et que leur contenu ne soit pas modifié ou manipulé par une intervention non autorisée (Zhu et al. 2011). La confidentialité signifie que les informations ne pas disponibles et non divulguées à des individus non-autorisés (Cheminod et al. 2013).
Au cours de l'année 2017 et après étude des vulnérabilités des programmes de commande, nous avons détecté une nouvelle attaque qui affecte l'intégrité des langages de la norme IEC 61131-3 (IEC 2013).

3. Description détaillée

L'objectif de ce stage est d'étudier la faisabilité de cette attaque et son impact sur les IHM industrielles. Il s'agira, d'une part, de définir les moyens à mettre en œuvre pour mener cette attaque et, d'autre part, d'étudier l'impact de cette attaque sur un exemple de système industriel (système de gestion d'eau douce embarqué dans un navire). Pour cela, trois verrous sont à lever. Le premier verrou consiste à étudier les objectifs d'une telle attaque et aussi les techniques qu'un attaquant peut utiliser pour mener cette attaque au niveau des IHM industrielles. Le deuxième verrou consiste à valider les résultats sur un exemple de système industriel afin d'étudier l'impact de ce type d'attaque sur ce dernier. Le troisième verrou porte sur la définition des contre-mesures afin de faire face à cette attaque. L'efficacité de ces contre-mesures sera évaluée sur le système de gestion d'eau douce sanitaire.

Résumé de la démarche envisagée :

- Etat de l'art et appropriation des travaux précédents
- Etude d'une attaque d'intégrité sur une IHM industrielle, ses types et ses impacts
- Définition du protocole expérimental
- Expérimentation de la solution

4. Contact

Merci de nous faire parvenir votre candidature (lettre de motivation et CV) sous la référence **SEF-2019-LA-11** à l'adresse suivante : **Soraya.KESRAOUI@segula.fr**

5. Références bibliographiques

ANSSI. (2012). Maîtriser la SSI pour les systèmes industriels.

Cheminod, M., Durante, L. et Valenzano, A. (2013). Review of security issues in industrial networks. IEEE Transactions on Industrial Informatics, 9(1), 277 293. doi:10.1109/TII.2012.2198666

IEC. Programmable controllers - Part 3 : Programming languages. International Electrotechnical Commission, 2013

Niel, E., & Craye, E. (2002). Maîtrise des risques et sûreté de fonctionnement des systèmes de production. Productique: information, commande, communication. Lavoisier.

Zhu, B., Joseph, A., & Sastry, S. (2011, October). A taxonomy of cyber attacks on SCADA systems. In 2011 IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing (pp. 380-388). IEEE.