Modélisation des vulnérabilités et automatisation des tests d'intrusions pour les systèmes industriels

Référence du stage : SEF-2019-LA-06
Encadrant : Soraya Kesraoui (Soraya.KESRAOUI@segula.fr)
Compétances requises : cyber-sécurité, tests logiciels, modélisation formelle.
Mots clés : Test, Modélisation, Cyber-sécurité, Vulnérabilités, Contrôle-commande, 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. Cette grande durée de vie des installations entraine souvent une « superposition » de composants hétérogènes.
Les systèmes industriels actuels intègrent de plus en plus les technologies de l'information sans tenir compte des vulnérabilités qu'elles peuvent introduire. 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 adoptés les mêmes correctifs ce qui constitue un vrai risque pour les systèmes industriels. 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,…).
Les tests d'intrusion (ou pentests) sont souvent conduits afin d'étudier la vulnérabilité d'un système face à des scénarios d'attaques (Dalalana Bertoglio et et Zorzo, 2017). L'utilité des tests d'intrusion a été largement démontrée dans la littérature. Cependant, la réalisation des tests est une tâche fastidieuse et très coûteuse en temps et en ressource et souvent sujette à des omissions et des erreurs. En effet, l'élaboration des tests nécessite la définition des objectifs de tests qui décrivent le but général et abstrait de tests. A partir de ces objectifs, des jeux de tests comprenant des données réelles sont alors déduits. Plusieurs jeux de tests sont souvent nécessaires pour un seul objectif de test. Enfin, les jeux de tests sont exécutés sur le système à tester et les résultats obtenus sont comparés aux résultats attendus (bouquet et al. 2014).
L'automatisation des tests en général et les tests de vulnérabilités en particulier est alors nécessaire pour faciliter et pour assister les testeurs *(Lebeau et al. 2013 ; Javed et al. 2016)*. Les approches de tests basées sur les modèles semblent une solution prometteuse pour l'automatisation des tests (Zander-nowicka, 2008, Zulkernine et al. 2009 ; Botella et al. 2014 ; Qiu et al. 2014; Bouquet et al. 2014 ; Stefinko et al. 2016, Stefinko et al. 2017). En effet, le comportement du système à tester et les objectifs de tests sont modélisés par des modèles à

partir desquels des jeux de tests sont générés automatiquement. Ces jeux de tests sont ensuite exécutés automatiquement ou manuellement sur le système à tester. L'automatisation peut aussi porter sur la comparaison des résultats de tests et les résultats attendus.

3. Description détaillée

Dans le but de garantir, en plus de la sûreté de fonctionnement, la confiance et la robustesse des systèmes industriels face aux cyber-attaques, nous envisageons la définition d'une solution pour la génération automatique des tests d'intrusion. Pour cela, deux grands verrous sont à lever.
Le premier verrou porte sur la définition des différentes vulnérabilités des systèmes industriels. Malgré la présence de plusieurs classifications des vulnérabilités dans la littérature, celles-ci portent essentiellement sur les systèmes informatiques et les sites web. Une étude approfondie des systèmes industriels et des propositions de classification existantes (Bompard et al. 2012 ; Igure et al. 2006) permettra de proposer une classification des attaques et des vulnérabilités de ces systèmes.
Cette liste de vulnérabilités sera ensuite utilisée pour conduire des tests d'intrusion sur les systèmes industriels complexes. Le deuxième verrou porte alors sur l'automatisation de ces tests d'intrusion en adoptant une approche basée sur les modèles. Il sera alors nécessaire de modéliser formellement les vulnérabilités (objectifs de tests) (Mammar et al.2007) et aussi le système à tester. Enfin une approche permettant la génération automatique des jeux de tests à partir de ces modélisations sera proposée.

Résumé de la démarche envisagée :

- Etat de l'art et appropriation des travaux précédents
- Modélisation formelle des vulnérabilités
- Développement d'une solution pour la génération automatique des tests
- 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-06** à l'adresse suivante : **Soraya.KESRAOUI@segula.fr**

5. Références bibliographiques

Bompard, E., Cuccia, P., Masera, M. et Fovino, I. N. (2012). Cyber vulnerability in power systems operation and control. Lncs, 7130, 197 234.

Botella, J., Legeard, B., Peureux, F. et Vernotte, A. (2014). Risk-based vulnerability testing using security test patterns. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8803, 337 352. doi:10.1007/978-3-662-45231-8_24

Bouquet, F., Peureux, F. et Ambert, F. (2014). Model-Based Testing for Functional and Security Test Generation. Foundations of Security Analysis and Design VII, 8604, 1–33.

Dalalana Bertoglio, D. et Zorzo, A. F. (2017). Overview and open issues on penetration test. Journal of the Brazilian Computer Society, 23(1), 1 16. doi:10.1186/s13173-017-0051-1

Igure, V. M., Laughter, S. A. et Williams, R. D. (2006). Security issues in SCADA networks. Computers and Security, 25(7), 498 506. doi:10.1016/j.cose.2006.03.001

Javed, H., Mehmood Minhas, N., Abbas, A. et Muhammad Riaz, F. (2016). Model Based Testing for Web Applications: A Literature Survey Presented. Journal of Software, 11(5), 347 361. doi:10.17706/jsw.11.4.347-361

Lebeau, F., Legeard, B., Peureux, F., & Vernotte, A. (2013, March). Model-based vulnerability testing for web applications. In Software Testing, Verification and Validation Workshops (ICSTW), 2013 IEEE Sixth International Conference on (pp. 445-452). IEEE

Mammar, A., Cavalli, A., Oca, E. De, Ardi, S., Byers, D. et N. (2007). Modélisation et détection formelles de vulnérabilités logicielles par le test passif. Shields-Project.Eu, 215995(215995).

Stefinko, Y. Y. et Piskuzub, A. Z. (2017). Modeling penetration testing Building algorithm for pentesting expert system.

Stefinko, Y., Piskozub, A., & Banakh, R. (2016, February). Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. In Modern Problems of Radio Engineering. Telecommunications and Computer Science (TCSET), 2016 13th International Conference on (pp. 488-491). IEEE.

Qiu, X., Wang, S., Jia, Q., Xia, C., & Xia, Q. (2014, October). An automated method of penetration testing. In Computing, Communications and IT Applications Conference (ComComAp), 2014 IEEE (pp. 211-216). IEEE.

Zander-Nowicka, J. (2008). Model-based testing of real-time embedded systems in the automotive domain. Fraunhofer-IRB-Verlag.

Zulkernine, M., Raihan, M. F., & Uddin, M. G. (2009, September). Towards model-based automatic testing of attack scenarios. In International Conference on Computer Safety, Reliability, and Security (pp. 229-242). Springer, Berlin, Heidelberg.