Projet de recherche ANR ASTRID
Scénarios d'Attaque Contre Automates avec Distribution et Encapsulation (SACADE)

Stéphane Mocanu[1], Roland Groz[2], Marie-Laure Potet[3], Jean-Marc Thiriet[4]

Le projet SACADE fait partie de l'appel ANR ASTRID 2016. Il a démarré en mai 2017 et arrivera à sa fin en septembre 2019. Le projet est porté par Roland Groz (Laboratoire d'Informatique de Grenoble) dans un partenariat entre les laboratoires LIG, Verimag et Gipsa-lab.

Contexte et objectifs.
Les systèmes de contrôle des équipements industriels et des infrastructures d'importance vitale constituent un enjeu majeur pour la défense de la nation, et ont fait l'objet d'une attention particulière dans la loi de programmation militaire de décembre 2013. Les évènements majeurs de la dernière décade (dont Stuxnet, BlackEnergy, Industroyer, Triton parmi les plus connus) ont montré l'impact considérable des attaques sur les sites industriels et ont motivé le démarrage de plusieurs programmes de recherche.

Le projet SACADE vise la réalisation d'outils logiciels permettant de détecter automatiquement des vulnérabilités de systèmes de contrôles industriels (SCADA) face à des attaques jouant sur plusieurs niveaux de communication et exploitant les failles des logiciels embarqués. C'est un projet de recherche exploratoire compte tenu de l'état de l'art dans la détection automatique de vulnérabilités. Un volet important du projet concerne la réalisation d'un démonstrateur mettant en évidence de telles attaques multi-niveaux (TRL 3).

L'approche méthodologique est basée sur une modélisation cyber-physique : nous nous intéressons aux attaques cyber sur le système physique contrôlé qui ne violent pas les spécifications des protocoles de communication. L'approche est fortement inspirée par l'expérimentation : les attaques et les contremesures sont testées sur un démonstrateur composé d'équipements industriels de contrôle/commande réels.

Résultats.
Le financement demandé n'incluait pas de thèse, les moyens alloués étant dédiés au développement des démonstrateurs, bibliothèques d'attaque et implémentation des IDS. Les résultats méthodologiques se sont appuyés sur 3 thèses associées (Oualid Koucham – thèse DGA, Maxime Puys, Maëlle Kabir-Querrec – thèse CIFRE). Les livrables disponibles aujourd'hui incluent :

- une bibliothèque d'attaques basées sur les violations des ordres de commandes dans un système SCADA ainsi que le système de détection. Des jeux de données de capture de trafic ont été publiés sur la plateforme grenobloise PerSCIDO (https://persyval-platform.univ-grenoble-alpes.fr/DS236/detaildataset)
- une bibliothèque d'attaques spécialisée dans les attaques sur les protocoles multicast Ethernet de la pile CEI 61850
- un démonstrateur d'exploitation des failles des langages de programmation CEI 61131. Ce démonstrateur sera présenté au RESSI 2019.

Perspectives et retombées.
Au niveau méthodologique certains types d'attaque mis en évidence (usurpation du jeton ou d'esclave dans des réseaux à jeton, par exemple) feront l'objet de recherches dans le domaine de la détection. Une thèse sur la méthodologie de recherche des vulnérabilités dans les logiciels et systèmes d'exploitation embarqués démarrera à la rentrée 2019 motivée par les tests conduits sur les équipements de la plateforme. Le concept de l'approche méthodologie/démonstrateur a été repris dans les recherches des projets Cybersecurity Institute et IRT Pulse. Les perspectives pour la fin de projet concernent la publication de jeux de données supplémentaires contenant des caractéristiques détaillées des architectures, équipements et programmes des automates. Les démonstrateurs étant accessibles par VPN nous étudions aussi le montage des expérimentations à distance et d'éventuels couplages avec d'autres plates-formes.

U.G.A, CNRS, G-INP, [1] Inria, LIG, stephane.mocanu@imag.fr, [2] LIG, Roland.Groz@imag.fr, [2] Verimag, Marie-Laure.Potet@imag.fr, [3] G-INP, Gipsa-lab, jean-marc.thiriet@univ-grenoble-alpes.fr