**Appel à contributions**

**Soumission d'une présentation de projets de recherche collaboratifs pour RESSI 2019**

**Titre de la communication :** Les défis posés par la sécurisation de l'IoT industriel

**Présentateur :** Pierre-Henri Thevenon (CEA-Leti), Maxime Puys (CEA-Leti)

**Consortium :** Le consortium, du projet est constitué du CEA, experts en évaluation et sécurisation de de systèmes électroniques et de composants, et coordinateur de l'IRT Nanoelec[i], de l'Université Grenoble Alpes, experts dans le domaine du chiffrement et du génie logiciel, de Schneider Electrics, spécialiste mondial de la gestion de l'énergie et des automatismes et de ST-Microelectronics, fabricant de composants électroniques et de solutions pour la sécurité des objets connectés.

**Texte du résumé :**

La sécurisation de l'IoT industriel est désormais un enjeu comme le prouve plusieurs cyberattaques récentes. Pouvoir mettre en place des politiques de sécurité dans des infrastructures industrielles initialement non sécurisées nécessite de disposer de nouveaux outils de cybersécurité. Le projet lancé dans le cadre de l'IRT Nanoelec en 2018 a deux objectifs principaux. Le premier est le prototypage d'un dispositif électronique permettant de mettre en place des politiques de sécurité dans des systèmes industriels initialement non sécurisés. Le second objectif est de mettre en place un démonstrateur de système industriel afin de pouvoir conduire des tests de sécurité et des attaques sur ses sous-systèmes et valider des outils de cybersécurité sur des systèmes industriels.

Le dispositif électronique développé vise tout d'abord à rendre possible la mise en place d'un canal de communication sécurisé entre les sous-systèmes, à l'instar d'un VPN. Il permet ainsi d'analyser et de chiffrer les communications émises sur un bus de terrain tout en respectant les contraintes de latence imposées par le procédé physique opéré. Par ailleurs, il offre des capacités similaires à celles d'un module matériel de sécurité (HSM pour Hardware Security Module en Anglais) et permet de mettre en place des fonctions cryptographiques dans des dispositifs industriels n'embarquant pas de sécurité (ex : automates programmables « legacy »). Enfin, une interface spécialement dédiée, dite de commissioning facilitera le déploiement de ces dispositifs dans les architectures industrielles en permettant la mise à jour et la configuration des fonctions de sécurité. La maturité visée pour le prototype est celle d'un prototype industriel (TRL 4 à 6).

Lors du prototypage et dans la perspective d'un transfert, la sécurité intrinsèque du dispositif sera prise dans toutes les phases du cycle. Une analyse de risque, intégrant les exigences de sécurité énoncées par la norme IEC 62443, permettra d'atteindre un haut niveau de sécurité dans un environnement industriel. Un banc de test incluant des outils d'intégration continue permettra de réaliser aussi bien des tests de sécurité que de robustesse.

Le second objectif du projet est le développement d'une plateforme de sensibilisation et de tests sécuritaires. Cette plateforme sera représentative d'un système industriel réel et intègrera dans un même espace plusieurs dispositifs industriels de contrôle-commande typiques des installations des OIV. Plusieurs procédés physiques seront simulés et projetés en fonction des entrées et sorties des automates. Enfin, des scénarios d'attaques seront développés et pourront être déroulés afin de sensibiliser les acteurs industriels à la sécurité de leurs systèmes. La plateforme permettra de valider l'ensemble des fonctions de sécurité du dispositif réalisé, dans un environnement opérationnel.

**Etat de l'art :** Plusieurs travaux sur le filtrage de communications industrielles existent. En 2011, Cox [Cox, 2011] modélise le système industriel comme un système linéaire et détecte les déviations de l'état normal afin de filtrer des communications MODBUS. Toujours en 2011, Cárdenas et al. [Cárdenas et al., 2011] proposent une méthodologie similaire qu'ils mettent en application sur la modélisation d'un réacteur. Dans ces deux travaux, le filtrage est donc effectué sur la base de l'observation du procédé et non sur les commandes échangées. En 2014, Chen et Abdelwahed [Chen and Abdelwahed, 2014] présentent un mécanisme de filtrage applicatif de communications MODBUS reposant également sur des systèmes linéaires. En conservant un historique des valeurs de variables ils estiment les valeurs futures par des classificateurs bayésiens et repèrent ainsi si l'état du système industriel va varier de façon anormale. Une réponse est alors prise de façon automatique ou proposée à l'opérateur basée sur différents critères (coût, efficacité, impact sur les performances). Enfin en 2017, Badrignans et al. [Badrignans et al., 2017] proposent dans le cadre du projet ARAMIS un dispositif de rupture de protocole intégrant des fonctions de filtrage applicatif sur les protocoles MODBUS et OPC-UA. Une des particularités du dispositif ARAMIS est son architecture, divisée en trois systèmes physiquement distincts afin de limiter la propagation des attaques.

**Positionnement par rapport à l'état de l'art et verrous :** Les travaux de Cox [Cox, 2011] et Cárdenas et al. [Cárdenas et al., 2011] se basent sur des relevés de l'état courant du système. Cela signifie que, dans leur cas, un message ne respectant pas la politique de sécurité ne sera détecté qu'une fois ses effets sur le système détectés. Par ailleurs, tous les travaux mentionnés se focalisent sur des protocoles basés sur TCP/IP. La solution que nous proposons vise la version RTU de MODBUS basée sur une communication série. Ce protocole est principalement déployé sur les bus terrains et permet de répondre aux contraintes temps-réel imposées aux bus industriels en relations avec les actionneurs/capteurs du procédé physique. Ainsi, les principaux verrous du projet sont le développement d'une solution de sécurisation à faible coût, n'imposant pas de modifier le système industriel et permettant de respecter des contraintes de latence inférieures à 10 ms. Le respect de ces contraintes nécessite des choix d'optimisation à tous les niveaux (matériel, cryptographie, protocoles, etc). Enfin, la durée de vie d'un dispositif industriel impose une gestion de son cycle de vie (configuration initiale, mise à jour et fin de vie). Pour cela, une interface dédiée permettra aux différents utilisateurs de système (intégrateur de solutions, fournisseur, exploitant) d'opérer avec différent niveaux de permissions relatives à ses fonctions (gestion des logs, configuration du filtrage, provisionnement des clés cryptographiques, etc).

[i] Ce travail a été financé par le programme national français Programme d'Inverstissements d'Avenir, IRT Nanoelec ANR- 10-AIRT-05.