SUJET DE THESE G-SCOP 2017

Titre de la thèse : Etude de la porosité des contraintes physiques à des fins de construction de barrières contre les cyber-attaques d'une infrastructure de contrôle commande industrielle.

Directeur de thèse : Eric ZAMAI

Ecole doctorale : EEATS

Date de début (souhaitée) : septembre 2017

Financements envisagés – Contexte – Partenaires éventuels : demande une allocation de recherche de votre Ecole Doctorale

Description du sujet :

Contexte des travaux

Depuis ces trente dernières années, le souci principal des industriels s'est porté sur l'automatisation des procédés industriels afin d'améliorer sans cesse la performance de l'outil de production. Tirant parti des progrès technologiques dans le domaine de la communication, des automatismes industriels (interfaces ou services Web embarqués dans les automates programmables industriels) ou encore dans les domaines de l'électronique et de l'informatique (IOT, RFID, réseaux de capteurs, composants logiciels embarqués, PC…), ces systèmes automatisés intègrent aujourd'hui une part importante de technologies de l'information et de la communication distribuées au cœur même des processus de production et des produits. Ceci se concrétise aujourd'hui par le concept d'usine intelligente, flexible, l'industrie « 4.0 » ou smart-industry. Cette conception est au confluent de toutes les évolutions numériques, elle suppose une communication totale, aussi bien entre ses différents composants internes qu'avec l'extérieur. L'ouverture des infrastructures de contrôle commande industrielles (Industrial Control Systems (ICS)) vers l'extérieur est une évolution irréversible. Le concept d'Industrie 4.0 ne verra probablement pas son déploiement complet avant 2025 mais cette tendance de fond est à prendre en compte car elle augmente par la même la fragilité des ICS face aux actes de malveillance volontaires ou non.

Nous pouvons dire aujourd'hui que les ICS sont facilement accessibles (accès internet quasi systématique à toutes les couches du CIM, pas ou peu de protection sécurisé, etc …) à des logiciels malveillants qui chercheraient à en prendre le contrôle pour exécuter des actions dangereuses ou paralysantes pour les installations.

Dès 2010, nous avons pu assister à la première attaque exploitant de telles failles avec le virus STUXNET. Cette attaque, révélée au grand jour dans les médias, a fait prendre conscience des risques que courent les infrastructures vitales de nos pays, ainsi que l'intérêt de pouvoir mener de telles cyber-attaques sans exposer la vie des attaquants. D'autres ont fait suite, comme par exemple, Duqu, Flame, Gauss, Shamoon, ou encore le déraillement via Internet d'un tramway en Pologne en 2009, la cyber-attaque d'un réseau ferroviaire aux USA (2011), les

attaques répétées et continues de gazoducs aux USA (2012), la cyber-attaque de la centrale de Three Miles Island (2012).

Tous ces exemples s'appuient sur des ICS qui se révèlent être donc critiques pour la sécurité : leur défaillance peut entraîner un préjudice irréparable tant sur le plan de la partie physique que sur celui des hommes. Ces systèmes sont amenés à gérer des infrastructures critiques nationales, telles que les réseaux de distribution d'énergie électrique, du gaz, de l'eau, des eaux usées, des systèmes de transport, des centres médicaux, …. La perturbation de ces ICS peut ainsi avoir un impact significatif sur la santé et la sécurité de tous et également sur le plan économique (paralysie de grands sites industriels, …).

Problématique Scientifique

Au moins 2 axes de résistance à ces attaques doivent être développés, que ces attaques soient ciblées, correspondant à des « challenges » ou non ciblées.
Le premier de ces axes réside dans la sécurisation des échanges d'information au sein du système informatique de communication. Ici, des travaux tels que le cryptage sécurisé de l'information, le développement de nouveaux protocoles de communication sécurisés, ou la mise en place de pare feux industriels intelligents dédiés, sont autant de travaux à explorer et à maîtriser. Ce type d'approches doit intervenir en tant que première barrière aux attaques, à savoir interdire à un attaquant d'accéder à l'ICS via un média facilement accessible. De nombreux travaux sont d'ailleurs développés en ce sens et font également l'objet de la rédaction du guide blanc de la cyber-sécurité des systèmes industriels publié par l'ANSSI.

Cependant, si un logiciel malveillant réussi à franchir ce niveau de protection, ce qui n'est pas à exclure compte tenu de sa sensibilité aux erreurs humaines, l'ICS est entièrement accessible et donc vulnérable.

Aussi faut-il conforter cette première barrière de sécurité informatique et réseaux de communication par une autre, plus spécifique, et donc en profondeur, au cœur de métier du contrôle-commande ; un système de communication ne connait pas et ne dépend pas de la sémantique des informations qu'il véhicule, ce qui n'est absolument pas le cas de l'ICS ; une variable physique (une température de consigne, une vitesse de rotation, une information issue d'un capteur de vibration, …) présente un caractère qui a une résonnance particulière pour un spécialiste métier (hydraulique, électrique, aéroportuaire, fondeur, nucléaire, …), résonnance qui lui permet de déterminer si telle ou telle consigne est normale ou anormale ou encore si telle ou telle information issue du système de captage est également normale ou anormale.

C'est dans ce second axe que se place ce sujet de recherche afin de contribuer à la mise en place des mécanismes de détection et de filtrage bas niveau, entre les automates programmables industriels et l'instrumentation. Afin de mettre en place ce type de barrières, il s'agira d'étudier dans cette thèse les niveaux de **porosité des contraintes physiques afin de mettre en place des mécanismes de détection efficaces et minimisant les fausses alarmes.**

Contact : eric.zamai@grenoble-inp.fr