Classification des approches de détection d'intrusions dans les systèmes de contrôle industriels et axes d'amélioration

Oualid Koucham *[1], Guillaume Hiet[2], Stéphane Mocanu[1], Jean-Marc Thiriet[1] et Frédéric Majorczyk[3]

[1]GIPSA-Lab, Univ. Grenoble Alpes, Grenoble - France
[2]CIDRE/INRIA, CentraleSupélec, Cesson-Sévigné - France
[3]DGA/INRIA

1 Contexte

Les systèmes de contrôle industriels (ICS pour Industrial Control Systems) jouent un rôle primordial dans le contrôle et la supervision d'installations physiques. On les retrouve dans un nombre important de secteurs vitaux de l'économie tels que la génération et la distribution d'énergie (électrique, hydraulique, nucléaire, ...), le transport (aérien, ferroviaire, infrastructures routières, ...), l'industrie du gaz et du pétrole, mais aussi dans des applications de manufacture. À la lisière entre le monde physique et le monde numérique, ces systèmes s'avèrent être potentiellement dangereux pour l'environnement en cas de dysfonctionnement d'origine accidentelle ou malveillante.

L'histoire des systèmes industriels est celle d'une convergence croissante avec les systèmes informatiques classiques dits "de gestion". Sous la pression des enjeux économiques, ces systèmes initialement considérés comme isolés ont dû s'incorporer de plus en plus aux réseaux traditionnels de gestion. La migration vers des solutions TCP/IP et l'utilisation de plateformes standards (architecture, système d'exploitation,...) a significativement augmenté le risque d'attaques numériques sur des systèmes critiques manquant fondamentalement de dispositifs de sécurité et considérés initialement comme isolés des réseaux traditionnels de gestion. Il est donc impératif de développer des mécanismes de sécurité adéquats au contexte des systèmes industriels et ayant pour but d'éviter, de transférer ou de réduire les risques identifiés. Les travaux de cette thèse s'intéressent à l'un de ces mécanismes : la détection d'intrusions.

Il existe des particularités fondamentales qu'il convient de prendre en compte lorsqu'il s'agit de penser la sécurité au sein des systèmes industriels. Une simple transposition des démarches et mesures de sécurité propres aux systèmes classiques ne saurait être justifiée au vu de certaines divergences majeures. Ainsi, les systèmes de contrôle industriels ont des exigences fermes en termes de performances en temps réel et de déterminisme [7]. Les données aux niveaux les plus bas de ces systèmes doivent répondre à des contraintes strictes de durées de traitement et de temps de réponse afin de garantir les performances des boucles de contrôle. De plus, la nature des systèmes industriels, au contact du processus physique, exige une haute disponibilité. L'arrêt d'un système de contrôle industriel doit être prévu à l'avance au risque d'affecter la production. Les équipements embarqués ou temps réel tels que les automates sont munis d'une architecture matérielle dédiée et ajustée à leurs besoins compliquant l'implémentation de fonctions de sécurité du type chiffrement ou authentification. Toutes ces différences motivent la nécessité de travaux de détection d'intrusions tenant compte des spécificités de ces systèmes.

2 Classification des travaux existants

1 Les installations industrielles sont hétérogènes de par leur emplacement au confluent des systèmes numériques et du monde physique. De ce fait, les solutions de détection d'intrusions doivent faire face à des systèmes nécessitant plusieurs perspectives pour en garantir une couverture optimale. Afin de mieux saisir et appréhender l'état de l'art des approches de détection d'intrusions dans les ICS, on adoptera une classification qui reflète cette multiplicité de perspectives.

D'abord et au plus haut niveau, on distingue entre une vue orientée *communication* et une vue orientée *nœuds intelligents*. De ce point de vue abstrait, ces perspectives se retrouvent dans les systèmes

*Contact : oualid.koucham@gipsa-lab.grenoble-inp.fr

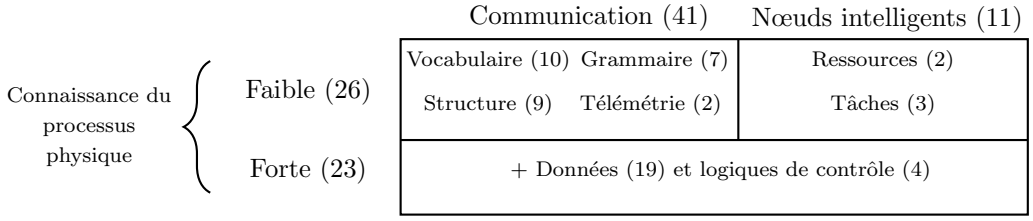

FIGURE 1 – Classification des approches de détection d'intrusions orientées ICS

informatiques classiques et correspondent par exemple à la traditionnelle distinction faite entre IDS (Intrusion Detection System) orientés réseau et IDS orientés hôte. Elles coïncident aussi respectivement à la *transmission* et au *traitement* des flux d'information parcourant le système. La vue orientée *communication* inclut les problématiques de *vocabulaire* [4] et de *grammaire* [9] des protocoles, de *structure* [4] (qui communique, avec qui, depuis quelle zone et vers quelle zone) des communications entre les entités ainsi que le profil *télémétrique* [13] du réseau (méta informations sur les données transmises dans le réseau tel que les données temporelles sur l'arrivée et la taille des paquets, ...). La vue orientée *nœuds intelligents* concerne les automates, superviseurs, capteurs/actionneurs intelligents et généralement toute entité du réseau exécutant des opérations de calcul. On s'attachera ici à des problématiques de *ressources* telles que la *mémoire* et le *calcul* mais aussi d'*ordonnancement*, d'*état* et d'*exécution* des *tâches* [18] pour les nœuds opérant en temps réel.

De façon orthogonale à cette première dimension *communication-noeuds intelligents*, on identifie une autre dimension relative au degré de connaissance ou de conscience qu'a l'IDS de l'interaction du système avec le processus physique. Cette dimension s'intéresse aux *logiques de contrôle* [3] utilisées par les contrôleurs afin de commander le processus. Ces logiques de contrôle peuvent être séquentielles (Grafcet, réseaux de Petri) mais aussi continues (fonctions de transferts, équations différentielles). Un autre aspect important concerne les *données de contrôle* [16] qui regroupent les données envoyées aux actionneurs et reçues des capteurs, les commandes reçues des superviseurs ou opérateurs, et les données échangées entre contrôleurs. L'observation de l'état du processus physique ne pouvant généralement pas se faire directement, ces *données de contrôle* représentent le moyen utilisé par les contrôleurs pour estimer cet état.

L'inconvénient principal d'une méthode à forte connaissance du processus physique réside dans le coût de développement de l'IDS. Une telle approche demande la convergence d'expertises issues de différents domaines (informatique, automatique, ...). Cependant, cette connaissance est cruciale pour une détection adaptée au contexte industriel. Les approches classiques ne sont pas suffisantes pour détecter des attaques ciblées. Par exemple, les systèmes industriels sont sujets à des attaques de type injection de commandes, de réponses ou de données. L'attaquant est capable de forger de fausses commandes ou mesures afin de mener le processus physique vers un état critique [8]. Une connaissance du processus est indispensable afin de comprendre la portée des commandes ou mesures injectées. D'autres attaques de type usure ou résonance présentent des difficultés analogues [10].

La figure 1 schématise la classification et donne quelques indications quantitatives sur la répartition des approches. Au total, 49 références ont été analysé. À noter que plusieurs approches s'intéressent à plus d'une vue du système (par exemple communication et nœuds intelligents [17]).

Une caractéristique majeure des travaux autour de la détection d'intrusions dans les ICS est la prépondérance des approches comportementales par rapport aux approches par signatures (voir [5] pour une taxonomie classique des IDS). Ainsi, l'écrasante majorité des travaux justifie la pertinence d'une approche comportementale par la régularité et la stabilité des systèmes industriels. Parmi les caractéristiques invoquées on trouve la topologie statique des systèmes [4], le trafic régulier et fortement périodique [16, 9] ou encore la simplicité des protocoles [4].

L'approche comportementale de la détection d'intrusions, de loin la plus répandue parmi les travaux orientés systèmes industriels, souffre d'un nombre de déficiences déjà identifiées dans les systèmes d'information traditionnels. On constate entre autres [14] : (i) le coût prohibitif des erreurs notamment en termes de faux positifs, (ii) l'inadéquation voir l'absence de données d'apprentissage, (iii) la faible interprétation sémantique des résultats de façon à être utile pour l'administrateur et (iv) la variabilité

des données sur lesquelles se base la détection. Or si l'on peut en effet constater une certaine régularité relative, le reste des faiblesses identifiées peut en réalité être exacerbé par le contexte particulier de tels systèmes. Le coût des erreurs en termes de faux positifs et de faux négatifs est accru du fait de l'interaction avec des processus physiques critiques alors que la faible interprétation sémantique des résultats ne permet pas à l'opérateur de comprendre, de contextualiser ou d'affecter des priorités aux alertes ce qui complique toute prise de décision. De plus, et au vu du caractère sensible des systèmes industriels, l'obtention de données réelles permettant de tester les solutions de façon adéquate est beaucoup plus difficile. Force est donc de constater qu'une approche comportementale pouvant apparaitre séduisante dans un premier temps s'avère être plus délicate à mettre en place.

3 Orientations des travaux de thèse

Les travaux de cette thèse se placent dans le contexte particulier de la détection d'intrusions dans les systèmes de contrôle industriels et visent à pallier certaines des déficiences identifiées précédemment. Nous nous intéressons à l'exploitation des logiques de contrôles utilisées pour commander les processus physiques afin d'améliorer la détection d'intrusions ainsi que la corrélation d'alertes. Les systèmes industriels se caractérisent par une dualité entre un comportement séquentiel et un comportement continu. Si ce dernier a fait l'objet de plusieurs travaux notamment autour du développement d'estimateurs d'états robustes [12], le comportement séquentiel reste jusqu'à présent largement inexploré.

Les spécifications à la base du développement des logiques séquentielles peuvent être exprimées à l'aide de formules de logique temporelle, ouvrant la possibilité de développer des moniteurs surveillant toute transgression des spécifications [11]. Cependant, l'écriture de ces spécifications reste un exercice difficile. Nous nous intéressons donc à des méthodes d'inférence automatique ou semi-automatique de spécifications exprimées en logique temporelle. Aussi, l'inférence s'appuie sur des motifs de spécifications (*specification patterns* [6]) incluant les cas les plus courants tout en facilitant la compréhension des motifs inférés. De plus, certains états du système peuvent être associés à des échanges entre automates permettant ainsi de mieux comprendre certains flux horizontaux aléatoires au sein de la zone de contrôle. Nos travaux s'attachent à examiner l'apport conjugué du contexte dans lequel évolue les sondes de détection ainsi que du comportement séquentiel visible au niveau des automates dans l'amélioration des performances de la détection d'intrusion.

Au sein des systèmes informatiques classiques, la corrélation d'alertes est perçue comme une voie possible d'atténuation des erreurs de détection, de contextualisation des alertes et d'identification d'attaques [15]. Les recherches concernant la corrélation au sein des systèmes industriels sont cependant rares et limitées [2]. Aussi, nos travaux visent à proposer des solutions de corrélation en s'appuyant notamment sur une représentation formelle du système industriel au travers de formalismes logiques tels que les logiques de description [1] dont le compromis expressivité/décidabilité est soigneusement étudié et adapté au développement d'ontologies. Cette représentation formelle a pour objet d'inclure entre autres des données de topologie, de cartographie, de vulnérabilités, d'attaques, ainsi que des informations sur les sondes déployées au sein du système industriel. Le but est de contextualiser les alertes reçues, et de raisonner sur la configuration du système au travers de services d'inférences. Les sources des alertes couvrent les IDS des différentes catégories évoquées en section 2, mais aussi les moniteurs de spécifications issus du processus d'inférence.

Références

[1] Franz Baader, Diego Calvanese, Deborah L. McGuinness, Daniele Nardi, and Peter F. Patel-Schneider, editors. *The Description Logic Handbook : Theory, Implementation, and Applications*. Cambridge University Press, 2003.

[2] Linda Briesemeister, Steven Cheung, Ulf Lindqvist, and Alfonso Valdes. Detection, correlation, and visualization of attacks against critical infrastructure systems. In *Eighth Annual International Conference on Privacy Security and Trust (PST), 2010*, pages 15–22, 2010.

[3] Alvaro a. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks Against Process Control Systems : Risk Assessment, Detection, and Response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11)*, pages 355–366, 2011.

[4] Steven Cheung and Keith Skinner. Using Model-based Intrusion Detection for SCADA Networks. In *Proceedings of the SCADA Security Scientific Symposium*, pages 127–134, 2007.

[5] Hervé Debar, Marc Dacier, and Andreas Wespi. A revised taxonomy for intrusion-detection systems. *Annales Des Télécommunications*, 55(7-8) :361–378, 2000.

[6] Matthew B. Dwyer, George S. Avrunin, and James C. Corbett. Property specification patterns for finite-state verification. In *Proceedings of the Second Workshop on Formal Methods in Software Practice*, FMSP '98, pages 7–15, New York, NY, USA, 1998. ACM.

[7] Brendan Galloway and Gerhard P. Hancke. Introduction to Industrial Control Networks. *IEEE Communications Surveys & Tutorials*, 2013.

[8] Wei Gao, Thomas Morris, Bradley Reaves, and Drew Richey. On SCADA control system command and response injection and intrusion detection. In *eCrime Researchers Summit (eCrime) 2010*, pages 1–9, 2010.

[9] Niv Goldenberg and Avishai Wool. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, 6(2) :63–75, 2013.

[10] Jason Larsen. Breakage. Black Hat Federal, 2008.

[11] Martin Leucker and Christian Schallhart. A brief account of runtime verification. *Journal of Logic and Algebraic Programming*, 78(5) :293–303, may/june 2009.

[12] Kebina Manandhar, Xiaojun Cao, Fei Hu, and Yao Liu. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE Transactions on Control Of Network Systems*, 1(4) :370–379, 2014.

[13] Stanislav Ponomarev and Travis Atkison. Industrial Control System Network Intrusion Detection by Telemetry Analysis. *IEEE Transactions on Dependable and Secure Computing*, PP(99), 2015.

[14] Robin Sommer and Vern Paxson. Outside the closed world : On using machine learning for network intrusion detection. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 305–316, May 2010.

[15] Eric Totel, Bernard Vivinis, and Ludovic Mé. A language driven intrusion detection system for event and alert correlation. In *Security and Protection in Information Processing Systems*, volume 147 of *IFIP*, pages 209–224. Springer US, 2004.

[16] Man-ki Yoon and Gabriela F Ciocarlie. Communication Pattern Monitoring : Improving the Utility of Anomaly Detection for Industrial Control Systems. In *NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, 2014.

[17] Chunjie Zhou, Shuang Huang, Naixue Xiong, Shuang-hua Yang, Huiyun Li, Yuanqing Qin, and Xuan Li. Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. *IEEE Transactions on Systems, Man, and Cybernetics : Systems*, 45(10) :1345–1360, 2015.

[18] Christopher Zimmer, Balasubramany Bhat, Frank Mueller, and Sibin Mohan. Time-based intrusion detection in cyber-physical systems. In *Proc. of the First ACM/IEEE International Conference on Cyber-Physical Systems*, pages 109–118, 2010.