Revue des systèmes de détection d'anomalies dans les réseaux SCADA et attaques internes

Raogo Kabore, Yvon Kermarrec, Philippe Lenca

Revue des systèmes de détection d'anomalies dans les réseaux SCADA et attaques internes

Raogo KABORE [1,2], Yvon KERMARREC [1], Philippe LENCA [1]

1. IMT Atlantique – Lab-STICC UMR CNRS 6285 – UBL
Technopole Brest Iroise
F-29238 Brest cedex
{raogo.kabore, yvon.kermarrec, philippe.lenca}@imt-atlantique.fr

2. ESATIC - DRIT
18 BP 1501 Abidjan 18, Côte d'Ivoire

RÉSUMÉ. Pour des raisons de coûts et de commodité d'administration, les systèmes SCADA, utilisés pour la gestion des infrastructures industrielles et des infrastructures critiques en particuliers ont adopté des protocoles, matériels et logiciels standards et ont surtout été interconnectés aux réseaux d'entreprises ainsi qu'à Internet. Ces changements exposent les réseaux SCADA aux mêmes menaces que l'informatique traditionnelle notamment les cyber-attaques. Le présent travail fait une revue des travaux de recherche pour sécuriser ces systèmes contre les menaces internes ainsi que celles pour développer des systèmes de détection d'anomalies spécifiques aux réseaux SCADA.

ABSTRACT. For costs reasons and administrative convenience, SCADA systems, used for the management of industrial and critical infrastructures in particular, have adopted standard protocols, hardware and software, and have mainly been interconnected to enterprise networks and to the Internet. These changes expose SCADA networks to the same attacks as those faced by traditional IT systems, including cyberattacks. This paper reviews the research efforts to secure these systems against insider threats as well as to develop SCADA-specific anomaly detection systems.

MOTS-CLÉS : Détection d'anomalies, SCADA, IDS, intrusion, ICS, systèmes de contrôle industriels.

KEYWORDS: Anomaly detection, SCADA, IDS, intrusion, ICS, Industrial Control Systems

1. Introduction

Les systèmes SCADA (Supervisory Control and Data Acquisition) permettent le contrôle et la surveillance des systèmes tels que les systèmes de distribution d'eau, les systèmes de traitement des eaux usées, les systèmes de transmission et de distribution de l'énergie électrique, les pipelines de pétrole et de gaz, les systèmes de transport public, etc. Ces systèmes collectent les informations des sites distants, les transfèrent sur un ordinateur central, et une Interface Homme-Machine (IHM) permet aux opérateurs de surveiller et contrôler le système tout entier à partir d'un point central (Stouffer et al. 2011, Kolski 1997).

Cette intégration des systèmes SCADA à la gestion des systèmes industriels permet de gagner en performance et de réduire les coûts d'exploitation (Boyer, 2009), mais elle expose du même coup ces systèmes aux attaques dont est victime l'informatique traditionnelle. Les conséquences d'une attaque sur ces systèmes peuvent être des pertes de production, des pertes financières, des désastres environnementaux et dans le pire des cas, des pertes en vies humaines (Valdes et Cheung, 2009, Zhu et al. 2011). Les réseaux SCADA ont déjà été la cible d'attaques telles que celle de Maroochy Water System en Australie (Slay et Miller., 2007), la centrale nucléaire de Davis-Besse dans l'Ohio aux Etats Unis, Duqu, Flame (Miller et Rowe, 2012.), Stuxnet (Falliere et al., 2011), les centrales électriques en Ukraine (Lee et al., 2016) et de Vermont aux USA (Perez, 2017).

Les systèmes SCADA sont différents de l'informatique traditionnelle par la spécificité des protocoles utilisés, la nature déterministe des communications, la difficulté d'application des patchs. Ces systèmes ont aussi un nombre élevé de matériels obsolètes en leur sein, exigent d'une disponibilité temps-réel, ont des composants ayant une capacité de traitement limité, et enfin, ont une topologie relativement statique (Cardena et al., 2011, Zhu et Sastry. 2010).

Nous exposons dans cet article quelques cas d'attaques internes des systèmes SCADA et les mesures pour y faire face, et nous faisons une revue des systèmes de de détection d'anomalies spécifiques aux réseaux SCADA.

Dans la section 2 nous décrivons des attaques de systèmes SCADA orchestrées par des personnes internes et des approches pour y remédier, la section 3 est consacrée à une revue des systèmes de détection d'anomalies SCADA et nous procédons à une conclusion dans la section 4.

2. Attaques internes sur les systèmes SCADA

Le cas le plus emblématique parmi les attaques internes des systèmes SCADA reste celle perpétrée contre le système de traitement des eaux usées de Maroochy à Queensland en Australie en 2000, par un contractuel mécontent parce qu'il n'avait pas réussi à se faire embaucher dans l'entreprise (Slay et Miller, 2007). Au moyen d'un ordinateur portable et d'un émetteur radio, l'attaquant a pris le contrôle de 150 stations de pompage des eaux usées et provoquer le déversement de millions de

litres d'eaux usées non traitées dans l'environnement qui a provoqué une pollution majeure.

Leall (2009) quant à lui relate l'attaque faite par un agent de sécurité nocturne sur un système de contrôle de chauffage et de ventilation dans un hôpital de Dallas, au Texas. Il propose que des mesures soient prises pour assurer la sécurité physique des systèmes SCADA par des contrôles d'accès physique et la mise en place de mécanismes de traçabilité de l'accès aux salles qui seront à la fois dissuasives et utiles en cas d'investigation.

Ce qui précède tend à renforcer la théorie de l'homme étant le maillon le plus faible de la sécurité informatique. Ceci est prouvé une fois de plus par une équipe d'experts en sécurité qui a utilisé l'ingénierie sociale pour manipuler les employés et prendre le contrôle total du réseau SCADA d'une entreprise d'énergie électrique en l'espace de quelques heures (Greene, 2008). La cause principale de cette attaque est le passage des systèmes SCADA d'environnements fermés à des systèmes ouverts, interconnectés à Internet et aux intranets des entreprises. L'utilisation de logiciels et matériels standards et la réticence des entreprises à appliquer des patchs perpétuent ces faiblesses. Greene recommande l'utilisation de logiciels spécifiques SCADA, mieux testés et qui permettent une correction rapide, sans oublier la segmentation des réseaux.

Enfin, Nicholson et al. (2007) préconisent à l'attention des organisations industrielles, la conception et la mise en œuvre de politiques, de procédures et de protocoles de sécurité (PPP) qui permettent de prévenir les attaques internes.

3. Revue des systèmes de détection d'anomalies dans les systèmes SCADA

Pour contrecarrer les attaques internes dont l'impact est souvent important et le taux de succès élevé, Nasr et Varjani (2014) proposent une méthode de détection d'anomalie statistique (SADM), basée sur les techniques de moyenne et d'écart-type appliquées au nombre d' «alarmes non-résolues» sur l'écran de l'opérateur. Ce nombre symbolise le comportement de l'opérateur.

Kiss et al (2014) ont élaboré une approche pour détecter les attaques cyber-physiques en appliquant des techniques de clustering sur les données des processus industriels. La technique utilisée combine un algorithme k-means et le clustering soustractif. L'architecture de leur système utilise une infrastructure Big Data Hadoop avec le framework Mapreduce pour traiter les grandes séries chronologiques issues de plusieurs capteurs.

Pour la détection d'anomalie dans les systèmes de contrôle de processus, Valdès et Cheung (2009) proposent une architecture multicouche et de corrélation. Le système proposé surveille les événements du système à plusieurs niveaux (périphérique, réseau et hôtes) et met en corrélation les événements à plusieurs niveaux (centre de contrôle, fournisseur et secteur). Le système effectue une détection basée sur le modèle, en exploitant la régularité et la prévisibilité des modèles de communication des systèmes de contrôle de processus. L'architecture

utilise également un framework de gestion des incidents de sécurité hiérarchique pour corréler les alertes des IDS et les événements potentiellement anormaux générés par le système de contrôle de processus. La solution intègre un outil de visualisation pour aider les analystes humains à mieux comprendre les anomalies du trafic réseau et éviter que le périmètre de défense ne soit violé ou contourné.

Barbosa et al. (2012) s'appuient sur le caractère périodique et régulier du trafic dans les systèmes SCADA, pour proposer une approche de détection d'anomalies. La périodicité du trafic est caractérisée par la fréquence et la taille en nombre de paquets des émissions périodiques du trafic. Le système comporte quatre modules : un analyseur de trafic qui filtre le trafic non pertinent, un générateur de flux réseau qui regroupe les paquets de façon significative en utilisant le port transport côté serveur, un module d'apprentissage de périodicité qui apprend le comportement normal du système en extrayant les deux éléments qui caractérisent la rafale périodique, c'est-à-dire la période et la taille, et enfin, un moteur de détection. Malheureusement, l'approche est manuelle et donc non déployable.

Pour détecter les attaques injectant les fausses données dans les systèmes de contrôle, Wang et al. (2014) proposent une approche basée sur la relation des états. L'approche proposée est un système en temps réel qui surveille les états du système, détecte des états incohérents et déduit les origines des attaques. Au moyen du graphe de relation entre les variables, quand un état anormal est détecté, l'on peut remonter la chaîne des dépendances du ou des variables en cause et déduire la possible origine de l'attaque. L'architecture du système comporte trois parties : un module d'analyse de composants qui analyse automatiquement les variables du système pour extraire des composants et générer un graphe décrivant les états du système valide ainsi qu'un autre graphe de relations entre les variables. Ici, des vecteurs d'alternance qui enregistrent les relations d'alternance entre deux états continus sont aussi utilisés pour représenter les états en temps réel d'un composant en fonctionnement normal. Le deuxième module est un module de détection qui utilise le graphe d'états pour générer une alerte d'état non valide si un nouveau vecteur d'alternance n'est pas trouvé dans le graphe des états ou une alerte de transition invalide si l'état actuel n'a pas pu être atteint en partant d'un état précédent. Enfin, un module d'inférence d'origine aide à localiser l'origine de ou des attaques par injection de fausses données. L'évaluation du système par Wang et al. donne un taux de détection de 95,83% et un taux de faux positifs de (0,0125%).

Un appareil utilisant une approche de détection d'intrusion multi-algorithmes pour le protocole Modbus TCP a été développé par Cheung et al. (2007). Cette approche est basée sur un modèle de niveau de protocole, un modèle de patterns de communication attendus et un modèle de détection de serveur et de services. Le modèle de niveau de protocole utilise les codes de fonction, les codes d'exception, l'implémentation de règles basées sur Snort ainsi que le langage PVS pour spécifier formellement un périphérique Modbus spécifique. Dans le modèle de patterns de communication prévus, les modèles de communication entre les différents composants du réseau SCADA sont créés, et des règles basées sur Snort sont développées pour détecter les écarts par rapport à ces modèles. Notons qu'ici, les règles Snort sont écrites pour détecter le "complément" des modèles symbolisant le

fonctionnement normal. Le dernier composant qui s'appuie sur l'apprentissage pour détecter les changements dans la disponibilité du serveur ou du service est constitué de deux détecteurs qui sont un capteur EMERALD Bayes et EModbus. Les expériences montrent que l'approche de détection d'intrusion basée sur un modèle est efficace pour surveiller les réseaux SCADA et qu'elle est complémentaire à l'approche basée sur la signature.

4. Conclusion

Les systèmes SCADA permettent la surveillance et le contrôle d'installations industrielles en général et des infrastructures critiques en particulier. Les menaces qui pèsent sur ces systèmes peuvent être externes ou internes. Pour faire face à ces derniers cas, il est impératif de mettre en place des mesures de surveillance des salles de contrôle, de bien segmenter les réseaux, d'élaborer et implémenter des politiques et procédures de sécurité au sein des organisations. En plus des recommandations organisationnelles et techniques données par ANSSI (2012), les systèmes de détection d'anomalies spécifiques aux systèmes SCADA permettent de renforcer leur protection. En somme, nous pouvons dire comme Slay et Miller (2007), que «seule la combinaison de solutions technologiques et de meilleures pratiques humaines peut offrir la garantie de systèmes SCADA sécurisés et fiables».

Bibliographie

Axelsson S. (2000). Intrusion detection systems: A survey and taxonomy, *Technical report,* Vol 99.

ANSSI (2012). Maîtriser les SSI pour les systèmes industriels, *ANSSI*, 2012

Barbosa R. R. R., Sadre R., Pras A. (2012). Towards periodicity based anomaly detection in SCADA networks. *In Emerging Technologies & Factory Automation (ETFA), 2012 IEEE 17th Conference*, p. 1-4.

Boyer, S. A. (2009). SCADA: supervisory control and data acquisition. International *Society of Automation*. USA, 2009.

Cárdenas A. A., Amin S., Lin Z. S., Huang Y. L., Huang C. Y., Sastry S. (2011). Attacks against process control systems: risk assessment, detection, and response. *Proceedings of the 6th ACM symposium on information, computer and communications securit*y, p. 355-366.

Cheung S., Dutertre B., Fong M., Lindqvist U., Skinner K., Valdes, A. (2007). Using model-based intrusion detection for SCADA networks, *Proceedings of the SCADA security scientific symposium,* Vol. 46, p. 1-12.

Falliere N., Murchu L. O., Chien E., W32 (2011), Stuxnet dossier *White paper, Symantec Corp., Security Response 5* , p. 6.

Garitano I., Uribeetxeberria R., Zurutuza U. (2011). A review of SCADA anomaly detection systems, *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*, p. 357-366, Springer Berlin Heidelberg.

Greene T. (2008). *Experts hack power grid in no time*. http://www.networkworld.com/article/2277908/lan-wan/experts-hack-power-grid-in-no-time.html.

Igure V. M., Laughter S. A., Williams R. D., (2006), Security issues in SCADA networks, *Computers & Security*, vol. 25, n° 7, p. 498–506.

Kalapatapu R. (2004). SCADA protocols and communication trends. *ISA2004* 5-7 October 2004, Houston, Texas.

Kiss I., Genge B., Haller P., Sebestyén G. (2014). Data clustering-based anomaly detection in industrial control systems, *Intelligent Computer Communication and Processing (ICCP), 2014 IEEE International Conference*, p. 275-281.

Kolski C. (1997). *Interfaces Homme-machine : application aux systèmes industriels complexes*, Hermès, Paris.

Leall N. (2009). *Lessons from an insider attack on SCADA systems*. https://blogs.cisco.com/security/lessons_from_an_insider_attack_on_scada_systems.

Lee R. M.; Assante M. J., Conway T. (2016) Analysis of the cyber-attack on the Ukrainian power grid. *SANS Industrial Control Systems*, 2016.

Miller B., Rowe D. (2012). A survey SCADA of and critical infrastructure incidents. *Proceedings of the 1st Annual conference on Research in information technology*, New York, ACM, p. 51-56.

Nasr P. M., Varjani A. Y. (2014). Alarm based anomaly detection of insider attacks in SCADA system. *Smart Grid Conference (SGC)*. Tehran, IEEE, p. 1-6.

Nicholson A., Webber S., Dyer S., Patel T., Janicke H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, Vol 31 n° 4, p. 418-436.

Perez E. (2017) *Vermont utility finds alleged Russian malware on computer*, http://edition.cnn.com/2016/12/30/us/grizzly-steppe-malware-burlington-electric/.

Slay J., Miller M. (2007) Lessons learned from the maroochy water breach, *International Conference on Critical Infrastructure Protection,* Boston*,* Springer, p. 73–82.

Stouffer K., Falco J., Scarfone K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication, 800(82)*, p. 16-16.

Valdes A., Cheung, S. (2009). Intrusion monitoring in process control systems. *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference.* Waikoloa, *IEEE*, p. 1-7.

Wang Y., Xu Z., Zhang J., Xu L., Wang H., Gu G. (2014). Srid: State relation based intrusion detection for false data injection attacks in SCADA. *European Symposium on Research in Computer Security*, *2014*, Wroclaw, Springer International Publishing, p. 401-418.

Zhu B., Joseph A., Sastry S. (2011). A taxonomy of cyberattacks on SCADA systems. *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing,* Dalian, IEEE, p. 380-388.

Zhu B., Sastry S. (2010). SCADA-specific intrusion detection/prevention systems: a survey and taxonomy. *Proceedings of the 1st Workshop on Secure Control Systems (SCS)*, 2010, Stockholm, Vol. 11.