Survivre à l'internet des objets : le monde physique à la rescousse

Etienne Helluy-Lafont
Univ. Lille, CNRS, IRCICA, Centrale Lille, UMR 9189 - CRIStAL
Centre de Recherche en Informatique Signal et Automatique de Lille, F-59000 Lille, France
Email: etienne.helluy-lafont@univ-lille1.fr

***Abstract*—Les objets connectés sont de plus en plus nombreux et variés. Les méthodes classiques de sécurité sont souvent trop intrusives pour être mises en œuvre dans ces systèmes. Nous souhaitons développer des capacités de détection d'intrusion et de comportement anormaux efficaces dans ce contexte. Nous avons donc besoin d'indicateurs qui puissent être exploités sur le plus grand nombre d'objets. Une piste est de tirer partie de la matérialité des objets connectés, et d'observer leurs manifestations physiques. Dans cet article, nous présentons le résultat d'un travail bibliographique au cours duquel nous avons recensé les techniques de détection d'intrusion qui interviennent aux frontières des domaines cyber et physique.**

I. Introduction

Les objets connectés sont de plus en plus nombreux et peuvent être des cibles et des vecteurs d'attaques, comme on l'a vu récemment avec le botnet Mirai [KKSV17]. Le terme d'objets connectés regroupe une grande variété de systèmes. Dans ce contexte, la détection d'intrusion fait face à plusieurs défis : les systèmes sont hétérogènes ; il utilisent des moyens de communication variés ; dans beaucoup de cas les plateformes d'exécution sont fermées, il n'est pas possible d'y ajouter de logiciel. Il semble donc peu réaliste que l'on puisse faire face aux menaces qui pèsent sur l'IoT en leur adjoignant simplement des IDS et antivirus initialement développés pour les ordinateurs. Les objets connectés étant globalement des boîtes noires, la seule solution de sécurité disponible pour l'utilisateur reste l'utilisation de dispositifs externes, comme des systèmes de détection d'intrusion (IDS) ou des pare-feux.

Le premier composant d'un IDS est la *collecte* d'informations. Ces informations proviennent de divers indicateurs, par exemple un antivirus pourra surveiller les fichiers téléchargés sur le réseau, la liste des processus en cours d'exécution, des séquences d'appels systèmes.

Certains auteurs proposent de baser des IDS sur indicateurs physiques (IPH), plutôt que sur des indicateurs "cyber" (ou "logiques") habituellement utilisé dans les systèmes d'information classiques [YHK+15], [CWF17]. Ainsi plutôt que de rechercher les traces informatiques d'une intrusion en cours, ces techniques vont directement s'attacher à surveiller des caractéristiques physiques de la machine ciblée pour vérifier qu'elle se comporte bien comme prévu. Pour le dire autrement, on peut distinguer les indicateurs basés sur les canaux primaires de ceux utilisant des canaux auxiliaires.

Ce type d'indicateurs pourrait présenter des avantages pour un IDS sur l'IoT : comme l'objet n'est observé que d'un point de vue extérieur, il n'est donc pas nécessaire de savoir précisément comment il fonctionne, ni d'interférer avec.

Le domaine de la fabrication additive fournit un bon exemple d'IPH : ces systèmes pourraient être ciblés par des tentatives de sabotage, visant à introduire à divers niveaux des défauts dans la pièce en cours d'impression. Il est possible d'exploiter des canaux auxiliaires comme les vibrations acoustiques [CCAF16], [BSY+17] ou la consommation énergétique [MGB+17] pour observer le comportement de l'imprimante 3D et vérifier la conformité de la pièce imprimée.

Cet article présente le résultat d'un travail bibliographique dans lequel nous avons cherché à recenser les indicateurs à notre disposition. Plusieurs domaines manipulent et analysent des IPH, et nous avons donc également élargi nos recherches aux travaux qui d'une manière plus générale traitent de détection d'anomalies sur des grandeurs physiques.

Dans la section II, nous proposons une classification des indicateurs disponibles, en tenant compte du domaine qu'ils observent et des systèmes auxquels ils s'appliquent. Dans la section III, nous en présentons une courte analyse. La section IV conclut cet article et présente nos travaux futurs.

II. Classification

A. Description

Nous avons besoin d'une grille de lecture pour classifier les méthodes identifiées. Il existe des travaux sur la sécurité "interdomaine", qui s'intéressent aux problématiques de sécurité survenant à la croisée des domaines "cyber" et "physiques". [NT11] propose une taxonomie des attaques interdomaines dans les *smart-grids*. Ils trient les attaques en fonction du domaine dont elles proviennent et du domaine qu'elles affectent. Par exemple, une attaque cyber-physique - menée depuis le domaine cyber pour provoquer des dommages physiques, sera différente d'une attaque physique-cyber - qui utilise des moyens physiques pour affecter le fonctionnement d'un système informatique.

De la même manière, nous proposons de classer les méthodes de détection selon la situation de l'observateur et le type d'effets qu'il cherche à détecter. Ainsi on peut envisager d'observer des comportements physiques pour détecter des anomalies dans du logiciel : on parlera d'indicateur physique-cyber ; ou d'observer des traces informatiques pour prédir des dommages physiques : on parlera d'indicateur cyber-physique.

B. Cyber-Cyber

Cette catégorie comprend les techniques utilisant des indicateurs cyber pour surveiller des systèmes purement informatiques. Cela représente la majorité de la littérature sur les systèmes de détection d'intrusion. Il est donc difficile d'en donner une image complète dans ce paragraphe. On y trouve les IDS réseau (NIDS), basés sur l'hôte (HIDS), ou encore sur le moniteur de machines virtuelles (VMM Based). Ils peuvent agir par reconnaissance de motifs, comme Snort [R99] sur le réseau, ou ClamAV [LRLT12] sur l'hôte, ou utiliser des analyses comportementale ou statistique, comme Bro [PAX99].

C. Physique-Physique

On y retrouve les systèmes de détection de sabotage sur les imprimantes 3D, qui peuvent utiliser le son [CCAF16], [BSY+17], ou la consommation énergétique [MGB+17] pour détecter une altération de la pièce imprimée.

[VLG15] compare les performances d'un IDS utilisant des entrées cyber uniquement ou cyber+physiques pour détecter des attaques sur un robot. Dans des travaux ultérieurs sur la même plateforme, [BLGA17] montre que l'exploitation d'indicateurs cyber et physiques est seule à même d'identifier des attaques provenant des deux domaines.

Un autre domaine qui utilise des IPH pour surveiller des systèmes physiques est celui du *prognostics & health management* (PHM). Les techniques de PHM servent à estimer le niveau d'usure des équipements, typiquement dans les installations industrielles, en analysant des données physiques comme les vibrations acoustiques [GZC+14], [JGZ17]. Ces méthodes n'ont pas un objectif de sécurité mais plutôt de sûreté, et n'incluent pas de modèle de menace. Nous nous y intéressons donc plus pour leur capacité à collecter et traiter des informations physiques sur le fonctionnement d'une installation.

D. Physique-Cyber

[KSS08] utilise l'analyse de consommation énergétique pour créer une base de signature de malwares, et détecter des menaces connues et inconnues sur un appareil Windows mobile. [CRR+13] propose WattsUpDoc qui utilise une approche similaire pour détecter des malwares dans des équipements de santé en analysant leur consommation électrique. Ses auteurs notent que cette technique est mieux adaptée à des systèmes embarqués, plus faciles à modéliser.

D'autres ont cherché à adapter ces méthodes sur des téléphones mobiles pour détecter des attaques ou des malwares [HNH13], [MMF14], [CGL+16]. Ils proposent surtout des techniques logicielles pour récupérer des indicateurs de consommation énergétique et créer des profils précis de consommation tenant compte du comportement de l'utilisateur et autres paramètres externes.

Un autre champ de la recherche s'intéresse à la détection de trojans dans des circuits intégrés (IC) ou des automates programmables industriels (PLC). Par exemple, on peut utiliser des canaux auxiliaires comme la consommation d'énergie et les émanations électromagnétiques pour créer une signature d'un IC "fiable", et détecter ensuite des contrefaçons qui auraient une signature trop différente [WSTP08], [ZYX12]. De façon similaire, des travaux plus récents s'attaquent cette fois à la vérification du firmware de PLC et autres microcontrôleurs, en utilisant les mêmes canaux auxiliaires pour identifier avec précision les instructions exécutées, éventuellement en s'aidant du graphe de flot de contrôle, et détecter des modifications dans le code [CBZ+16], [LWZ+16].

Un tout autre domaine est celui du *radio fingerprinting* dans lequel on distingue des transmetteurs radio en s'intéressant à la couche physique plutôt qu'aux paquets démodulés dans les couches supérieures. Pour détecter l'usurpation d'un équipement sans-fil, ou développer de nouvelles méthodes d'authentification [DZC12], [TVT+16].

Enfin, dans [HS17] l'activité des composants radio d'un téléphone est surveillée en observant l'activité de leurs canaux de contrôle au moyen d'un "moteur d'introspection" matériel externe.

E. Cyber-Physique

Dans cette catégorie, on trouve surtout des systèmes de détection d'intrusion dédiés aux systèmes cyber-physiques (CPS) et aux infrastructures industrielles, qui travaillent sur l'analyse du trafic échangé sur leurs réseaux de contrôle ([MCT14] fournit une revue détaillée). Ils peuvent réutiliser des capacités des IDS réseau classiques. Ainsi, Quickdraw [PET09] propose plusieurs préprocesseurs Snort pour gérer des protocoles tels que Modbus et DNP3, ainsi que des jeux de règles de détection. Sur ce type de réseau, il est possible de tirer partie de la régularité des échanges pour modéliser précisément le trafic. [GW13] modélise le trafic Modbus d'un système de distribution d'énergie sous forme d'un automate fini déterministe. De cette manière il est possible de détecter des déviations avec une grande précision.

Certains des IDS pour CPS prennent également en compte l'état physique du système. Par exemple dans [KET17] les valeurs de capteurs accessibles sur le réseau SCADA peuvent être utilisées pour détecter la violation de seuils.

III. Discussion

Nous avons présenté des exemples variées de techniques qui permettent de détecter des attaques ou des anomalies, en retenant celles qui utilisent des indicateurs physiques. Nous aurions pû nous attendre à ce que les IPH soient principalement utilisés pour surveiller des systèmes très physiques, mais ce n'est pas le cas, surtout lorsque l'on tient compte des travaux les plus récents.

En revanche, on remarque sans surprise une assez nette distinction entre les deux classes d'indicateurs : les indicateurs cyber sont mieux à même de prévenir des attaques, en détectant les modes d'intrusion, tandis qu'avec les IPH, on cherche essentiellement à détecter la présence d'un intrus dans le système par ses canaux auxiliaires, avec une approche comportementale. D'ailleurs plusieurs des techniques utilisant des IPH sont pensées pour être utilisées périodiquement plutôt qu'en continu comme c'est le cas avec la plupart des IDS classiques. Cela leur autorise l'emploi d'appareillage de

mesure plus coûteux car le dispositif n'a pas besoin d'être en permanence attaché à la cible.

Notre classification connait des limites. Le choix des critères cyber/physiques permet d'appréhender des indicateurs variés et leur champ d'application mais est trop floue pour permettre un classement précis. Il serait désormais intéressant de confronter ces technologies avec les taxonomies existantes sur les IDS pour déterminer lesquels de ces critères peuvent être pris en compte sur des objets connectés.

IV. Conclusion

Nous avons proposé d'étudier les techniques de détection disponibles pour les objets connectés. En centrant cette recherche sur les indicateurs physiques, nous avons pû identifier des méthodes à travers des domaines variés. Nous en avons proposé une classification, et montré que les canaux auxiliaires peuvent être utilisés pour surveiller des systèmes informatiques même lorsqu'ils interagissent peu avec le monde physique. Dans nos travaux futurs, nous évaluerons la pertinence de ces indicateurs pour la détection d'anomalies sur des objets connectés.

References

[KKSV17] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. DDoS in the IoT: Mirai and Other Botnets. In *Computer*, 50(7):80–84, 2017.

[NT11] C. Neuman and K. Tan. Mediating cyber and physical threat propagation in secure smart grid architectures. In *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 238–243, Oct 2011.

[YHK+15] M. Yampolskiy, P. Horváth, X. Koutsoukos, Y. Xue, and J. Sztipanovits. A language for describing attacks on cyber-physical systems. In *International Journal of Critical Infrastructure Protection*, 8:40–52, jan 2015.

[F16] E. Fernandez. Threat Modeling in Cyber-Physical Systems. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing*, pages 448–453. IEEE, aug 2016.

[CWF17] S. Chhetri, J. Wan, and M. Al Faruque. Cross-domain security of cyber-physical systems. In *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, pages 200–205. IEEE, jan 2017.

[R99] M. Roesch. Snort – Lightweight Intrusion Detection for Networks. In *13th USENIX Conference on System Administration*, pages 229–238, Seattle, Washington, 1999. USENIX Association.

[LRLT12] H. Liao, C. Richard Lin, Y. Lin, and K. Tung. Intrusion detection system: A comprehensive review. In *Journal of Network and Computer Applications*, 36:16–24, 2012.

[PAX99] V. Paxson. Bro: a system for detecting network intruders in real-time. In *Computer Networks*, 31(23-24):2435–2463, 1999.

[WSTP08] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic. Hardware Trojan detection and isolation using current integration and localized current analysis. In *Proceedings - IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, pages 87–95, 2008.

[ZYX12] J. Zhang, H. Yu, and Q. Xu. HTOutlier: Hardware Trojan detection with side-channel signature outlier identification. In *Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2012*, pages 55–58, 2012.

[CRR+13] S. Clark, B. Ransford, A. Rahmati, S. Guineau, J. Sorber, K. Fu, and W. Xu. WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices. In *USENIX Workshop on Health Information Technologies*, 2013.

[CBZ+16] R. Callan, F. Behrang, A. Zajic, M. Prvulovic, and A. Orso. Zero-overhead profiling via EM emanations. In *Proceedings of the 25th International Symposium on Software Testing and Analysis - ISSTA 2016*, pages 401–412, New York, New York, USA, 2016. ACM Press.

[LWZ+16] Y. Liu, L. Wei, Z. Zhou, K. Zhang, W. Xu, and Q. Xu. On Code Execution Tracking via Power Side-Channel. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[XXJ+17] Y. Xiao, W. Xu, Z. Jia, Z. Ma, and D. Qi. NIPAD: a non-invasive power-based anomaly detection scheme for programmable logic controllers. *Frontiers of Information Technology & Electronic Engineering*, 18(4):519–534, Apr 2017.

[KSS08] H. Kim, J. Smith, and K. Shin. Detecting Energy-Greedy Anomalies and Mobile Malware Variants. In *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, 2008.

[MMF14] A. Merlo, M. Migliardi, and P. Fontanelli. On energy-based profiling of malware in Android. In *Proceedings of the 2014 International Conference on High Performance Computing and Simulation, HPCS 2014*, pages 535–542, 2014.

[CGL+16] L. Caviglione, M. Gaggero, J. Lalande, W. Mazurczyk, and M. Urbaski. Seeing the Unseen: Revealing Mobile Malware Hidden Communications via Energy Consumption and Artificial Intelligence. *IEEE Transactions on information forensics and security*, 11(4), 2016.

[HS17] B. Huang and E. Snowden. Against the Law: Countering Lawful Abuses of Digital Surveillance. *The Journal of Open Engineering*, 2017.

[CCAF16] S. Chhetri, A. Canedo, M. Abdullah, and A. Al Faruque. KCAD: Kinetic Cyber-Attack Detection Method for Cyber-Physical Additive Manufacturing Systems. In *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Austin, TX, 2016, pp. 1-8.

[BSY+17] S. Belikovetsky, Y. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici. Detecting Cyber-Physical Attacks in Additive Manufacturing using Digital Audio Signing. In *CoRR*, abs/1705.06454, 2017.

[MGB+17] S. Moore, J. Gatlin, S. Belikovetsky, M. Yampolskiy, W. King, and Y. Elovici. Power Consumption-based Detection of Sabotage Attacks in Additive Manufacturing. *CoRR*, abs/1709.01822, 2017.

[BLGA17] A. Bezemskij, G. Loukas, D. Gan, and R. Anthony. Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian Networks. In *2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, 2017, pp. 98-103.

[VLG15] T. Vuong, G. Loukas, and D. Gan. Performance Evaluation of Cyber-Physical Intrusion Detection on a Robotic Vehicle. In *2015 IEEE International Conference on Computer and Information Technology*, pages 2106–2113. IEEE, oct 2015.

[GZC+14] Z. Gao, C. Cecati and S. Ding. A survey of fault diagnosis and fault-tolerant techniques. Part I: fault diagnosis With model-based and signal-based approaches. *IEEE Transactions on Industrial Electronics*, 62(6):3757–3767, 2014.

[JGZ17] K. Javed, R. Gouriveau, and N. Zerhouni. State of the art and taxonomy of prognostics approaches, trends of prognostics applications and open issues towards maturity at different technology readiness levels In *Mechanical Systems and Signal Processing*, pages 214-236, sep 2017.

[DZC12] B. Danev, D. Zanetti, and S. Capkun. On physical-layer identification of wireless devices. *ACM Computing Surveys*, 45(1):1–29, nov 2012.

[TVT+16] T. Vo-Huu, T. Vo-Huu, and G. Noubir. Fingerprinting Wi-Fi Devices Using Software Defined Radios. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks - WiSec '16*, pages 3–14, 2016.

[GW13] N. Goldenberg and A. Wool. Accurate modeling of Modbus / TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, 6(2):63–75, 2013.

[PET09] D. Peterson. Quickdraw: Generating security log events for legacy SCADA and control system devices. In *Proceedings - Cybersecurity Applications and Technology Conference for Homeland Security, CATCH 2009*, pages 227–229, 2009.

[HNH13] J. Hoffmann, S. Neumann, and T. Holz. Mobile Malware Detection Based on Energy Fingerprints — A Dead End? In *Research in Attacks, Intrusions, and Defenses*, pages 348–368. 2013.

[JSLZ16] J. Zhang, S. Gan, X. Liu, and P. Zhu. Intrusion detection in SCADA systems by traffic periodicity and telemetry analysis. In *2016 IEEE Symposium on Computers and Communication (ISCC)*, pages 318–325. IEEE, jun 2016.

[NJC14] A. Nicholson, H. Janicke, and A. Cau. Safety and Security Monitoring in ICS/SCADA Systems. *2nd International Symposium for ICS & SCADA Cyber Security Research 2014*, pages 61–66, 2014.

[KET17] P. Kreimel, O. Eigner, and P. Tavolato. Anomaly-Based Detection and Classification of Attacks in Cyber-Physical Systems. In *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*, pages 1–6. ACM Press, 2017.

[MCT14] R Mitchell and I. Chen, and V. Tech. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Comput. Surv. Article*, 46(29), 2014.