COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Avoiding the internet of insecure industrial things

Lachlan Urquhart *, *Derek McAuley*

Horizon Digital Economy Research Institute, University of Nottingham, Nottingham, United Kingdom

Keywords:
Industrial internet of things
Cybersecurity
Network and information security
Data protection
Smart grids
Industrial control systems
Autonomous vehicles

A B S T R A C T

Security incidents such as targeted distributed denial of service (DDoS) attacks on power grids and hacking of factory industrial control systems (ICS) are on the increase. This paper unpacks where emerging security risks lie for the industrial internet of things, drawing on both technical and regulatory perspectives. Legal changes are being ushered by the European Union (EU) Network and Information Security (NIS) Directive 2016 and the General Data Protection Regulation 2016 (GDPR) (both to be enforced from May 2018). We use the case study of the emergent smart energy supply chain to frame, scope out and consolidate the breadth of security concerns at play, and the regulatory responses. We argue the industrial IoT brings four security concerns to the fore, namely: appreciating the shift from offline to online infrastructure; managing temporal dimensions of security; addressing the implementation gap for best practice; and engaging with infrastructural complexity. Our goal is to surface risks and foster dialogue to avoid the emergence of an Internet of Insecure Industrial Things.

1. Introduction to the industrial IoT

The industrial internet of things (IIoT) is an emerging commercial trend that seeks to improve management of the creation, movement and consumption of goods and services. It is part of a wider shift towards cyber physical systems (CPS) which are ". . .integrations of computation with physical processes. . .embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. . .".[1] IIoT is distinct from the consumer led IoT trend where ambient sensing occurs by remotely controllable and constantly connected physical objects embedded in domestic settings. These devices with a digital presence and backend computational infrastructure (e.g. cloud, databases, servers), networking and an

* *Corresponding author.* Horizon Digital Economy Research Institute, University of Nottingham Innovation Park, Triumph Road, Nottingham, NG7 2TU, United Kingdom.
E-mail address: lachlan.urquhart@nottingham.ac.uk (L. Urquhart).

Abbreviations: APTs, advanced persistent threats; CPS, cyber physical systems; C&Cs, command and control servers; CMA, UK computer misuse act 1990; DDoS, distributed denial of service; GDPR, general data protection regulation 2016; GPS, global positioning system; ICS, industrial control systems; IoT, internet of things; IIoT, industrial internet of things; NIS, network and information security; RFID, radio frequency identification.

[1] Edward A Lee, "Cyber Physical Systems: Design Challenges," *Technical Report No. UCB/EECS-2008-8*, 2008, http://www.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html.

https://doi.org/10.1016/j.clsr.2017.12.004
0267-3649/

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004

associated ecosystem of stakeholders[2]. The IIoT departs by applying these technologies to industrial contexts. Instead of convenience, comfort or entertainment, the goal is to increase connectivity and track activity across supply chains.

IIoT is set for significant growth, estimated by Accenture to add $14.2 trillion to the global economy by 2023.[3] Major industrial investment in manufacturing, energy and transportation[4] is in automation, data driven sensing and actuation.[5] In a review of the domain, Xu et al highlight the following key use cases:

- Healthcare services – tracking healthcare inventory, global access and sharing of health data, and personalisation of patient care.
- Food supply chains – monitoring production from farm to plate including provenance tracking through Radio Frequency ID (RFID), distributed infrastructure and networking.
- Mining – safety applications like early warning sensing for natural disasters, chemical and biological sensors for worker disease detection underground.
- Transport and logistics – tracking physical objects being transported from origin to destination.
- Firefighting – detecting possible fires and providing early warning.[6]

Given the ubiquity of possible IIoT contexts, the breadth of risks can be vast, especially when intersecting with consumer led IoT.[7] For IIoT in healthcare, hacking of insulin pumps or pacemakers is a noteworthy concern.[8] Similarly, in the food supply chain, use of agricultural drones to survey farmland raises concerns for drone hacking, especially for larger vehicles.[9]

More broadly though, the industrial threat landscape already involves a multitude of actors utilising different IT vulnerabilities to leverage a variety of attacks.[10] These include:

- State sponsored hackers attacking foreign infrastructure either in advanced persistent threats (APTs) to steal military secrets or intelligence, or in patriotic campaigns to spread propaganda and interfere with foreign elections.[11] APTs often use zero day vulnerabilities (unpatched security flaws) in software to compromise critical infrastructure and steal confidential information.[12] There can also be **commercial cyber-espionage and sabotage** to obtain commercial intelligence, gain competitive advantage over rival businesses, and cause down-time.[13]
- Organised criminal groups **hacking** into organisations to access compromising information (e.g. trade secrets, emerging intellectual property, and evidence of malpractice).[14] They may also use malware campaigns to infect laptops or smartphones with remote access tools to record victims on their webcams in precarious acts and extorting them to prevent release of the footage as part of ransomware campaigns.[15]
- Loosely united hacker collective groups, like Lulzsec or Anonymous, use hacking or DDoS attacks[16] for social justice and retaliation against organisations for perceived immoral acts.[17] They will target websites or critical infrastructure to create service disruption and downtime, with associated financial and reputational costs.[18]
- Individuals can also create disruption. **Insider threats** posed by disgruntled employees involve use of their internal system access and credentials, or 'social engineering' attacks, to get sensitive information that can be traded with the highest bidder. [19] **Solitary** hackers breaking into military or na-

[2] Lachlan Urquhart and Tom Rodden, "New Directions in Information Technology Law: Learning from Human–computer Interaction," *International Review of Law, Computers & Technology* 31, no. 2 (2017): 1–19. – their working definition is derived from surveying a range of IoT stakeholder definitions e.g. Internet Engineering Task Force; International Telecommunications Union; Cisco; Internet Society etc.

[3] Accenture Technology, "Driving Unconventional Growth through the Industrial Internet of Things," 2015, https://www.accenture.com/gb-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf.

[4] World Economic Forum / Accenture, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services" (Cologny, 2015), http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf.

[5] Li Da Xu et al., "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics* 10, no. 4 (2014), doi:10.1109/TII.2014.2300753.

[6] Ibid.

[7] Derek O'Halloran and Elena Kvochko, "Industrial Internet of Things: Unleashing the Potential of Connected Products and Services," *World Economic Forum*, no. January (2015): 40.

[8] Iain Thomson, "BBC's Micro:bit Turns out to Be an Excellent Drone Hijacking Tool • The Register," *The Register*, 2017, https://www.theregister.co.uk/2017/07/29/bbcs_microbit_drone_hijacking_tool/.

[9] Jim Finkle, "J & J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," *Reuters*, 2016, http://uk.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUKKCN12411L.Lily Hay Newman, 'Medical Devices Are the Next Security Nightmare', *Wired*, 2017, https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

[10] ENISA, *Threat Landscape Report 2016* (ENISA, Heraklion, 2017), 67–72.

[11] Dmitri Alperovitch, "Revealed: Operation Shady RAT," *White Paper*, 2011, https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[12] Brendan Koerner, "Inside the OPM Hack, The Cyberattack That Shocked the US Government," *Wired*, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[13] Thomas Rid, *Cyber War Will Not Take Place* (Hurst & Company, 2013); German Steel Mill example, discussed in more detail below.

[14] Marisa Randazzo et al., "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector," *Software Engineering Institute*, June 1, 2005, http://repository.cmu.edu/sei/457.

[15] Rebecca S. Portnoff et al., "Somebody's Watching Me?: Assessing the Effectiveness of Webcam Indicator Lights," *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems* 1 (2015): 1649–58, doi:10.1145/2702123.2702164.

[16] Distributed Denial of Service.

[17] Pammy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (Back Bay Books 2013).

[18] Argyro P. Karanasiou, "The Changing Face of Protests in the Digital Age: On Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks," *International Review of Law, Computers & Technology* 28, no. 1 (January 15, 2014): 98–113, doi:10.1080/13600869.2014.870638.

[19] UN Office on Drugs and Crime, "Comprehensive Study on Cybercrime" (New York, 2013), https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf.

Please cite this article in press as: Lachlan Urquhart, Derek McAuley, Avoiding the internet of insecure industrial things, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.12.004