IoT and SCADA: Lessons Learned & Case Studies (P2P3-T09)
COL (R) Lawrence D. Dietz, USAR, Esq.

SCADA and Internet of Things (IoT) Reference List

1. https://www.rsaconference.com/events/us17/agenda/sessions/7065-iot-and-scada-lessons-learned-and-case-studies

2. This session will review key lessons learned about SCADA and IoT breaches and attacks such as Stuxnet and Mirai. We will look at the consequences of SCADA breaches and potential legal fallout, analyze two case studies, and discuss best legal and security practices. Case studies will feature two different potential attackers: a hostile nation state and aggrieved employees.

3. https://nakedsecurity.sophos.com/2017/01/12/pacemakers-patched-against-potentially-lifethreatening-hacks/

4. http://www.gamingtechlaw.com/2016/11/industrial-internet-of-things-legal.html

5. In 2000 major SCADA attack on Australian vendor controlling sewage; leak of 800K liters of raw sewage (https://pdfs.semanticscholar.org/78df/bff3c64097ef061035839b7254f7f4dceacd.pdf

6. https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?utm_source=pocket&utm_medium=email&utm_campaign=pockethits&_r=0

7. https://www.hpematter.com/iot-issue/5-industries-transformed-by-iot?jumpid=em_4qyihserkn_AID-510039514

8. https://www.hpematter.com/iot-issue/industry-experts-top-iot-predictions-for-2017?jumpid=em_rwc4ib7agt_AID-510039514

9. https://www.hpematter.com/iot-issue/ask-the-futurists-10-bold-predictions-for-2030?jumpid=em_kc671trsz8_AID-510039514

10. https://www.bbvaopenmind.com/7-tendencias-de-internet-de-las-cosas-en-2017/

11. https://nakedsecurity.sophos.com/2017/01/10/the-spy-sorry-the-fridge-who-loved-me/?utm_source=Naked+Security+-+Sophos+List&utm_campaign=b98c1a18ec-naked%252Bsecurity&utm_medium=email&utm_term=0_31623bb782-b98c1a18ec-454939865

12. http://oilprice.com/Latest-Energy-News/World-News/Saudi-Arabia-Blames-Iran-For-Serious-Cyber-Attacks.html

13. Chen, T M and S Abu-Nimeh. "Lessons From Stuxnet". *Computer* 44, no. 4 (2011): 91-93. Accessed December 22, 2016. http://ieeexplore.ieee.org.ezproxy1.apus.edu/document/5772960/.
14. Langner, Ralph. "Stuxnet: Dissecting A Cyberwarfare Weapon". *IEEE Security & Privacy Magazine* 9, no. 3 (2011): 49-51. Accessed December 2016. http://ieeexplore.ieee.org/document/5772960/?reload=true.
15. Schneier, Bruce. "The Story Behind The Stuxnet Virus." Forbes. October 7, 2010. Accessed December 22, 2016. http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html#.
16. Ellen Nakashima (2 June 2012). *Stuxnet was work of U.S. and Israeli experts, officials say*. The Washington Post. Accessed 22 December 2016
17. Broad, William J.; Markoff, John; Sanger, David E. (15 January 2011*). Israel Tests on Worm Called Crucial in Iran Nuclear Delay*. New York Times. Accessed 22 December 2016
18. Fildes, Jonathan (23 September 2010). *Stuxnet worm 'targeted high-value Iranian assets*. BBC News. Accessed 22 December 2016
19. James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival* 53, no. 1 (February – March 2011): 23, doi: 10.1080/00396338.2011.555586.
20. David C. Gompert & Martin Libicki, "Waging Cyber War the American Way," *Survival* 57, no. 4 (2015): 8, doi: 10.1080/00396338.2015.1068551.
21. AFP. 2016. "NSA Chief Worries About Cyber Attack on US Infrastructure." SecurityWeek, . Web. 24 Dec. 2016. <http://www.securityweek.com/nsa-chief-worries-about-cyber-attack-us-infrastructure>.
22. https://nakedsecurity.sophos.com/2017/02/03/pacemaker-data-used-to-help-indict-alleged-arsonist/?utm_source=Naked+Security+-+Sophos+List&utm_campaign=13840f459a-

naked%252Bsecurity&utm_medium=email&utm_term=0_31623bb782-13840f459a-454939865
23. https://qz.com/901823/the-easy-way-your-smart-coffee-machine-could-get-hacked-and-ruin-your-life/
24. JTAG and UART still good attack vectors: https://www.praetorian.com/blog/why-are-jtag-and-uart-still-effective-attack-vectors-for-iot-devices
25. IoT Threat environment; Cisco: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/C11-735871.pdf
26. https://securityintelligence.com/the-threat-from-weaponized-iot-devices-its-bigger-than-you-think/
27. http://www.ibtimes.co.uk/intel-security-chief-warns-iot-can-open-new-landscape-attack-vectors-future-hackers-1576940
28. https://www.hcltech.com/iot-survey?utm_source=google&utm_campaign=BM-IoT-Global-Report-012017&utm_medium=cpc&utm_term=us&utm_content=vb-iot-challenges&gclid=CJnruJmp_9ECFdRyfgodgMcCGw
29. https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf
30. http://www.cio.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html
31. IoT in Higher Education: https://www.utdallas.edu/info**security**/files/**IoT**-by-UT-Dallas-022416.**ppt**x
32. http://www.computerweekly.com/opinion/The-legal-considerations-of-the-internet-of-things
33. http://www.informationweek.com/iot/iot-raises-new-legal-challenges-for-business/d/d-id/1323926
34. http://www.wassom.com/top-5-legal-issues-internet-things-part-1-data-security-privacy.html
35. https://www.wrighthassall.co.uk/knowledge/legal-articles/2016/08/30/internet-things-what-it-and-what-are-legal-issues/
36. https://www.infosecurity-magazine.com/blogs/iot-denial-service-botnets-scada/
37. http://www.strategyr.com/MarketResearch/Internet_of_Things_IoT_Technology_Market_Trends.asp
38. http://harborresearch.com/harbor-research-the-top-18-iot-trends-to-watch-in-2016/
39. http://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#6c00eec34ba5
40.