CYBR 3520 – Paper Presentation Project

Following these instructions, you will find a list of research papers on Cyber-Physical or Internet of Things security from literature and reports. *This presentation project could be a teamwork* and you can make a team of 2 or 3 members. After that, choose one of the papers to read and prepare for your presentation. I will be sharing a spreadsheet on Google Sheets to allow for you to choose a paper to present. I will also share another spreadsheet shortly allowing you to sign up for a presentation day in class.

The presentation should be 12 to 15 minutes long. You may use PowerPoint, Keynote, or Google Slides to prepare your presentation. Please submit a copy of your slides to Blackboard by 11/27.

Your presentation is expected to be original, but it may incorporate slides obtained from the authors of the papers. However, if you do include slides or material that is not your own, you MUST attribute it!

After each presentation, we will have a Q/A session and I’m expecting each team gives at least one technical question throughout the three presentation days to increase all our knowledge on the topic of Cyber-Physical security.

The list of papers below includes the paper’s titles and authors, as well as a web location to download it from. The list is divided into 2 sections. The first is from a special issue of a journal that our textbook author edited. The second is more journal or conference papers. I am not expecting you to understand all of the technical detail in the papers, but I am looking for a summary of the paper in the presentation, and perhaps any issues/agreement you might have with the author’s approach or conclusions.

There are 20 papers in the list, and we have 20 students, so there should be enough papers to cover all the teams. ***I will accept presentations on papers covering IOT or Cyber-Physical Security that are not in the list. However, please note you will need to get my approval of the paper first.*** Also note, I will be favoring papers from technical sources such as academic journals/conferences, or respected industry sources. A very high-level article from a mainstream media source such as Time or Newsweek is less likely to be accepted.

**List of Papers:**

Paper’s from Journal Issue that our Book Author edited:

* Paper 01 - Loukas, George and Charalampos Patrikakis, “Cyber and Physical Threats to the Internet of Everything” in Security in the Internet of Everything Era, Cutter IT Journal, 2016

URL: <https://www.cutter.com/sites/default/files/itjournal/2016/07/itj1607.pdf>

* Paper 02 - Baudoin , Claude R., “Security Challenges and Approaches in the Industrial Internet” in Security in the Internet of Everything Era, Cutter IT Journal, 2016

URL: <https://www.cutter.com/sites/default/files/itjournal/2016/07/itj1607.pdf>

* Paper 03 - Heartfield , Ryan and Diane Gan, “Social Engineering in the Internet of Everything” in Security in the Internet of Everything Era, Cutter IT Journal, 2016 URL: <https://www.cutter.com/sites/default/files/itjournal/2016/07/itj1607.pdf>
* Paper 04 - Tayouri , David, “Securing the IoT: It Takes the Global Village” in Security in the Internet of Everything Era, Cutter IT Journal, 2016

URL: <https://www.cutter.com/sites/default/files/itjournal/2016/07/itj1607.pdf>

* Paper 05 - Kogias, Dimitrios G., “Security and Privacy in the Internet of Things: How to Increase User Trust” in Security in the Internet of Everything Era, Cutter IT Journal, 2016 URL: <https://www.cutter.com/sites/default/files/itjournal/2016/07/itj1607.pdf>

Journal / Conference Papers:

* Paper 06 - Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." In Security and Privacy (SP), 2016 IEEE Symposium on, pp. 636-654. IEEE, 2016.

URL: <http://www.earlence.com/assets/papers/smartthings_sp16.pdf>

* Paper 07 - Chen Song, Feng Lin, Zongjie Ba, Kui Ren, Chi Zhou, Wenyao Xu. "My Smartphone Knows What You Print: Exploring Smartphone-based Side-channel Attacks Against 3D Printers." CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Pages 895–907, 2016.

URL:<http://www.buffalo.edu/content/dam/www/news/photos/2016/09/smartphone-hacks-3D-printer.pdf>

* Paper 08 - Tian, Yuan, Nan Zhang, Yueh-Hsun Lin, XiaoFeng Wang, Blase Ur, XianZheng Guo, and Patrick Tague. "SmartAuth: User-Centered Authorization for the Internet of Things." In 26th {USENIX} Security Symposium ({USENIX} Security 17), pp. 361-378. USENIX} Association}, 2017.

URL: <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-tian.pdf>

* Paper 09 - Wilson, Judson, Riad S. Wahby, Henry Corrigan-Gibbs, Dan Boneh, Philip Levis, and Keith Winstein. "Trust but Verify: Auditing the Secure Internet of Things." In Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services, pp. 464-474. ACM, 2017.

URL: <https://nsr.cse.buffalo.edu/mobisys_2017/papers/pdfs/mobisys17-paper32.pdf>

* Paper 10 - Malisa, Luka, Kari Kostiainen, Thomas Knell, David Sommer, and Srdjan Capkun. "Hacking in the Blind:(Almost) Invisible Runtime User Interface Attacks." In International Conference on Cryptographic Hardware and Embedded Systems, pp. 468-

489. Springer, Cham, 2017.

URL: <https://eprint.iacr.org/2017/584.pdf>

* Paper 11 - Fabio Arena, Giovanni Pau, and Mario Collotta. "A survey on driverless vehicles: from their diffusion to security features." Journal of Internet Services and Information, 2018.

URL: <http://isyou.info/jisis/vol8/no3/jisis-2018-vol8-no3-01.pdf>

* Paper 12 - Lebeck, Kiron, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. "Securing augmented reality output." In Security and Privacy (SP), 2017 IEEE Symposium on, pp. 320-337. IEEE, 2017.

URL: <http://www.ieee-security.org/TC/SP2017/papers/541.pdf>

* Paper 13 - Yuan, Xuejing, Yuxuan Chen, Yue Zhao, Yunhui Long, Xiaokang Liu, Kai Chen, Shengzhi Zhang, Heqing Huang, Xiaofeng Wang, and Carl A. Gunter. "CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition." arXiv preprint arXiv:1801.08535 (2018).

URL: <https://arxiv.org/pdf/1801.08535.pdf>

* Paper 14 - Le Guan, Jun Xu, Shuai Wang, Xinyu Xing, Lin Lin, Heqing Huang, Peng Liu, Wenke Lee. “From Physical to Cyber: Escalating Protection for Personalized Auto

Insurance.” In ACM SenSys, 2016.

URL: <http://xinyuxing.org/pub/p42-guan.pdf>

* Paper 15 - Faruque, Al, Mohammad Abdullah, Sujit Rokka Chhetri, Arquimedes Canedo, and Jiang Wan. "Acoustic side-channel attacks on additive manufacturing systems." In Proceedings of the 7th International Conference on Cyber-Physical Systems, p. 19. IEEE Press, 2016.

URL: <https://ieeexplore.ieee.org/document/7479068>

* Paper 16 - Babun, Leonardo, et al. "Real-time analysis of privacy-(un) aware iot applications." Proceedings on Privacy Enhancing Technologies 2021.1 (2021): 145-166.

URL: https://www.ftc.gov/system/files/documents/public\_events/1582978/realtime\_analysis\_of\_privacy\_unaware\_iot\_applications\_.pdf

* Paper 17 - Yu, Miao, Jianwei Zhuge, Ming Cao, Zhiwei Shi, and Lin Jiang. "A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices." Future Internet 12, no. 2 (2020): 27.

URL: <https://www.mdpi.com/1999-5903/12/2/27/pdf>

* Paper 18 - Salam, Abdul. "Internet of things for sustainability: perspectives in privacy, cybersecurity, and future trends." In Internet of Things for Sustainable Community Development, pp. 299-327. Springer, Cham, 2020.

URL:<https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1034&context=cit_articles>

* Paper 19 - Gupta, Nikhil, Akash Tiwari, Satish TS Bukkapatnam, and Ramesh Karri. "Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks." IEEE Access 8 (2020): 47322-47333.

URL: <https://ieeexplore.ieee.org/iel7/6287639/8948470/09026901.pdf>

* Paper 20 - McNabb, John. " Vulnerabilities of Wireless Water Meter Networks", Black Hat USA, Las Vegas, USA, August 3, 2011.

URL: <http://162.114.3.165/PSCSCF/2012%20cases/2012-00428/Public%20Comments/20140221_PSC_Response%20E-mail%20to%20Holloway%2002.pdf>