SIL765: Networks and System Security

Semester II, 2023-2024

Project Selection and Paper Presentation

February 3, 2024

Top Security Venues

The top venues for submitting any work related to the security and privacy can be found at [1]. For the network and system security, the list consists of the following top-four conferences.

1. ACM Symposium on Computer and Communications Security (CCS)
2. IEEE Symposium on Security and Privacy (S&P)
3. USENIX Security Symposium
4. Network and Distributed System Security (NDSS) Symposium

Finding a Project Topic

There could be a variety of ways to select the topic and the relevant paper for your project. Please feel free to find your way. The following can be considered as a general suggestion.

- Find the program of any of the top four conferences and read through the session titles.
- If you find a session title interesting, read the paper titles.
- If you find a paper title interesting, read its abstract.
- If you find the abstract interesting, read the captions of the figures and the tables.
- If you still find the paper interesting, read the introduction.

Once you have read the introductions of some of the papers, you should be able to judge whether you would be interested in carrying out the project work in that area.

Previously Shared Projects

- IoT Device Security [2, 3]
- Program Analysis [4]
- IoT Application Security [5, 6, 7, 8]
- Edge Computing Security Issues [9]
- Machine Learning for IoT/CPS security [10, 11]
- Sensor/Actuator Security [12, 13]

- Voice-Controlled Devices [14, 15]
- Attacks to Power Grid System [16]
- Autonomous Vehicle Security [17, 18, 19]
- Fault Identification and Tolerance [20, 21]
- IoT/CPS Fuzzing [22, 23]
- Program Analysis for Security [24, 25]
- Control Systems Security [26]
- 5G Network Security
- Mobile App Analysis
- WLAN Security
- Mobile device security

Finding a Relevant Paper for Presentation

- The selected paper should have been published in one of the top four conferences.
- It should have been published after the year 2013.
- It should have at least 100 citations.
- It should "not" be a survey paper or systematization-of-knowledge (SoK) paper.

Submission

You are expected to do the following.

- Create a few slides about the work described in the selected paper.
- Record your presentation. The presentation recording must not be more than 10 minutes. Any recording of more than 10 minutes will not be evaluated.
- Store the recording such that it can be accessed by anyone with the recording link.
- Add the recording link on the title page of the presentation.
- Submit the presentation (in pdf format) on Gradescope.

References

[1] "Top venues for publishing papers on security," https://scholar.google.com/citations?view_op=top_venues&hl=en&vq=eng_computersecuritycryptography, 2023, [Online; accessed March 1, 2023].

[2] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *IEEE Symposium on Security and Privacy (S&P)*, 2019, pp. 1362–1380.

[3] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All things considered: An analysis of IoT devices on home networks," in *USENIX Security Symposium*, 2019, pp. 1169–1185.

[4] Z. B. Celik, E. Fernandes, E. Pauley, G. Tan, and P. McDaniel, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–30, 2019.

[5] W. Zhou, Y. Jia, Y. Yao, L. Zhu, L. Guan, Y. Mao, P. Liu, and Y. Zhang, "Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms," in *USENIX Security Symposium*, 2019, pp. 1133–1150.

[6] Q. Wang, P. Datta, W. Yang, S. Liu, A. Bates, and C. A. Gunter, "Charting the attack surface of trigger-action IoT platforms," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 1439–1453.

[7] X. Wang, Y. Sun, S. Nanda, and X. Wang, "Looking from the mirror: Evaluating IoT device security through mobile companion apps," in *USENIX Security Symposium*, 2019, pp. 1151–1167.

[8] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands: laser-based audio injection attacks on voice-controllable systems," in *USENIX Security Symposium*, 2020, pp. 2631–2648.

[9] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J. P. Jue, "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, vol. 98, pp. 289–330, 2019.

[10] J. Li, F. Schmidt, and Z. Kolter, "Adversarial camera stickers: A physical camera-based attack on deep learning systems," in *International Conference on Machine Learning*, 2019, pp. 3896–3904.

[11] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 2267–2281.

[12] J. Han, A. J. Chung, M. K. Sinha, M. Harishankar, S. Pan, H. Y. Noh, P. Zhang, and P. Tague, "Do you feel what i hear? enabling autonomous IoT device pairing using different sensor types," in *IEEE Symposium on Security and Privacy (S&P)*, 2018, pp. 836–852.

[13] S. Birnbach and S. Eberz, "Peeves: Physical event verification in smart homes," 2019.

[14] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems," in *IEEE Symposium on Security and Privacy (S&P)*, 2019, pp. 1381–1396.

[15] H. Mohajeri Moghaddam, G. Acar, B. Burgess, A. Mathur, D. Y. Huang, N. Feamster, E. W. Felten, P. Mittal, and A. Narayanan, "Watching you watch: The tracking ecosystem of over-the-top TV streaming devices," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 131–147.

[16] B. Huang, A. A. Cardenas, and R. Baldick, "Not everything is dark and gloomy: Power grid protections against IoT demand attacks," in *USENIX Security Symposium*, 2019, pp. 1115–1132.

[17] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, 2011, pp. 447–462.

[18] M. D. Pesé, T. Stacer, C. A. Campos, E. Newberry, D. Chen, and K. G. Shin, "LibreCAN: Automated CAN message translator," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019, pp. 2283–2300.

[19] A. Ganesan, J. Rao, and K. Shin, "Exploiting consistency among heterogeneous sensors for vehicle anomaly detection," SAE Technical Paper, Tech. Rep., 2017.

[20] J. Choi, H. Jeoung, J. Kim, Y. Ko, W. Jung, H. Kim, and J. Kim, "Detecting and identifying faulty IoT devices in smart home with context extraction," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018, pp. 610–621.

[21] M. S. Ardekani, R. P. Singh, N. Agrawal, D. B. Terry, and R. O. Suminto, "Rivulet: A fault-tolerant platform for smart-home applications," in *Proceedings of the ACM/IFIP/USENIX Middleware Conference*, 2017, pp. 41–54.

[22] T. Kim, C. H. Kim, J. Rhee, F. Fei, Z. Tu, G. Walkup, X. Zhang, X. Deng, and D. Xu, "RVFUZZER: Finding input validation bugs in robotic vehicles through control-guided testing," in *USENIX Security Symposium*, 2019, pp. 425–442.

[23] Y. Zheng, A. Davanian, H. Yin, C. Song, H. Zhu, and L. Sun, "FIRM-AFL: high-throughput greybox fuzzing of IoT firmware via augmented process emulation," in *USENIX Security Symposium*, 2019, pp. 1099–1114.

[24] Y. Chen, C. M. Poskitt, and J. Sun, "Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system," in *IEEE Symposium on Security and Privacy (S&P)*, 2018, pp. 648–660.

[25] Z. Huang, D. Lie, G. Tan, and T. Jaeger, "Using safety properties to generate vulnerability patches," in *IEEE Symposium on Security and Privacy (S&P)*, 2019, pp. 539–554.

[26] M. Zhang, C.-Y. Chen, B.-C. Kao, Y. Qamsane, Y. Shao, Y. Lin, E. Shi, S. Mohan, K. Barton, J. Moyne *et al.*, "Towards automated safety vetting of PLC code in real-world plants," in *IEEE Symposium on Security and Privacy (S&P)*, 2019, pp. 522–538.