IoT Security Assurances and IoT Threat Modelling

Naresh Adhikari
Slippery Rock University of Pennsylvania
naresh.adhikari@sru.edu

ABSTRACT

Internet of Things (IoT) refers to the set of miniature sensing devices connected via the Internet [1]. IoT has gained popularity in several areas of business, education, and communications. Primarily, IoT has been used for real-time sensing and monitoring of an environment, such as that belonging to homes, businesses, industries, and farming, among others [2]. According to IoT Analytics, the number of IoT devices grew by 9% to reach 12.3 B globally in 2021(https://bit.ly/3XPS99p (accessed on 30 December 2022)). It is estimated that IoT devices will reach 27 B by 2025 and will generate 79.4 zettabytes (ZB) of data by the year(estimated) 11 trillion dollars (https://bit.ly/3iXjRCy (accessed on 14 June 2022)). In the meantime, 58% of cyberattacks over IoT infrastructure, were mainly Denial of Distributed Attacks (DDoS). The cost of such attacks is expected to grow 15 % over the next five years to reach USD 10.5 trillion/annum by 2025 (https://bit.ly/3iT3sPz (accessed on 14 June 2022)).

IoT security assurances are the consumer(s) confidence in an IoT system's security aspects. General yet critical security assurances to an IoT include data confidentiality, integrity, availability, and physical security [3]. These keywords apply to various IoT assets such as infrastructure (e.g. sensors and sensor networks), communication, applications, and data. They should be concretely defined to capture all critical security needs of IoT provisioning, deployment, and maintenance. High confidence in meeting these security needs defines the trustworthiness of IoT systems [4]. Nevertheless, in most of the literature on IoT and its security, such assurances are poorly defined. Poor definitions enjoy poor recommendations. Poor security recommendations have led to the continuation of vulnerable IoT (sub)-systems. Thus, we must address the demand for a comprehensive definition of IoT security assurances and their meaningful examples. It will aid motivation in utilizing secure and robust IoT infrastructure. IoT threat modeling [5] is a process of identifying, isolating, scoring, communicating, and mitigating the events or properties that lower the "trustworthiness" of an IoT system. The artifacts (structures, diagrams, tables, etc.) that are born out of the process are threat model(s). While many kinds of literature [6],[7] generalize the IoT security assurances and the threat modeling, they are both specific to the consumer base's needs. Through this presentation, we attempt to shed light on fine-grained qualities of IoT security assurances, trustworthy IoT systems, and IoT threat models. **Note:** This abstract is based on the same authors' journal article [8].

References

[1] D. B. Ahire, Dr. V. J. Gond, and N. L. Ahire, "IoT Based Real-Time Monitoring of Meteorological Data: A Review," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.4043518.

[2] J. M. Ibrahim, A. Karami, and F. Jafari, "A Secure Smart Home using Internet-of-Things," in *Proceedings of the 9th International Conference on Information Management and Engineering*, Barcelona Spain, Oct. 2017, pp. 69–74. doi: 10.1145/3149572.3149577.

[3] B. Alotaibi, "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review," *IEEE Sens. J.*, vol. 19, no. 23, pp. 10953–10971, Dec. 2019, doi: 10.1109/JSEN.2019.2935035.

[4] F. Wei, S. Tate, M. Ramkumar, and S. Mohanty, "A Scalable Trustworthy Infrastructure for Collaborative Container Repositories," *Distrib. Ledger Technol. Res. Pract.*, vol. 1, no. 1, pp. 1–29, Sep. 2022, doi: 10.1145/3554760.

[5] Drake, Victoria, "Threat Modeling," *Threat Modeling*, Feb. 18, 2023. https://american-cse.org/csce2023/special_issues (accessed Feb. 18, 2023).

[6] V. Casola, A. De Benedictis, M. Rak, and U. Villano, "Toward the automation of threat modeling and risk assessment in IoT systems," *Internet Things*, vol. 7, p. 100056, Sep. 2019, doi: 10.1016/j.iot.2019.100056.

[7] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 181, p. 103007, May 2021, doi: 10.1016/j.jnca.2021.103007.

[8] N. Adhikari and M. Ramkumar, “IoT and Blockchain Integration: Applications, Opportunities, and Challenges,” *Network*, vol. 3, no. 1, pp. 115–141, Jan. 2023, doi: 10.3390/network3010006.