Detection of Unauthorized IoT Devices Using Machine Learning Techniques

Tabinda Shehzadi[1], Lee Kasowaki[2], and Miles Kingerberg[2]

[1]Affiliation not available
[2]University of Washington

August 23, 2022

Detection of Unauthorized IoT Devices Using Machine Learning Techniques

Lee Kasowaki, Miles Kingerberg

University of Washington

ABSTRACT

Security experts have demonstrated numerous risks imposed by Internet of Things (IoT) devices on organizations. Due to the widespread adoption of such devices, their diversity, standardization obstacles, and inherent mobility, organizations require an intelligent mechanism capable of automatically detecting suspicious IoT devices connected to their networks.

INTRODUCTION

The Internet of Things (IoT) is globally expanding, providing diverse benefits in nearly every aspect of our lives. Unfortunately, the IoT is also accompanied by a large number of information security vulnerabilities and exploits. [1-3]

SYSTEM AND ATTACK MODEL: In this research, the system we assume is a typical large enterprise, facing an ever growing range of IoT-related cyber threats. *Untargeted:* The connected IoT device has been previously infected by a malware of indiscriminate nature, virally spreading among as many devices as possible. Cross-contamination provides a mechanism for this kind of attack. *Specifically targeted:* The malware was intentionally implanted on the IoT device by an attacker, based on the assumption that the device would likely be connected to a specific organizational network in the future[4, 5].

White Listing For IOT Devices:

White list of authorized device types marked as safe is much smaller than the ever growing list of presumably insecure types, unauthorized by default. As a result, a shorter list contributes to the increased efficiency of the machine learning (ML) processes underlying the proposed white listing method, including model training, validation, testing, and deployment.[6, 7]

PROPOSED METHOD:

Given a set of authorized device types (i.e., the white list) and a structured set of traffic data, we treat the task of IoT device type identification as a multi-class classification problem. That is, we wish to map each IP stream to the type of IoT device that is most likely to have produced it. [8, 9]

Classifier Training:

The Random Forest supervised ML algorithm is selected for model training. According to a recent survey on ML methods in cyber security, this algorithm which combines decision tree induction with ensemble learning has several advantages relevant to our study, including[10]:

- There is no need for prior feature selection.
- It requires just a few input parameters.
- The algorithm is resistant to over fitting.
- When the number of trees increases, the variance is decreased without resulting in bias.

Parameter Tuning

SECURITY CHALLENGES AND THREAT MODELS IN IOT

Physical Attacks:

In physical attacks, the attackers have direct access to the devices and manipulate different aspects of the devices. To get access to the physical devices, social engineering is one of the most prominent methods where the attackers access the devices and perform real attack that ranges from physical damage to the device to eavesdropping, side-channels, and other related attacks[11]

Physical (PHY) and Link Layer Security Issues:

IoT combines various communication technologies at the lower layers of TCP/IP protocol stack and thus-forth provides a complex heterogeneous network. The heterogeneity is introduced at physical layer of the IoT and then different amendments are made at data link layer, for instance special channel design and so forth, depending on the underlying physical layer technology[12]. There are different security issues in physical layer of IoT depending on the underlying technology, for instance in case of sensor nodes, physical attacks on sensor nodes must be mitigated[13].

Network Layer Attacks:

At the network level, the attacks are aimed at routing, data and traffic analysis, spoofing, and launching man-in-the middle attack. Besides, Sybil attacks are also possible at the network layer where fake identities/Sybil identities are used to create illusions in the network.

Transport Layer Attacks:

Transport layer is responsible for process to process delivery where transport protocols enable the processes to exchange data. In the context of IoT, the traditional transport layer security issues still persist. The most serious attack at this layer is the denial of service attack that chokes the network and results in denial of services to the applications.

Conclusion:

Security experts have demonstrated numerous risks imposed by Internet of Things (IoT) devices on organizations. Due to the widespread adoption of such devices, their diversity, standardization obstacles, and inherent mobility, organizations require an intelligent mechanism capable of automatically detecting suspicious IoT devices connected to their networks.

References:

[1] M. Heydari, Z. Xiaohu, L. K. Keung, and Y. Shang, "Entrepreneurial Intentions and Behaviour as the Creation of Business: Based on the Theory of Planned Behaviour Extension Evidence from Polish Universities and Entrepreneurs," *Propósitos y representaciones,* vol. 8, no. 2, p. 46, 2020.

[2] Z. Xiaohu, M. Heydari, K. K. Lai, and Z. Yuxi, "Analysis and modeling of corruption among entrepreneurs," *REICE: Revista Electrónica de Investigación en Ciencias Económicas,* vol. 8, no. 16, pp. 262-311, 2020.

[3] M. Heydari, K. K. Lai, and Z. Xiaohu, *Corruption, Infrastructure Management and Public–Private Partnership: Optimizing through Mathematical Models*. Routledge, 2021.

[4] R. Oak, "Poster: Adversarial Examples for Hate Speech Classifiers," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019, pp. 2621-2623.

[5] J. Asad and N. Mazher, "Load Balancing Protocol for dynamic resource allocation in cloud computing," 2018.

[6] N. Mazher and I. Ashraf, "A Survey on data security models in cloud computing," *International Journal of Engineering Research and Applications (IJERA),* vol. 3, no. 6, pp. 413-417, 2013.

[7] R. Oak, M. Du, D. Yan, H. Takawale, and I. Amit, "Malware detection on highly imbalanced data through sequence modeling," in *Proceedings of the 12th ACM Workshop on artificial intelligence and security*, 2019, pp. 37-48.

[8] M. Heydari *et al.*, "Emergency and Disaster Logistics Processes for Managing ORs Capacity in Hospitals: Evidence from United States," *International Journal of Business and Management (IJBM),* vol. 1, no. 1, pp. 63-85, 2022.

[9] R. Oak, M. Khare, A. Gogate, and G. Vipra, "Dynamic Forms UI: Flexible and Portable Tool for easy UI Design," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018: IEEE, pp. 1926-1931.

[10] M. Heydari, Z. Xiaohu, M. Saeidi, K. K. Lai, Y. Shang, and Z. Yuxi, "Analysis of the role of social support-cognitive psychology and emotional process approach," *European Journal of Translational Myology,* vol. 30, no. 3, 2020.

[11] R. Oak, "Extractive techniques for automatic document summarization: a survey," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 4, no. 3, pp. 4158-4164, 2016.

[12] N. Mazher, M. Alhadaad, and O. Shagdar, "A Brief Summary of Cybersecurity attacks in V2X Communication," 2022.

[13] R. Oak, "A study of digital image segmentation techniques," *Int. J. Eng. Comput. Sci,* vol. 5, no. 12, pp. 19779-19783, 2016.