Review of Electromagnetic Side Channel Attacks in IoT devices for Smart Homes

William Daniel Hiromoto

***Abstract*—The abstract goes here.**

I. Introduction

AS the notion of an internet of things (Iot) becomes more prevalent, the usage of an IoT environment within the consumer home market is only becoming more popular. The usage of an IoT in this environment would be what most people refer to 'Smart Homes', where many aspects of the living environment can now be accessed and automated. Typical configuration or access is done by mobile app, voice control, or web portal. However, the presence of these IoT devices in the home exposes a larger attack surface for malicious actors surveil users. In addition to being vulnerable to the typical malware attacks, IoT devices also expose more information about the user's home wirelessly, which can be monitored and analyzed in unexpected ways regardless of encryption. Other papers [1] organize research in terms of device usage or application in the home. In contrast, attacker intent seems to be less investigated and will be explored in more detail.

December 12, 2024

II. Background

III. Categorization

Research papers from the last five years were selected based on the paper's relation to smart Home EM side-channel attacks. The papers were then broken into 3 categories based on the intent of the attacker: finding the location and behavior of a device(s) and person(s). Many of the attacks uses inferences based on or supplemented by machine learning algorithms. All of the inference attacks are effective against encryption and they all have similar countermeasures.

A. Analyzing Device Activity

Papers involving adversarial models in which the objective is to infer the identity, state, and activity of the device ([2], [3], [4], [5]) based on analyzing the wireless traffic of the smart home. This research focuses on analyzing the traffic of the smart home network, regardless of the encryption status. Of the four papers analyzed in this category, all except one [2] use machine learning to supplement a portion of the attack.

B. Locate Devices or People

This research focuses more on the location of devices or people. The threat models in these articles assume that the attacker does not have physical access to the interior of the target property but has limited access around the property to place sniffers ([6], [7], [8]). Unlike the previous category, the attacks rely less on the size or timings of the packet sent over the network, but more on the presence of packets at all. In [8], information found by the packet header is not required, but [6], [7] require the packet headers to identify the devices for localization which can be interfered with as mentioned in [2]. [7] localizes the device as part of a multistage attack but fits more inline with the next category.

C. Infer Information about Users Inside the Home

Beyond finding a device's activity or location based on EM side channel information, attack goals in this category seek to infer and even predict user behavior inside of a smart home ([9], [10], [7], [11]). These attacks will typically use information about the device state and use a trained model to infer user behavior. While [10] is referenced by many other papers analyzed here, [7] goes a step further and attempts to predict user behavior based on information from the traffic.

IV. Analysis

V. New Research Directions

References

[1] M. Hasan, P. Biswas, M. T. I. Bilash, and M. A. Z. Dipto, "Smart home systems: Overview and comparative analysis," *2018 Fourth International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2018.

[2] N. Shafqat, D. J. Dubois, D. Choffnes, A. Schulman, D. Bharadia, and A. Ranganathan, "Zleaks: Passive inference attacks on zigbee based smart homes," *arXiv: Cryptography and Security*, 2021.

[3] C. Wang, S. Kennedy, H. Li, K. Hudson, G. Atluri, X. Wei, W. Sun, and B. Wang, "Fingerprinting encrypted voice traffic on smart speakers with deep learning," *Wireless Network Security*, 2020.

[4] R. Trimananda, J. Varmarken, A. Markopoulou, and B. Demsky, "Ping-pong: Packet-level signatures for smart home device events," *arXiv: Networking and Internet Architecture*, 2019.

[5] S. Dong, Z. Li, D. Tang, J. Chen, M. Sun, and K. Zhang, "Your smart home can't keep a secret: Towards automated fingerprinting of iot traffic," 2020.

[6] Y. He, Q. He, S. Fang, and Y. Liu, "Precise wireless camera localization leveraging traffic-aided spatial analysis," *IEEE Transactions on Mobile Computing*, 2024.

[7] Q. Zou, P. Cheng, L. Qing, L. Ruoyu, Y. Huang, J. Xiao, Y. Jiang, Q. Zou, Q. Li, R. Li, Y.-C. Huang, G. Tyson, and J. Xiao, "Iotbeholder: A privacy snooping attack on user habitual behaviors from smart home wi-fi traffic," *Proceedings of the ACM on Interactive Mobile Wearable and Ubiquitous Technologies*, 2023.

[8] Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng, "Et tu alexa? when commodity wifi devices turn into adversarial motion sensors." *Network and Distributed System Security Symposium*, 2020.

[9] K. Huang, Y. Zhou, K. Zhang, J. Xu, J. Chen, D. Tang, and K. Zhang, "Homespy: The invisible sniffer of infrared remote control of smart tvs," *USENIX Security Symposium*, 2023.

[10] A. Acar, H. Fereidooni, T. Abera, A. K. Sikder, M. Miettinen, H. Aksu, M. Conti, A.-R. Sadeghi, and A. S. Uluagac, "Peek-a-boo: i see your smart home activities, even encrypted!" *Wireless Network Security*, 2020.

[11] A. Maiti and M. Jadliwala, "Light ears," *Proceedings of the ACM on Interactive Mobile Wearable and Ubiquitous Technologies*, 2018.