Leveraging Electromagnetic Emanations for IoT Security

Nader Sehatbakhsh[&], Robert Callan[$], Monjur Alam[&], Milos Prvulovic[&], and Alenka Zajic[$]
School of Computer Science[&], School of Electrical Engineering[$], Georgia Institute of Technology, USA

The Internet of Things (IoT) has introduced new security risks for both consumers and businesses. Mitigation of these risks is difficult in part because IoT devices often have limited resources that can be leveraged to monitor their security, and often have limited hardware and system support for isolation and protection. Unfortunately, existing malware detection techniques require significant computation power and resources on the monitored device itself, making their deployment on IoT devices challenging.

To mitigate this problem, we will demonstrate a new method to detect malware by externally observing Electromagnetic (EM) signals emitted by an IoT system. The proposed demo is an extension of the work in [1] and does not require any resources or infrastructure on, or any modifications to, the monitored system itself. Specifically, our method can identify malicious code injection into a known application that is running on an IoT device with >95% accuracy and with a detection latency <45 ms of executed code. To demonstrate the effectiveness of our method, we have implemented a number of malicious activities such as control-flow hijacking, Mirai bot-net, and Ransomware on an IoT device, then used our method to monitor the IoT system while it is executing embedded applications (the MiBENCH embedded benchmark suite) that are subjected to malicious code injection.

In this demo, we will use the setup shown in Fig. 1 (left). It consists of IoT device (A13-OLinuXino board) that runs one of the applications from the MiBENCH [2] suite. The MiBENCH suite is commonly used to evaluate performance of processors intended for the embedded market, and it was designed to be representative of the computation that are needed in that market, while being easy to port to platforms that have limited development infrastructure and system resources. The A13-OLinuXino board is a single-board computer that has an in-order, 2-issue Cortex A8 ARM processor and runs Debian Linux operating system, and it is commonly used as a platform for prototyping IoT systems. Our experimental setup receives EM signals using a commercially available horn antenna 50-100 cm away from the IoT device. The signals collected by the antenna are recorded with a software defined radio (SDR) and spectrum is displayed on the laptop. Examples of spectrogram with and without malware are shown in Fig. 1 (right). Then, we run our Matlab code that identifies malware and displays its position in spectrum.

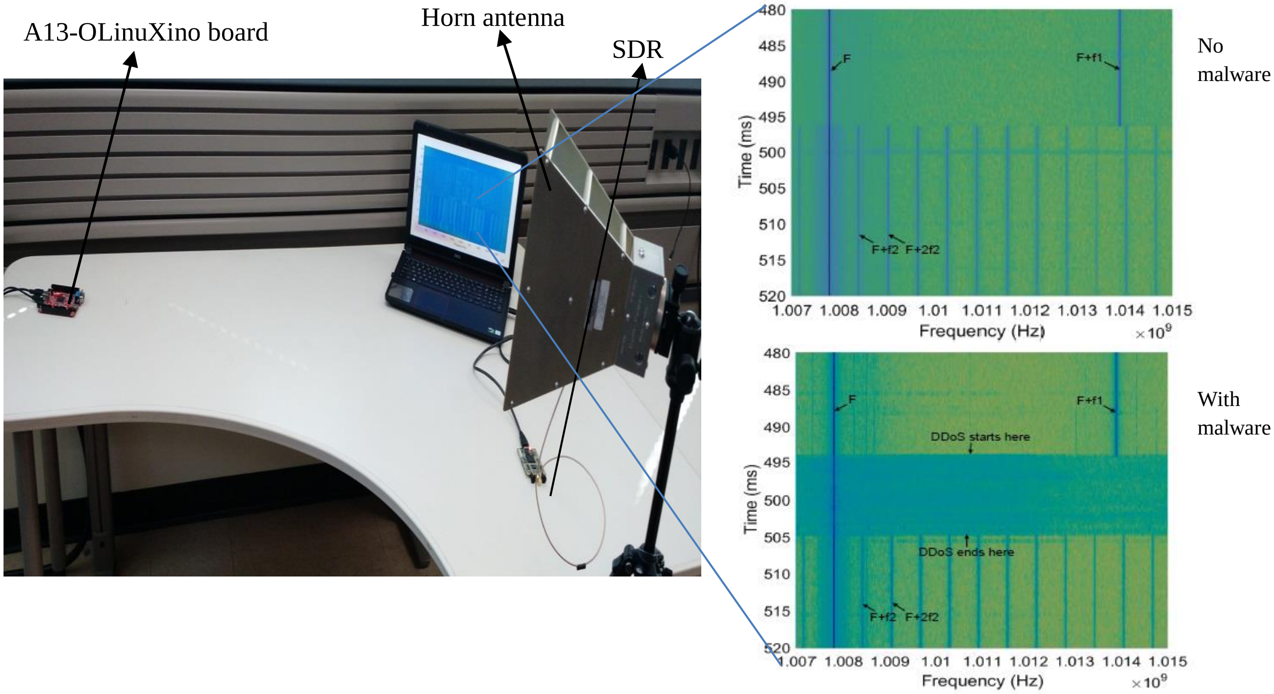

Fig. 1 Demo setup and some of the displayed results.

[1] N. Sehatbakhsh, A. Nazari, A. Zajić, and Milos Prvulovic "Spectral Profiling: Observer-Effect-Free Profiling by Monitoring EM Emanations," *the 49th Annual IEEE/ACM International Symposium on Microarchitecture*, pp.1-11, Taipei, Taiwan, October 2016.

[2] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "Mibench: A free, commercially representative embedded benchmark suite," in Workload Characterization, 2001. WWC-4. 2001 IEEE International Workshop on, pp. 3–14, IEEE, 2001.