Application Inference using ML based Side Channel Analysis

Nikhil Chawla, Arvind Singh, Monodeep Kar,
Nael Mizanur Rahman and Saibal Mukhopadhyay

April 6, 2019

Application Inference using ML based Side Channel Analysis

[1]N. Chawla, [1]A. Singh [2]M. Kar, [1]N.M. Rahman, [1]S. Mukhopadhyay
[1]Georgia Institute of Technology, Atlanta, GA; [2]Intel, Hillsboro, OR

1 Hardware Demo Objectives

*In the demonstration session, we will be presenting a side channel measurement setup comprising of a Snapdragon 820 development board, to measure side channel activity of the applications being executed on a processor, through EM emissions and DVFS states. (**the paper based on the same was submitted at International Joint Conference on Neural Networks (IJCNN), in January 2019 [1])***

2 Introduction

Electromagnetic emissions (EM) have been shown to reveal information about programs running on a device and have also been used as a defense mechanism to identify malicious code [2]. It has been shown to compromise security of many computing devices but only recently researchers have started exploring the interactions of DVFS and security. DVFS is an integral part of modern system on chips that help improve energy efficiency and battery life. The use of DVFS has been demonstrated as a countermeasure to power side channel attacks on encryption engines [3]. The use of fast DVFS enabled by on-chip regulator and adaptive clocking, has been shown to deter extraction of encryption keys in hardware accelerators [4]. Similarly, authors have shown that by performing unconstrained overclocking/under-volting, faults could be injected during encryption to recover the secret key [5]. We experimentally demonstrate (on a Snapdragon 820 development board) DVFS as a source of information leakage in software and utilize supervised machine learning (ML) based classification models to exploit the relationship between time-varying EM-emissions and DVFS states with an application's characteristics to identify applications running on the processor. Altogether, we profile legitimate applications in order to protect against untrusted application that can infer activities on a device through eavesdropping software events by hiding in the background

3 Attack Model

We will demonstrate simultaneous acquisition of both EM signatures as well as DVFS states. EM side channel emissions from Snapdragon 820 development board are acquired with beehive EMC probes (large loop area – 0.85") and a high bandwidth – 1GHz Picoscope, which samples the analog/digital signals and transfers it to a PC where the signatures are displayed. DVFS states are polled from two binary executables (one for each core) loaded onto the Snapdragon processor using an Android Debug Interface (ADB). A Trigger signal generated by an Arduino is used to synchronize EM and DVFS measurements. The Trigger signal is sent to the PC to initiate the application to profile. Once the application is triggered, the DVFS monitoring script logs the frequency states and time stamps for an observation period of 10s. At the end of 10s, the logged data is retrieved through the ADB debug interface to generate the DVFS signature.

This is followed by pre-processing steps and Machine Learning training and inference steps. We have performed the dimensionality reduction (windowed PCA) on the gathered dataset in pre-processing step. Features are extracted from each window to form reduced dimensional feature vector. We have utilized both time-domain and frequency domain features for classifying applications. We chose supervised learning models (KNN, SVM and RF) to train the models based on extracted features, and finally perform inference at test time to find applications executing on device

4 Experimental Results

We will show classification accuracies with different ML models for both EM and DVFS signatures study the latency associated with detecting an application with DVFS signatures and compare that with EM based detection. The analysis following trace acquisition, involving post-processing on captures traces, training and inference is implemented in python environment. EM and DVFS signatures, classification accuracies and detection plots will be displayed on UNIX based GUI. We will also prepare a video describing the measurement setup and signature acquisition in our lab environment in case there of any problems during demo session and explain the results with poster.

5 Key Observations and Outcomes

Applications running on a Snapdragon 820 processor can be identified using EM side channel and DVFS information. In general, DVFS provide a less complex path for identifying applications with high accuracy and lesser time to detection in comparison to EM side channel which is compute intensive and prone to measurement noise. We showed 100% accuracy and 700ms to detect all applications in the explored dataset.

6 List of Equipment

List of the equipment required for demonstration is listed here: 1) Snapdragon 820 development board, 2) EM-probe 3) Picoscope for signal acquisition, 4) Personal computer for processing, 5) Power supplies – through USB cables 6) Monitor to display the waveforms and analysis results.

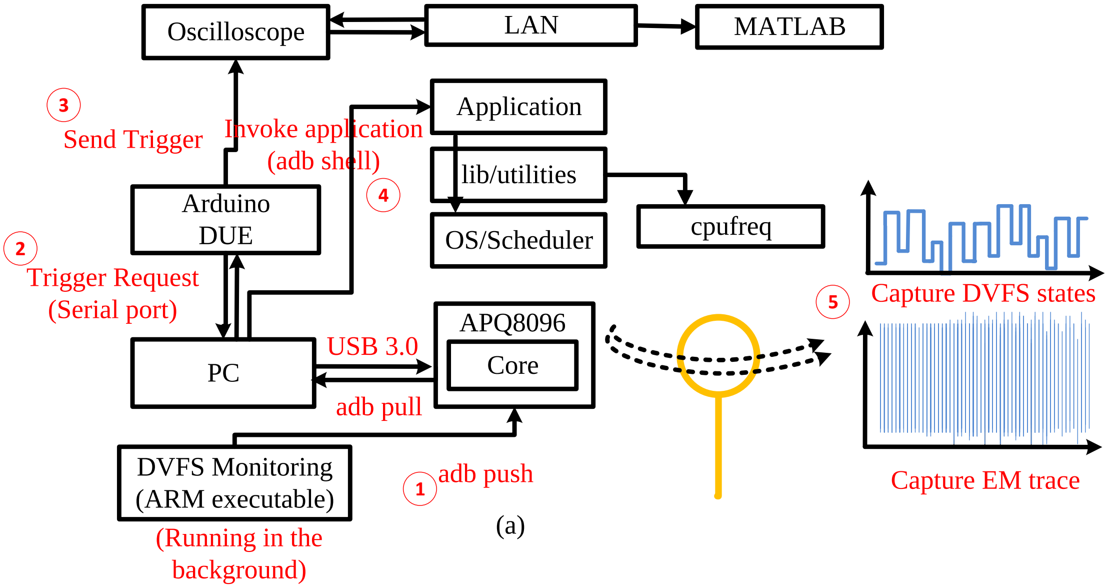

Fig.1 Measurement Setup details to acquisition of DVFS and EM-signatures

7 References

[1] *N. Chawla, A. Singh, M. Kar and S. Mukhopadhyay, "Application Inference using ML based Side Channel Analysis", in 2019 International Joint Conference on Neural Networks (IJCNN) [Submitted]*

[2] *S. S. Clark, B. Ransford, A. Rahmati, S. Guineau, J. Sorber, K. Fu, and W. Xu, "Wattsupdoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices," in Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies ser. HealthTech'13. Berkeley, CA, USA*

[3] *S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," in Design, Automation and Test in Europe, March 2005, pp. 64–69 Vol. 3.*

[4] *A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Improved power/em side-channel attack resistance of 128-bit aes engines with random fast voltage dithering," IEEE Journal of Solid-State Circuits, pp. 1–15, 2018.*

[5] *A. Tang, S. Sethumadhavan, and S. Stolfo, "Clkscrew: Exposing the perils of security-oblivious energy management," in Proceedings of the 26th USENIX Conference on Security Symposium, ser. SEC'17. Berkeley, CA, USA: USENIX Association, 2017, pp. 1057–1074. [Online]. Available: http://dl.acm.org/citation.cfm?id=3241189.3241272*