SPOILD: Side-channel POwer-based Instruction-Level Disassembler

Fahim Rahman, Jungmin Park, Xiaolin Xu, Domenic Forte and Mark Tehranipoor
Florida Institute for Cybersecurity Research
University of Florida, Gainesville, Florida 32611
Email: {fahim034, jungminpark}@ufl.edu, {xiaolinxu, dforte, tehranipoor}@ece.ufl.edu

I. Introduction

Most consumer electronics has turned digital, which greatly favored the connection worldwide, but also inherited all the problems of the digital world, especially the security vulnerabilities. In the networked world of 1990's and onwards, cyber-attacks were limited only to networked systems and devices. In the modern consumer electronics landscape, physical side-channel attacks have appeared as a new threat, which are not mounted through the interfaces of Internet. Side-channel attacks can extract private data hosted by these devices, and therefore, such secret data leakage compromises private keys embedded within a device. This can, in turn, either violate access rights within an embedded device -by unauthorized firmware upgrades or unauthorized content access, or it can allow for forged identities for networked devices. The problem is exacerbated for IoT class consumer electronics devices that hold sensitive private information. Side-channel vulnerabilities are especially pronounced for this class of devices. The secret data leakage through power side-channel has been studied quite extensively over the last decade. An emerging threat, however, is assembly level disassembly solely through power side channel. This disassembler can be used to obtain a copy of protected firmware or software as well as secret data by an adversary. In the defense point of view, it can be also exploited to check whether the malicious code is inserted in your system or whether the code in the competitor's system is copied from your code.

Instruction level disassembly or program level reverse engineering solely through power side channel is relatively new. It is more difficult than the private data leakage, this is because an instruction from the program executes only once per execution path. Hence, the adversary has little time to make the match. S/he does not have the chance to repeat thousands of experiments to deduce the secret data. Moreover, the adversary instruction level classifier or distinguisher only has as much time to classify as the processor's throughput. If a processor executes 4 instructions every clock cycle at 3 GHz, the distinguisher only has approximately 0.08 nano-seconds per instruction. The secret data distinguisher is often viewed as an off-line activity since the data is not going anywhere.

In this proposal, we demonstrate power side-channel based disassembler of AVR micro-controller using hierarchical quadratic discriminant analysis (QDA) classifier and neural network classifier. We believe that our method can be a starting point to disassemble recent embedded micro-controllers. Our accomplishment includes estimating which registers are used and what value the registers have as well as which instructions are being executed.

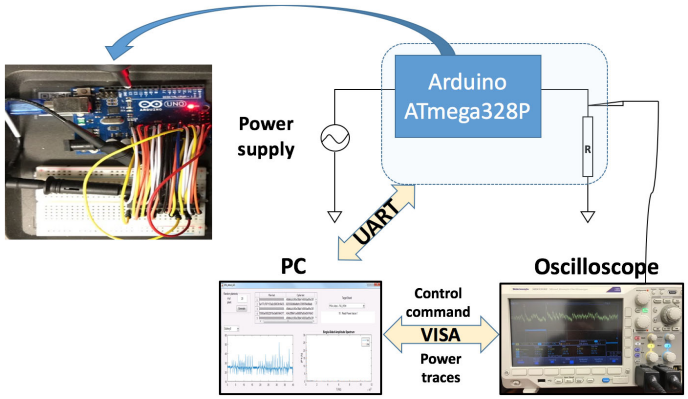

Fig. 1. Demonstration Setup

II. Demonstration Setup

The target device of our SPOILD work is an Arduino Uno based on ATmega328P micro-controller which has 2 pipeline stages with a clock frequency of 16 MHz. In our experiment, a Tektronix MDO3102 is used to sample power traces between a 330 Ω shunt resistor connected to the ground pin. The sampling rate is 2.5 GS/s and the bandwidth is 20 MHz. A PC is used to control the target device and oscilloscope, to store measured power traces and to profile and classify those traces. The PC and the target device are connected through UART and the PC communicates with the oscilloscope through VISA (Virtual Instrument Software Architecture) protocol. Fig. 1 shows our demonstration setup. The profiling or training about instructions, used registers and operands is pre-executed. Based on the profiled data, measured power signatures during program execution are translated into assembly codes simultaneously. The assembly code is shown as the result.

We developed a software tool for getting, profiling and classifying power traces as well as communication with an oscilloscope and the target device using MATLAB. This software tool can be used for disassembling other target devices.