Chapter 13
Side-Channel Attacks in the Internet of Things: Threats and Challenges

Andreas Zankl
Fraunhofer AISEC, Germany

Hermann Seuschek
Technical University of Munich, Germany

Gorka Irazoqui
Nagravision, Spain

Berk Gulmezoglu
Worcester Polytechnic Institute, USA

ABSTRACT

The Internet of Things (IoT) rapidly closes the gap between the virtual and the physical world. As more and more information is processed through this expanding network, the security of IoT devices and backend services is increasingly important. Yet, side-channel attacks pose a significant threat to systems in practice, as the microarchitectures of processors, their power consumption, and electromagnetic emanation reveal sensitive information to adversaries. This chapter provides an extensive overview of previous attack literature. It illustrates that microarchitectural attacks can compromise the entire IoT ecosystem: from devices in the field to servers in the backend. A subsequent discussion illustrates that many of today's security mechanisms integrated in modern processors are in fact vulnerable to the previously outlined attacks. In conclusion to these observations, new countermeasures are needed that effectively defend against both microarchitectural and power/EM based side-channel attacks.

DOI: 10.4018/978-1-5225-2845-6.ch013

INTRODUCTION

Currently, we experience exciting times for the advancement of computing technology. Driven by ubiquitous connectivity, miniaturization of devices, and new developments in sensor technology, the gap between the virtual and the physical world is rapidly closing in what is known today as the Internet of Things (IoT). Devices that operate as part of the IoT must often meet strict requirements regarding energy consumption, complexity, and cost per unit. While computational resources and performance are often limited, many IoT ecosystems deploy backend servers that collect information for in-depth analysis, advanced customer services, or feedback to actuators in the field. While this symbiosis of smart devices and backend systems enables innovative business models, it also raises concerns over the privacy of data and the security of the devices processing it. Among the most critical components in this ecosystem are the main processing units. Due to an ever-growing number of transistors, processor designers are able to implement sophisticated mechanisms that continuously improve performance for every product generation. However, the secure execution of sensitive applications can often not be assured when these performance enhancements are active. This is because execution properties, e.g. the program runtime or the accompanying power consumption, heavily depend on the specific data and instructions that are processed. Anyone that observes the execution can therefore infer what is being processed. For security applications, this eventually means that confidential information is leaked to outside observers. Such information leaks are generally studied in the area of side-channel attacks, a subset of which will be addressed in this chapter. In literature, the field of *microarchitectural attacks* (Acıiçmez & Koç, 2009) studies how the properties of a processor's instruction set implementation affect the security and privacy of executed applications. Typical targets are resources shared by processor cores or execution threads, such as caches, branch prediction and shared functional units like arithmetic logic units (ALUs). By observing, manipulating or competing for these shared resources, adversaries can learn critical details of programs running on the processor. This can quickly become a serious issue when multiple customers share a backend system or when multiple applications are running concurrently on an IoT device. If one customer has malicious intents or if one application is compromised, the security of everyone else is suddenly at stake. In addition, IoT devices face another threat. Since they are deployed in great numbers, it is feasible in many cases to get physical access to them. This enables an adversary to exploit yet another type of side-channel. With the appropriate measurement equipment, it is possible to observe the power consumption and the closely related electromagnetic (EM) emanation of a device, while it is working on a task. In literature, the fields of *power analysis* (Kocher et al., 1999; Mangard et al., 2008) and *electromagnetic analysis* (Quisquater et al., 2001; Gandolfi et al., 2001) study physical properties of devices to learn about their inner workings and to infer the information processed by them. Due to the implementation of modern electronics, the power consumption varies depending on the data that is being processed. This inevitably leaks information to adversaries observing the power and EM side-channels of the device.

In response to these threats, this chapter gives a comprehensive overview of state of the art literature in the field of microarchitectural attacks. In addition, it outlines the capabilities of power and EM based attacks, and shows how they might be combined with microarchitectural observations to derive new threats once physical access to IoT devices is obtained. After establishing the state of the art, a selection of security features on modern processors and their utility against the previously described attacks is discussed. In particular, trusted execution environments are described, which are used to encapsulate security critical computations in enclaves that are separated from the rest of the system with the help