Chapter 12
Analysis of Cyber Attack on Processor Architecture Through Exploiting Vulnerabilities

L. K. Hema
Aarupadai Veedu Institute of Technology, India & Vinayaka Mission's Research Foundation, India

Rajat Kumar Dwibedi
Aarupadai Veedu Institute of Technology, India

S. Regilan
Aarupadai Veedu Institute of Technology, India

Dheenadhayalan K.
Aarupadai Veedu Institute of Technology, India

Kommera Vinay Kumar
Aarupadai Veedu Institute of Technology, India

Survi Satish Kumar
Aarupadai Veedu Institute of Technology, India

ABSTRACT

A computer exploit exploits a system vulnerability to attack processor architectures including ARM, AMD, and Intel. The main CPU architectures nowadays are 32-bit (x86) and 64-bit (x86-64, IA64, and AMD64). Processor data route width, integer size, and memory address width vary per architecture. The chapter exploits processor architecture flaws. This study examines ARM and INTEL processor vulnerabilities. Modern processors like Intel, AMD, and ARM are vulnerable to Spectre. A malicious application can read data from an inaccessible area by breaking inter-process and intra-process isolation. Hardware and software protection prevents such access (for inter-process isolation). CPU architecture has a weakness that allows bypassing defences. The hardware fault makes it tough to rectify without replacing the CPUs. Spectre is a breed of CPU design vulnerability. Security education benefits from them and the Meltdown issue. In this chapter, the authors executed Spectre and Meltdown on ARM and INTEL processors to explore their vulnerabilities. The ARM processor was not vulnerable because the chip was patched, but the INTEL processor was vulnerable and retrieved the information.

DOI: 10.4018/979-8-3693-1355-8.ch012

INTRODUCTION

An unsuccessful attempt to obtain illegal access to a computer, computing system, or computer network that is connected to the internet in order to do damage is referred to as a cyber-attack. Computer systems can be disabled, disrupted, or controlled by cyberattacks, or the data that is stored within the systems can be altered, blocked, deleted, manipulated, or stolen without permission (Genkin et al. 2014; 2016a). The launch of a cyberattack can come from any location and be carried out by any individual or organisation using any number of different attacks. Cybercriminals and hackers are the terms that are most commonly used to describe individuals who carry out cyberattacks (Albert et al., 2023). These individuals include those who have carried out a single attack on their own, leveraging on their knowledge of computers to create and carry out malicious attacks (Buragadda et al., 2022). When it comes to information technology, a vulnerability is a flaw that an attacker can take advantage of in order to carry out a successful attack (Chakravarthi & Venkatesan, 2015a). As a result of defects, features, or human error, they can occur, and attackers will attempt to exploit any of these vulnerabilities, frequently combining one or more of them in order to accomplish their ultimate objective (Chakravarthi & Venkatesan, 2015b).

Additionally, cyberattacks have been launched by organisations of computer specialists that are funded by the government (Cristian Laverde Albarracín et al., 2023). At the same time that they have been identified as nation-state attackers, they have also been accused of attacking the information technology (IT) field infrastructure of other governments and nongovernment entities, such as businesses and nonprofit organisations, which are also working to secure the data and utilities (Khan & Altayar, 2021). Cyberattacks are intentionally planned to inflict damage to a system. The advanced silicon chips, which are available in small form, are gadgets that are designed and developed by people and are complex but accurate technology. In addition to memory modules and interfacing circuitry, it houses the CPU that has a higher performance potential (Ganesh et al., 2016). The bulky supercomputers that cost approximately ten to fifteen million dollars twenty years ago have been rendered obsolete by these sophisticated CPUs (Jain et al., 2022). On the other hand, the processors that are utilised in embedded applications, such as mobile phones, personal computers, personal digital assistants, and Internet of Things devices, are more powerful in terms of performance and ergonomics (Gras et al.,2017).

It is possible for the processors to carry out the task that has been allocated to them by sequentially executing arithmetic, logic, and control instructions. Instruction Set Architecture is the name given to both the instruction and the byte-level encoding of the instruction. A variety of processors, including ARM, Intel, AMD, and IA32, among others (Alzubi et al., 2023). A programme that was compiled in one type of system will not be able to operate in another type of system since these processors have their own distinct instruction sets (ISAs) (Oak et al., 2019). On the other hand, distinct processors of varying models are developed by each manufacturer in response to the various technical breakthroughs and the requirements of the market (Rao et al., 2023) and also ISA32 is an example of this kind. A conceptual layer of abstraction is made possible by this ISA for the developers of the compiler (Prasanth et al., 2023). These developers will be aware of which instructions are allowed to run in different models, as well as the encoding techniques and other related information (Sholiyi et al., 2017). Furthermore, the designers will construct the machines that are responsible for carrying out the numerous instructions (Al-Najdawi et al., 2016).

This perspective will assist us in gaining a deeper comprehension of the inner workings of computers as well as the technological obstacles that are faced by computer manufacturers (Sudheer et al., 2015). There is a significant difference between the model of computation that is implied by the ISA and the