The Rise of Hardware Security in Computer Architectures

Patrick Schaumont, Virginia Polytechnic Institute and State University
Paolo Montuschi, Polytechnic University of Turin

This installment of Computer’s series highlighting the work published in IEEE Computer Society journals comes from IEEE Transactions on Computers.

Computing systems have become truly pervasive, up to serving as alter-egos for their human owners. They control critical aspects of our life and act as data repositories for everything important to us. And this trend is only accelerating: smart assistants tend to our every need—from turning on the television to ordering groceries—and in the cloud, data aggregation leads to improved analysis and, ultimately, decisions that benefit both society and the individual.

These exciting computing innovations have spawned equally exciting technical problems. The research community has already made great strides toward low power and energy, increased reliability, usability, and performance. Among the technical factors, security still stands out as a top priority. Security’s basic issues are well known: How can we protect personal user data? How can we protect user privacy? How can we guarantee fair and consistent service of computing resources to their users? The recently introduced General Data Protection Regulation (GDPR; www.eugdpr.org) is dramatically changing the scenario by clearly stating roles, rules, and responsibilities. It’s now a matter of fact that we need (certified) secure computing systems.

A fundamental principle of execution in computer architectures is to keep applications isolated from each other and the underlying software environment and operating systems. That isolation is provided through hardware-supported techniques such as privilege levels, virtual memory, sandboxes, and secure containers. In practical architectures, the isolation is virtual, and doesn’t extend into the computer hardware. Hence, software applications still share the same physical memory chips, processor, and communication buses.

Computer security is built on the isolation provided by computer architectures. Indeed, the best way to maintain confidentiality and integrity of an application’s secure data is to ensure that the data is unreachable by anyone but the application itself. To understand how effective isolation is in its support of computer security, one must consider the attacker’s abilities, or the attacker model.
We distinguish three attacker models, but current computer isolation techniques are only effective against two of them (see Figure 1). The first model, the input/output attacker, is based on manipulation of the input data to the application. This attacker is responsible for a vast body of computer exploits, including, for example, stack buffer overflows and cross-site scripting attacks. The second model, the memory attacker, coexists in the same physical memory space as the secure application. This attacker aims to snoop or manipulate directly into the memory space of the application. The third model, the hardware attacker, can observe and manipulate the physics of the computations performed in hardware. This attacker exploits side-channel leakage or intentional fault injection to circumvent privileges and isolation boundaries in the hardware.

The hardware attacker model is an enormous challenge to the future of computer security. Computer architectures have traditionally been developed using logical abstractions, and are optimized to execute software applications as quickly and as efficiently as possible. They deploy a wide array of techniques to make the most likely case execute the fastest. These techniques might include cache memory, memory hierarchies, branch prediction, and translation lookaside buffers. All of these optimization techniques are transparent to the input/output attacker model and the memory attacker model. However, they are visible to the hardware attacker, and have become the source of a novel family of attacks, including the Meltdown and Spectre attacks disclosed earlier this year.

IEEE Transactions on Computers (TC) is committed to publishing the latest research on innovations and countermeasures in hardware security within the context of secure computer architectures. A 2018 special section collected recent results and findings in this field. Dealing with the hardware attacker will require revisiting some of the basic design assumptions in the field.

The first assumption is that the hardware architecture of computers might require a deep understanding of isolation and attestation of applications at the hardware level. A rich design space of solutions affects the broad domain of computer architectures, from embedded cores to mainstream processors.1 A second assumption is that we might need to revise computing mechanisms itself, developing computing methods that enable the use of computer architectures that might not be fully trusted. Such solutions would integrate cryptographic techniques with computing such that secure data remains protected at all times.2 A third assumption is that processor hardware might need to be revised so that it deals with the hardware attacker at the lowest level possible by eliminating harmful observation or manipulation of the physics of computing.3

IEEE Transactions on Computers (TC) will closely follow these exciting developments in secure computer architectures with the latest academic and industry research. Please stay tuned for upcoming issues to keep current on this topic, as well as computing architectures, memory technologies, real-time systems, and much more. [ ]

REFERENCES