Race to the bottom: Malicious Hardware

Angelos D. Keromytis Simha Sethumadhavan Ken Shepard
Columbia University in the City of New York
angelos@cs.columbia.edu simha@cs.columbia.edu shepard@ee.columbia.edu

Increasingly, hardware design and fabrication has come to resemble that of software: hardware logic modules (resembling software libraries) are licensed from third parties and combined in designs of greater complexity, while the fabrication is outsourced to a low-cost manufacturer or otherwise off-shored.

While this new way of constructing hardware has brought great benefits in terms of design reuse, rapid development and prototyping, and lower component and product costs, it has also introduced new vulnerabilities for high-value or sensitive users of such technologies. In particular, a sufficiently motivated adversary (or a disgruntled employee) can introduce backdoors (*Hardware Easter Eggs*, or HEEs) during the hardware design or fabrication phases. For instance, a hardware designer, by changing less than ten lines of Verilog code, can easily modify an on-chip memory controller to send data items it receives to a shadow address in addition to the original address. Such HEEs can be used in attacking confidentiality (*e.g.,* by exfiltrating sensitive information), integrity (*e.g.,* by disabling security checks such as memory protection), and availability (*e.g.,* by shutting down the component based on a timer or an external signal). HEEs cannot be detected using standard state-of-the-art pre-fabrication testing techniques because the attacker is likely to delay enabling or opening the backdoors until after deployment using simple control circuits. It is even possible to create low-gate-count general-purpose HEEs that can be leveraged by attackers to launch a variety of powerful attacks against the system.

Because hardware components (including embedded HEEs) are architecturally positioned at the lowest layer of a computational device, it is very difficult to detect attacks launched or assisted by those components: it is theoretically impossible to do so at a higher layer, *e.g.,* at the operating system or application, and there is little functionality available in current processors and motherboards to detect such misbehavior. The state of practice is to ensure that hardware comes from a trusted source and is maintained by trusted personnel: a virtual impossibility, given current design and manufacturing realities. In rare circumstances, when volumes are relatively low and the risk is high, physical inspection and verification of the hardware may be conducted. Such inspection is destructive, costly, and time-consuming, and thus can only be applied in few cases and for a small number of samples.

Establishing trust in the hardware components underlying all modern IT will likely prove a key future challenge for the security and hardware design communities. While HEE-based attacks are virtually unheard of to date, economic, technological, and social drivers make these attacks more likely than ever before, while the potential damage from such an attack is extremely high: shutting down an hypothetical adversary's cyber-infrastructure (or "just" a significant or sensitive part of it) in the event of an armed conflict or during a period of diplomatic tensions can be an effective and cheap way of forcing the outcome.

Addressing the problem requires a concerted, long-term effort in physical design and manufacturing methodologies, secure and trusted fabrication practices and operations, post-fabrication testing and verification techniques, and runtime HEE detection and mitigation. The problem domain represents both challenges (in terms of the physical parameters, low-level of abstraction, ease of implementing certain catastrophic attacks, and lack of access to IC internal state) and opportunities (the IC's interface to the rest of the environment is limited and can be completely controlled). We believe that a combination of techniques, combined with updated manufacturing practices, can help mitigate the risks at acceptable cost, both in terms of research expenditures and manufacturing/operational practices.