Chapter 16
Conclusion and Future Work

Swarup Bhunia and Mark M. Tehranipoor

Hardware Trojan horse or hardware Trojan attacks have been the subject of active research for the past decade. The scope of this research has broadened over time – with the possibility of malicious hardware modification extending to different stages of integrated circuit's life cycle (from IP to microchips) as well as to different levels of hardware abstractions (from microchips to printed circuit boards). It now represents a new branch of hardware security. Security concerns caused by hardware Trojans are relevant to various parties involved in the life cycle of electronic hardware – from system-on-chip designer to original equipment manufacturers (OEMs) to end users. The fact that the electronic hardware is subject to malicious alterations is an intriguing departure from conventional wisdom, which assumes that hardware is hard to compromise, is fundamentally more secure and trustworthy than its software counterparts, and hence can be used as trust anchors or "root of trust" for diverse computing and communication systems.

Over the past decades, research on hardware Trojan has followed one of the two broad tracks: (1) exploration of the threat models and attack modalities and (2) approaches to deal with the attacks at different levels. The first track has focused on discovering how hardware can be modified for malicious purpose at different stages of hardware manufacturing process and how different payload can be implemented to satisfy multitude of attack objectives. The second track has focused on countermeasures, which fall into two classes: (1) hardware trust verification and (2) "design-for-security" (DfS) solutions. The problem of hardware Trojan is rapidly creating a new field of *hardware trust verification*, which aims at analyzing a hardware – either IP or chip or PCB – to verify its trustworthiness with respect to malicious design artifacts. The first class of countermeasure comprises of wide-ranging hardware trust verification solutions, which include targeted functional test,

S. Bhunia (✉) • M.M. Tehranipoor
Department of Electrical & Computer Engineering, University of Florida, Gainesville, FL, USA
e-mail: swarup@ece.ufl.edu; tehranipoor@ece.ufl.edu

S. Bhunia, M.M. Tehranipoor (eds.), *The Hardware Trojan War*,
https://doi.org/10.1007/978-3-319-68511-3_16

statistical test, and formal verification approaches. The second class, on the other hand, follows a preemptive approach where protection against Trojan attacks is built into a design before the hardware is fabricated. Such solutions can try to "harden" a design making malicious implantation difficult or infeasible, or make trust verification easier, or allow online monitoring of Trojan activation to detect and/or tolerate Trojan effect during field operation. In particular, design techniques for *Trojan resilience* or *Trojan tolerance* (similar to the concept of fault tolerance) during field operation usher in a promising new direction of Trojan research.

The book has tried to capture all these aspects of hardware Trojan research over the past decade (2007–2017) in a collection of chapters contributed by prominent researchers and practitioners in this field. The chapters try to cover the spectrum of vulnerabilities of modern electronic hardware in terms of Trojan attacks as well as the whole gamut of possible protection approaches. We hope the chapters would collectively serve as a comprehensive resource on hardware Trojan attacks and would provide researchers, students, and practitioners with fundamentals of hardware Trojan attacks. We are glad to be able to collect these high-quality chapter contributions to produce the first book of this kind that includes compendium of materials on this important topic in the field of hardware security.

Over the past decade, Trojan attacks and hardware trust assurance have primarily been of interest to the Department of Defense. This is due to the potential for catastrophic consequence caused by hardware infected with malicious implantation in diverse military applications. Untrusted hardware has emerged as serious concerns for our national security. Such concerns are aggravated by rapidly diminishing control over microelectronic design and fabrication cycle and a complex distributed supply chain for electronics which involves multiple untrusted parties. The relative ease of cloning modern chips and PCBs allows an adversary to incorporate cloned chips with embedded malicious circuits into a supply chain. Recent reports show that cloning of chips adds a new and critical dimension to the hardware trust issue. It is extremely challenging for a system integrator (e.g., OEM) to verify trust of chips acquired from a supply chain primarily due to the lack of golden chip instances or reference designs. Trust verification of electronic components acquired from a supply chain will remain a critical problem and an area of active research in the foreseeable future. Such a problem may trigger key innovations in hardware trust verification fundamentally different from the scenario where a chip designer tries to verify the trust of chips fabricated in an untrusted foundry. In the latter case, the chip designer would have access to the entire design and knowledge of its expected functional/parametric behavior.

The issue of hardware trust is, however, gradually being accepted as a problem of growing significance in the mainstream semiconductor industry. Malicious implants of different forms, e.g., design modifications in untrusted IPs that may leak secret information, are being considered to be a valid concern for the system-on-chip designers. We expect to see increasing emphasis in research and development activities related to hardware Trojan from the major chip design and electronic design automation companies in the coming years.

16.1 Future Work

While the book covers well prior and ongoing research activities in this area, we hope it would stimulate new research explorations in many directions. In particular, it is expected to create new research pathways on the following topics:

1. More Complex Attacks

Research on mounting complex and powerful attacks on a computing system enabled by malicious hardware modification is expected to remain an active research topic. Clever hardware modification that can be leveraged by software or data during field operation needs to be investigated and appropriate countermeasures developed. Such modifications can lead to leaking secret information from inside a hardware unit or cause malfunction, possibly at an adversary-controlled time. Hardware modification can also be studied for its effectiveness in mounting different forms of physical attacks, including side-channel attacks – e.g., fault injection attacks, where a Trojan can facilitate key leakage through fault injection. Finally, a Trojan can be implemented that exploits the collusion across multiple parties – e.g., a rogue physical designer in the design house and an adversary in the foundry. Such Trojans can be significantly more difficult to detect with post-silicon test since they may alter functional or parametric behavior of a design under a very rare operating condition unlikely to be activated during test.

2. Automatic Vulnerability Analysis

There is a growing need to develop CAD tools to automatically analyze a design with respect to its trustworthiness or its vulnerability for malicious modifications. The first tool will be important for evaluating trustworthiness for untrusted IPs that are integrated into an SoC. Such a tool would help us to understand possible malicious behavior of an IP with respect to known Trojan models, before it is used by a SoC designer. Note that it is possible that in addition to deliberate malicious alterations, apparently benign nonfunctional design artifacts, such as design-for-test (DFT) or design-for-debug (DFD) infrastructure, can be exploited by an attacker for malicious intent, such as information leakage. An automatic vulnerability analysis tool should ideally catch these issues too. The second tool is important to analyze how vulnerable a design is with respect to malicious modification in a foundry. It should highlight the components or regions of a design which are more vulnerable than others. There will be a growing need for such automatic analysis tools with increasing reliance of chip designers on third-party IP blocks and growing trust concerns in the chip manufacturing process.

3. Metrics and Benchmarks

Associated with the CAD tools, new research is needed to develop trust metrics and benchmarks for different hardware abstraction levels. For example, ways to quantify trust for hardware IP blocks would involve a number of important research

questions – e.g., (1) what structures can be considered untrusted, (2) what functional behavior of the IP or components of an IP (e.g., the arithmetic logic unit of a processor) can raise trust issues, and (3) can we come up with a set of well-defined properties which can be checked for an IP and the results can be used for trust quantification? A trust metric needs to consider all aspects of trust evaluation to come up with an aggregate trust value. Similarly, there will be growing demand for trust benchmarks to evaluate trust verification or trusted design solutions. While there have been some prominent efforts in this regard, further research is needed to augment the benchmark suites with respect to emerging attack modalities and to cover various hardware abstractions.

4. Trust Verification

It is well accepted that a "silver bullet" solution which can reliably protect against Trojan attacks of all types, forms, and sizes is extremely difficult to achieve. Effective trust verification which can provide high confidence against diverse trust issues would remain to be an active research. Trust verification through logic testing and side-channel analysis has been extensively investigated. The book has dedicated chapters that elaborate on these solutions. However, the current solutions are often effective for very specific types of Trojan or have unrealistic assumptions. Further, golden-free trust verification problem has not received adequate attention from the research community. There is a clear need for significant new research in this area.

5. Design-for-Security (DfS) Approaches

While trust verification solutions are attractive since they do not incur hardware or design overhead and can work for legacy components, they suffer from limited effectiveness and fail to provide complete trust assurance. Trust verification solutions can provide much higher confidence if combined with commensurate design solutions. Trust-aware design approaches try to make Trojan insertion difficult, i.e., effectively "harden" a design, and/or make a Trojan easy to activate/observe. Low-overhead design solutions which are amenable for automation and provide significant benefit in trust assurance are expected to remain attractive research topic in both academia and industry.

6. Trojan Attacks in Nanoscale Devices

Continuous scaling of CMOS technology has brought us to sub-10 nm technology regime, where new nanoscale devices with interesting switching characteristics have emerged. These devices often exploit unique material properties and introduce fundamentally new device structure or state variables (e.g., spins of electrons, mechanical state of a cantilever, or resistive state of a solid dielectric material). They exhibit promising behavior in many aspects – e.g., performance, power, nonvolatility, reliability, manufacturability, and integration density. The operating principles of nanoscale devices are also expected to modify the concepts of hardware Trojans. For example, the current in nanoscale transistors strongly depends on the channel stress, which can be modified through changes in the process steps or even small layout changes. The more challenging problems will be reliability

Trojans where malicious changes are engineered to radically accelerate the device aging process. Similar Trojans are possible in non-charge-based devices, e.g., by marginally modulating spin polarization, or magnetic tunnel junction (MTJ) resistance. Future research is expected to focus on exploring Trojan attacks for nanoscale devices and Trojan-resilient design approaches for these devices.