COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

TIMOTHY TRIPPEL

Developing Trustworthy Hardware with Security-Driven Design & Verification

Thursday, April 29, 2021
10:00 AM
Virtual (Passcode: 735562)

ABSTRACT: Over the past several decades, computing hardware has evolved to become smaller, yet more performant and energy-efficient. Unfortunately these advancements have come at a cost of increased complexity, both physically and functionally. Physically, the nanometer-scale transistors used to construct Integrated Circuits (ICs), have become astronomically expensive to fabricate. Functionally, ICs have become increasingly dense and feature rich to optimize application-specific tasks. To cope with these trends, IC designers outsource both fabrication and portions of Register-Transfer Level (RTL) design. Outsourcing, combined with the increased complexity of modern ICs, presents a security risk: we must trust our ICs have been designed and fabricated to specification, i.e., they do not contain any hardware Trojans.

Working in a bottom-up fashion, I initially study the threat of outsourcing fabrication. While prior work demonstrates fabrication-time attacks (modifications) on IC layouts, it is unclear what makes a layout vulnerable to attack. To answer this, in my IC Attack Surface (ICAS) work, I develop a framework that quantifies the security of IC layouts. Using ICAS, I show that modern ICs leave a plethora of both placement and routing resources available for attackers to exploit. Next, to plug these gaps, I construct the first routing-centric defense (T-TER) against fabrication-time Trojans. T-TER wraps security-critical interconnects in IC layouts with tamper-evident guard wires to prevent foundry-side attackers from modifying a design.

After hardening layouts against fabrication-time attacks, outsourced designs become the most critical threat. To address this, I develop a dynamic verification technique (Bomberman) to vet untrusted third-party RTL hardware for Ticking Timebomb Trojans (TTTs). By targeting a specific type of Trojan behavior, Bomberman does not suffer from false negatives (missed TTTs), and therefore systematically reduces the overall design-time attack surface. Lastly, to generalize the Bomberman approach to automatically discover other behaviorally-defined classes of malicious logic, I adapt coverage-guided software fuzzers to the RTL verification domain. Leveraging software fuzzers for RTL verification enables IC design engineers to optimize test coverage of third-party designs without intimate implementation knowledge. Overall, this dissertation aims to make security a first-class design objective, alongside power, performance, and area, throughout the hardware development process.

CO-CHAIRS: Profs. Kang G. Shin and Matthew Hicks