Notice and Invitation

Oral Defense of Doctoral Dissertation
The Volgenau School of Engineering, George Mason University

Rakibul Hassan
Bachelor of Science, Ahsanullah University of Science and Technology, 2016

Securing Embedded Systems: from Device Level to Network Level

Wednesday, May 31, 2023, 10:00 am - 11:30 am
ENGR 3507
All are invited to attend.

Committee

Dr. Sai Manoj Pudukotai Dinakarrao, Chair
Dr. Khaled N. Khasawneh
Dr. Brian L. Mark
Dr. Haiying Shen

Abstract

In recent years, ICs have suffered multi-dimensional security challenges from design to network/application stages. For example, Rouge employees in an untrusted foundry may modify ICs and insert Hardware Trojans, and locked ICs (in terms of logic-locked key gates) suffer from SAT-based attacks. In addition, while deployed as IoT devices, these ICs face severe security challenges against malware attacks. In this dissertation, we propose a bottom-up solution to protect ICs from the design phase to the network phase.

In the design phase, Hardware Trojans (HTs) pose a critical security threat to modern integrated circuits (ICs) through malicious activities, including leaking critical information, executing unauthorized commands, and reducing IC lifetime. To address this challenge, we propose an IC design-aware Trojan detection approach that extracts different structural features and behavioral information to achieve a detection accuracy of 98%. In addition, to defend against the multiple state-of-the-art Boolean satisfiability (SAT) attacks, we propose a cognitive solution using a neural network-based SAT-hard clause translator called SATConda. Our proposed SATConda successfully defends against multiple state-of-the-art SAT attacks with minimal area and power overhead while preserving the original functionality.

Finally, we focus on the security challenges that modern ICs suffer while deployed as IoT devices. We propose a Trust Evaluation Framework with a dynamic access revocation technique to secure IoT devices in a distributed IoT network. Our proposed Trust Evaluation Framework successfully detects malicious activity at the node level with an average accuracy of about 98%, and dynamically takes measures like revoking read-only access or eliminating write access with about 95% accuracy based on that trust score.