Title

New frontiers in Security Verification: Fuzzing and Penetration Testing

Abstract

Modern Systems-on-Chips (SoCs) integrate numerous insecure intellectual properties to meet design-cost and time-to-market constraints. Incorporating these SoCs into security-critical systems severely threatens users' privacy. Traditional formal/simulation-based verification techniques detect vulnerabilities to some extent. However, these approaches face challenges in detecting unknown vulnerabilities and suffer from significant manual efforts, false alarms, low coverage, and scalability. Fuzzing and penetration techniques should be developed to mitigate pre-silicon hardware verification limitations. Nevertheless, these techniques suffer from major challenges such as slow simulation platforms, extensive design knowledge requirements, and lacking consideration of untrusted inter-module communications. In this talk, I will present an emulation-based hybrid framework by combining formal verification and fuzz/penetration testing, leveraging their own benefits to effectively detect security vulnerabilities in large SoCs.

Bio

Dr. Farimah Farahmandi is the endowed Wally Rhines Professor of Hardware Security, an Assistant Professor in the Department of Electrical and Computer Engineering (ECE) at the University of Florida, the Associate Director of both the Edaptive Computing Inc., Transition Center (ECI-TC) and the Florida Institute for Cybersecurity (FICS) at the University of Florida. Her research in hardware security verification, formal methods, fault-injection attack analysis, and post-silicon validation and debug has been sponsored by a wide range of companies and government agencies. For her work, she was recently awarded the ACM/IEEE DAC Under 40 Innovators Award (2024), the Service Excellence Award (2023) and the Research Excellence Award (2022) from the ECE department at UF, and the Young Faculty Award by SRC in 2022. She is also the recipient of the NSF Career Award.