COMPUTER SCIENCE and ENGINEERING

Software Systems Lab LECTURE

SRAM fingerprinting using power-up state minimum data retention voltages

Dan Holcomb
Postdoctoral Researcher
Unviersity of Michigan

Tuesday, October 22, 2013
12:00 pm – 1:00 pm
3725 BBB

Abstract: This talk will summarize two recent works in the area of SRAM fingerprinting. In the first part, he will discuss the use of SRAM power-up state as unique IC fingerprints, and show how these fingerprints can also be used as seeds for true random number generation. In the second part, he will discuss an approach for deriving the fingerprints from the minimum data retention voltage of each SRAM cell instead of the power up state. The data retention voltage is related to power-up state, but has the potential for more informative fingerprints, albeit at a higher measurement cost

Bio: Dan recently defended his PhD thesis "Formal Verification and Synthesis for Quality-of-Service in On-Chip Networks" under the advisorship of Prof. Sanjit Seshia at UC Berkeley. Dan has a background in circuits and design automation with an eye toward security, and worked several years at Intel on QoS of communication fabrics and mitigation of particle-strike induced errors. He previously earned a masters from UMass Amherst ECE with the thesis "Chip ID and True Random Number Generation" under the advisorship of Prof. Wayne Burleson (now Senior Fellow at AMD). Dan has researched PUF security technology based on SRAM remanence decay, and has published at USENIX Security, DAC, and DATE among others

COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY of MICHIGAN