Cyber Security Research and Education Institute (CSI)

ERIK JONSSON SCHOOL OF ENGINEERING & COMPUTER SCIENCE AT THE UNIVERSITY OF TEXAS AT DALLAS

2016 Distinguished Lecture Series

Towards Security Without Secrets

Dr. Srini Devadas
Massachusetts Institute of Technology

Wednesday, January 20th at 11:30am
TI Auditorium, ECSS 2.102

Physical Unclonable Functions (PUFs) are a promising new cryptographic primitive that leverage manufacturing variation to create unclonable secrets in embedded systems. In this case, the secret is no longer stored permanently in digital form, but rather as the physical properties of the manufactured chip. Further, the recent proposal of "Public Model Physical Unclonable Functions" (PPUFs) does not contain any secrets at all. Instead, PPUFs propose to use a constant-factor computational speedup to distinguish an unclonable hardware device from a digital simulation.

This talk presents a new computational fuzzy extractor and stateless PUF leveraging Learning Parity with Noise (LPN). This method improves over the state-of-the-art in extracting stable secrets from PUFs and has a clear security reduction to a well-accepted cryptographic assumption (LPN).

In addition, this talk proposes a formalism describing Public Model Physical Unclonable Functions based on ordinary differential equations (ODEs), a conjecture on the form of ODE integrators, and a formal reduction of PPUF security to this conjecture. This result is extended to compare analog and digital computing more generally. Finally, this talk provides direction for implementing a PPUF.

Srini Devadas is the Webster Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology (MIT) where he has been on the faculty since 1988. He served as Associate Head of the Department of Electrical Engineering and Computer Science, with responsibility for Computer Science, from 2005 to 2011.

Devadas's research interests span Computer-Aided Design (CAD), computer security and computer architecture and he has received significant awards from each discipline. In 2015, he received the ACM/IEEE A. Richard Newton Technical Impact award in Electronic Design Automation. He received the IEEE Computer Society Technical Achievement Award in 2014 for inventing Physical Unclonable Functions and single-chip secure processor architectures. Devadas's work on hardware information flow tracking published in the 2004 ASPLOS received the ASPLOS Most Influential Paper Award in 2014. His papers on analytical cache modeling and the Aegis single-chip secure processor were included as influential papers in "25 Years of the International Conference on Supercomputing." He is an IEEE and ACM Fellow.

Refreshments at 11:15am