CANCELLED: Run-time Accessible DRAM PUFs in Commodity Devices

Jakub Szefer
Yale University

1/26/2017 at 11:00 am
CoRE A 301

Abstract

Physically Unclonable Functions (PUF) are a unique and stable physical characteristics of a piece of hardware, which emerge due to variations in the fabrication processes. PUF can be considered a type of fingerprint that is unique to each device. PUFs are a promising cryptographic primitive, which can enable secure key storage, hardware-based device authentication and identification. Most PUF constructions presented by other researchers have required an addition of new hardware or special FPGA implementations for their operation. Recently, various researchers have investigated intrinsic PUFs that can be found in commodity devices. Unfortunately, most of the proposals are based on SRAM and suffer from the drawback that they can only be accessed at boot time of the system. This talk will present details of a new, run-time accessible PUF based on DRAM. The presented work leverages decay characteristics intrinsic to DRAM in commercial off-the-shelf systems. The DRAM decay-based PUF requires no additional hardware or use of special FPGA. One of the key advantages of the new PUF construction is that it can be queried during run-time of a Linux system. Furthermore, by exploiting different decay times of individual DRAM cells, the challenge-response space is increased. The new DRAM PUF is used in lightweight protocols for device authentication and secure channel establishment that will be presented in the talk as well. The talk will conclude with discussion of current research challenges and opportunities they present for further work on advancing DRAM PUFs.

Bio

Jakub Szefers research interests are at the intersection of computer architecture, system software and hardware security. His research focuses on secure hardware-software architectures for servers and mobile devices, virtualization and cloud security, hardware security verification, physically unclonable functions, and hardware FPGA implementation of cryptographic algorithms. His research is supported through National Science Foundation and industry donations. He joined Yale University in summer 2013 as an Assistant Professor of Electrical Engineering, where he started the Computer Architecture and Security Laboratory (CAS Lab). Prior to joining Yale, he received Ph.D. and M.A. degrees in Electrical Engineering from Princeton University and worked with Prof. Ruby B. Lee on secure hardware architectures. He received B.S. with highest honors in Electrical and Computer Engineering from University of Illinois at Urbana-Champaign.

Faculty Host: Abhishek Bhattacharjee