Department of
ELECTRICAL & COMPUTER ENGINEERING
George Washington University

ECE TALK

Exploiting and Mitigating Timing Channels in Microprocessors

Dr. Dmitry Ponomarev

Professor, Department of Computer Science at SUNY Binghamton

Friday, April 21, 2017, 6:00 pm - 7:00 pm
Science & Engineering Hall, Room B1270, 800 22nd Street, NW

Abstract

In this talk, we will overview our recent research on exploiting and mitigating timing channels in modern microprocessors. In the first part of the talk, we will present two new covert channels - one through the hardware random number generation unit and one through the branch predictor. We will describe the mechanisms for creating covert communication, analyze the channel capacity and its practical implementation, and suggest mitigation strategies. In the second part of the talk, we will present a new side-channel attack on the branch predictor that allows to either bypass or significantly weaken address-space layout randomization. In the third part of the talk, we will present Relaxed Inclusion Caches (RIC) as a mechanism to protect last-level caches against side-channel attacks without sacrificing performance and retaining snoop filtering capabilities. Finally, we will overview other activities in our lab.

Biography

Dmitry Ponomarev is a Professor in the Department of Computer Science at SUNY Binghamton, he leads the Architecture for Security Lab. His research interests are in the areas of computer architecture, cybersecurity, high-performance computing and energy-efficient system design. He published in top-tier conferences in these areas, including papers in ISCA, MICRO, HPCA, CCS, DAC, ICS, PACT, ISLPED and IPDPS. His research has been funded by the National Science Foundation, the Air Force Research Laboratory, the Air Force Office of Scientific Research and Intel. He received SUNY Chancellor's Award for Excellence in Scholarship and Creative Activities.