پژوهشگاه دانش‌های بنیادی
پژوهشکده علوم کامپیوتر

IPM

سخنرانی علمی

Towards Hardware Cybersecurity

By: Dr. Houman Homayoun
George Mason University

Abstract

Electronic system security, trust and reliability has become an increasingly critical area of concern for modern society. Secure hardware systems, platforms, as well as supply chains are critical to industry and government sectors such as national defense, healthcare, transportation, and financial. Traditionally, authenticity and integrity of data has been protected with various security protocol at the software level with the underlying hardware assumed to be secure, and reliable. This assumption however is no longer true with an increasing number of attacks reported on the hardware. Counterfeiting electronic components, inserting hardware trojans, and cloning integrated circuits are just few out of many malicious byproducts of hardware vulnerabilities, which need to be urgently addressed. In the first part of this talk I will address the security and vulnerability challenges in the horizontal integrated hardware development process. I will then present the concept of logic obfuscation through using hybrid spin-transfer torque CMOS look up tables which is our latest effort on developing a cost-effective solution to prevent physical reverse engineering attacks. In the second part of my talk I will present how information at the hardware level can be used to address some of the major challenges of software security vulnerabilities monitoring and detection methods. I will first discuss these challenges and will then show how the use of microarchitecture data at the hardware level in combination with an effective machine learning based predictor helps protecting systems against various classes of hardware vulnerability attacks. I will conclude the talk by emphasizing the importance of this emerging area and proposing a research agenda for the future.

Biography

Houman Homayoun is an Associate Professor in the Department of Electrical and Computer Engineering at George Mason University. He also holds a courtesy appointment with the Department of Computer Science as well as Information Science and Technology Department. He is the director of GMU's Accelerated, Secure, and Energy-Efficient Computing Laboratory (ASEEC). Prior to joining GMU, Houman spent two years at the University of California, San Diego, as NSF Computing Innovation (CI) Fellow awarded by the CRA-CCC. Houman graduated in 2010 from University of California, Irvine with a Ph.D. in Computer Science. He was a recipient of the four-year University of California, Irvine Computer Science Department chair fellowship. Houman received the MS degree in computer engineering in 2005 from University of Victoria and BS degree in electrical engineering in 2003 from Sharif University of Technology. Houman conduct research in hardware security and trust, data-intensive computing and heterogeneous computing, where he has published more than 100 technical papers in the prestigious conferences and journals on the subject. Since 2012 he leads eleven research projects, a total of $7.6 million in funding, supported by DARPA, AFRL, NSF, NIST, and GM on the topics of hardware security and trust, big data computing, heterogeneous architectures, machine learning for malware detection, side-channel attacks, and biomedical computing. Houman received the 2016 GLSVLSI conference best paper award for developing a manycore accelerator for compute-intensive biomedical applications. Houman is currently serving as Member of Advisory Committee, Cybersecurity Research and Technology Commercialization (R&TC) working group in the Commonwealth of Virginia. Since 2017 he has been serving as an Associate Editor of IEEE Transactions on VLSI. He was the technical program co-chair of GLSVLSI 2018 and is currently serving as the general chair of 2019 GLSVLSI conference.

زمان : پنج‌شنبه ۹۸/۰۴/۱۳ – ساعت ۱۵

مکان : فرمانیه – خیابان شهید لواسانی – جنب برج کوه نور – نبش خیابان فربین – پژوهشگاه دانش‌های بنیادی – طبقه همکف

***** شرکت برای عموم علاقه‌مندان آزاد است *****