UCF Faculty Cluster Initiative and Dept. of Computer Science

Spring 2018 Seminar Series

Revisiting the Future Roles of Computer Architecture in Cybersecurity Research

February 2nd 2018

Time 9:15am-10:15am – HEC 101A

Trustworthy software execution is increasingly demanded in multiple situations, including the cloud computing environment where customers execute their software in cloud servers, and in edge computing where computing may be performed on the edge nodes. Customers require strong privacy and security guarantees from a secure trust base in hardware. Recognizing this, chipmakers recently introduced secure execution environment, such as Intel SGX and AMD SEV. A key component of secure execution environment is memory encryption and integrity verification. In this talk, I will give a short overview of key milestones in memory encryption and integrity verification technologies. Then, I will discuss how these technologies are not adequate in providing secure execution environment in the future, for several reasons. First, the threat model is incomplete. The pervasiveness of side channel vulnerabilities and attacks in both cloud servers and edge nodes can bypass the protection provided by SGX and SEV. This is evident in the recent Spectre and Meltdown security vulnerabilities. Second, these technologies are not compatible with new memory technologies that are coming online, such as 3D-stacked DRAM, and non-volatile main memory (NVMM). Third, they are too expensive for use in Internet of Things (IoT) devices, especially ones that require low power consumption or ones with intermittent energy supply.

In the second portion of the talk I will discuss my thoughts on emerging topics on cybersecurity research, and my thoughts on making cluster collaboration successful

Yan Solihin

Professor of Electrical and Computer Engineering at North Carolina State University and an IEEE Fellow.

Yan Solihin is a Professor of Electrical and Computer Engineering at North Carolina State University and an IEEE Fellow. He founded the ARPERS research group, where his group has contributed to several key computer architecture and security technologies found in current Intel processors, 90+ publications, 40+ patents and patent applications, and several software releases. He is listed in the top five in HPCA Hall of Fame (as of 2017). His research has received MICRO Best Paper Runner-up Award (2017), IEEE Micro Top Picks (2011) and several best paper nominations (ISPASS 2013, IPDPS 2012, and HPCA 2005). From Oct 2015 to Jan 2018, he was a Program Director at the Division of Computer and Network Systems (CNS) at the National Science Foundation, managing the NSF-wide computer security flagship program, Secure and Trustworthy Cyberspace (SaTC). In addition, he also manages several other programs: Computer Systems Research (CSR), Scalability and Parallelism in the eXtreme (SPX), and NSF/Intel Partnership on Foundational Microarchitecture Research (FoMR).

He obtained his B.S. degree in computer science from Institut Teknologi Bandung in 1995, B.S. degree in Mathematics from Universitas Terbuka Indonesia in 1995, M.A.Sc degree in computer engineering from Nanyang Technological University in 1997, and M.S. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 1999 and 2002. He is a recipient of 2010 and 2005 IBM Faculty Partnership Award, 2004 NSF Faculty Early Career Award, and 1997 AT&T Leadership Award.

His contributions to cybersecurity include split counter mode architecture (ISCA 2006), discovery of counter replay attacks (ISCA 2006), distributed shared memory encryption (PACT 2006), Bonsai Merkle Tree (MICRO 2007), self-encrypting non-volatile main memory (ISCA 2011), zero-cost page shredding (ASPLOS 2016), and low-cost memory access pattern obfuscation (ISCA 2017). Many of these key discoveries and designs have been incorporated into Intel SGX Memory Encryption Engine.

Hosted by: ***Dr. Gary Leavens***

UCF

4328 Scorpius Street Orlando, FL 32816

WWW.CS.UCF.EDU