UCF | Electrical and Computer Engineering

Summer 2017 Seminar Series

Memory Encryption and Access Pattern Obfuscation in the Era of Non-Volatile Main Memory

WEDNESDAY MAY 31, 2017

11:00 AM – HEC 450

Trustworthy software execution in the cloud requires strong privacy and security guarantees from a secure trust base in hardware. Recognizing this, chipmakers recently introduced secure execution environment, such as Intel SGX. A key component of secure execution environment is memory encryption and integrity verification. In this talk, I will give an overview of key milestones in memory encryption and integrity verification technologies. Then, I will discuss how these technologies need to be redesigned to work with new memory technologies. The rise of new memory technologies, such as 3D-stacked DRAM, and non-volatile main memory (NVMM), provide new requirements, challenges, and opportunities to providing secure execution environment.

I will discuss our recent discovery of significant write amplification from memory encryption on NVMM. Then, I will discuss writes that occur as a result of one of the most frequent OS operations, shredding processes' data. Shredding data is the process of zero initializing any new physical page by the kernel before mapping it to a process. We observe that the kernel zero initialization process can contribute to a large percentage of the overall number of main memory writes. Our secure NVMM memory controller, Silent Shredder, enables shredding pages at zero cost. Furthermore, it speeds up reading shredded cache lines and improve the performance. Silent Shredder eliminates an average of 48.6% of the writes in

Yan Solihin

National Science Foundation

Dr. Yan Solihin is a Program Director at the Division of Computer and Network Systems (CNS) at the National Science Foundation. His responsibilities include managing the following programs: Secure and Trustworthy Cyberspace (SaTC), Computer Systems Research (CSR), Scalable Parallelism in the eXtreme (SPX), and BigData. He is also a Professor of Electrical and Computer Engineering at North Carolina State University.

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. He is listed in the HPCA Hall of Fame. He is a senior member of the IEEE. His research interests include computer architecture, memory hierarchy design, non-volatile memory architecture, programming models, and workload cloning.

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). Some of the key discoveries and designs have been incorporated into Intel SGX Memory Encryption Engine (MEE).