UNIVERSITY OF CENTRAL FLORIDA
DEPARTMENT OF COMPUTER SCIENCE
& FACULTY CLUSTER INITIATIVE

## Cyber Security & Privacy Cluster

# *“Side-Channel Attacks and Defenses for Intel SGX”*

## Guoxing Chen, Ph.D.

**Research Scientist--Facebook, Inc.**

**Date:**
February 20, 2020

**Time:**
9:30am-11am

**Location:**
Research 1, Rm 101

**For more information please contact:**

**Dr. Yan Solihin**
Yan.Solihin@ucf.edu

OR

**Jade Laderwarg**
Jade@ucf.edu

**Abstract** - Intel Software Guard Extensions (SGX) is an emerging hardware feature that provides software applications a Trusted Execution Environment (TEE) to protect their code and data from untrusted system software. However, prior studies have shown that SGX is vulnerable to side-channel attacks and demonstrated the extraction of secret data, such as sensitive user inputs and cryptographic keys.

This talk will cover some of our works on SGX side-channel attacks and defenses. Particularly, we will first present SgxPectre Attacks, the SGX-variants of the Spectre attacks. SgxPectre Attacks leverage two types of code patterns in the enclave binary. These vulnerable code patterns are found in popular SGX SDKs (e.g., Intel SGX SDK, RustSGX, and Graphene-SGX), indicating any enclaves developed using these SDKs are vulnerable to SgxPectre Attacks. This work was one of the first to demonstrate that Intel SGX’s security guarantees can be completely broken, thus leading to rethinking the security limitations of Intel SGX and other similar TEEs. Second, we will present HyperRace, which is an LLVM-based tool, to close side channels facilitated by Intel Hyper-Threading Technology, such as L1 and L2 caches, branch prediction units (BPU), store buffers and floating-point units (FPU). The idea to create a shadow enclave thread and request the OS to schedule it on the sibling logical core, leaving no room for malicious code to share the same physical core with the logical core running the enclave code. Since the OS is not trusted, we proposed a novel approach for the verification of its scheduling arrangement, by introducing contrived data races. HyperRace is a turn-key solution to the open research problem of defending against Hyper-Threading-enabled side-channel attacks on Intel SGX. Finally, this talk will also outline some of our future research plans and discuss opportunities for collaboration.

**About the candidate** - Dr. Guoxing Chen is a Research Scientist at Facebook, Inc. He received a Ph.D. in computer science and engineering from The Ohio State University in 2019. His research interests are in the areas of computer security and privacy, including system security, side channels, and data privacy. He received his B.S. and M.S. degrees from Shanghai Jiao Tong University in 2010 and 2013 respectively.