UCF | Electrical and Computer Engineering

Spring 2018 Seminar Series

Architectural Support for Scalable Oblivious RAM on Cloud Servers

FRIDAY FEBRUARY 16, 2018

11:30 AM – HEC 356

To protect privacy and secrecy of user's data, encryption is not enough. The physical address on the memory bus cannot be encrypted if there is no computation power on memory DIMM. The attacker is capable to observe address access pattern and infer sensitive information in the program. Oblivious RAM (ORAM) is a cryptographic primitive that can completely hide the information leakage through access pattern. One simple and practical ORAM algorithm, Path ORAM, was proposed to optimize memory bandwidth consumed by the protocol to O(log N). However, from the architectural perspective, the Path ORAM operation is still highly memory intensive to be adopted on scalable computing architectures.

In this talk, I will talk about our recent works which enable Path ORAM runs in the cloud server with architectural enhancement. We first identify the root cause of slow down when multiple applications are co-run on the server. Next, we propose a flexible and effective bandwidth allocation algorithm that optimizes the resource sharing between secure and non-secure applications. Further, we reduce the co-run interference by leveraging the buffer-on-board memory architecture to delegate the Path ORAM primitives. Our proposals expedite both types of applications and provide a feasible solution of implementing Path ORAM on scalable cloud servers.

.

Rujia Wang

University of Pittsburgh

Rujia Wang is a Ph.D. Candidate from Electrical and Computer Engineering Department at the University of Pittsburgh. She received her M.S. degree from University of Pittsburgh in 2015 and her B.E. from Zhejiang University in 2013. Her research experience spans across multiple areas in computer engineering, including novel memory architecture, secure computing architecture, system reliability and high-performance computing, and her work has been published in top conferences in computer architecture area.