UCF | Electrical and Computer Engineering

Spring 2018 Seminar Series

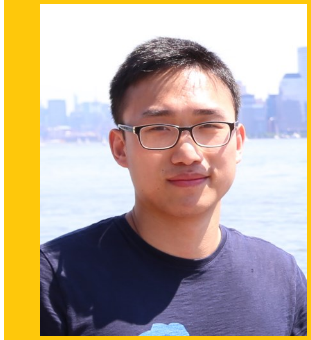
Understanding and Taming Information Leakage in Multi-Core Architectures

FRIDAY MARCH 30, 2018

11:00 AM – BA 1-122

As end users are increasingly relying on online services for data storing and processing, security and privacy are evolving as one of the major factors in computer system design. Although the advent of performance-optimized multi-core architecture significantly bolsters system performance, it exposes new attack surfaces where adversaries can exploit various micro-architectural effects to carry out information leakage. These attacks are even more dangerous compared to software-based exploitations as they manipulate only hardware resources and do not leave any physical traces for forensic analysis. While a significant amount of attention has been directed to application-level security, hardware security is still a new frontier that is actively being explored.

In this talk, I will present our recent work that demonstrates the information leakage vulnerability in processor cache coherence protocol infrastructure. For the first time, our work shows that cache coherence protocol, which is a widely supported performance-enhancing feature in modern processors, can be exploited to implement covert timing channel attacks. We systematically characterize the latency profiles for cache accesses to memory blocks in various coherence states. We then constructed several different scenarios for covert channel construction. Our results show that with proper tuning, adversaries can steal information at very high bitrates. We further discuss mitigation mechanisms to defend future attacks that exploit the new vulnerability.



Fan Yao

George Washington University

Fan Yao is a Ph.D. candidate in the Electrical and Computer Engineering department at the George Washington University. His research interests are in the areas of architecture security, software vulnerability analysis, energy efficient computing in data centers and mobile security. His works have been published in several leading hardware and software venues such as IEEE HPCA, IEEE/IFIP DSN, IEEE TIFS, ACM GLSVLSI and IEEE CLOUD. Mr. Yao is a recipient of the GWU Norris and Betty Hekimian Engineering Endowment fellowship in 2017. Prior to joining GWU, he received his B.E. degree in Software Engineering from Huazhong University of Science and Technology, Wuhan, China.