USC Viterbi School of Engineering
Ming Hsieh Department of Electrical Engineering

Ming Hsieh Institute Seminar Series
Ming Hsieh Department of Electrical Engineering

Computer Engineering

Network Side Channel Attacks: An Oversight Yesterday, A Lingering Threat Today

Zhiyun Qian
University of California Riverside

Thursday, September 20, 2018
2:00 - 3:00 PM
EEB 132

In this talk, I will discuss the history of attacks against one of the most widely used protocol --- TCP. As side channels were never really considered a threat when network protocols are designed, they suffer almost an endless stream of problems. I will demonstrate a blind off-path attacker can use side channels to hijack a remote TCP connection. Recently, we show two serious attacks: (1) a completely blind off-path attacker (not MITM) can hijack a TCP connection between any two arbitrary hosts (i.e., inferring the existence of connection, and sequence numbers). (2) a variation of the attack which exploits a fundamental design of Wi-Fi which is unfortunately impossible to patch in the short term. I will also give insights on how to systematically discover such problems.

Dr. Zhiyun Qian is an associate professor at University of California, Riverside. His research interest is on system and network security, including vulnerability discovery, system building, applied program analysis, Internet security (e.g., TCP/IP), Android security, side channels. He has published more than a dozen papers at the top security conferences including IEEE Security & Privacy, ACM CCS, USENIX Security, and NDSS. His projects have resulted in real-world impact with security patches applied in Linux kernel, Android, macOS, and firewall products. His work on TCP side channel attacks won the most creative idea award at GeekPwn 2016 and winner award at GeekPwn 2017. His research is supported by 8 NSF grants (including the NSF CAREER Award) and two industrial gifts.

Hosted by Xuehai Qian, x04459, xuehai.qian@usc.edu