Rochester Joint Chapter of the IEEE Computer and Computational Intelligence Societies

Rochester, New York

presents

Cache Side-Channel Attack and Defense on Mobile and IoT Devices

by

Ziming Zhao

Assistant Professor in the Department of Computing Security at RIT

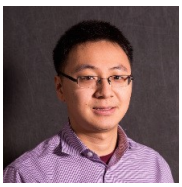
Date: Tuesday, April 9, 2019
Time: 4:30 p.m. to 5:25 p.m. Presentation
Location: RIT Campus, Louise Slaughter Hall - Bldg 78, Room 2120
Computer Society announcements and venue information:
http://ewh.ieee.org/r1/rochester/computer
Cost: Free. Open to IEEE members and non-members.
IEEE Event Feed: https://events.vtools.ieee.org/m/196087
Note: This event is part of the IEEE Rochester Section's Joint Chapters Meeting (JCM), which does have a fee associated with the optional dinner (reservations required) and keynote address.
See: https://meetings.vtools.ieee.org/m/190998

Abstract

It is found that existing and powerful cache side-channel attacks on Intel architectures, including Prime+Probe, are ineffective on mobile and Internet-of-things (IoT) devices powered by ARM architectures. The trust in ARM's hardware-isolated execution environments, namely TrustZone, was also reinforced by these findings. However, those discoveries do not rule out novel and more sophisticated cache side-channel attacks that leverage overlooked hardware features. In this talk, I will present a novel Prime+Count attack that can be used to build reliable covert channels between the normal and secure world of TrustZone, which breaks one of its fundamental security guarantees.

On the other hand, protections that can defeat previous cache side-channel attacks on Intel architectures are not necessarily effective in mitigating novel cache attacks on ARM platforms. Such solutions attempt to mitigate attacks by explicitly or implicitly creating a private space, in which constant-time access to sensitive data is assured. However, some of the attempts utilize hardware features available only on certain Intel processors. In this talk, I will also discuss a defense against cache side-channel attacks that can protect against both dedicated cache (L1) and shared cache (L2) attacks on mobile and IoT devices.

Speaker's Biography



Ziming Zhao is an assistant professor in the computing security department of RIT. He received the PhD degree in computer science from Arizona State University in 2014. His research foci include system and software security, network security, usable and user-centric security, cybercrime and threat intelligence analytics. His research has led to 45+ publications in security conferences and journals, including IEEE S&P, ACM CCS, USENIX Security, NDSS, ACSAC, TISSEC, etc. He won a best paper award in ACM CODASPY 2014 and IEEE ITU Kaleidoscope 2016. He directs the CyberspACe securiTy and forensIcs lab (CactiLab, http://cactilab.info/).