NJIT

Department of Computer Science

Side-Channel Threats on Modern Platforms

Xiaokuan Zhang
Ohio State University

Hosted by Reza Curtmola

DATE: Monday, February 22, 2021
TIME: 11:00AM – 12:00 PM
Webex Link: https://njit.webex.com/njit/j.php?MTID=m55b350a15aa9d09103ab2b1a60cb849e

https://cs.njit.edu/seminars

Abstract: In side-channel attacks, the adversary may learn secrets of a system or an application that are otherwise well protected, by observing traces (e.g., timing, power, or resource usage) of its execution. Recent studies have shown that attackers can learn sensitive information (e.g., cryptographic keys) through side channels, which jeopardizes the user's security and privacy. In this talk, I will talk about my research on exploring side-channel attack surfaces on smartphones (iOS), and applying differential privacy mechanisms to thwart traffic analysis attacks.

The first part of this talk covers our exploration of OS-level side channels on iOS, which are side channels exposed by public APIs. I will present the public APIs we found that caused cross-app side-channel leakages on iOS, and explain how they can be used to extract private user information (e.g., inferring foreground apps). I will also talk about our proposed countermeasures, which were integrated into iOS 11.1 and MacOS 10.13.1. In the second part of my talk, I will present our efforts on applying differential privacy to defeating streaming traffic analysis attackers. I will talk about how to adapt differential privacy mechanisms to add noise to the video streams, and present our implementation of a Chrome extension, which adds differentially private noise to Youtube streaming traffic. I will discuss future research directions at the end of my talk.

Bio: Xiaokuan Zhang is a Ph.D. candidate at the Ohio State University. He graduated from Shanghai Jiao Tong University with the bachelor's degree in Computer Science in 2015. His research interest lies in the broad area of system security and privacy, including side channels, mobile security, IoT security, etc. He is one of the three winners worldwide to receive the 2020 NortonLifeLock (formerly Symantec) Graduate Fellowship. His papers were selected as the top 10 finalists of NYU Cyber Security Awareness Week (CSAW) applied research paper competition in 2016 and 2018, respectively, and his research has helped Apple reduce side-channel attack surfaces in iOS. He has interned at Google and Microsoft Research.