College of Engineering and Applied Science
UNIVERSITY OF COLORADO
DENVER | ANSCHUTZ MEDICAL CAMPUS

Cyber-Physical Systems (CPS) Seminar Series

Title: Emerging Threats in the Mobile Ecosystem

Speaker: Dr. Huan Feng, Research Scientist, Facebook

Abstract: During the past decade, we are moving swiftly towards a mobile-centered world. This thriving mobile ecosystem builds upon the interplay of three important parties: the mobile user, OS, and app. These parties interact via designated interfaces many of which are newly invented for or introduced to the mobile platform. Nevertheless, as these new ways of interactions arise in the mobile ecosystem, what is enabled by these communication interfaces often violates the expectations of the communicating parties. This shakes the foundation of the mobile ecosystem and results in significant security and privacy hazards.

In this talk, we describe our attempts to fill this gap by: 1.) securing the conversations between trusted parties, 2.) regulating the interactions between partially trusted parties, and 3.) defending the communications between untrusted parties. First, we deal with the case of two opposing parties, mobile OS and app, and analyze the Inter-Process Communication protocol (Binder) between them. We found that the OS is frequently making unrealistic assumptions on the validity (sanity) of transactions from apps, thus creating significant security hazards. We analyzed the root cause of this emerging attack surface and secured this interface by developing effective precautionary testing framework and runtime diagnostic tool. Then, we study the deficiency of how existing mobile user interact with app, a party he can only partially trust. We found that in the current mobile ecosystem, information about the same user in different apps can be easily shared and aggregated, which clearly violates the conditional trust mobile user has on each app. We address this issue by providing an OS-level extension that allows the user to track and control, during runtime, the potential flow of his information across apps. Last, we elaborate on how to secure the voice interaction channel between two trusted parties, mobile user and OS. The open nature of the voice channel makes applications that depend on voice interactions, such as voice assistants, difficult to secure and exposed to various attacks. We solve this problem by proposing the first system that provides continuous and usable authentication for voice commands. It takes advantage of the neck-surface acceleration to filter only those commands that originate from the voice of the owner.

Biography: Dr. Huan Feng is a research scientist, working on spam fighting and abuse prevention in Instagram. He shares a general interest in security and privacy in cyber spaces, with both industrial experiences in Facebook, Airbnb, Instagram, and academic background in system security. Before joining the industry, he received his Ph.D. degree from the University of Michigan, where he developed practical defenses to secure smartphone systems.

Date: Monday, Jan 29, 2018
Time: 3:30PM-4:45PM
Location: King 312

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Campus Box 109 | 1380 Lawrence Street | 8th Floor | P.O. Box 173364 | Denver, CO 80217-3364
Phone 303.315.1408 | fax 303.315.1410