Security and Privacy Issues in Modern Computing Devices

Longfei Wu
Department of Computer and Information Sciences
Temple University

Tuesday, Jan. 17, 1PM, GH 218

Abstract:

The growing ubiquity of computing technologies has brought our daily lives more convenience and fun. Nowadays, we are connected with each other and to the outside world via a variety of computing devices. However, what if these devices get compromised or even controlled by a malicious attacker? In this talk, I will discuss my work on enhancing the security of smartphones and implantable medical devices (IMDs).

Smartphones are not well protected as PCs, due to the limitations on hardware, size and battery. Many reliable security schemes running on PCs cannot be migrated to the mobile platform, leaving the smartphones vulnerable to both conventional cyber attacks and mobile-specific attacks. In the first part, I will present my research on mobile clickjacking attack. Specifically, an opaque and untouchable layer is inserted on top of the screen, and tricks the user into clicking on a specific position (e.g. a button). The click event, seemingly going to the top front window, actually goes to the victim window underneath. Three side-channels in Android system are investigated, by which the malicious app can listen to the user input events and react correspondingly to avoid of being exposed. To prevent user input from being hijacked, a lightweight and independent detection service is added into the Android OS. This solution requires no user/developer effort and is compatible with existing apps. Then, I will turn to the spy camera attacks on smartphones. Two advanced attacks are discovered: the first one allows the remote attacker to stealthily monitor the victim user through camera view in real time; the second attack records the user's eye movements when entering password/PINs, considering that the user's eyes may move along with the keys being touched. I demonstrated that it is possible to recover simple passwords, like PINs used for locking the screen and apps, through an offline processing of the video containing the eye movements. An effective detection scheme is proposed based on the specific attack patterns.

The access control of implantable medical devices (IMD) is critical since it is closely related to the patient's conditions monitoring and medical treatment. To secure the wireless interface of the IMD and reduce the computation overheads, I choose to pair it with the patient's smartphone so that the phone can perform the access control on behalf of the IMD. The IMD programmer attempting to access has to be physically present near the patient, and connect to the phone through a USB to audio jack adapter. A pair of symmetric keys will be issued to the IMD and the programmer for future secure communication. The use of a wired channel between the phone and the programmer can prevent an adversary from eavesdropping, forging, and tampering the messages with a software-defined radio. Attribute-based encryption is applied to the session key sent to the programmer, which requires the programmer operator (e.g. a doctor) to possess a set of attributes in terms of speciality, certification, license validity, etc, in order to decrypt the session key and communicate with the IMD. Our scheme can work even if the user cannot participate (e.g., unconscious) and with the phone screen being locked.

Bio:

Longfei Wu received his Bachelor's degree in Telecommunication Engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 2012. He is currently a final-year PhD student in Department of Computer and Information Sciences at Temple University, Philadelphia, PA, advised by Dr. Xiaojiang (James) Du. His research focuses on the security and privacy issues of modern computing systems and devices, including mobile devices, medical devices, Internet-of-Things. Additionally, he is also interested in wireless network and security, big data security, and mobile computing. He is a Technical Program Committee (TPC) member of IEEE conferences ICC, WCNC, and ICCC.