Securing BYOD (Bring Your Own Device)

Guofei Gu
Texas A&M University

One important IT trend in the business world is the emerging computing paradigm of bring your own device (BYOD). It began when employees expressed their desire on using their own mobile devices (e.g., smartphones, tablets, laptops) rather than (or in addition to) using the company's one. Some recent studies indicated that around 44% of users in developed countries and 75% in developing countries are adopting BYOD in 2012. While providing convenience and productivity, BYOD also brings significant challenges to network security. With mobile devices belonging to different entities frequently and dynamically connecting/disconnecting to the network, the boundaries of different networks and trusted zones are blurred. In this case, the valuable data/server assets inside the network may face new threats from compromised/malicious mobile devices.

In this project, we propose novel techniques to secure BYOD at two levels: device level and network infrastructure level. First, for Android-based smartphone/tablet devices that will connect to the BYOD infrastructure, we design new techniques to vet malicious applications for them. We will leverage the PI's strong expertise on android security and malware research to design new practical solutions. Second, for app communications to the BYOD network infrastructure, we propose a new security solution to enable fine-grained, application-level network security programmability for the purpose of network management and policy enforcement on mobile apps and devices. We will leverage the PI's unique expertise in SDN (Software-defined Networking) security to apply SDN concept in a new context and design novel solutions for programmable BYOD security even without the actual deployment of SDN switches/routers in enterprise networks.