COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

DISSERTATION DEFENSE

Renuka Kumar

Exploiting App Differences for Security Analysis of Multi-Geo Mobile Ecosystems

Friday, March 10, 2023
10:00am – 12:00pm
3901 Beyster
Hybrid – Zoom

ABSTRACT: Billions of users worldwide access essential Internet services for banking, education, and social networking through mobile apps on their phones. Given their proximity to users, and the amount of sensitive information they allow access to, mobile apps have become a prime target for security attacks. In response, ecosystems with a large mobile presence, like Google Play and Unified Payments Interface (UPI), have made concerted efforts to protect end-users by vetting mobile apps and providing mitigations to well-known attacks. However, the response to threats has primarily been reactionary and places a significant burden on the user. They rely on users installing highly-rated apps from official app markets and examining app privacy policies before granting apps access to sensitive information on the phone. This dissertation raises this question and asserts that there is, in fact, a practice gap in the security and privacy offerings of widely deployed mobile ecosystems. In this work, we present and discuss the security analysis of two of the world's largest mobile ecosystems (i) Google Play for app distribution and (ii) the Unified Payments Interface (UPI) for free bank-to-bank micropayments. We make significant contributions by demonstrating how security assessments and measurements of black-box systems can be made feasible even within the confines of a severely fragmented ecosystem with no sophisticated tools or access to their backend infrastructure. We reverse-engineer these ecosystems across nation-state boundaries from the point of view of an attacker having access to multiple vantage points, specifically, multiple versions of highly-rated apps integrated with these platforms. We expose critical flaws in these mobile ecosystems, some of them basic, that expose millions of users to significant security and privacy threats, even when using highly-rated apps from official app markets. When combined with other ecosystem vulnerabilities, attackers can exploit these flaws to launch large-scale attacks. Disclosures from this work led to critical actions from the Indian government that owns UPI and Google Play. The principled techniques, insights, and recommendations provided by this thesis will serve as a reference to the security community, governments, and businesses wanting to build, secure, and FOCI the mobile ecosystem at scale.

CHAIR: Prof. Atul Prakash and Prof. Roya Ensafi