Capacity Building through Curriculum and Faculty Development on Mobile Security

Li Yang, Kai Qian, Prabir Bhattacharya, Joseph Kizza, Kathy Winter, Fan Wu

University of Tennessee at Chattanooga, Southern Polytechnic State University, University of Cincinnati, Tuskegee University

Introduction

The computing landscape is shifting rapidly towards mobile platforms, and PCs are no longer the dominant form of computing. Mobile devices are becoming general-purpose computing platforms, and often store tremendous amounts of personal, financial, and commercial data. As such, mobile devices attract both targeted and mass-scale attacks. With more schools developing teaching materials on mobile application development, the development of mobile security materials is needed. By doing so, the security will become a natural and integral part of mobile application development instead of an add-on components. Moreover, the wealth of sensors and GPS information available in mobile devices allow us to design interesting hands-on materials, such as using sensors to explore randomness in cryptography.

Our work strives to build capacity in mobile security by teaching materials, hands-on labs and faculty development workshops.

Objectives

- Develop teaching materials on mobile security with a collection of hands-on materials that will improve the ability of students to apply mobile security techniques to solve real-world problems
- Build faculty expertise and partnership in mobile security through faculty development

Mobile Security Topics

- Topic 1: Introduction to Mobile Computing
- Topic 2: Android Overview, Sensors and Networks
- Topic 3: Mobile Security Basics

Discuss current state and scope of mobile security. Also covers basic measures to stay safe in using mobile devices such as using password, download apps from trusted sources, being alert for unusual behaviors, etc.

- Topic 4: Mobile OS Security Model Comparison
- Topic 5 Threats and vulnerabilities in mobile application

It covers Mobile malware, Web-based and network-based threats, Physical threats from lost or stolen devices, Social engineering, and Vulnerabilities of mobile applications.

- Topic 6 Secure development in mobile computing
- Topic 7 Using cryptography in mobile computing
- Topic 8 Secure communication of mobile devices
- Topic 9 Security Policy and Governance

Manage Permissions to subsystems such as networking, messaging, address book, global positioning system, etc.

- Topic 10 Mobile cloud computing – future of mobile computing

Hands-on Labs

- Installation tutorial for Android SDK with Eclipse.
  - Installation of JDK
  - Installation of Eclipse
  - Installation of Android SDK for eclipse
- Threats of Lost or Stolen Mobile Devices.
  - Backup
  - Encryption
  - Remote Lock or Wipe
- Unauthorized Mobile Resource Access.
  - Authentication: Single Sign-on
  - Authentication: Two Factor Authentication
- Data, Location and Cryptography Privacy.
  - Encryption/ Decryption on SMS-
- Mobile Malware
  - Detecting and removing malware via tool
  - Mobile Malware Attack : Trojan
  - Mobile Malware Defense
- Mobile Spyware
  - Detecting and removing spyware by tool
  - “Penetration Test and Analysis” on Spyware Threat/Attack
  - Defence: Reverse Engineering Analysis

Summer Faculty Workshops

We will have the first summer faculty workshop at UTC with 40 participants (with 20 on-site and 20 distant participants) in summer 2014. Please check back the website (http://www.utc.edu/faculty/li-yang/mobilesecurity.php) for additional information.

Contact Information

Li Yang, Li-Yang@utc.edu
Kai Qian, kqian@spsu.edu
Prabir Bhattacharya, bhattapr@ucmail.uc.edu
Joseph Kizza, Joseph-Kizza@utc.edu
Kathy Winters, Kathy-Winters@utc.edu
Fan Wu, wuf@mytu.tuskegee.edu

Acknowledgement

This project is sponsored by NSF Scholarship for Service Program (Award No.: 1241651 and 1241670) from 2012 to 2015