

CS 528 Mobile and Ubiquitous Computing

Secure Mobile Software Development (SMSD)

Emmanuel Agu





Secure Mobile Software Development Modules



Introduction

- Many Android smartphones compromised because users download malicious software disguised as legitimate apps
- Malware vulnerabilities can lead to:
 - Stolen credit card numbers, financial loss
 - Stealing user's contacts, confidential information
- Frequently, unsafe programming practices by software developers expose vulnerabilities and back doors that hackers/malware can exploit
- Examples:
 - Attacker can send invalid input to your app, causing confidential information leakage



Secure Mobile Software Development (SMSD)

- **Goal:** Teach mobile (Android) developers about backdoors, reduce vulnerabilities in shipped code
- **SMSD:**
 - Hands-on, engaging labs to teach concepts, principles
 - Android plug-in: Highlights, alerts Android coder about vulnerabilities in their code
 - Quite useful



SMSD: 8 Modules

- M0: Getting started
- M1: Data sanitization for input validation
- M2: Data sanitization for output encoding
- M3: SQL injections
- M4: Data protection
- M5: Secure inter-process communication (IPC)
- M6: Secure mobile databases
- **M7: Unintended data leakage**
- **M8: Access control**

- You should
 - Pre-Survey
 - **Lab:** Go through M7, M8
 - Post-survey afterwards





M7 & M8 Overview

- M7: Blah
- Unintended Data Leakage
 - Understand fundamental concepts of unintended data leakages from the clipboard
 - Understand defenses against these unintended data leakages
- M8: Inter-App Secure IPC vulnerabilities
 - Malicious app can exploit security loophole in Broadcast Receivers to intercept valuable information



Important: This Lab REPLACES Worst Quiz

- Counts as quiz 6
- I will drop your worst quiz and replace it with score from SMSD
- Basically, I will use your best 5 scores
- Just do this lab online,
- Due by class time, Thursday, December 5, 2019