Mobile Computing Security and Privacy

Class Introduction and Ethics

Today's Agenda

- Overview of class
  - Course Objectives
  - Philosophy
  - Expectations
  - Resources
  - Assignments
  - Ethics
  - Application of topics

Typical Live Class Time

- Informal Q&A about the material you have read BEFORE class
- Discussion of practical application of concepts in readings
- Hands-on demonstrations/experiments
  - Some might not work as planned

Course Objectives

- Describe the architecture and components of iOS and Android apps as they relate to security vulnerabilities and mitigations
- Apply testing standards, models and tools to assess the security of a mobile app
- Explain basic operations, potential vulnerabilities, and appropriate security measures for WiFi, Bluetooth, LTE and 5G communications
- Given a mobile app scenario, identify privacy threats and appropriate mitigations

My approach to class

I act as your guide, not your authoritative source. Class will include:

- Current and authoritative resources that you can use beyond class
- Meaningful hands-on opportunities to explore topics
  - Things change very quickly in the mobile space and some things might not work as planned
- I want to challenge everyone in class, but have very reasonable expectations

Resources

- OWASP Mobile Application Security Testing Guide
  - Considered the authoritative standard for mobile testing
  - VERY big document, but I have provided condensed versions of some sections
    - Focus on the concepts and testing methods
  - Combination of testing techniques and secure development practices
- NIST Documents
  - Federal standards and guidelines for evaluating and securing things
- Select textbook chapters
- Select web articles

Assignments

- Start early and ask questions
  - Those with expertise should share it in discussions
- Some assignments are steppingstones to final project, so learn from each submission and IMPROVE your final result
  - Errors or omissions are not corrected for the final project will result in substantial points deductions

Quizzes Exams and Labs

- Quizzes and exams will be based on readings and class discussions
- Assignments
  - They are designed to be a challenge because the world needs problem solvers
  - Results will be uploaded to WebCampus

Testing Focus and Issues

- Instructions and in-class work will focus on Android
  - NOT because iOS is more secure, it's just more difficult to test
  - Android testing can be done from LME machines for those who don't have the testing setup
- We will look at some iOS image and data captures to see vulnerabilities
- You are welcome to test iOS if you have a Mac and a jailbroken iPhone
  - The MASTG describes steps and I provide a few apps for practice
- Mac M1 computers
  - These present some challenges
  - Some info provided on M1 work arounds and encourage class members to share findings

Bring a Laptop

- NOT required, but will be useful during WiFi and Bluetooth modules.

Final Exam and Project

- Final exam will cover all topics AFTER midterm exam
  - See syllabus in Canvas for date and time
- Final project overview
  - Find a potentially vulnerable
  - Perform a penetration test of the mobile app
  - Prepare a formal pen test report
  - Several weekly assignments will be steppingstones to the final project
- Graduate research paper – in addition to class project
  - Aim for a published paper
  - Research literature for a current mobile security or privacy topic and use or create lab tools to test or demonstrate examples
  - Be prepared to present findings in class

Questions 

Cybersecurity Ethics

Why it's important

- The study of cybersecurity requires understanding of tools and techniques used in hacking, cybercrime and cyberwarfare
- This class will introduce several of these tools and techniques and allow you to experiment with them in a controlled, virtual machine environment
- Using these tools and techniques outside of a strictly controlled environment is unethical and potentially illegal
- Using these tools and techniques outside of a strictly controlled environment has the potential to cause serious harm to you and others

When to experiment with hacking tools

- When using these tools insure they are used in a strictly controlled environment
  - Virtual machines and or test networks
- If others are involved, they must be informed of the risks and provide explicit consent to participate
  - It's not okay to try to hack a neighbor or coffee shop WiFi network
  - It's not okay to scan public websites to look for vulnerabilities, without their knowledge and permission
  - It is okay to setup your own vulnerable machines and sites in a controlled environment and experiment with them.

General Cyber Ethics

- To be considered a professional in cybersecurity, one must perform ethically
- The ACM Code of Ethics and Professional Conduct provides an excellent example of the rules we should follow: https://ethics.acm.org/code-of-ethics/
- The following points from The ACM Code of Ethics and Professional Conduct are most important during our studies
  - 1.2 Avoid harm
  - 1.3 Be honest and trustworthy
  - 1.6 Respect privacy
  - 1.7 Honor confidentiality

News

- https://www.bleepingcomputer.com/news/security/spyloan-android-malware-on-google-play-downloaded-12-million-times/
- https://www.bleepingcomputer.com/news/security/google-explains-how-android-malware-slips-onto-google-play-store/
-