CS9233 - Selected Topics in Computer Science - Mobile Security

Instructor: Lok Yan
Email: lky207@nyu.edu

Course Overview

Mobile devices are everywhere. While the concept of a mobile device is not new, recent advancements in connectivity, processing power and power storage has allowed mobile devices to displace traditional desktops as the primary means of computing. Today's smartphones can effectively do everything that older desktop computers do (think of the Samsung Dex Docks) and yet are completely portable. Not surprisingly, smartphones and other mobile devices have been the target of cyber criminals since their inception. This, in itself, should not be a surprise and we should already be fully ready to analyze and understand the security implications and issues.

This special topics course is designed to give the student a little bit more insight on how to apply the basic principles of security learned in previous courses to the world of mobile security. Of particular importance is a focus on the new medium that modern mobile introduces. We will consider design changes such as a smaller screen (therefore one App is displayed at a time, while most others are running in the background) or even no screen at all (such as in Internet of Things devices), the communications infrastructure and its limitations such as the evolution from GSM (2G), UMTS (3G) and LTE (4G) to the upcoming 5G specifications, and we will also explore platform security models of some popular mobile device platforms including iOS and Android as well as older models such as Windows Phone.

As a reminder, this is a high-level graduate course that is meant to reinforce the student's ability to do independent learning on a new and/or up-and-coming topic of interest. Therefore, the main focus will be on "independence". Since one of the major tenets of education is that you don't truly understand something until you can teach it, this course will require students to present the most recent material on the topic of mobile security to the entire class. Students are then required to ask insightful questions and participate.

Prerequisites

- Undergraduate level knowledge of computer systems and networks.
- Owning a smart mobile device, such as a smart phone, will provide an added advantage.
- Knowledge of Operating Systems (such as from 6233) and Security (such as from 6813)

Textbooks

1. Mobile Application Security, Himanshu Dviwedi, Chris Clark and David Thiel, 1st Edition

2. Security of Mobile Communications, Noureddine Boudriga, 2010

Course Topics (Could Change with Developments)

1. Introduction to Mobile Security
2. Building Blocks – Basic security and cryptographic techniques.

3. Security of GSM Networks
4. Security of UMTS Networks
5. LTE Security
6. WiFi and Bluetooth Security
7. SIM/UICC Security
8. Mobile Malware and App Security
9. Android Security Model
10. IOS Security Model
11. Security Model of the Windows Phone
12. SMS/MMS, Mobile Geolocation and Mobile Web Security.
13. Security of Mobile VoIP Communications
14. Emerging Trends in Mobile Security

Course Load

The course has four homework assignments, one test, one project and two research paper presentations. In the interest of following the mobile trend, we will forego discussion forums and live presentations. Instead, we will be posting videos and have question and answer sessions (in the form of comments and responses) on the go. This course will be run in the graduate style where students are encouraged to be independent, take initiative and explore new topics on their own. THis should come naturally as part of the homework assignments and research paper presentations.

Homework Assignments: The homework assignments will consist of a series of questions for you to answer. Students have the option of answering the questions in the traditional written format, an audio (e.g., podcast) format or a video (e.g., vlog). Please keep in mind that while you might not be graded on style or production value, this is an opportunity for you to get practice in any of the three communications methods without judgment.

Final Exam: The final exam will assess your knowledge and mastery over the lecture material. We might forego with the final exam as well depending on the quality and sophistication of the projects.

Research Paper Presentation: Each student will be required to pick two research papers, summarize them and then record themselves presenting the paper as if they were presenting it at a conference. A good place to start is USENIX Security (https://www.usenix.org/conference/usenixsecurity18) which just took place in August. They have a mobile track, so it is a good place for you to find research papers. They also record all of the presentations so you have a good idea on what the presentations should look like. **Make sure you don't plagiarize their presentations**

Project: The project has to be conducted in teams of three. For the project, you will pick a topic - the project might involve experimentation, coding, simulation or anything of your choosing - that highlights a new principle or characteristic of mobile security that did not exist prior. All research topics must be approved by the instructor. In order to facilitate this, team are required to submit a two page "whitepaper" by the end of the 3rd week (earlier is fine). Then, the students will submit a detailed project report by the end of the semester.

Lectures: Pre-recorded lecture material are provided to the student as a quick overview. Students are expected to listen to the lecture material on a weekly basis. We will also be conducting live

sessions so we can have any questions answered, issues addressed, and additional topics discussed. The live sessions will also serve as a forum for project updates and meetings.

Grading Policy

Homework Assignments: 20%

Research Paper Presentation/Online Participation: 30%

Project and Project Presentation: 30%

Final Exam: 20%

Interaction Policy

- Live sessions will be held weekly on WebEx. Please join if available.
- Questions will be answered via email or through the virtual classroom sessions. For additional questions and interaction, please schedule an appointment.

Student Responsibilities

- **Online lectures:** Each lecture will consist of slides and video lectures. You are expected to read the relevant material in the textbook, and follow the video lectures.
- You are required to check online site daily for: Information, announcements, discussions, updated lecture notes, assignments, reading material etc.
- **Late Policy:** Submit assignments and tests on time **- no extensions will be granted.**

Academic Integrity Policy

Students must behave ethically at all times. All work should represent the students' original ideas and thoughts. When doing the assignment you may consult any relevant source or person, but if you take information in a substantial way from someone or somewhere, you should reference it. You are **NOT** allowed to copy code/content in **ANY FORM** from any source. All tests will be individual and open book, but timed, and you may not consult anyone during the test. Any violation of the academic integrity policy will be awarded **ZERO** points.