Mobile Security
Fall 2015

Patrick Tague
#1: Course Introduction
Class #1

- Brief overview of the course
- Logistics
- Course information
- Talk about projects (if there's time)
What is this course all about?

Time for a Quiz!
What is Mobile Security?
- or -
What makes security different in the mobile space?
What is Mobile Security?

- Protocols are different from Internet / Ethernet
- Devices are much more ubiquitous / varied
- Issues with resource constraints
- OSes are different across the ecosystem and compared to prev technologies (e.g., laptops)
- App dev / dist is different compared to laptop class
- Lots of sensitive data (e.g., location history, contacts)
- Wide variety of network technologies
- Mobility creates lots of opportunity for dynamics which causes problems
- Physical security !!!

- Entering passwords is horribly difficult
- Different kinds of users
- Controlling access to data across applications / services
- Attack surface is bigger
- Configuration is more opaque
- Lots of players involved (e.g., telecom) slow updates/patches
- Cable for charging and data transmission is the same
- Quantity of data may be limited due to mobile plan
- Lots of companies collecting and managing lots of user data
Mobile Security Topics

- In the Mobile Security course, we'll study:
  - Smartphone systems
    - Apps, services, etc.
  - Networks they use
  - External services they rely on
  - Security/privacy issues faced by users, devs, regulators, ...
  - Trade-offs re: usability, efficiency, etc.
Course Objectives

• Security & Privacy for Mobile System & App Developers

• Exploration and critical analysis of security and privacy issues in mobile systems
  – What are some security concerns in mobile devices?
  – What can devs do to protect customers and themselves?
Topic Roadmap

Smartphone Security & Privacy Issues WRT...

Networks
- Telecom
- WiFi
- PAN
- NFC

Sensing
- Simple Sensing
- Activity
- Context
- Support Services

Software
- OSs
- Apps
- Services
- Analytics

System
- Enterprise
- Infrastructure
- Cloud
- Vehicles
Goals of the Course

- Understand how to design secure applications and services in the mobile space
- Know what the infrastructure provides and what the developer must consider
- Hands-on experience in analysis and design of security-centric apps, services, protocols, etc.
- Cutting-edge research/project experience
What This Course is NOT...

• Crypto or basic InfoSec course
  – Take something like 18-631 / 14-741 instead

• Android / iOS development course
  – Take something like 18-641 instead

• Easy.
Questions about Content?

Any questions about content, focus, etc. before I start talking logistics...?
Logistics
Course Website

http://mews(sv).cmu.edu/teaching/14829/f15/
Prerequisites & Assumptions

• This course has official prereqs
  – You have taken a graduate-level Information Security course (e.g., 14-741, 18-631, 18-730)
  – You have taken a graduate-level Networking course (e.g., 14-740, 18-756, 15-641)

• In addition, we assume:
  – You are proficient in Java programming and either have experience with Android or have time to learn it on your own (HW#1 requires Android knowledge)
  – IMPORTANT: this course does not teach Android dev
Registration

- This course has 4 concurrent sections
  - It's important that you register for the right one

<table>
<thead>
<tr>
<th>If your location is:</th>
<th>If your home dept is:</th>
<th>Not ECE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pgh</td>
<td>18638 A</td>
<td>14829 A</td>
</tr>
<tr>
<td>SV</td>
<td>18638 SV</td>
<td>14829 SV</td>
</tr>
</tbody>
</table>
Waitlists

• If you're currently registered for this class, but not planning to stay: please drop

• If you're currently on the waitlist:
  1) Make sure you're on the correct waitlist (see the previous slide)
  2) Send me an email (tague@cmu.edu) detailing:
      1) What year/term of your program are you in (priority will go to students closer to graduation)?
      2) What degree requirements does this course fulfill (priority will go to students who need this course)?
      3) Why you want to take this course?
      4) What prereqs/qualifications do you have?
Deliverables & Grading

- Individual work - 30%
  - Four assignments
    - Late submission: 10%/day penalty, up to 2 days

- Group project
  - Four presentations (proposal, statement of work, progress update, final) - 25%
    - Graded individually, everyone must participate
  - Two written reports (SoW, final paper) - 25%
    - No late submissions accepted

- Exam - 20%
Individual Assignments

• Four assignments
  – Programming/app development component
  – Research/survey component
  – Assignments will use Android, some dev tools, and some analysis tools

• Assignment details and deadlines will be online

• Individual → each student is responsible for doing their own work
  – Discussion is encouraged, but work is individual
Group Project

• Project details:
  – Teams of 3-4 students
  – Some teams will work on “sponsored projects”, others will create their own projects
  – Background/proposal will be in late September, so form teams and get started soon
  – Statement of Work and milestone presentation in mid October
  – Progress report in early November
  – Final presentation in early December
  – Final report due December 17
Exam

• Individual in-class exam

• Format and style to be announced

• About ¾ through semester, tentatively 11/17
Important Dates

All important dates are on the course website
How to Contact Us

• Instructor: Patrick Tague
  – Email: tague@cmu.edu
  – Office: B23 218
  – Phone: 650-335-2827
  – Skype: ptague
  – Office hours: Open-door, open-calendar, by appt
    • Public Google calendar: http://goo.gl/FIVbRK

• TAs: Nandita Joshi
  – Email: nandita.joshi@sv.cmu.edu
  – Office hours and other details TBD (see web)
Some Syllabus-type Details

• Class meetings:
  – Tues/Thurs 9:00-10:20am PDT / 12:00-1:20pm EDT
  – B23 118 @ SV campus, CIC 1201 @ Pgh campus

• Class website
  – Schedule, slides, assignments, papers, projects, ...
  – Submissions are via Blackboard

• Textbooks
  – None, but some references are on the website

• Assigned reading
  – Papers, blog posts, media, etc.
Assigned Reading

- Between class readings, homework assignments, and project, *you'll be reading a lot of papers!*
  - Don't be surprised to see 100+ pages of reading/week

  - Reading research papers is not like reading textbooks, they're much more forgiving and can be read efficiently

  - **Hint:** read the pamphlet posted for reading material today
    - We'll also take some time in an upcoming class to talk about how to read efficiently.
Important Policies

• **Academic Integrity**: all students are expected to adhere to academic integrity policies set forth by CMU, CIT, ECE, INI, etc. See
  • ECE Academic Integrity Policy (and handbook)
  • INI Student Handbook
  • College of Engineering Policies
  • CMU Academic Integrity Policy

• **My Collaboration Policy**: discussion is encouraged, but assignments must be done individually
  • Copying is cheating, cheating → failing grade

• **Plagiarism**: no copying, attribute *all* content sources

• **My Wiki Policy**: if you cite Wikipedia (or similar) pages directly, you will fail the assignment/deliverable

• **Re-grading**: on a case-by-case basis, contact me
Ethics of S&P Work

• Research, development, and experimentation with sensitive information, attack protocols, misbehavior, etc. should be performed with the utmost care

• You are expected to follow a strict ethical code, especially when dealing with potentially sensitive information

• If anything is unclear, ask before going forward
Questions about Logistics?

Any questions about course logistics?

Feel free to email later.
Assignment #1

• Not a programming assignment, but requires knowledge of how Android works

• Due on September 15 (via BB)

• Tasks:
  – Read some papers about intent-based attacks in Android
  – Design a malicious app based on what you read
    • Building the app is optional
  – Do a nice write-up of your design
Projects
What topic should I choose?
Project Topics

• Projects must:
  – Relate to topics covered in class and focus on some aspect of mobile security
  – Strive for new research/development contributions - aim for something never done before
  – Not be a project you're working on for your research or another course

• Examples of past projects (see my office door for F14):
  – Understanding OAuth implementation and design flaws
  – Enabling “Private Mode” for Android apps
  – Per-app passive authentication controls
  – User-controlled permission management w/ rate limiting
  – BYOD analysis framework and study of current products
How should I form a project team?
Project Teams

• Forming teams and choosing topics:
  – These two things are not independent
  – Try to choose team members with common interests, different backgrounds, etc., not just your friends
  – Multiple teams cannot work on the same project
More Project Details

• Each project will have a faculty advisor
  – Probably me, but you can approach any faculty member who
    may have a relevant project to “sponsor”

• Project output will include a paper, poster, and demo
  – Aim for conference-quality results

• Some additional hardware may be available, if needed
September 3: Mobile Devices & General Security Challenges

More discussion of course deliverables