Mobile Security
14-829 - Fall 2011

Patrick Tague
Class #1 - Introduction & Logistics
Agenda

• Course objectives

• Administrivia

• Deliverables & important dates

• A brief introduction
Course Objectives

• “Security for Mobile System & App Developers”

• Exploration and critical analysis of security and privacy issues in mobile systems
  – What is a mobile system?
  – What will a mobile system look like in $N$ years?
  – What is security?
Course Objectives

- Topics include:
  - Telecom security & vulnerabilities
  - Mobile app & web security
  - Secure network services
  - Mobile location privacy
  - Ad hoc, mesh, & sensor network security
  - ...
Goals of the Course

• Understand how to design secure systems and applications in the mobile space

• Know what the infrastructure provides and what the developer must consider

• Hands-on experience in analysis and design of a security-centric app, service, or protocol

• Research publication or presentation
Administrivia (1)

- **Instructor:** Patrick Tague
  - Email: tague@cmu.edu
  - Office: B23 222
  - Phone: 650-335-2827
  - Office hours: Open-door, open-calendar, by appt

- **TA:** Yu Seung Kim
  - Email: yuseungk@andrew.cmu.edu
  - Office hours: TBD
• Class meetings:
  – Mon 10:00-11:30am PDT (1:00-2:30pm EDT)
  – Wed 9:30-11:30am PDT (12:30-2:30pm EDT)
  – B23 118 @ SV campus, INI DEC @ Pgh campus

• http://wnss.sv.cmu.edu/courses/14829-f11/
  – Schedule, slides, homework, papers, projects, ...

• Textbooks
  – Several textbooks are listed on the course website. None are required reading, just reference material for background reading and/or homework references.

• Other sources: media, papers, blogs, etc.
Administrivia (3)

- **Grading**
  - HW and surveys - 25%
    - 15 pts/HW, 40 pts/survey
  - Project presentations - 30%
    - 30 pts each for proposal and progress
    - 60 pts for final
  - Written project reports - 25%
    - 20 pts for proposal, 80 pts for final report
  - Exam - 20%
    - 80 pts

- **Late submission**: 10%/day penalty, up to 2 days
Administrivia (4)

- **Policies**
  - **Academic Integrity**: all students are expected to adhere to academic integrity policies set forth by CMU, CIT, ECE, INI, etc. See http://www.ece.cmu.edu/student/integrity.html http://www.ini.cmu.edu/current_students/policies/ http://www.cmu.edu/policies/documents/Cheating.html
  - **Collaboration**: discussion is encouraged, but homework must be done individually
    - Copying in any form constitutes cheating, ask if it's unclear
  - **Plagiarism**: no copying, attribute *all* content sources
  - **Re-grading**: on a case-by-case basis, contact me
  - **Do NOT cite Wikipedia**
Adminstrivia (5)

- Ethics
  - Research, development, and experimentation with security-sensitive information, attack protocols, misbehaviors, etc. should NEVER be performed in live, online systems
  - You are expected to follow a strict ethical code
  - If anything is unclear, ask.

*Whenever there is doubt, there is no doubt.*

Deliverables

• Homework assignments
• Survey presentations
• Exam
• Group project
Homework

• Assignments are intended to be exploratory, ex:
  - **Rogue Base Stations**: Attackers can configure and deploy rogue GSM base stations for the purpose of harvesting information from mobile users. Describe 1) the attack details, 2) systems that are vulnerable to such an attack, and 3) attackers’ capabilities and challenges in attracting users/devices to connect and use such rogue base stations.
  - **Legacy voice vs. Mobile voice vs. VoIP**: Investigate the authentication and encryption mechanisms used for popular voice-over-IP (VoIP) services such as Skype, Vonage, or Google Voice, both in wired and wireless scenarios. Perform a detailed comparison between VoIP services, legacy wired telephone services, 2G GSM, 2G CDMA, and 3G/UMTS services in terms of the difficulty of intercepting calls and recovering voice or data information (note: these systems allow vastly different attack types). In addition, comment on voice/data security and privacy issues in using a VoIP service over a 3G connection (e.g., Google Voice on your Android phone).

• Important dates and instructions online
Surveys

- Teams (~3 people) will have an entire class to present a topic based on a set of papers
  - Several class dates reserved for surveys
  - Everyone presents at least once, 2\textsuperscript{nd} time can replace a homework assignment grade if space permits
  - Sign up for a presentation slot/topic (FCFS)
Exam

• Individual in-class exam

• Open-books, open-notes

• About \( \frac{3}{4} \) through semester, tentatively 11/9
Course Project

• Group project
  – ~3 students per group
  – **Topic and scope are flexible, but must be sufficient effort (~6-8hrs/week/student)**
    • *Topics must be approved prior to proposal*
  
  – Project proposal (written + in-class presentation)
  – Progress report (in-class presentation)
  – Final (written report + in-class presentation)
  – Biweekly group-instructor meeting

  – More details and important dates on website
Project Topics

- Projects must:
  - Relate to systems covered in class and focus on some aspect of mobile security and privacy
  - Strive for research publication/presentation

- Examples of past projects:
  - Location privacy controls in Facebook Places
  - Secure location-based Twitter services
  - Physical layer attacks and defenses for mobile platforms
  - Using a web proxy to detect attacks on mobile phones
  - Secure phone-to-phone networking
  - Evaluating vulnerabilities in WiMAX/LTE
  - Robust mobile-to-mobile key establishment against MitM attacks
  - Attacks on location privacy in WiFi systems
# Important Dates
(tentative)

14-829: Mobile Security - Fall 2011

## Daily Schedule, Notes, & Papers

Note: all topics and dates are subject to change.

<table>
<thead>
<tr>
<th>DATE</th>
<th>TOPIC</th>
<th>READING</th>
<th>PRESENTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug 29</td>
<td>Course introduction &amp; logistics</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Aug 31</td>
<td>Components of a smartphone system</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sep 5</td>
<td>NO CLASS - Labor Day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sep 7</td>
<td>Telecommunications security - Authorization and authentication</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Sep 12</td>
<td>Telecommunications security - Information security and privacy</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Sep 14</td>
<td>Project proposals</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sep 19</td>
<td>SURVEY: Attacks on cellular systems</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Sep 21</td>
<td>SURVEY: Attacks on cellular infrastructure</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Sep 26</td>
<td>WIFI systems, vulnerabilities, and security - HW #1 Due</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Sep 28</td>
<td>SURVEY: WIFI attacks and defenses</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 3</td>
<td>Smartphones, PANs, and the IoT</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 5</td>
<td>SURVEY: PAN and IoT security issues</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 10</td>
<td>Mobile operating system security - iPhone and Android</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 12</td>
<td>SURVEY: Android security issues</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 17</td>
<td>Mobile application security - Vulnerabilities, threats, and attacks</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 19</td>
<td>SURVEY: Attacks using Mobile Apps</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 24</td>
<td>SURVEY: Mobile privacy</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Oct 26</td>
<td>Project progress reports</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Oct 31</td>
<td>Mobile ad hoc and mesh networks - HW #3 Due</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 2</td>
<td>MANET and mesh security</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 7</td>
<td>SURVEY: Securing MANETs</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 9</td>
<td>Exam</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nov 14</td>
<td>Location services in mobile phones and systems</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 16</td>
<td>Location security and privacy</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 21</td>
<td>SURVEY: Mobile location privacy - HW #4 Due</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 23</td>
<td>NO CLASS - Thanksgiving Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nov 28</td>
<td>Emerging mobile scenarios</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Nov 30</td>
<td>Emerging mobile scenarios</td>
<td>TBD</td>
<td>-</td>
</tr>
<tr>
<td>Dec 5</td>
<td>Final project presentations</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dec 7</td>
<td>Final project presentations</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Dec 14</td>
<td>Written project report due</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is a Mobile System?

Mobile telecom networks

Wireless Internet

MANET and WSN

©2011 Patrick Tague
Mobile Cellular Networks

• Structure:
  – Hierarchical infrastructure
  – Very large scale (cities, states, countries)

• Function:
  – Proprietary delivery & management of mobile voice, SMS, MMS, Internet, m-commerce, ...

• Features:
  – Seamless access to PSTN, ISDN, PLMN, PSDN/PSPDN, CSPDN
  – Broad coverage and hand-off for fast, long-duration mobility
WLAN Networks

• Structure:
  – Local infrastructure / gateway
  – Small scale (home, building, campus)

• Function:
  – Public or private Internet access (i.e., any IP-based service) using WiFi or similar wireless technology

• Features:
  – User- or operator-configurable for open or tightly controlled access
  – Local coverage, hand-off capabilities in multi-AP environments (CMU) for slow mobility
MANETs

- Structure:
  - Heterogeneous, usually* flat (not hierarchical), no fixed infrastructure
  - Variable and dynamic scale (room, building, company, city)

- Function:
  - Distributed interaction and data exchange, collaborative services, device-to-device comm and control, monitoring, ...

- Features:
  - Self-deploying, self-configuring, self-healing, self-controlling, self-*
  - Operates independent of infrastructure availability
  - “End-nodes are the network”
Hybrid Systems

- [My definition]: A *hybrid system* falls somewhere between the previous three w.r.t. structure, function, etc.

- Examples:

  - Wireless Mesh Network
  - Sensor Network w/ IP Gateway
Smartphone...
The Ultimate Mobile System?
What is Security?

- Authorization / permissions
- Authentication & crypto, security protocols
- Access control
- “Better-than-nothing” protection
- Data integrity
- Safety, protection from threats or theft
- Data or service availability
- Confidentiality
- Performs as expected
- Privacy
- User trust - confidence
- Obtaining consent

- Detection, prevention, footprinting - IDS/IPS
- Mapping networks
- Malware / rootkits
- Security policy
- Corporation security, nation v. nation, etc.
- Contingency planning
- Deterrence
- Assigning privileges
- Identity management
- Correctness, verifiability, predictability
- Non-repudiation
- Scalability, reliability
- Physical security (biometrics, CPS)
What is Security?

Information Security
Confidentiality
Authenticity
Integrity
Availability

Protocol Security
Reliability
Predictability
Quality of Service
Efficiency

Device/OS Security
Tamper-resistance
Code Verification

Resource Security
Availability
Fairness

Security Policy
Common Considerations

• Wireless is open
  – User/device/system verification is more difficult
    • Mutual authentication may be required
    • Currently, rogue BTS and BS can be deployed
  – Availability is difficult in a best-effort system
    • Most systems aren't designed with redundancy or w.r.t. resilience to malicious behavior
  – Many other concerns...

• Nothing is free
  – Security costs $$$, time, CPU cycles, bandwidth, user-experience, etc.
  – Incentives?
More Issues for Mobile

- Smartphone ecosystem introduces many new security considerations
  - Where does my software come from? Can I trust the developer? Is installing this app worth the risk?

  - How do intrusion/attack detection work when some traffic goes through cellular infrastructure, some goes through WiFi, some goes through Bluetooth, etc.? Who is responsible for my data/service?
µHomework Assignment

- µHW: briefly answer the following:
  
i. Why are you taking this class?

  ii. What is your relevant background (courses, research, etc.)?

  iii. What do you hope to get out of this class?

  iv. What are 2 or 3 specific things you want to learn about?

- Submit by email before next class
Next Time

• Components of a smartphone system
  – What makes a smartphone smart?
  
  – What components are involved in smartphone use?
  
  – What are the risks of this “smartness”?