Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #1 – Course Introduction & Logistics

Carnegie Mellon University
Silicon Valley

Registration

- This course has three different course numbers: 14-829, 18-638, and 96-835
  - It's important that you register for the right one

```
if location == Pgh
   if dept == ECE
      reg = 18-638;
   else
      reg = 14-829;
else if location == SV
   reg = 96-835;
```

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 telling me **why** you want to get in and **what prereqs/qualifications** you have
     - Email: **tague@cmu.edu**

Time for your 1st Quiz

What is Mobile Security?

- or -

What are its elements?

Think about it for a minute...

What is Mobile Security?

- Security in mobile OSs and networks
- Computers, telecom, radio communications
- Mobile app security
- Data encryption for mobile/wireless
- All other security properties relevant to wireless/mobile
- BYOD
- User privacy
- Physical device security
- Sniffing NFC communication
- Attacks on cellular/mobile networks and x-measures
- Mobile malware
- Network correctness
- Resilient wireless (anti-jamming)
- Data storage on/off devices
- GPS / location services; sensors
- Contacts; context information
- Advertising

Focus on the Smartphone

- 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, …
  - Maybe some usability issues

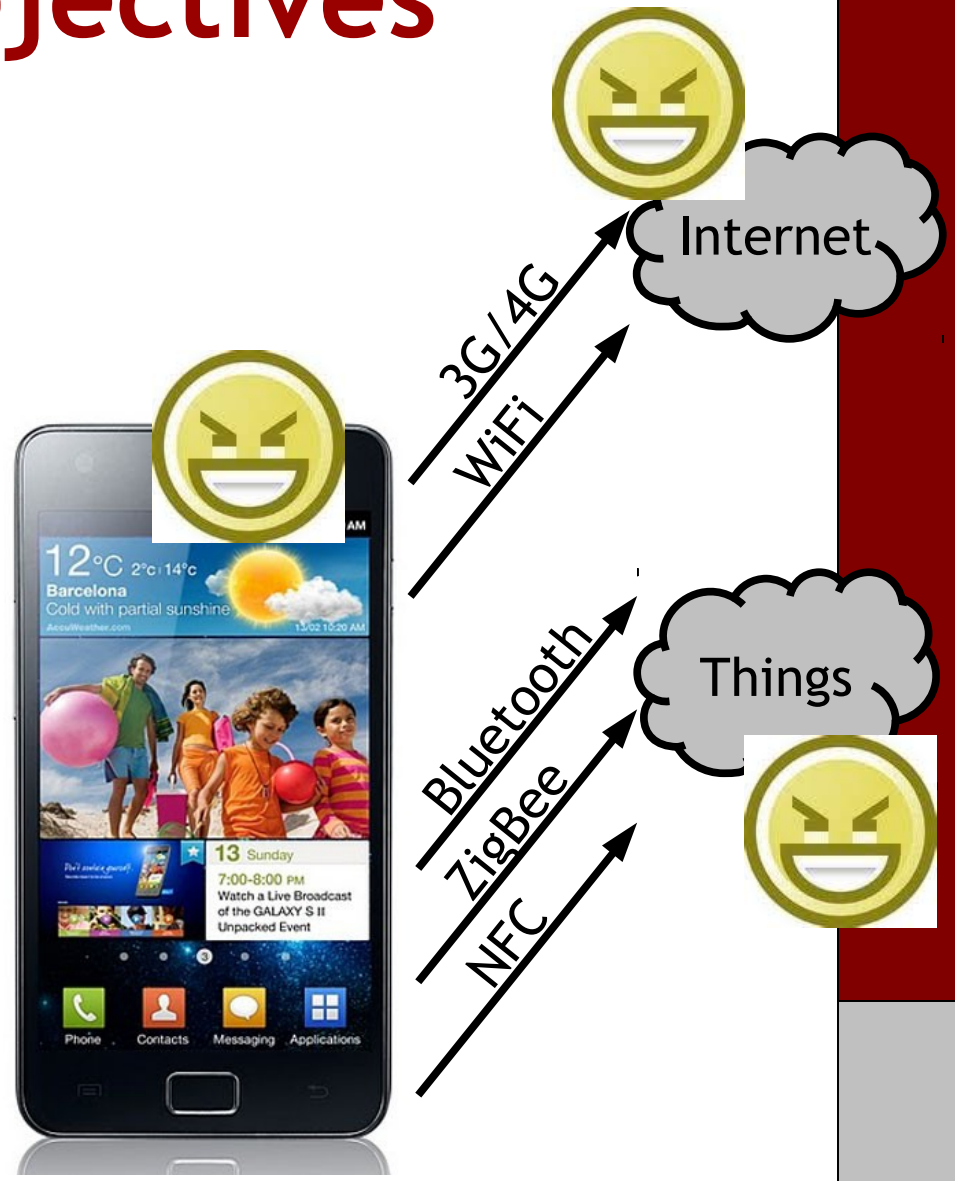
Course Objectives

- "Security & Privacy for Mobile System & App Developers"

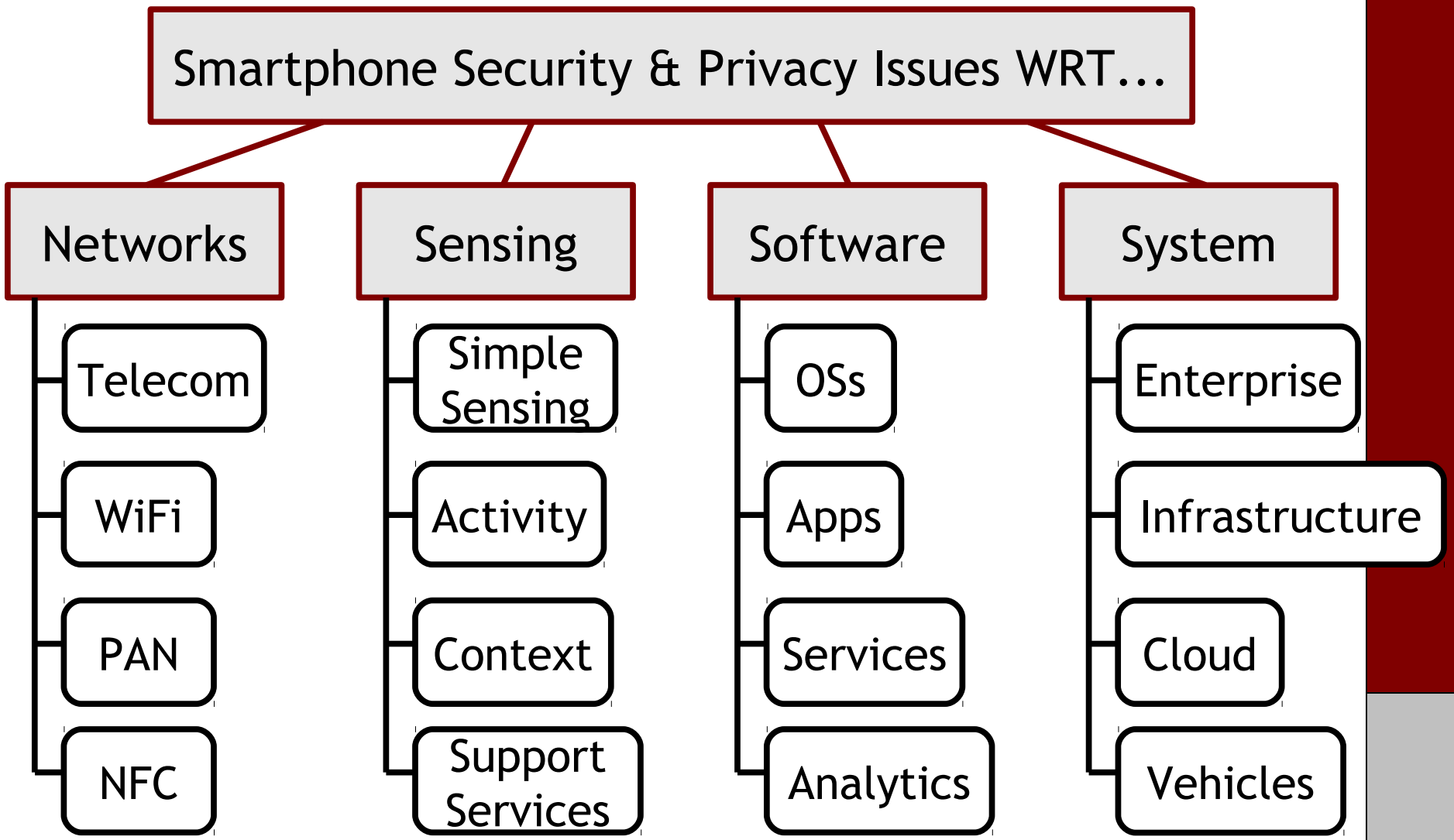
- Exploration and critical analysis of security and privacy issues in mobile systems
  - What are the security concerns in mobile devices?
  - What will the concerns be in ***N*** years?

Course Objectives

- Topics include:
  - Mobile network security & vulnerabilities
  - Mobile app & web security
  - Secure network services
  - Mobile location privacy
  - Emerging threats and challenges
  - ...



Topic Roadmap



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 security-centric apps, services, protocols, etc.

- Cutting-edge research experience

Questions about Content?

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

Course Website

http://wnss.sv.cmu.edu/courses/14829/f13/

Deliverables

- Individual work
  - Two assignments
  - Mobile app audit
- Group project
  - Topic area survey
  - Three presentations (proposal, progress, final)
  - Two written reports (proposal + final)
- Exam

Individual Assignments

- Two hands-on assignments
  - Programming/app development component
  - Research/survey component
  - You're expected to learn a little bit of Android development
- Assignment details and deadlines will be online
- Individual → each student is responsible for doing their own work
  - Discussion is encouraged, but work is individual

Mobile App Audit

- Individual project for the course duration
  - Each student chooses an app, either something that already exists or something new
  - App should be relatively “feature-rich” (otherwise the audit isn't very exciting)

- Goal is to audit the app on various aspects covered in class
  - Outcome is a report on the overall security and privacy of the app, what could be improved, etc.
  - Report can be presented to original developer or used to develop your own app/service

Group Project

- Project details:
  - Teams of 3-4 students
  - Form teams + choose topic area very soon; topic area survey must be completed by October 9
  - Topic, scope, and schedule of milestones / deliverables set by October 14 (proposal deadline)
  - Progress report in early November
  - Final presentation in early December
  - Final report due December 11

Exam

- Individual in-class exam
- Open-books, open-notes
- About ¾ through semester, tentatively 11/18

Important Dates

All important dates are on the course schedule:
http://wnss.sv.cmu.edu/courses/14829/f13/schedule.php

14-829: Mobile Security - Fall 2013

Daily Schedule, Notes, & Papers

Note: all topics and dates are subject to change.

Date	Topic	Reading
Aug 26	Course Introduction & Logistics	[1]
Aug 28	Mobile Device Components and Security Challenges	
Sep 2	**NO CLASS - Labor Day**	
Sep 4	Telecom from 1G to 4G	
Sep 9	Telecom System Security	
Sep 11	WiFi and Mobile WiFi	
Sep 16	WiFi Security & Privacy	
Sep 18	Personal Area Networks	
Sep 23	PAN Security Challenges	
Sep 25	NFC and Mobile Payment	
Sept 30	Smartphone Sensing - **Assignment #1 Due**	
Oct 2	Location Services	
Oct 7	Mobile Cloud Computing	
Oct 9	The Internet of Things - **Survey Deadline**	
Oct 14	**Project Proposal Due**	
Oct 16	Mobile OS Models	
Oct 21	Mobile App Security & Privacy	
Oct 23	Mobile Malware	
Oct 28	Android Security - **Assignment #2 Due**	
Oct 30	iOS Security	
Nov 4	**Project Progress Reports**	
Nov 6	**Project Progress Reports**	
Nov 11	Location Security & Privacy	
Nov 13	BYOD	
Nov 18	**Exam**	
Nov 20	CROSSMobile	
Nov 25	TBD	
Nov 27	**NO CLASS - Thanksgiving Break**	
Dec 2	**Final Project Presentations**	
Dec 4	**Final Project Presentations**	
Dec 11	**Written Project Report and Mobile App Audit Report Due**	

How to Contact Us

- Instructor: Patrick Tague
  - Email: tague@cmu.edu
  - Office: B19 1029
  - Phone: 650-335-2827
  - Skype: ptague
  - Office hours: Open-door, open-calendar, by appt
    - Public Google calendar under patrick.tague@west.cmu.edu

- TA: Yuan Tian
  - Email: yt@cmu.edu
  - Office hours and other details TBD (see web)

Some Syllabus-type Details

- Class meetings:
  - Mon/Wed 10:30-11:50am PDT (1:30-2:50pm EDT)
  - B23 118 @ SV campus, INI DEC @ 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

- Several papers will be assigned to read for every class day
  - Don't be surprised to see 100+ pages of reading/week
  - Most of these are research papers and can be read efficiently (not like a textbook)
  - **Helpful hint:** read the pamphlet posted for reading material today
    - Print it, fold it, learn it, love it

Grades

- Individual work – **25%**
  - 30 pts per HW, 40 pts for the Mobile App Audit
  - Late submission: 10%/day penalty, up to 2 days
- Group presentations – **30%**
  - 20 pts each for project proposal and progress
  - 50 pts for final project presentation
  - 30 pts for the survey
- Written project reports – **25%**
  - 20 pts for proposal, 80 pts for final report
- Exam – **20%**
  - 80 pts

Important 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 assignments must be done individually
  - Copying in any form constitutes cheating, ask if it's unclear
- **Plagiarism**: no copying, attribute ***all*** content sources
- For this class – ***Wikipedia is NOT a reputable source***
- **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.

August 28:
Mobile Device Components & Security Challenges

More discussion of course deliverables