Mobile Security
Fall 2015

Patrick Tague

#2: Mobile Devices and
General Security Challenges

Class #2

- A few reminders, announcements, and notes
- Decomposing a smartphone
- Some general S&P issues
- More discussion of projects

Waitlists

- If you want to get off the waitlist, you need to contact me TODAY
  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?

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

Assignments #2-#4

- You'll be doing active development, testing, and analysis of Android applications
- Deadlines are all on the website, details will be posted there too
- Most likely, what you do in Assignment #1 will affect your work in Assignment #2, which may affect Assignment #3, which may affect Assignment #4...consider this fair warning

Course Projects

- First project group presentation is in September → form groups and choose topics soon!
  - Mid-Sept presentation requires a literature survey, forming a high-level problem statement, and prep
- Blackboard discussion forum
  - Discuss project topics, find common interests, form teams, share related work, etc.
- Some additional HW available if needed

Android Devices

- We will loan an Android phone or tablet (w/o service) running Android 5.1+ to each student
  - Feel free to modify software at will, I'll reset them

- These devices belong to CMU – **treat them well or you'll be responsible for replacing them**
  - By accepting one of our devices, you are promising to return/replace everything we provide (otherwise, you'll get an incomplete and won't be allowed to graduate)

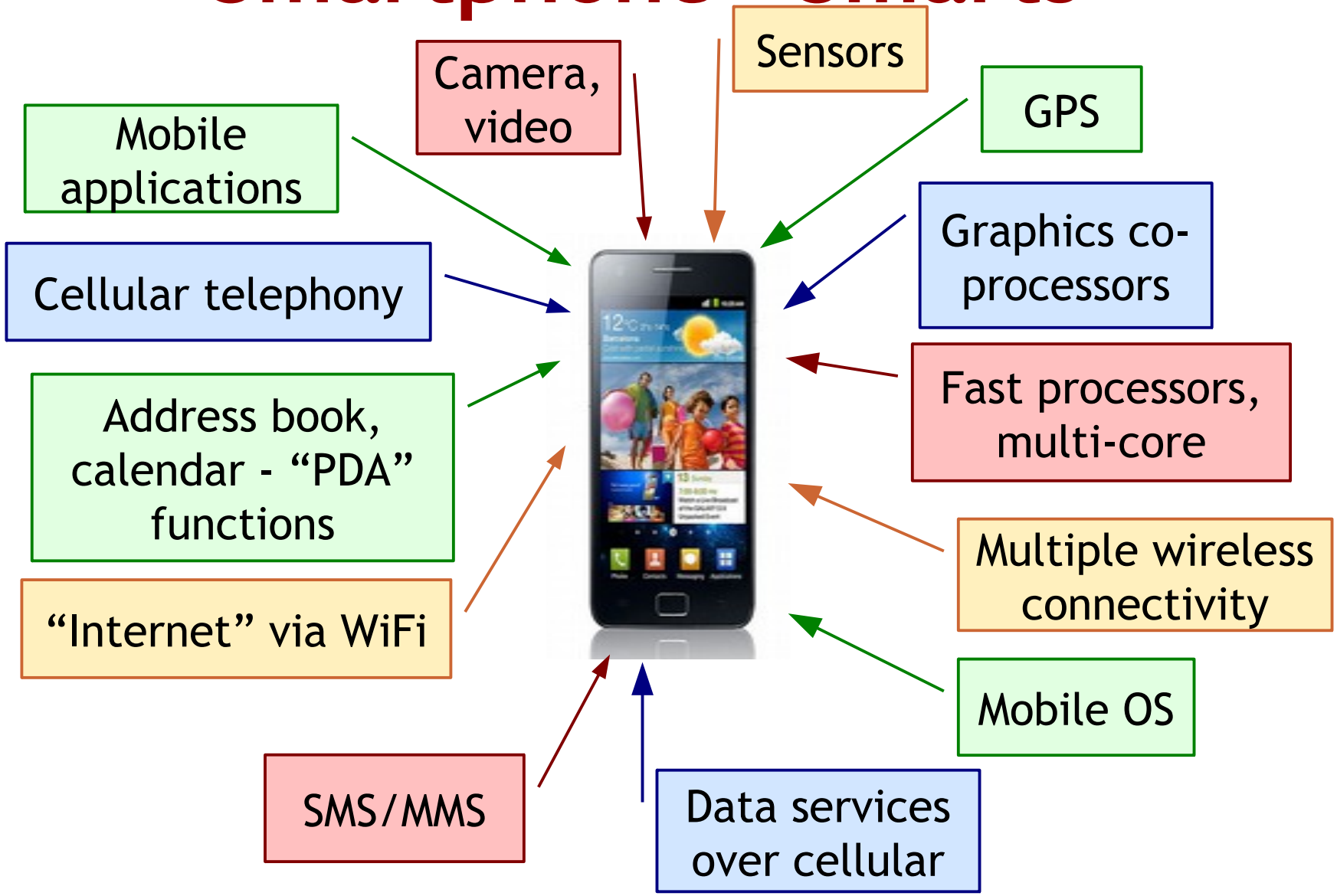
- If you decide you want to use your own phone, let us know (not really recommended)

Questions?

What is a Smartphone?

- Personal computer in phone form factor
- Phone that supports (3rd party) applications
- Phone with advanced OS
- Computing device with telecom capabilities
- … w/ Internet capabilities
-

Smartphone "Smarts"



So a Smartphone is...

Smartphone Components

Communication / networking

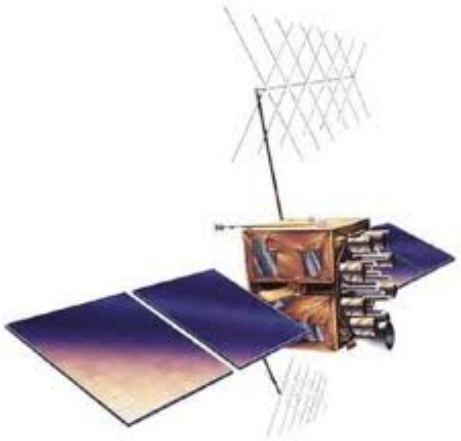
Computation / processing

Sensing / actuating / control

Entertainment / gaming

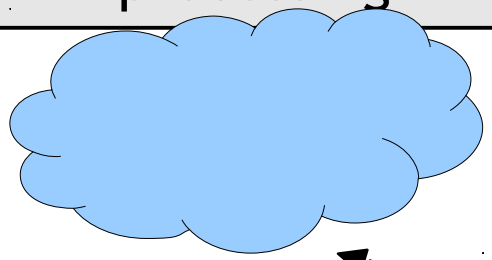
...

System Interactions



Mobile Computing

Cloud computing / processing



Embedded computing

Infrastructure-based computing, “cloudlets”

Onboard computing (single- or multi-core, GPU, …)

Collaborative / Peered processing

Mobile Operating Systems

- In order to deal with the variety of systems, services, and applications, elaborate operating systems became necessary
  - Aliyun, Android, bada, BlackBerry, Boot2Gecko, Brew, GridOS, iOS, Linux, Maemo, MeeGo, MXI, Palm, QNX, Symbian, Windows (Mobile / Phone / 8), Tizen, webOS
  - Each operating system has different standards, services, styles, behaviors, foci, interactions, etc.
  - Each operating system has different vulnerabilities...

Mobile Applications

- Mobile and web apps have emerged as the glue that binds all of the services and systems together to provide the mobile experience

- Apps have become a “service mash-up” with no limits in sight

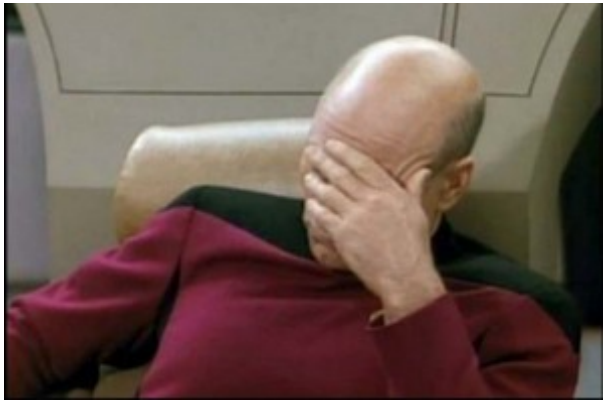
Risks and Realities

- When the Internet was born, nobody envisioned the threats we would face in coming decades

- We like to say *"We learn from our mistakes, and we won't make them again"...*

- Not surprising...

  Nobody envisioned the threats we would face in the mobile domain



As it turns out...

- Mashing together all of these services on one device...
  - Yeah, maybe we should have thought that one through a bit more...
  - The mashup of apps, protocols, services, and features of modern smartphones has opened the door to threats that **nobody completely understands**
  - The complex system-of-system mobile architecture continues to expose new threats, and probably still hides several other ones...

Examples

- Malware distribution has diversified
- Social networking apps can steal your private information
- Web browsers can interact with apps to subvert web-only or app-only protections
- Standard WiFi operations expose sensitive context information
- Sensors on your phone can leak your password
- Others?

Looking Forward

- During the semester, we'll study various aspects of security and privacy in smartphone systems
  - There's no way we can talk about everything!
  - This is where course projects and later assignments come into play: you have the freedom to expand topic coverage in whatever way you like

Toward Project Topics

- When thinking about project topics:
  - Don't limit yourselves to apps – think about different components, inter-dependencies, interactions, …
  - Pick an exciting topic, not an easy one – we'll grade you based on effort, not results
  - Be creative! Be innovative!

Sept 8:
Brief History of Telecom Security

Sept 10:
Telecom System Security Issues