Wireless Network Security
Spring 2015

Patrick Tague

Class #1 – Course Introduction & Logistics

Class #1

- Brief overview of the course
- Logistics
- Course information
- Talk about projects (if there's time)

What is this course all about?

What is Security?

A system is secure *with respect to a certain property* if one can **guarantee that property** with a reasonably high probability

What is Wireless Network Security?

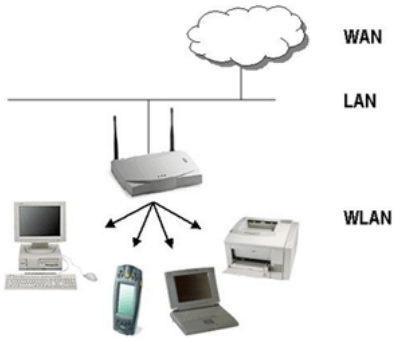
A probabilistic guarantee that a wireless network does its job *as expected*, even when faced with *a variety of threats*

Focus on the Networks

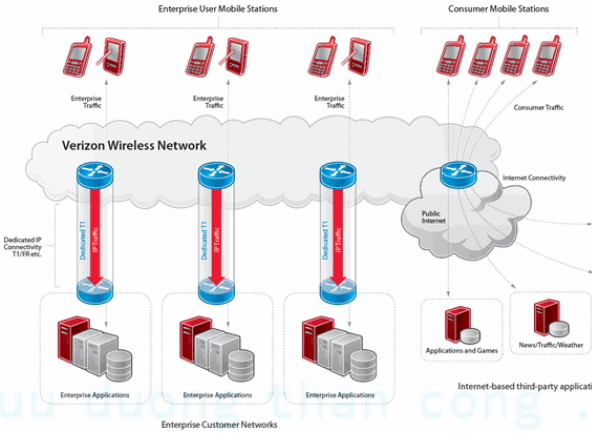
- In the Wireless Network Security course, we'll study:
  - Different network systems
  - Underlying technologies
  - Applications, systems, services, relying on them
  - Threats, security issues, privacy concerns, etc.

Wireless Networks

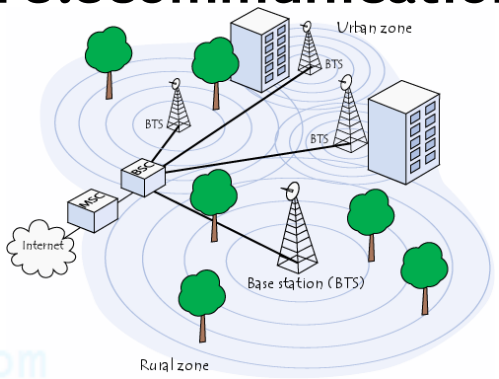
Enterprise Wireless

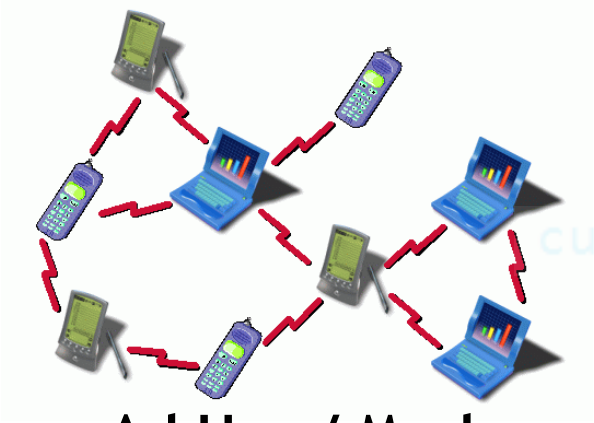


Wireless Internet

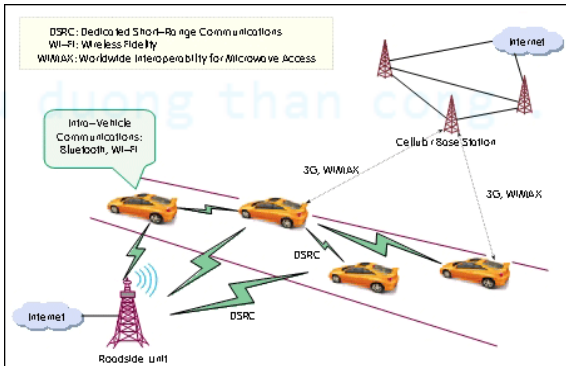


Telecommunications

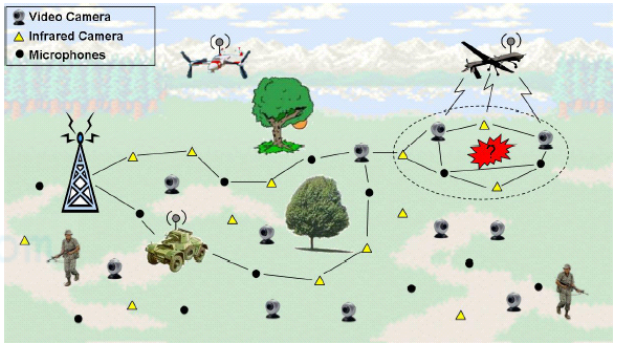




Ad Hoc / Mesh



Vehicular Networks



Sensing / Control Systems

Fundamental Challenges

- Wireless is open / shared
  - User/device/system verification is more difficult
  - System resource availability often cannot be guaranteed

- Wireless → batteries → resource constraints
  - Security costs $$$, time, energy, CPU cycles, bandwidth, scalability, etc.

Practical Challenges

- Wireless network protocols were designed around wired protocols
  - Higher layers were originally the same, until people realized it didn't work well
- Security mechanisms were (unfortunately) treated quite similarly
- Layered model doesn't translate well for all desired security properties
  - e.g. How to provide performance guarantees with only best-effort services?

Practical Challenges

- Not all wireless systems follow Internet-style (client-server) models
  - Ad hoc networks, sensor/actuator networks, fog
  - We must change the way we think about security!

- There are a lot of trade-offs between security, efficiency, performance, scalability, ...

Practical Challenges

- Each different network type, context, etc. has different properties, features, goals, ...
  - Protocols designed for WiFi Internet access probably shouldn't be used for safety-critical systems in cars...
  - Best-effort data delivery probably isn't sufficient for handling distributed control system inputs
  - ...

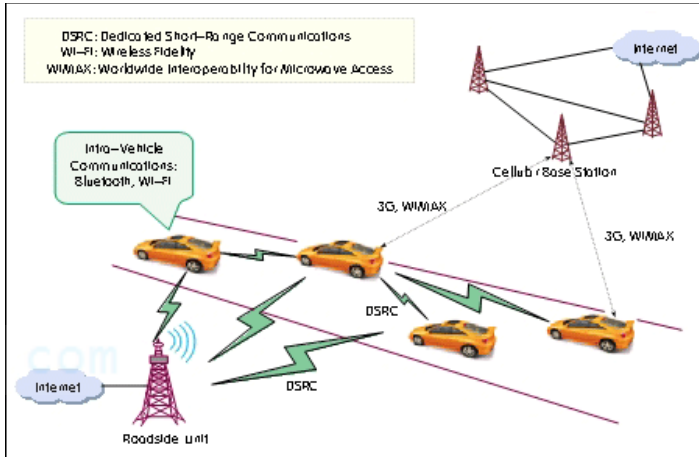
Diverse Wireless Systems

Each of these types of wireless networks has different structure, function, and purpose

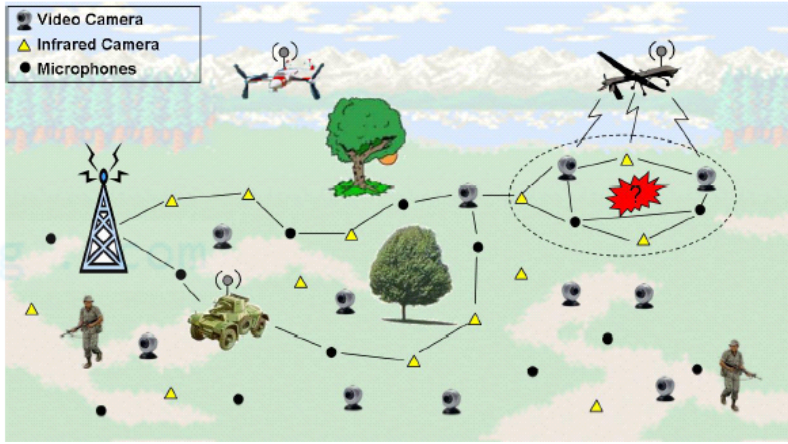
As such, we expect each to have **different functional and security requirements**

Course Objectives

- Understanding various security and privacy issues across different types of wireless systems



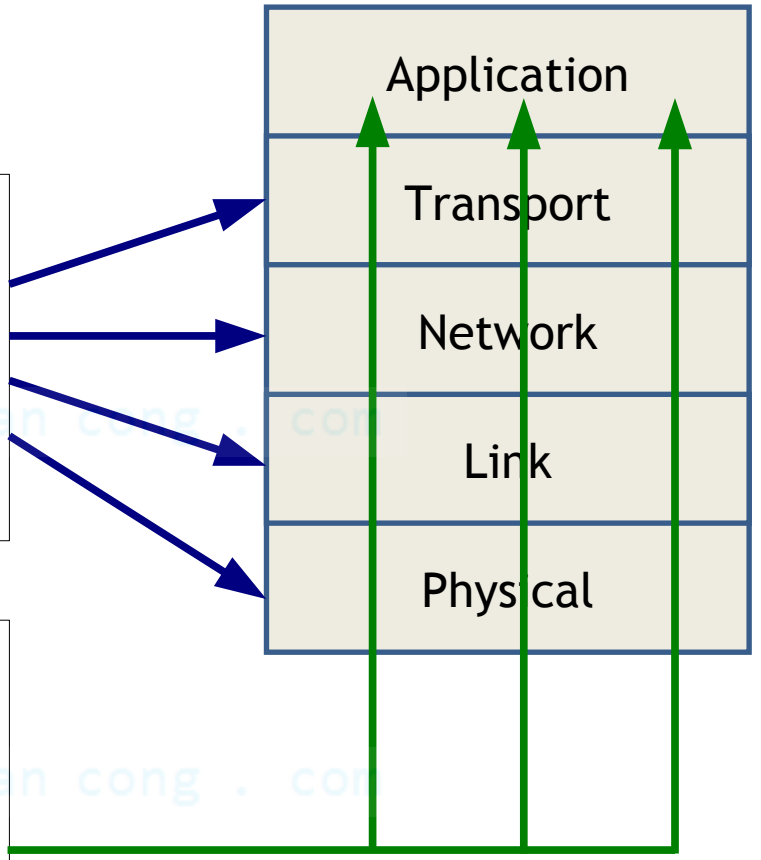
- Coverage includes both *classical* and *next-generation* wireless systems
  - WiFi networks
  - Mobile/telecom networks
  - Ad hoc & mesh networks
  - Distributed sensing and control systems



Course Roadmap

I) Layer-by-layer study of general wireless threats, issues, protections, etc.

II) Application-centric ("vertical") study of security and privacy issues



Goals of the Course

- Understand the inherent vulnerabilities of wireless networking

- Know what to consider in designing wireless systems, services, and applications

- Hands-on experience in vulnerability analysis and secure system/service/protocol design

- Research experience w/ publishable results

Questions about Content?

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

Logistics

Course Website

http://wnss.sv.cmu.edu/courses/14814/s15/

also a Blackboard page

Prerequisites v. Assumptions

- While this course has no official prereqs, we make several assumptions about you
  - 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)
  - You are a decent programmer (esp. C/C++) and can pick up new programming skills easily
  - We will not explicitly teach you these things, so some additional work may be needed if you don't match our assumptions

Registration

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

If your location is:	If your home dept is: ECE	If your home dept is: Not ECE
Pgh	18637 A	14814 A
SV	18637 SV	14814 SV

Waitlists

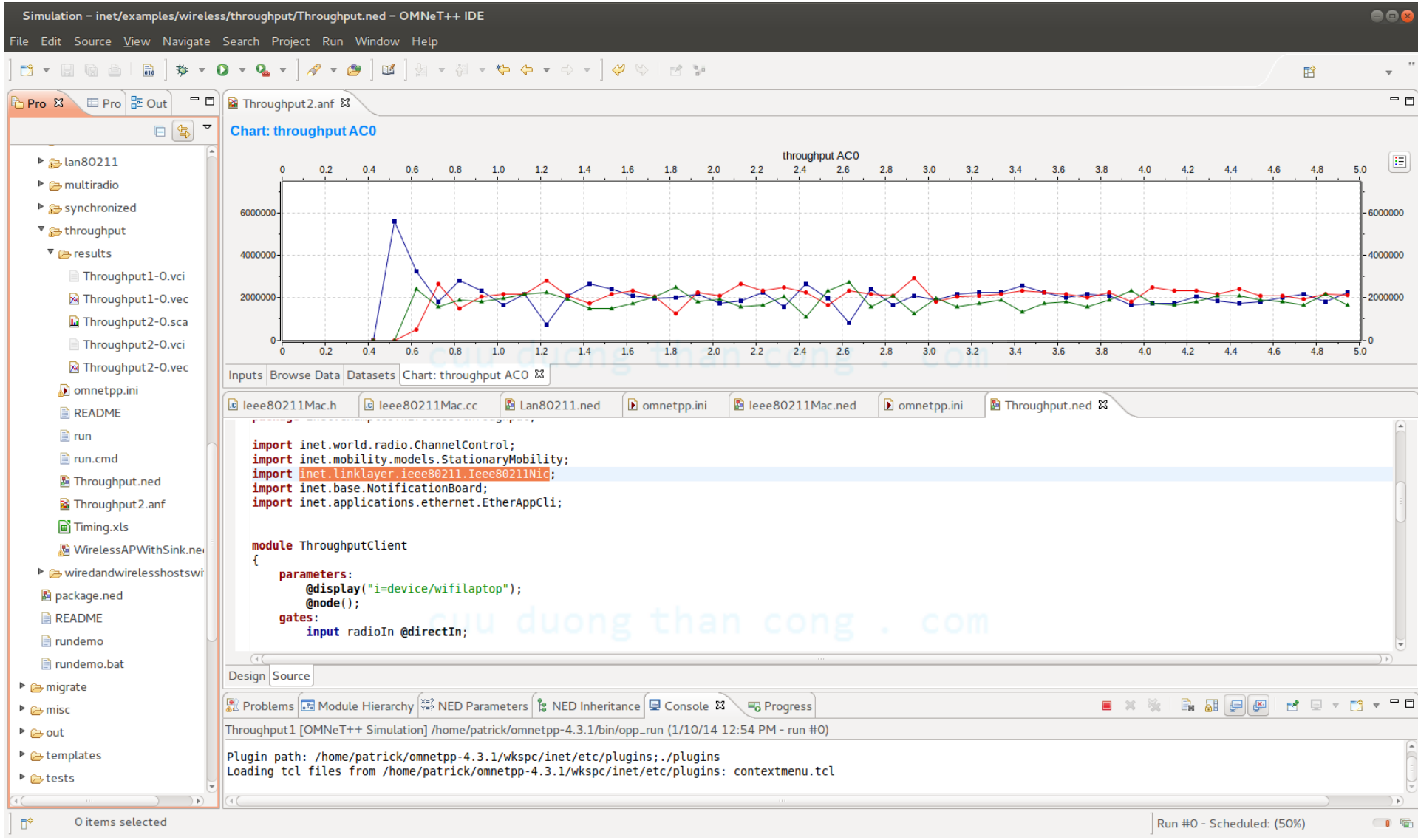
- If you're currently registered for this class, but not planning to stay: **please drop**

- 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?
     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 (intro, 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



Group Project

- Project details:
  - Teams of 3-4 students
  - Option to work on “sponsored project” or come up with your own project
  - First presentation on project background and topic proposal will be in **early February**, so form teams and get started soon
  - Statement of Work due and presentation on **Feb 26**
  - Progress report in **early April**
  - Final presentation in **late April**
  - Final report due **May 7**

What topic should I choose?

Project Topics

- Projects must:
  - Relate to systems covered in class and focus on some aspect of wireless network security
  - Strive for new research/development contributions – plan to submit a conference paper, poster, or demo
  - Not be a project you're working on for your research or another course (no double-dipping)
- Examples of past projects:
  - Attacks against location privacy in WiFi systems
  - Attack-resilient multi-path routing in MANETs
  - Localization in the presence of jammers
  - Detection of spoofing in VANETs
  - Secure dynamic address management in VANETs

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 an advisor/mentor
  - Any faculty member, researcher, or suitable PhD student can "sponsor" a project – let me know if you want to arrange an external project sponsor
- Project output will include a paper, poster, and demo
  - Aim for conference-quality results
- Some hardware may be available, if needed

Exam

- Individual in-class exam
- Closed-* exam, conceptual questions
- About ¾ through semester, tentatively **April 7**

Important Dates

All important dates are on the course schedule:

http://wnss.sv.cmu.edu/courses/14814/s15/schedule.php

Contact

- Instructor: Patrick Tague
  - **Email: tague@cmu.edu**
  - Office: B23 218
  - Phone: 650-335-2827
  - **Skype: ptague**
  - Office hours: Tues 1-3pm *Pacific Time* via Skype **only**, other times by appointment
    - Public Google calendar: **http://goo.gl/FIVbRK**
    - For an appointment, find an open time on my calendar and send an email to request a meeting (specify in person, Skype, etc.)

Some Syllabus-type Details

- Class meetings:
  - Tues/Thurs 10:30-11:50am PST / 1:30-2:50pm EST
  - B23 212 @ 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
    - Seriously, print it out and read it...several times. A few minutes now could save many hours later.

Important Policies

- **Academic Integrity:** all students are expected to adhere to academic integrity policies set forth by CMU, CIT, ECE, INI, etc. See
  - https://www.ece.cmu.edu/programs-admissions/masters/academic-integrity.html
  - http://www.ini.cmu.edu/current_students/handbook/index.html
  - http://engineering.cmu.edu/current_students/graduates/policies.html
  - http://www.cmu.edu/policies/documents/Academic%20Integrity.htm
- **My Collaboration Policy**: 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
- **My Wikipedia 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

- First assignment has been posted online
  - Please get started as soon as possible, it's due in 2 weeks
  - This assignment mainly attempts to get you comfortable with OMNET++ programming and simulations
    - We'll do a small tutorial next week to help, but try to get started on your own
  - OMNET++ is available for most platforms
    - If you're familiar with Linux, probably best to go that route
    - If you're not good with Linux, Windows is a good option
    - If you prefer OSX, it seems to work fine
      - We reported some bugs last year that we believe were fixed

January 15:
Wireless Security Basics & Threat Models