Wireless Network Security
Spring 2016

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?

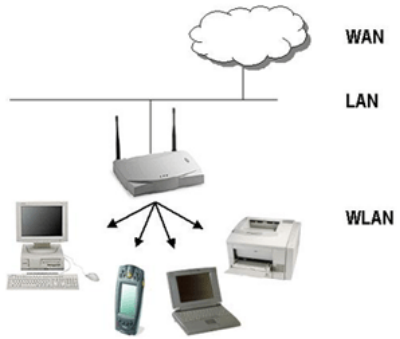
A probabilistic guarantee that a wireless network does a particular job *as expected*, even when faced with *a variety of threats*

Focus on the Networks

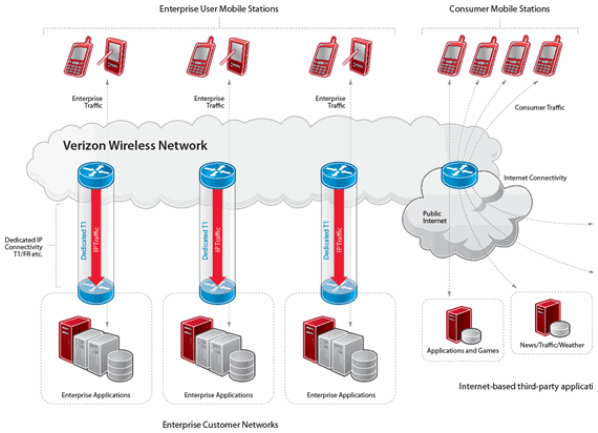
- In the Wireless Network Security course, we'll study:
  - Different network systems
  - Underlying technologies
  - Applications, systems, services relying on them
  - Threats, security issues, privacy concerns, etc.

Wireless Networks

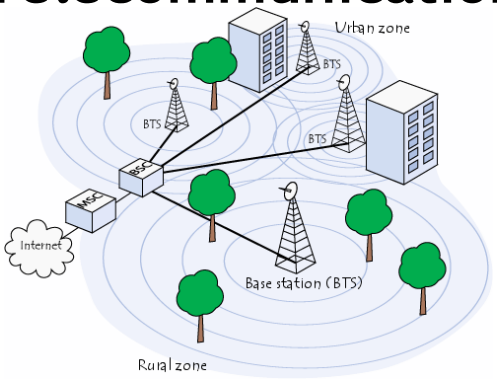
Enterprise Wireless

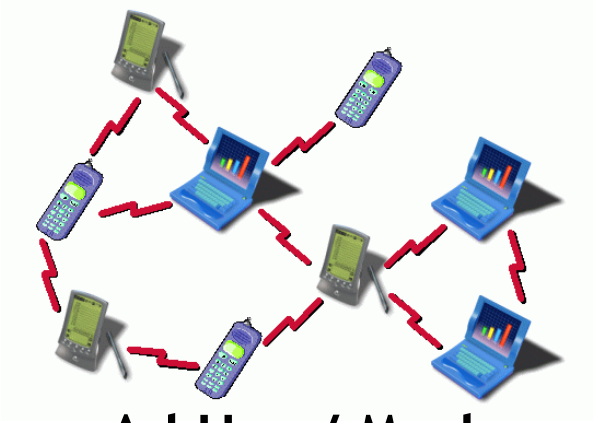


Wireless Internet

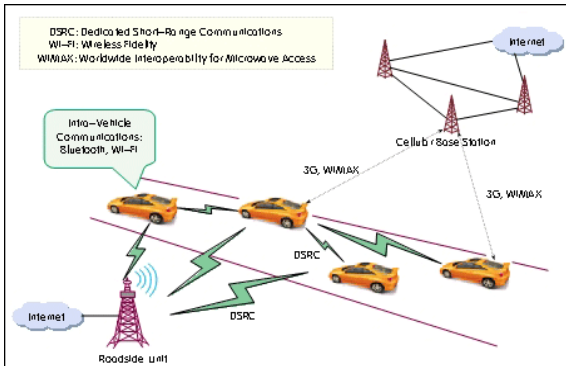


Telecommunications

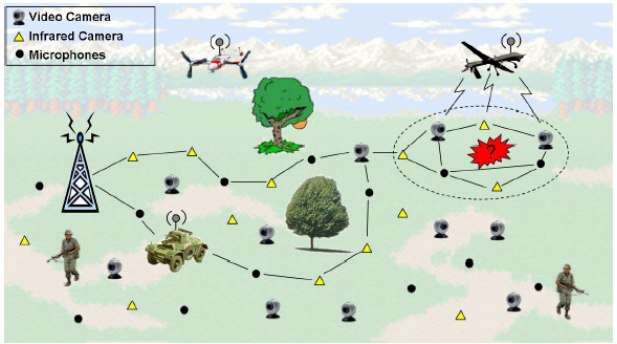




Ad Hoc / Mesh



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
  - ...

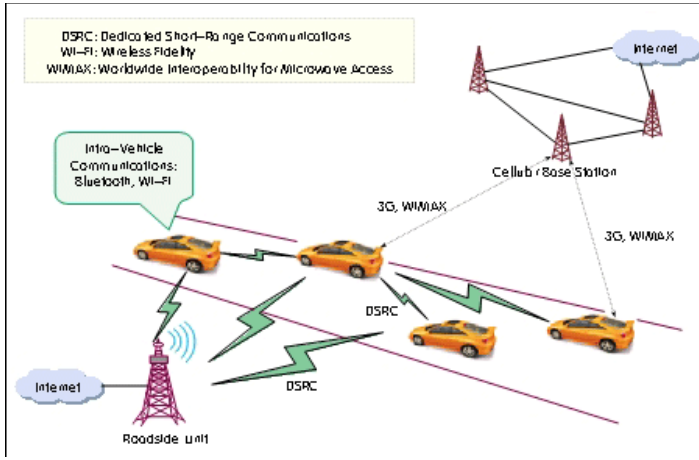
Diverse Wireless Systems

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

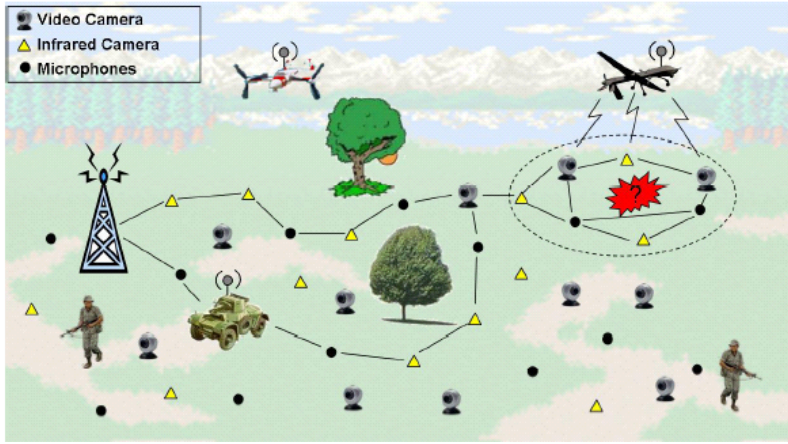
As such, we expect each to have **different functional and security requirements**

Course Objectives

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



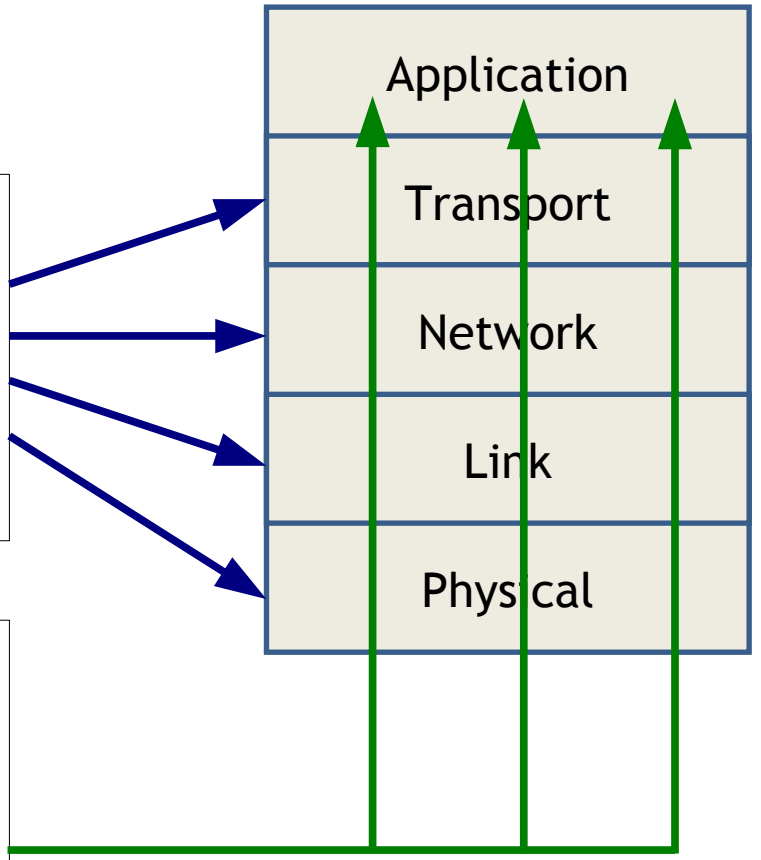
- Coverage includes both *classical* and *next-generation* wireless systems
  - WiFi networks
  - Mobile/telecom networks
  - Ad hoc & mesh networks
  - Distributed sensing and control systems



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://mews.sv.cmu.edu/teaching/14814/

also a Blackboard page

Prerequisites

- This course has official prereqs
  - You are a graduate student
  - 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)

Additional Assumptions

- In addition to the official prereqs, we assume:
  - You are a decent programmer (esp. C/C++) and can pick up new programming skills (language extensions, IDEs, tools, etc.)
  - You know how to use the Interwebs on your own to find manuals, tutorials, etc. to help you with the above

Registration

- This course has 4 concurrent sections
  - 14814 and 18637, section A and SV
  - If you are in Pittsburgh, register for section A
  - If you are in Silicon Valley, register for section SV
  - If you are an INI student, register for 14814
  - If you are an ECE student, register for 18637
  - Else, whatever

Waitlists

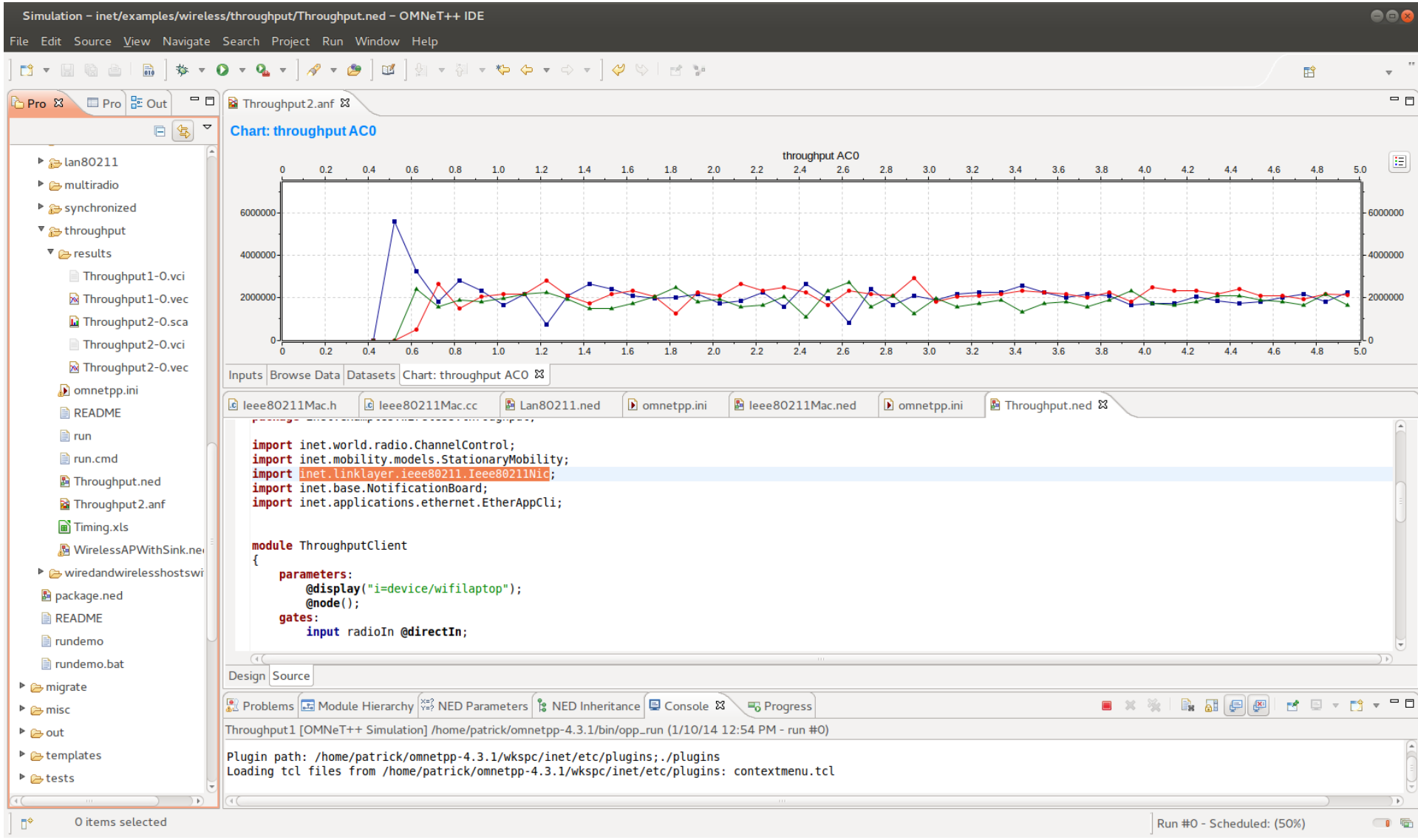
- If you're currently registered for this class, but not planning to stay: **please drop**

- 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** (if any) 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
  - Flexibility in project topics – can be industry-mentored, led by a CMU faculty member, or 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 in **late Feb**
  - Progress report in **late March**
  - Final presentation in **late April**
  - Final report due **May 5**

Exam

- Individual in-class exam
- Closed-* exam, conceptual questions
- About ¾ through semester, tentatively **April 5**

Important Dates

All important dates are on the course website

Contact

- Instructor: Patrick Tague
  - **Email: tague@cmu.edu**
  - Office: B23 218
  - Phone: 650-335-2827
  - **Skype: ptague**
  - Office hours: by appointment
    - Public Google calendar: **http://goo.gl/FlVbRK**
    - 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 211 @ 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!***
  - Reading research papers is not like reading textbooks, they're much more forgiving and can be read efficiently
  - If desired, I can teach you how to read a research paper very quickly

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

- 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 or OSX seem to work fine
    - I run OMNET++ in a VM, so it doesn't mess with anything else
    - I recommend the new OMNET++ 5.0b3 (still in beta)

January 14:
Wireless Security Basics & Threat Models