Discussion:
Two finals, one normal time, the other Wednesday @ 11am CS110

What is wireless?

**Client**: laptop, tablet

**Access Point**: the wireless "provider"

uses radio waves to send signal

**Wireless issues (our homework)**

- More accessible
- Physical access not needed
- More convenient / mobility

How are we exposed on wireless?

- Accidental identification: accessing wrong network
- Malicious intentions: purposely posing as wifi network to perform malicious action
- MAC address spoofing
- Man in the middle attack: sitting in between a "conversation"
  - Active
  - Passive
- Network injection: gaining access to network infrastructure
  - Hide SSID; turn off broadcast
  - Encrypt your wifi
  - Create a whitelist of who can access

**Business networks:**

- Strong perimeter security is no longer ideal for network security
  - At home users
  - Public-facing Services
  - BYOD - bring your own device
    - hard to administer
    - good because it's free (for the company)

**Mobile Devices**

- Location services are insecure
- Loss/stolen is easy
- Physical access is hard with sysadmins
How does wireless work?

- MAC layer is used to transfer messages to stations
- MAC communicates with an MPDU to find proper NTC
- Transmission protocol packets to the MAC layer

**Slides**

**Security**
- Wireless is susceptible to DoS attacks.
  - Easy to jam the signal
- Mobility is an issue as they have more risks

**Threats**
- DoS
- MAC spoofing
- Man in the middle
- Ad-hoc
- Malicious association

**Security wireless**
- Encryption/authentication is standard countermeasures
Mobile Device Security:

- Cloud based apps
- Growing use of new devices
- DC - perimeterization - less defined perimeters

Threats:
- Lack of physical security
- 3rd party apps
- Untrusted content

802.11a was bad, untested spec for wireless

802.11b first real wireless protocol

802.11g Better generation of wireless

802.11n

802.11ac newest/fastest