Access control

- Interface-based access control
  - Restrict by MAC address (like Stanford)
- Network-based access control
  - Restrict by incoming IP or domain
- Can be defeated
  - Put your network card in promiscuous mode and forge the source MAC address or IP address
  - Poison ARP caches with fake IP to MAC mappings that point to your MAC address

Spoofing TCP Source

- Send SYN with forged source IP
- SYN-ACK goes to that forged IP, but DoS him with syn flooding so he won't RST your connection
- Then guess the ACK seq # and send the guy data anyway
- Another way: desynchronize a real stream so that the real source can never send data; then you can inject data at will
- Related: see 3rd review session for numbers on a TCP RST attack

Denial of Service Attacks

- TCP SYN flood
  - OS allocates connection state upon getting a SYN packet
  - After a certain amount of incomplete SYNs, memory is used up and no new connections can be made
  - Solution: Defer state setup and use SYN cookies
- Indirection attacks
  - Make some request to a service that has a big payload as a response, with the target's IP as a spoofed source IP
  - Big payload goes to source == more amplification
- More powerful if you own a botnet and can ask for thousands of computers to do the attack, creating a DDoS (distributed denial of service)

Browser Level: Same Origin Principle

- Used in the browser, especially JavaScript
- A script running on a webpage on one domain cannot query or modify the properties of a webpage running on another domain
  - Otherwise, I could write a webpage that loads an IFRAME set to facebook.com
  - You are already logged into Facebook, so the IFRAME loads your Facebook cookie
  - I ask for that document's cookie and get your Facebook cookie
  - I become you on Facebook, and post something horrible
  - ???
  - Profit!!!
- Vulnerable to DNS attacks, since it is domain based
- Many other vulnerabilities, but too many to cover in this class (i.e., cross-site scripting)

Other Attacks

- DNS
  - Faulty glue records can poison cache
- ICMP Redirect
  - Allows you to change a host's routing table
- RIP/BGP attacks
  - No real authentication
  - You can advertise paths to networks you have no routes to with 0 cost
    - Now everyone routes through you and you

Cryptography

- Symmetric-key cryptography
  - Encrypt(Key, Plaintext) = Cipher
  - Decrypt(Key, Cipher) = Plaintext
- Public key cryptography
  - Encrypt(Key, Plaintext) = Cipher
  - Decrypt(Key^{-1}, Cipher) = Plaintext
  - Some function to generate the public/private key pair
- Hash functions (MD5, SHA1, …)
  - Take a large message and hash it to a number in a fixed-sized range of values
  - Example: MD5 hashes arbitrary-length message into 128 bits
  - Lets us know if a message has been modified in transit to a good probability
  - Append shorter hash (MAC) of message to the message, then transmit Send (Encrypt(Key, Message) + Hash of that encrypted msg)

Symmetric Key Cryptography

- One-time pad
  - E(K, P) = K XOR P = C
  - D(K, C) = K XOR C = P
  - Downside: hard to distribute key, key can't be reused, key length must be same as message
- Stream ciphers
  - Generate pseudo-random pad from a shorter key, then XOR as above
- Block ciphers
  - ECB mode: encrypt each block independently of other blocks
  - CBC (cipher-block chaining): output of each block depends on feedback from previous block
  - Which is preferable?