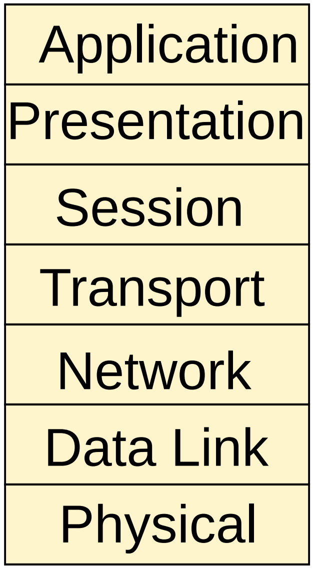
CSE561 – Network Security

David Wetherall

djw@cs.washington.edu

Network Security

- Focus:
  - How can protocols be abused?



Application

Presentation

Session

Transport

Network

Data Link

Physical

Take-home exam

- Available from CSE660 (Mel/Julie) starting Mon 6/7
- Must return to David's office CSE654 by 5pm Fri 6/11
  - Just slide it under the door …

- 3 hours, design-oriented questions (not like homeworks)
- Open textbook/notes, but no Web or non-course papers
- On the Honor system.
  - Strictly no discussion of any exam material, problems or solutions, with anyone else in the class or out of it. Seriously.

Network security

- Threat model
  - Know what you are trying to stop, under what assumptions
  - Real security is risk management, not mathematics

- Encryption can be used for:
  - Message confidentiality, integrity, authentication
  - With symmetric (secret) and asymmetric (public/private key) methods

- Computers can be compromised
  - Many, many implementation vulnerabilities

- Take a security course!

Two issues

- Administrative boundaries
  - What should we do to secure the boundaries between networks?
    - e.g., one ISP to another, Internet to customer
  - Q: what does IP do for us? A: nothing

- How can protocols be co-opted or otherwise abused?
  - Even when they are implemented correctly; no bugs
  - “Don’t think of TCP as a protocol, think of it as an opportunity,” StefanSavage
    - e.g., traceroute w/ IP/ICMP, Sting for TCP
  - Can attack or interfere with resource allocation

Administrative boundaries

- Firewalls
  - Scalable point of defense
  - Break/allow connectivity
  - Useful, but brittle
- ISP boundaries
  - Accounting
  - Check IP addresses (ingress filtering, e.g., uRPF)
  - Filter routes (BGP policy)
  - Block "control traffic" with routes and over multiple hops

"Oh hey! I just love these things!
...Crunchy on the outside and a chewy center!"
Copyright Gary Larson, 1980. All rights reserved.

Co-opting protocols

- IP (packet format, affects forwarding)
  - Can send anything, anywhere, e.g., spoof source address
  - Leads to packet floods, denial-of-service
  - Amplify with broadcast
- TCP (allocates bandwidth, server resources)
  - Can send or ACK aggressively; other connections pushed aside
  - Can tie up server state (SYN floods and 3-way handshake)
- IP/ICMP (returns error messages)
  - Can trigger unwarranted error messages, concealing source
  - Can tie up host resources (fragments that don’t reassemble)
- DNS
  - Can generate fake replies to change host to IP mapping