Networking Problems & Solutions

- Technical Problems
- Security Problems
No Physical Layer

- Wire not connected, hub not powered
- Wireless Access Point not turned on, not configured, or wrong password
- Hardware broken or about to break
  - computer hardware can fail
  - so can wires, fibers, etc.
- fix physical problem, or do the best possible with what is available
Ethernet Issues

- Wiring connected in a loop
- Failing Hardware
- Insane manufacturer reuses MAC addresses

- find and eliminate loop, or use STP
- replace (or live with) hardware
- buy from a different manufacturer
IP issues

- Bad routing tables
- Two hosts using the same IP address
- Interface mis-configuration

- use or reconfigure routing protocol
- provide DHCP
  - make sure you have enough addresses
  - NAT if necessary
TCP/UDP issues

- Congestion control and binary exponential backoff make TCP very slow when enough packets are lost
- Connections close when IP address changes
- NAT may “forget” slow UDP flows
- restart TCP connection
- send unnecessary UDP packets (keepalives)
HTTP issues

- Loss of privacy
  - cookies
  - 1-pixel images
  - Java and JavaScript
- Slow due to inadequate DNS service
  - and loading from too many sources
- ~ be careful with browser privacy settings
Email issues

- Spam, phishing
- Little or no authentication
- Insufficient encryption
- Remembered forever
- don’t trust links sent over email
- don’t trust email too much
- don’t send sensitive material over email
Social Network Issues

- Loss of control over privacy
- Remembered forever
- Intended audience may not match actual audience
  - future employers, potential spouses, etc.
- be somewhat cautious
- take advantage of SN privacy settings
DNS issues

- Names are globally unique, so only one can have each name
  - even if the name rightfully belongs to more than one entity
- Bad DNS servers
- UDP packet loss
- use better DNS servers, e.g. 4.2.2.1
Protecting computers

- Attackers sometimes break into computers

- firewalls

- secure protocols

- keep software up to date

- reduce the value of what is on the computer
  - e.g. don’t save SSNs unless required
  - same for passwords, bank info, etc.
  - encrypt (parts of) hard disk
Communications Privacy

- Use secure encryption algorithms: RSA, AES, one-time pad
- Use secure and authenticated key exchange
- Secure endpoints
  - no “shoulder surfing”
  - PIN should be entered securely
- Attacks: traffic analysis, man in the middle, unencrypted portion of traffic (e.g. DNS)
Authenticated Communication

- Digital Signatures
  - used for software releases
  - occasionally found in email
  - first, must securely exchange keys

- Certificates
  - Certificate Authorities

- Passwords
  - sometimes hard to remember
  - if written down, can be copied
Denial of Service attacks

• Denial of Service
  – if routers only forward packets that could legally have originated in their networks (same origin policy), it may be easier to track down attackers
  – other solutions: overprovision (use cloud)
    wait for attack to end
    identify attack packets, block at firewall
Human attacks

- Social engineering: convince or trick an insider into giving you the information
- Get people to follow a link to a website that can attack their browser
  - crafted email or advertisement
- Use a name similar to a popular name, wait for people to make mistakes
- In general, security that depends on people doing “what they should” is not secure
Game Theory

• The study of how incentives can be set up so people will want to behave as desired by the game designer

• E.g. second-price sealed-bid (Vickrey) auction rewards people who truthfully declare their value for the item

• People behave differently if the interaction is:
  - likely to be very limited (one-time)
  - likely to continue over time