Lecture notes for 7.3-7.4 Network defenses 1

[Suggest that students use textbook tables with attacks & defenses to guide their study]

Design for attack resiliency
- Redundancy / failover [reduce single points of failure]
- [Story of cnn.com on sep 11] [bring details]

Encryption [there was a reason for chapter 2]
- Provides authentication, confidentiality, & integrity
- Link encryption
  - Each hop encrypts differently
  - Ex: WEP / WPA / WPA2
  - VPN: give impression of private network over public Internet
  - Link encryption because it goes between client & VPN gateway server
    - [Draw a picture of that]
- End-to-end (for OS endpoints)
  - Encryption between client & server Oses
  - Ex: IPsec
- End-to-end (process endpoints)
  - Encryption between client & server processes
  - Ex: SSL (as a library)
  - [How is this different from OS endpoints regarding security?]
- Encapsulation: Wrap protected data w/ header indicating encryption info
- Advantages of lower layers: easy reuse, invisible to higher layers, apps unaware of encryption still benefit
- Advantages of higher layers: less opportunity for attack

Distribution of keys for encryption
- Secret key system: key distribution center (KDC)
  - Ex: Kerberos
- Public key system: certificate authority (CA)
  - Public key infrastructure (PKI)
  - Ex: Verisign
- All systems are management headaches

Protocol examples
- SSH (own negotiation of crypto use)
  - Key distribution done manually
- SSL/TLS
  - Certificate distribution done via OS
- IPsec (OS-to-OS endpoints, needs Ipv6)

- S/MIME (encrypted email)
- Kerberos (authentication)

Kerberos v4
- Secret key system
- Goal: Alice communicates to Bob w/ encryption & mutual authentication
- Entities: Alice, Bob, Ticket granting server (authenticates users & distributes secret keys)
- Objects: Ticket, Ticket granting ticket
- [LOOK THIS UP]
- Shortcomings: apps must be kerberized, kerberos does not scale

Wireless security
- Encryption between client & access point
- WEP (wired equivalent privacy)
  - Crackable in a few minutes
- WPA / WPA2 (Wifi protected access)
  - WPA2 uses AES

Traffic flow analysis
- Sigint
- Learn information simply by seeing who talks to who

Intrusion detection
- IDS monitors traffic entering / within network
- Honeypots attract attackers, monitor their activity
- Firewalls provide network access control

Firewalls
- Reference monitor for network, needs refmon properties
- Stateless packet filters
- Stateful packet filters
- Deep packet inspection
- Personal firewalls

Integrity protection
- Error correcting codes repair bit flips
- Cryptographic checksum / hash / digest
  - “hard” for attacker to recompute if alter message