Lecture notes for 7.1-7.2 Network Threats

[Draw picture]
- [Endpoints A & B]
- [Routers in the interior]
- IP addresses
- Routers pass to next hop closer to destination
- DNS system
- Port numbers

Internet properties
- Global scale
- Limit single points of failure (route around failures when possible)
- Human anonymity
- Heterogeneous networks / hardware / software

General network vulnerabilities
- Eavesdropping on network (incl. wireless)
- Replay / insertion
- Block traffic
- Malcode breaks out of sandbox (e.g. Java / JavaScript)
- Accidental misdelivery
- Theft of service (home user with open access point)

Web site vulnerabilities
- Web site defacement
- Directory traversal

DDoS
- Standard with zombies
- Reflection attack (difficult to identify sources of attack)

Exploration
- Port scans
- OS fingerprinting
- War driving

Address spoofing
- Attacker can generate packets with incorrect source address
- Consider: From: <VictimIP, echo> To: <VictimIP, echo>
- Egress filtering

MITM attacks
- [Use D-H key exchange from prog 1 as example]
- Users A & B, attacker C spoofs each identity to the other

Session hijacking
- Similar to MITM...
- Eavesdrop on communication between A & B
- Then take over one side of connection (say B) and pretend to be B

Routing attacks
- BGP vulnerabilities (Youtube vs. Pakistan)
- Route hijacking: advertise own network as route to victim's IP space

DNS attacks
- Poisoning: enter erroneous mappings of <VictimName, AttackerIP>
- Alter local DNS server settings to use malicious server with wrong entries
- Direct attack against DNS (9 of 13 root nameservers disrupted in october 2002)

Signal Intelligence (sigint)
- Analyze flows, even if cannot read traffic

Amplification
- Send to broadcast address