ICS 351: Today's plan

- Network Security
- Attacks
- Defenses
- Limitations
- Small-scale network security

Wireless Ad-hoc Networks: Security

- Monitoring networks can be used to detect forest fires or enemy attack
- An adversary (or a prankster) might wish to send a *false positive* signal
- Or a false negative, suppressing a real alarm
- It is likely that the adversary will obtain access to one or more nodes
- What should be protected?
- Which node(s) should be trusted?

Network Security

- Whenever the parties to an exchange have different goals, there is a potential for conflict
- Much of this is resolved through ethics and law
- But sometimes there is malicious behavior
- Attackers may be after resources, or attempt to deny resources to the target
- Resources include money (in many forms), network connectivity, human attention

Attacks

- Denial of service, usually by a flood of legitimate-looking packets, often from distributed senders (a botnet)
- Intrusion into, or takeover of a specific computer or computers, often by exploiting a weakness in a server or password, e.g. by a virus
- Snooping of traffic to obtain information, perhaps by forging DNS translations
- Transmitting undesirable information, e.g. spam

Defenses

- Detection of DoS attack, blacklisting of senders, more robust algorithms (e.g. SYN cookies)
- Firewalls to prevent connection from outside, Intrusion Detection Systems (IDS) to monitor traffic, honeypots to detect attacks, SELinux to restrict servers to only their design behavior
- Encryption, certificates, SSL/TLS, secure DNS, ssh
- Blacklisting, spam filters

Limitations

- Publishing a weakness can help the attackers
- Hiding a weakness encourages denial and complacency
- It is hard to prevent monitoring traffic volume
- Often can only defend against attacks that are already successful
- Security is expensive: software must be designed more carefully. If security gets in the way of getting work done, security often gets second place

Small-scale network security

- Firewall
- Use good passwords, keep them safe
- Use a reliable product to monitor traffic, especially web traffic: blacklisted sites, suspect javascript, SQL injection, etc
- Harden all of the servers (machines and programs) as much as possible, e.g. apache
- Install updates whenever they are available
- Keep short-term and long-term backups