Network Security
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Some Important Network Characteristics for Security

- Degree of locality
- Media used
- Protocols used

Degree of Locality

- Some networks are very local
  - E.g., an Ethernet
  - Benefits from:
    - Physical locality
    - Small number of users and machines
    - Common goals and interests
- Other networks are very non-local
  - E.g., the Internet backbone
  - Many users/sites share bandwidth

Network Media

- Some networks are wires, cables, or over telephone lines
  - Can be physically protected
- Other networks are satellite links or other radio links
  - Physical protection possibilities more limited

Protocol Types

- TCP/IP is the most used
  - But it only specifies some common intermediate levels
  - Other protocols exist above and below it
- In places, other protocols replace TCP/IP
- And there are lots of supporting protocols
  - Routing protocols, naming and directory protocols, network management protocols
  - And security protocols (IPSec, ssh, tls)

Implications of Protocol Type

- The protocol defines a set of rules that will always be followed
  - But usually not quite complete
  - And they assume everyone is at least trying to play by the rules
  - What if they don't?
- Specific attacks exist against specific protocols

Threats To Networks

- Wiretapping
- Impersonation
- Attacks on message
  - Confidentiality
  - Integrity
- Denial of service attacks

Wiretapping

- **Passive wiretapping** is listening in illicitly on conversations
- **Active wiretapping** is injecting traffic illicitly
- **Packet sniffers** can listen to all traffic on a broadcast medium
  - Ethernet or 802.11, e.g.
- Wiretapping on wireless often just a matter of putting up an antenna

Impersonation

- A packet comes in over the network
  - With some source indicated in its header
- Often, the action to be taken with the packet depends on the source
- But attackers may be able to create packets with false sources

Violations of Message Confidentiality

- Other problems can cause messages to be inappropriately divulged
- Misdelivery can send a message to the wrong place
  - Clever attackers can make it happen
- Message can be read at an intermediate gateway or a router
- Sometimes an intruder can get useful information just by traffic analysis

Message Integrity

- Even if the attacker can't create the packets he wants, sometimes he can alter proper packets
- To change the effect of what they will do
- Typically requires access to part of the path message takes