Mar 30, 2005 -- Lecture 26

22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

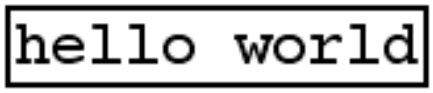
Network Threats

The obvious

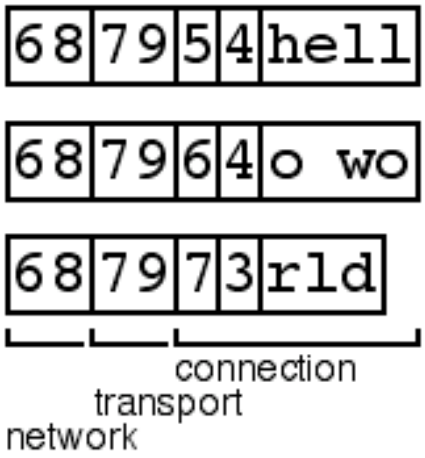
Wiretaps

interception of transmission
requires access to network medium

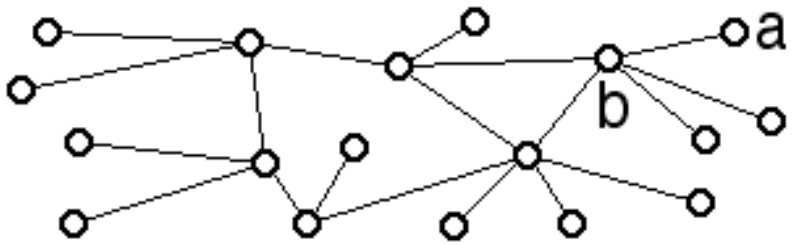
The data



What is sent



Topology

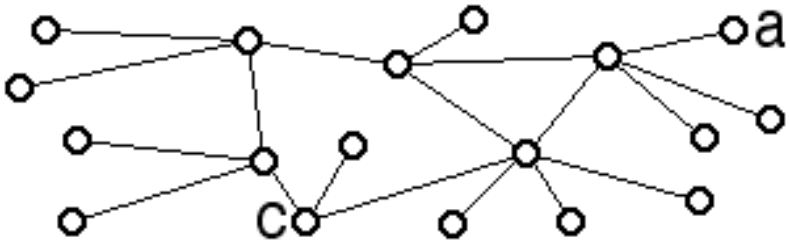


Suppose many machines talk to a
ping messages "are you there"

Service through b can be crippled
basis of a ping attack

Denial of Service to a
and all other users of b

More topology



Suppose someone broadcasts

c is on the fastest route to a!

network routing tables get updated.

Allows c to

Censor or monitor traffic to a

Allows others to

Create bottleneck at c

Recruitment

How does attacker get hosts to send pings

Social engineering

Get all your friends to ping Fred

Trojan horse attack through e-mail

Click on the attachment for XXXfun

Virus or worm attack

An insecure operating system on a network can threaten the integrity of the entire network!

A Major Problem Today

Viruses and trojans

- *used to recruit hosts to send spam*

Spam frequently comes from hijacked hosts

Could prosecute spam advertisers for

- *theft of computing resources*
- *hacking into computers not their own*

Simple solution?

- *Ban word, office, windows, express ...*
  - A bit drastic

Defense

Social engineering

don't respond to requests to ping

don't click on attachments, ever!

Universal coverage difficult.

Someone will ignore your advice!

Anti-virus software (and anti-trojan)

interferes with recruitment

The arms race will never end

because of computability limits

Firewalls to partition the network