

April 4, 2005 -- Lecture 28



22C:169

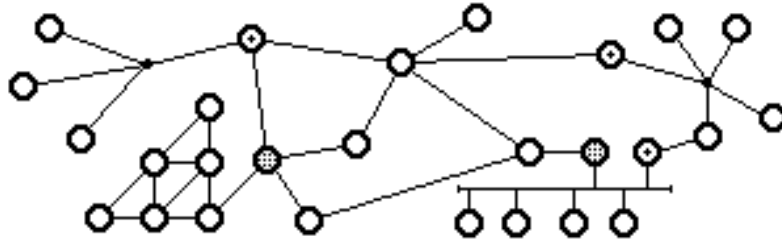
# Computer Security

Douglas W. Jones

Department of Computer Science

Firewalls

# What is an Internet




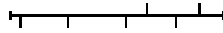
each interconnected differently

*10baseT, ethernet, point-to-point*

each with different mix of hosts

*PCs, Macs, supercomputers*

# Internet components

Hub    
*passive device*

Host   
*supports user computation*

Gateway or bridge   
*connects multiple networks*

Router   
*a gateway that isn't a host*

## **Good gateways crucial**

Morris's internet worm:

*1988, Robert Morris, student at Cornell,  
almost shut down the internet.*

Iowa was largely unaffected!

we had VAX and Sun hosts

gateway/mail-server was an Encore!

The worm could infect VAX and Sun hosts  
but it did not understand the Encore.

## **Common gateway functions**

Router

*Lifts data to the network layer  
isolates link layers from each other*

Performs packet routing functions  
*send each incoming packet out  
on the most appropriate link*

Can perform flow control

Can block access to selected hosts

## **One step above routers**

Network firewalls

*Lift data to the transport layer*

Can block or monitor

*Access to specific hosts*

*Access to specific ports of any host*

*Access to specific ports of specific hosts*

## **Local network firewalls**

"install a firewall on your computer"

*Software to block and monitor network  
can block certain ports*

This is design by afterthought

*Network architectures designed with  
security in mind should have treated  
network ports as protected objects,  
just like files or memory pages.*

## **An idealized world**

In any network security domain  
*(A,B) is transport layer right  
to send message from A to B*

Communication rights are just rights!  
*Enforcement mechanisms are needed  
Capability lists or Access Control Lists  
would both be appropriate.*

Firewalls (or equivalent) still needed at  
*Gateways between domains*



## **Security domains in networks**

A security domain contains

*Hosts with common administration*

*Hosts with shared security requirements*

*Hosts with uniform operating system*

Homogeneity need not be total

*Common naming conventions,*

*All users in domain have unique names*

Total homogeneity gives Multicomputers

*Networks of hosts that appear to be  
a single logical computing resource*