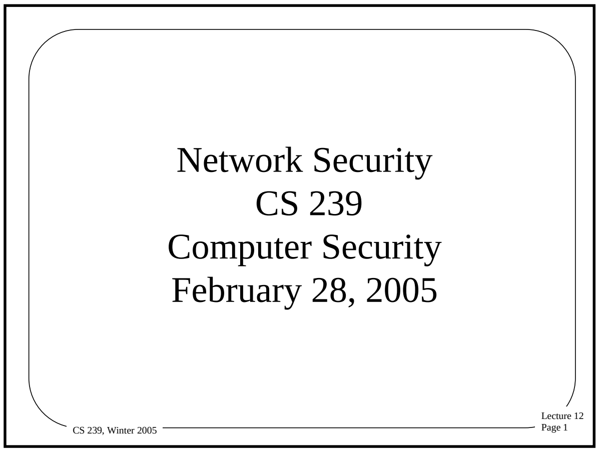
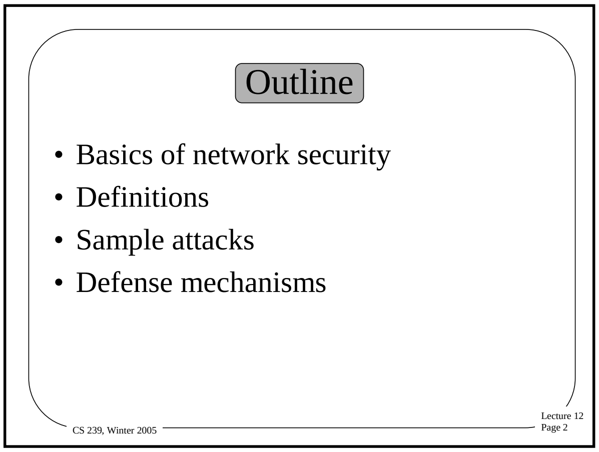
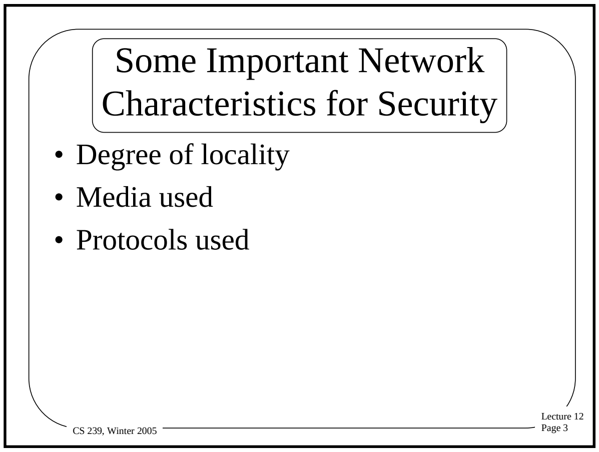


Network Security
CS 239
Computer Security
February 28, 2005



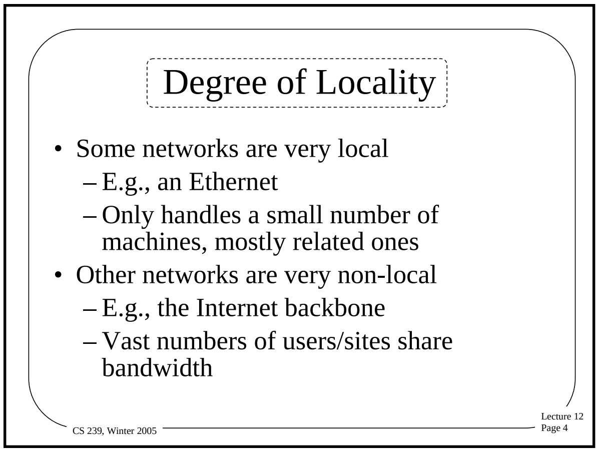
Outline

- Basics of network security
- Definitions
- Sample attacks
- Defense mechanisms



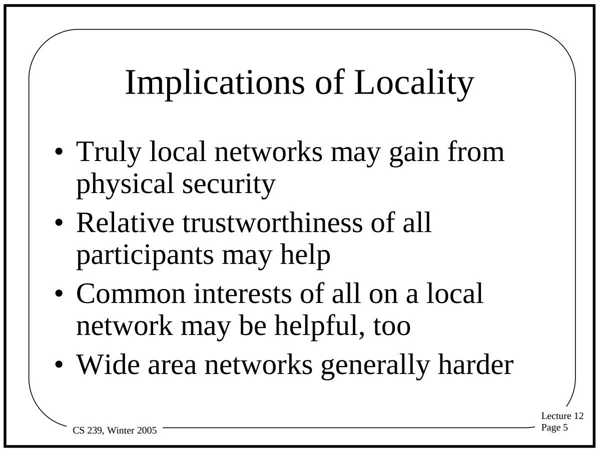
Some Important Network Characteristics for Security

- Degree of locality
- Media used
- Protocols used



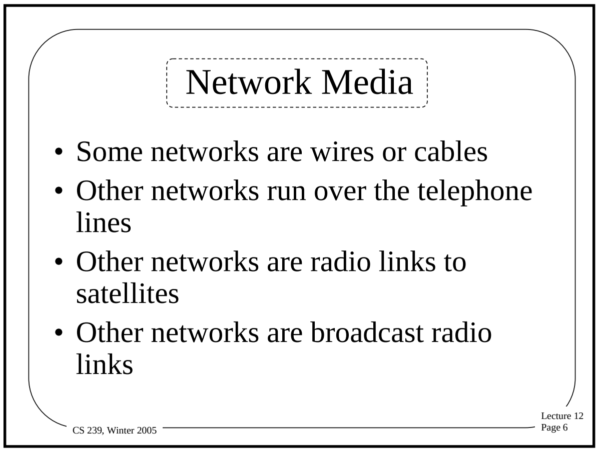
Degree of Locality

- Some networks are very local
  - E.g., an Ethernet
  - Only handles a small number of machines, mostly related ones
- Other networks are very non-local
  - E.g., the Internet backbone
  - Vast numbers of users/sites share bandwidth



Implications of Locality

- Truly local networks may gain from physical security
- Relative trustworthiness of all participants may help
- Common interests of all on a local network may be helpful, too
- Wide area networks generally harder



Network Media

- Some networks are wires or cables
- Other networks run over the telephone lines
- Other networks are radio links to satellites
- Other networks are broadcast radio links

Implications of Media Type

- Wires can sometimes be physically protected
- Radio links generally can’t
  - Though power and technology requirements for satellite links may provide some help
  - Directional antennae can also help

Protocol Types

- TCP/IP is probably the most widespread
  - 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, ssl)

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 Network Security

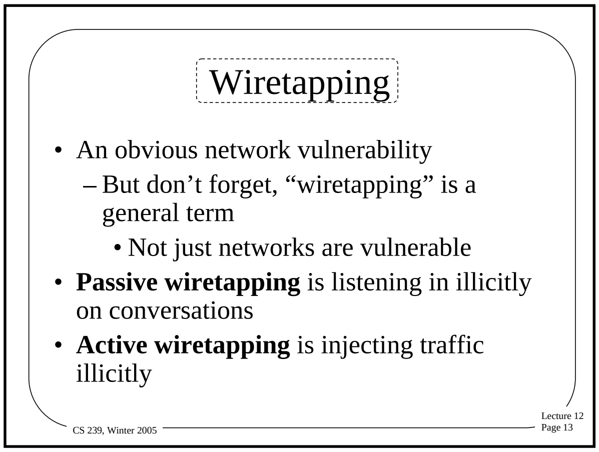
- Pretty much the usual suspects:
  - Wiretapping
  - Impersonation
  - Message confidentiality
  - Message integrity
  - Denial of service

Why Are Networks Especially Threatened?

- Many “moving parts”
- Many different administrative domains
- Everyone can get some access
- In some cases, trivial for attacker to get a foothold on the network
- Networks encourage sharing
- Networks often allow anonymity

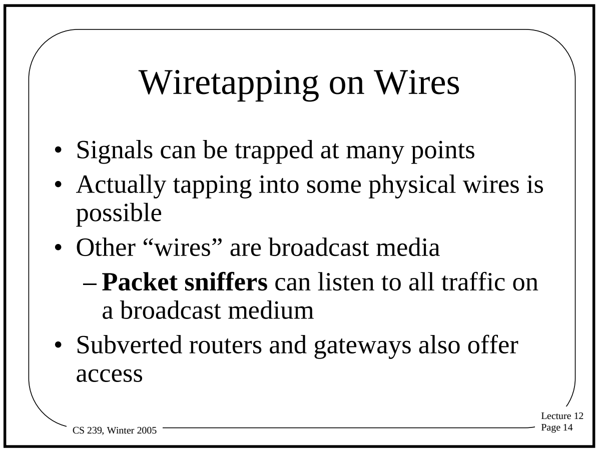
What Can Attackers Attack?

- The media connecting the nodes
- Nodes that are connected to them
- Routers that control the traffic
- The protocols that set the rules for communications



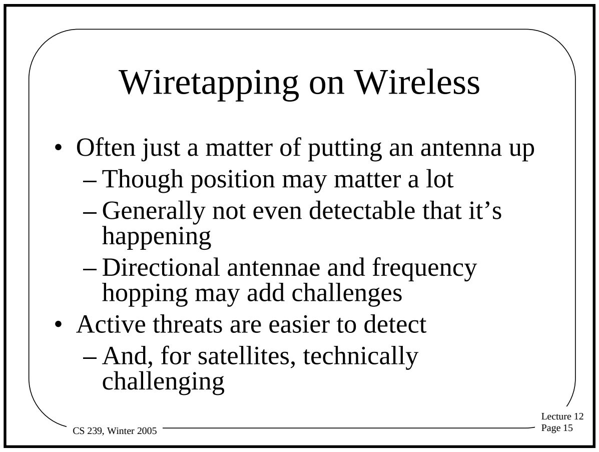
Wiretapping

- An obvious network vulnerability
  - But don't forget, "wiretapping" is a general term
    - Not just networks are vulnerable
- **Passive wiretapping** is listening in illicitly on conversations
- **Active wiretapping** is injecting traffic illicitly



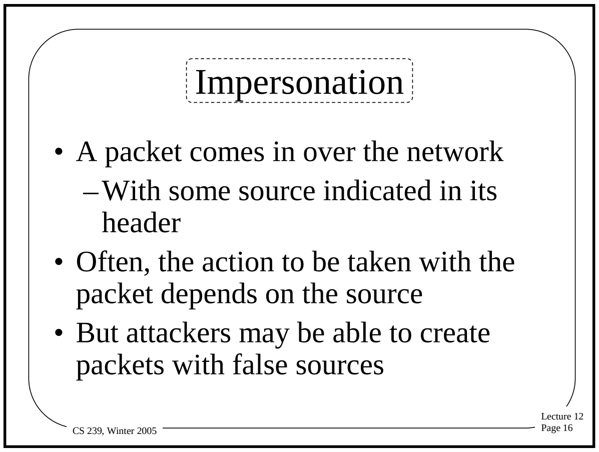
Wiretapping on Wires

- Signals can be trapped at many points
- Actually tapping into some physical wires is possible
- Other "wires" are broadcast media
  - **Packet sniffers** can listen to all traffic on a broadcast medium
- Subverted routers and gateways also offer access



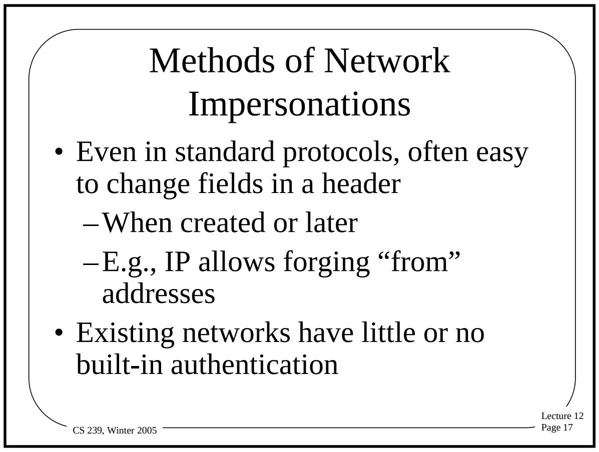
Wiretapping on Wireless

- Often just a matter of putting an antenna up
  - Though position may matter a lot
  - Generally not even detectable that it's happening
  - Directional antennae and frequency hopping may add challenges
- Active threats are easier to detect
  - And, for satellites, technically challenging



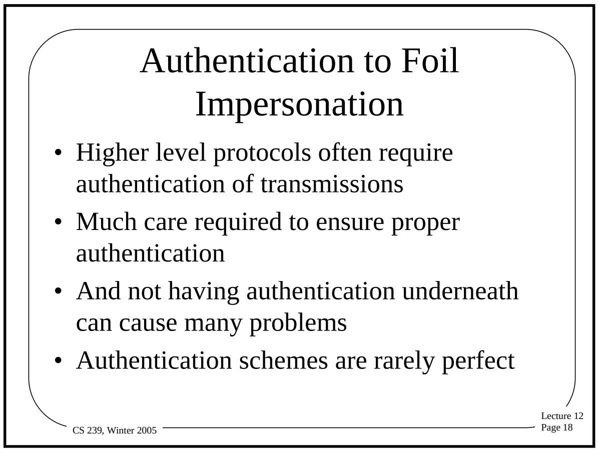
Impersonation

- 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



Methods of Network Impersonations

- Even in standard protocols, often easy to change fields in a header
  - When created or later
  - E.g., IP allows forging "from" addresses
- Existing networks have little or no built-in authentication



Authentication to Foil Impersonation

- Higher level protocols often require authentication of transmissions
- Much care required to ensure proper authentication
- And not having authentication underneath can cause many problems
- Authentication schemes are rarely perfect

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

Methods of Attacks on Message Integrity

- Replacing part of a packet
- Changing headers to alter destination of a packet
  - Or its source
- Inserting improper packets into a proper packet stream

Denial of Service

- Attacks that prevent legitimate users from doing their work
- By flooding the network
- Or corrupting routing tables
- Or flooding routers
- Or destroying key packets

How Do Denial of Service Attacks Occur?

- Basically, the attacker injects some form of traffic
- Most current networks aren’t built to throttle uncooperative parties very well
- All-inclusive nature of the Internet makes basic access trivial
- Universality of IP makes reaching most of the network easy

Some Sample Attacks

- Smurf attacks
- SYN flood
- Ping of Death

Smurf Attacks

- Attack on vulnerability in IP broadcasting
- Send a ping packet to IP broadcast address
  - With forged “from” header of your target
- Resulting in a flood of replies from the sources to the target
- Easy to fix at the intermediary
  - Don’t allow IP broadcasts to originate outside your network
- No good solutions for victim

SYN Flood

- Based on vulnerability in TCP
- Attacker uses initial request/response to start TCP session to fill a table at the server
- Preventing new real TCP sessions
- SYN cookies and firewalls with massive tables are possible defenses

Normal SYN Behavior

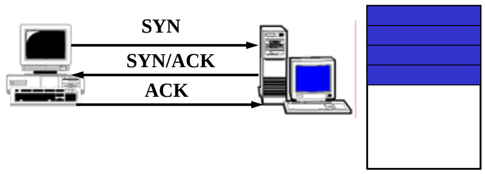
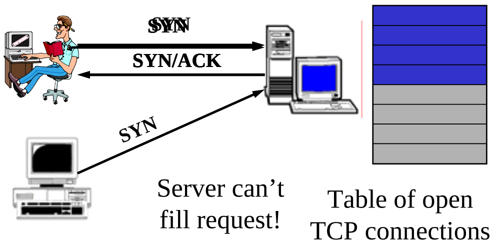


Table of open
TCP connections

A SYN Flood

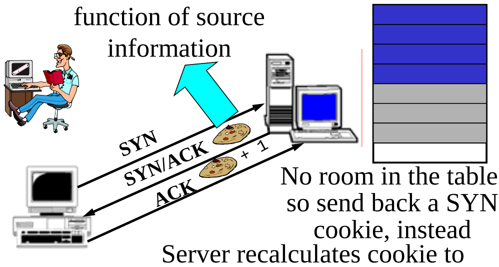


Server can’t
fill request!

Table of open
TCP connections

SYN Cookies

SYN/ACK number is
function of source
information

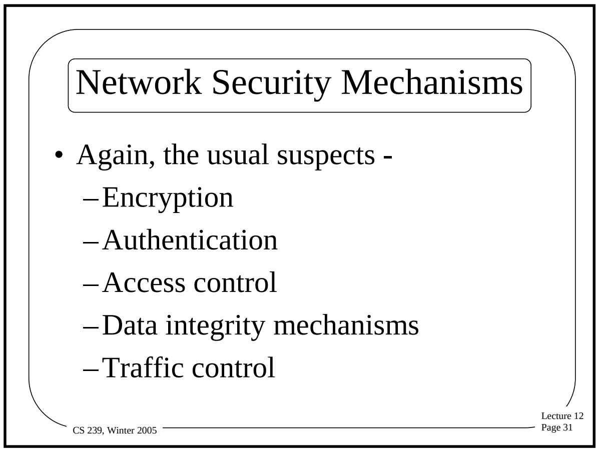


No room in the table,
so send back a SYN
cookie, instead

Server recalculates cookie to
determine if proper response

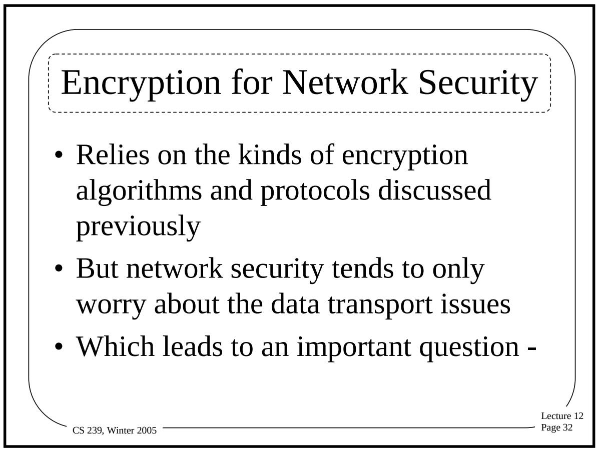
The Ping of Death

- IP packets are supposed to be no longer than 65,535 bytes long
- Can improperly send longer IP packets
- Some OS networking software wasn’t prepared for that
  - Resulting in buffer overflows and crashes
- Can filter out pings, but other IP packets can also cause problem
- OS patches really solve the problem



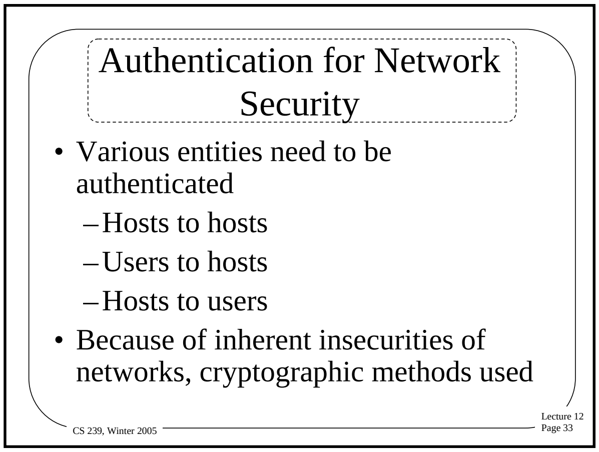
Network Security Mechanisms

- Again, the usual suspects -
  - Encryption
  - Authentication
  - Access control
  - Data integrity mechanisms
  - Traffic control



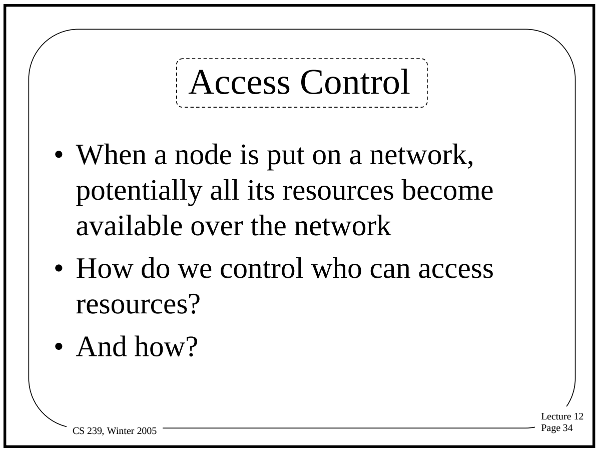
Encryption for Network Security

- Relies on the kinds of encryption algorithms and protocols discussed previously
- But network security tends to only worry about the data transport issues
- Which leads to an important question -



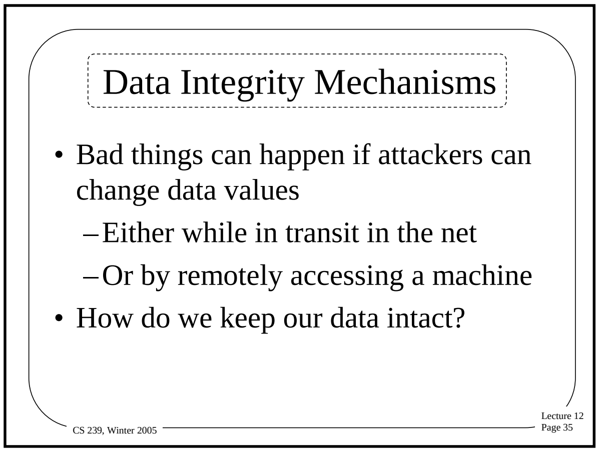
Authentication for Network Security

- Various entities need to be authenticated
  - Hosts to hosts
  - Users to hosts
  - Hosts to users
- Because of inherent insecurities of networks, cryptographic methods used



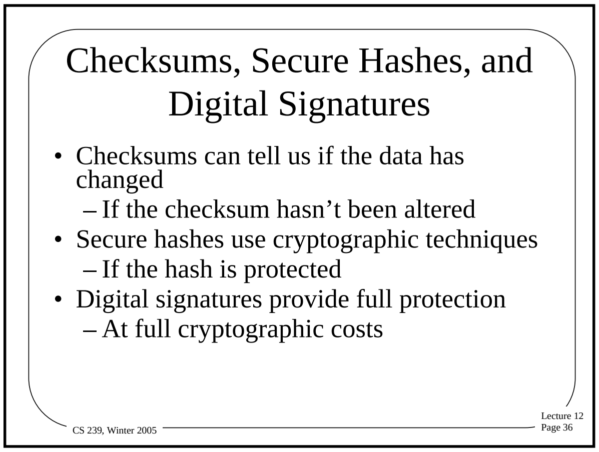
Access Control

- When a node is put on a network, potentially all its resources become available over the network
- How do we control who can access resources?
- And how?



Data Integrity Mechanisms

- Bad things can happen if attackers can change data values
  - Either while in transit in the net
  - Or by remotely accessing a machine
- How do we keep our data intact?



Checksums, Secure Hashes, and Digital Signatures

- Checksums can tell us if the data has changed
  - If the checksum hasn’t been altered
- Secure hashes use cryptographic techniques
  - If the hash is protected
- Digital signatures provide full protection
  - At full cryptographic costs

Traffic Control Mechanisms

- Filtering
  - Source address filtering
  - Other forms of filtering
- Rate Limits
- Protection against traffic analysis
  - Padding
  - Routing control

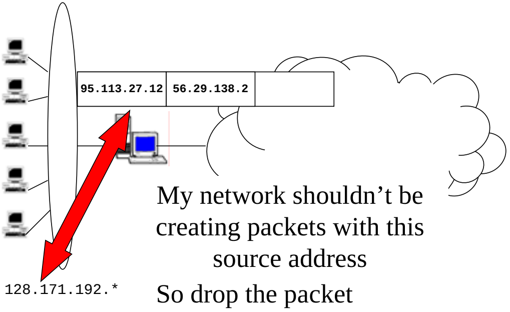
Source Address Filtering

- Filtering out some packets because of their source address value
  - Usually because you believe their source address is spoofed
- Often called ingress filtering
  - Or egress filtering . . .

Source Address Filtering for Address Assurance

- Router "knows" what network it sits in front of
  - In particular, knows IP addresses of machines there
- Filter outgoing packets with "from" addresses not in that range
- Prevents your users from spoofing other nodes' addresses
  - But not from spoofing each other's

Source Address Filtering Example



My network shouldn't be creating packets with this source address

So drop the packet

Source Address Filtering in the Other Direction

- Often called egress filtering
  - Or ingress filtering . . .
- Occurs as packets leave the Internet and enter a border router
  - On way to that router's network
- What addresses shouldn't be coming into your local network?

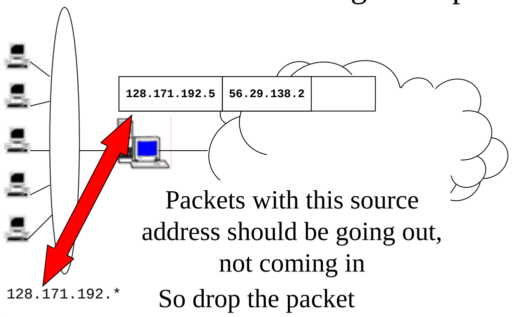
Ingress/Egress Filtering

- Filtering source addresses for validity often called either ingress filtering or egress filtering
- Unfortunately, a lot of confusion on which is which
  - Conflicting RFCs, for example
- Basically, *ingress* is going in
- And *egress* is coming out
- Usually, it's a question of perspective

Filtering Packets Entering an Edge Network

- Packets coming from outside your router shouldn't have source addresses of your local network
- Filter any that do
- If local network performs some access control based on IP address, very important

Another Address Filtering Example



Packets with this source address should be going out, not coming in

So drop the packet

Other Forms of Filtering

- One can filter on things other than source address
  - Such as worm signatures, unknown protocol identifiers, etc.
- Also, there are unallocated IP addresses in IPv4 space
  - Can filter for packets going to or coming from those addresses
- Also, certain source addresses are for local use only
  - Internet routers can drop packets to/from them

Rate Limits

- Many routers can place limits on the traffic they send to a destination
- Ensuring that the destination isn't overloaded
  - Popular for denial of service defenses
- Limits can be defined somewhat flexibly
- But often not enough flexibility to let the good traffic through and stop the bad

Padding

- Sometimes you don't want intruders to know what your traffic characteristics are
- Padding adds extra traffic to hide the real stuff
- Requires that fake traffic is not differentiable from real
- Usually means encrypt it all
- Must be done carefully, or clever attackers can tell the good stuff from the noise

Routing Control

- Use ability to control message routing to conceal the traffic in the network
- Especially important when trying to handle **covert channels**
  - Encapsulated users or programs trying to leak information out