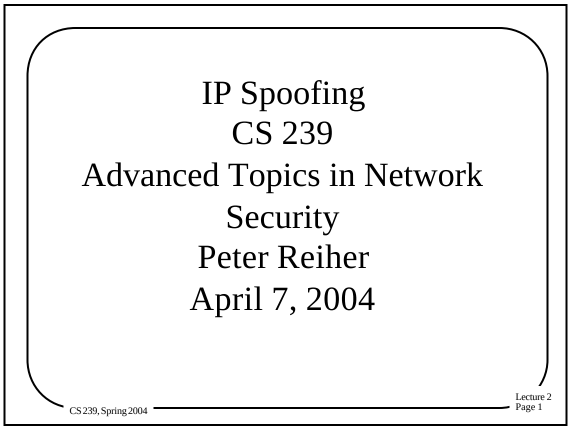
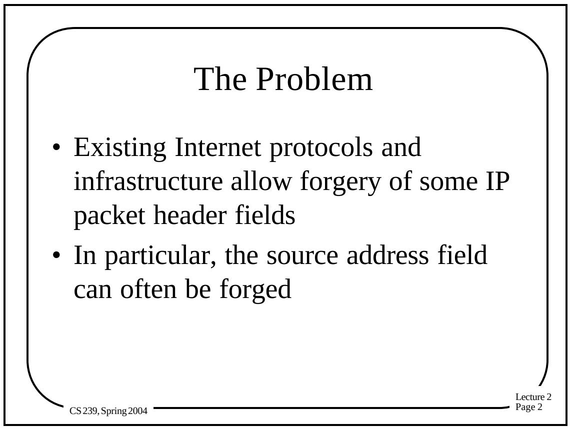
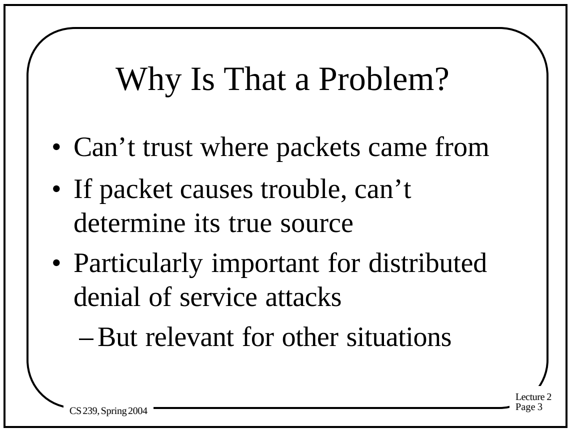


IP Spoofing
CS 239
Advanced Topics in Network Security
Peter Reiher
April 7, 2004



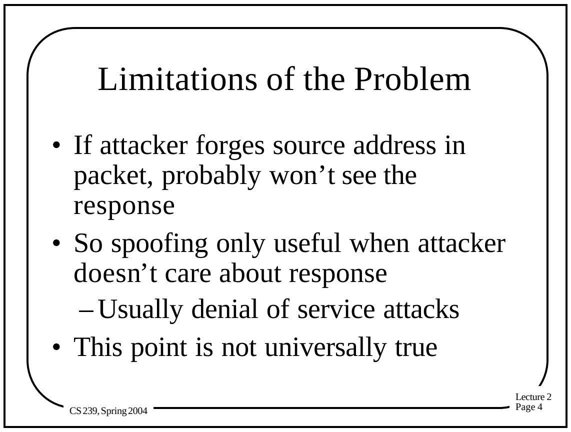
The Problem

- Existing Internet protocols and infrastructure allow forgery of some IP packet header fields
- In particular, the source address field can often be forged



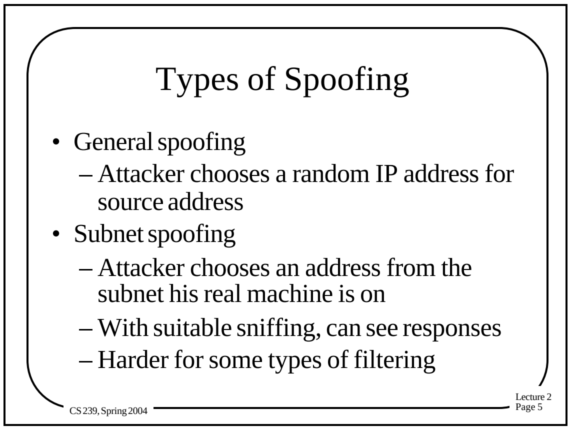
Why Is That a Problem?

- Can’t trust where packets came from
- If packet causes trouble, can’t determine its true source
- Particularly important for distributed denial of service attacks
  - But relevant for other situations



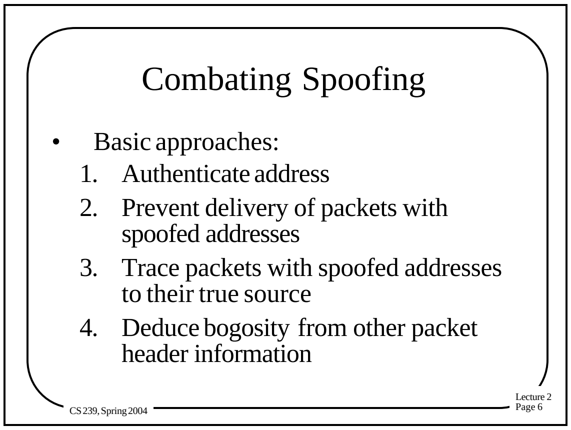
Limitations of the Problem

- If attacker forges source address in packet, probably won’t see the response
- So spoofing only useful when attacker doesn’t care about response
  - Usually denial of service attacks
- This point is not universally true



Types of Spoofing

- General spoofing
  - Attacker chooses a random IP address for source address
- Subnet spoofing
  - Attacker chooses an address from the subnet his real machine is on
  - With suitable sniffing, can see responses
  - Harder for some types of filtering



Combating Spoofing

- Basic approaches:
  1. Authenticate address
  2. Prevent delivery of packets with spoofed addresses
  3. Trace packets with spoofed addresses to their true source
  4. Deduce bogosity from other packet header information

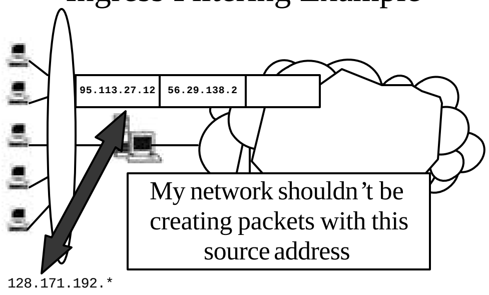
Authenticate Address

- Probably requires cryptography
- Can be done with IPSec
- Incurs cryptographic costs
- Only feasible when crypto authentication is feasible
- Could we afford to do this for all packets?

Preventing Delivery of Spoofed Packets

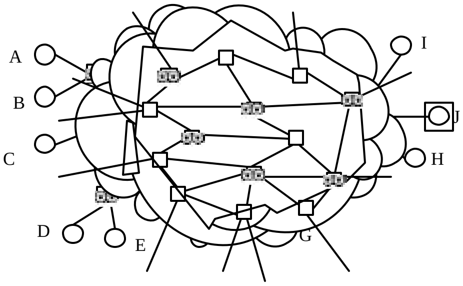
- Somehow recognize that address is spoofed
  – Usually based on information about network topology and addresses
- Simple version is ingress filtering
- More sophisticated methods are possible

Ingress Filtering Example



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

Diagram for Detection Approaches

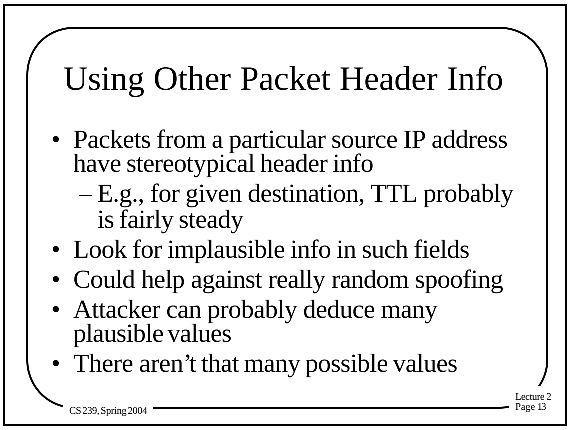


Potential Problems With Approaches Requiring Infrastructure Support

- Issues of speed and cost
- Issues of trustworthiness
- Issues of deployment
  – Why will it be deployed at all?
  – How will it work partially deployed?

Packet Tracing

- Figure out where the packet really came from
- Generally only feasible if there is a continuing stream of packets
- Will be discussed in more detail in later class
- Challenges when there are multiple sources of spoofed addresses



Using Other Packet Header Info

- Packets from a particular source IP address have stereotypical header info
  - E.g., for given destination, TTL probably is fairly steady
- Look for implausible info in such fields
- Could help against really random spoofing
- Attacker can probably deduce many plausible values
- There aren’t that many possible values

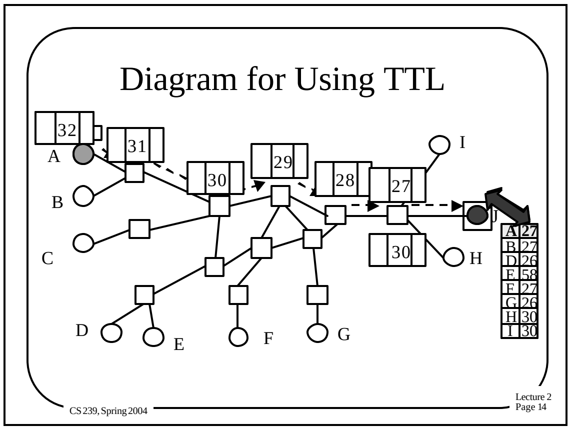
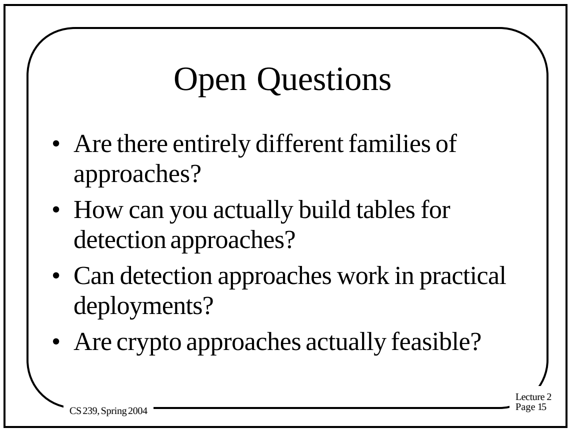


Diagram for Using TTL

A	27
B	27
D	26
E	58
F	27
G	26
H	30
I	30



Open Questions

- Are there entirely different families of approaches?
- How can you actually build tables for detection approaches?
- Can detection approaches work in practical deployments?
- Are crypto approaches actually feasible?