

IP Spoofing  
CS 239  
Advanced Topics in Network  
Security  
Peter Reiher  
April 2, 2003

CS 239, Spring 2003

Lecture 2  
Page 1

## 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

CS 239, Spring 2003

Lecture 2  
Page 2

## 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

CS 239, Spring 2003

Lecture 2  
Page 3

## 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

CS 239, Spring 2003

Lecture 2  
Page 4

## 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

CS 239, Spring 2003

Lecture 2  
Page 5

## 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

CS 239, Spring 2003

Lecture 2  
Page 6

## 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?

CS 239, Spring 2003

Lecture 2  
Page 7

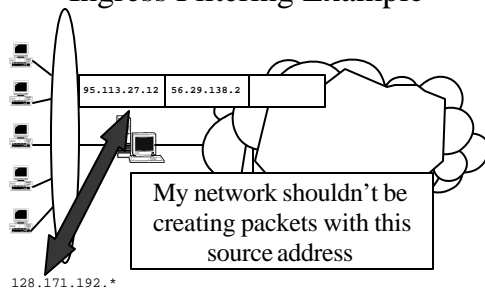
## Preventing Delivery of Spoofed Packets

- 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

CS 239, Spring 2003

Lecture 2  
Page 8

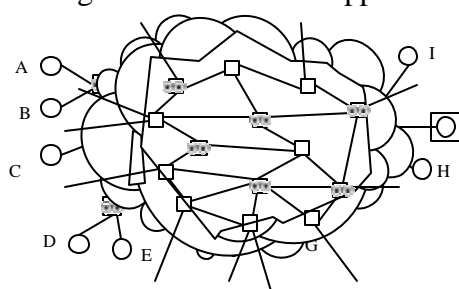
## Ingress Filtering Example



CS 239, Spring 2003

Lecture 2  
Page 9

## Diagram for Detection Approaches



CS 239, Spring 2003

Lecture 2  
Page 10

## 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?

CS 239, Spring 2003

Lecture 2  
Page 11

## 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

CS 239, Spring 2003

Lecture 2  
Page 12

## Open Questions

- Are there entirely different families of approaches?
- Can detection approaches work in practical deployments?
- Are crypto approaches actually feasible?