

## Security

15-441

With slides from: Debabrata Dash, Nick Feamster, Vyas Sekar, and others

## Our "Narrow" Focus

- Yes:
  - ♦ Protecting network resources and limiting connectivity (Part I)
  - ♦ Creating a "secure channel" for communication (Part II)
- No:
  - ♦ Preventing software vulnerabilities & malware, or "social engineering".

## Flashback .. Internet design goals

1. Interconnection
2. Failure resilience
3. Multiple types of service
4. Variety of networks
5. Management of resources
6. Cost-effective
7. Low entry-cost
8. Accountability for resources

**Where is security?**

## Why did they leave it out?

- Designed for connectivity
- Network designed with implicit trust
  - ♦ No "bad" guys
- Can't security be provided at the edge?
  - ♦ Encryption, Authentication etc
  - ♦ End-to-end arguments in system design

## Security Vulnerabilities

- At every layer in the protocol stack!
- Network-layer attacks
  - IP-level vulnerabilities
  - Routing attacks
- Transport-layer attacks
  - TCP vulnerabilities
- Application-layer attacks

15-411: security

5

## IP-level vulnerabilities

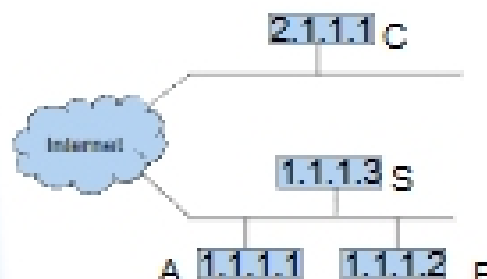
- IP addresses are provided by the source
  - Spoofing attacks
- Using IP address for authentication
  - e.g., login with `.rhosts`
- Some "features" that have been exploited
  - Fragmentation
  - Broadcast for traffic amplification

15-411: security

6

## Security Flaws in IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - `r`-utilities (`rlogin`, `rsh`, `rhosts` etc..)

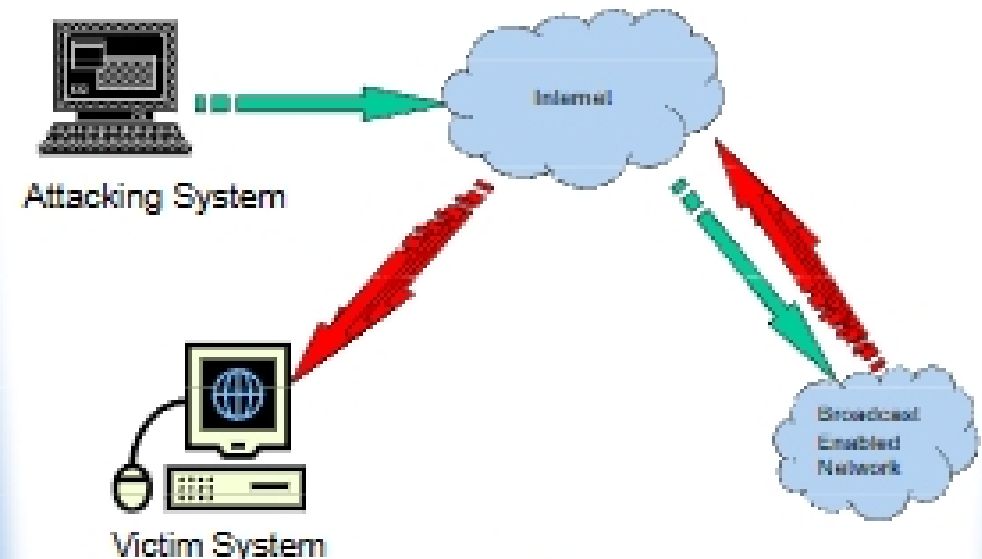


- Can A claim it is B to the server S?
- ARP Spoofing
- Can C claim it is B to the server S?
- Source Routing

15-411: security

7

## Smurf Attack



15-411: security

8

## ICMP Attacks

- No authentication
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - Man in the middle attack, sniffing
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
- Many more...
  - <http://www.sans.org/m/whitepapers/threats/477.php>

## Routing attacks

- Divert traffic to malicious nodes
  - Black-hole
  - Eavesdropping
- How to implement routing attacks?
  - Distance-Vector:
  - Link-state:
- BGP vulnerabilities

## Routing attacks

- Divert traffic to malicious nodes
  - Black-hole
  - Eavesdropping
- How to implement routing attacks?
  - Distance-Vector: Announce low-cost routes
  - Link-state: Dropping links from topology
- BGP vulnerabilities
  - Prefix-hijacking
  - Path alteration

## TCP-level attacks

- SYN-Floods
  - Implementations create state at servers before connection is fully established
- Session hijack
  - Pretend to be a trusted host
  - Sequence number guessing
- Session resets
  - Close a legitimate connection