

# Security Threats

Dr. Arjan Durrezi  
Louisiana State University  
Baton Rouge, LA 70810  
Durrezi@csc.lsu.edu

These slides are available at:  
[http://www.csc.lsu.edu/~durrezi/CSC4601\\_07/](http://www.csc.lsu.edu/~durrezi/CSC4601_07/)



- Security threats
- IP flaws
- Attacks

## The Security Life-Cycle

- **Threats**
- Policy
- Specification
- Design
- Implementation
- Operation and Maintenance

## Taxonomy of Threats

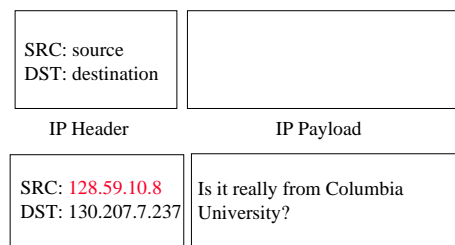
- Taxonomy - a way to classify and refer to threats (and attacks) by names/categories
  - Benefits - avoid confusion
  - Focus/coordinate development efforts of security mechanisms
- No standard yet
- One possibility: by results/intentions first, then by techniques, then further by targets, etc.
  - Associate severity/cost to each threat

## A Taxonomy Example

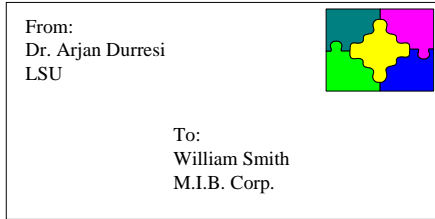
- By results then by (high-level) techniques:
  - Illegal root
    - Remote, e.g., buffer-overflow a daemon
    - Local, e.g., buffer-overflow a "root" program
  - Illegal user
    - Single, e.g., guess password
    - Multiple, e.g., via previously installed back-door
  - Denial-of-Service
    - Crashing, e.g., teardrop, ping-of-death, land
    - Resource consumption, e.g., syn-flood
  - Probe
    - Simple, e.g., fast/regular port-scan
    - Stealth, e.g., slow/"random" port-scan

## Threat Examples - IP Spoofing

- A common first step to many threats.
- Source IP address cannot be trusted!

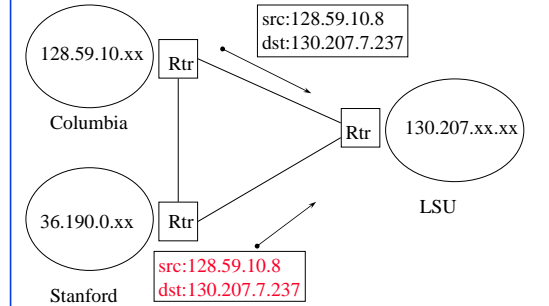


## Similar to US Mail (or E-mail)



US mail maybe better in the sense that there is a *stamp* put on the envelope at the *location* (e.g., town) of collection...

## Most Routers Only Care About Destination Address



## Why Should I Care?

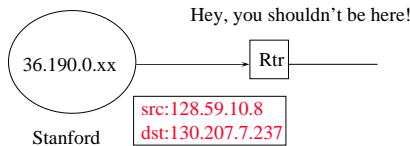
- ❑ Attack packets with spoofed IP address help hide the attacking source.
- ❑ A *smurf* attack launched with your host IP address could bring your host and network to their knees.
- ❑ Higher protocol layers (e.g., TCP) help to protect applications from direct harm, but not enough.

## Current IPv4 Infrastructure

- ❑ No authentication for the source
- ❑ Various approaches exist to address the problem:
  - Router/firewall filtering
  - TCP handshake

## Router Filtering

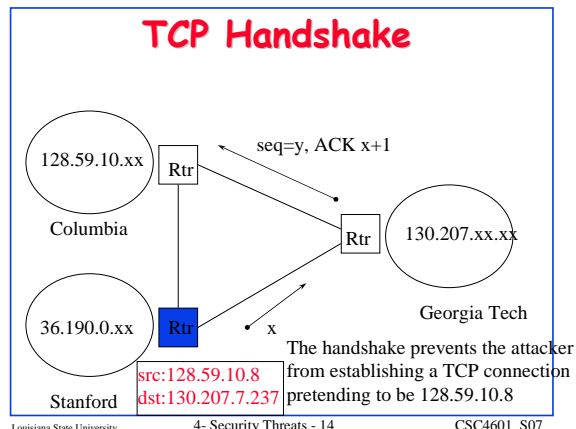
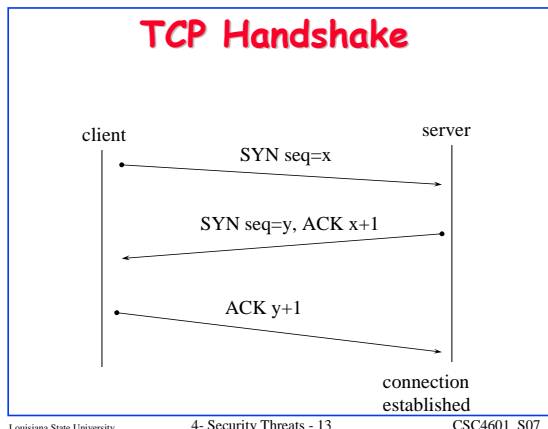
- ❑ Decide whether this packet, with certain source IP address, should come from this side of network.



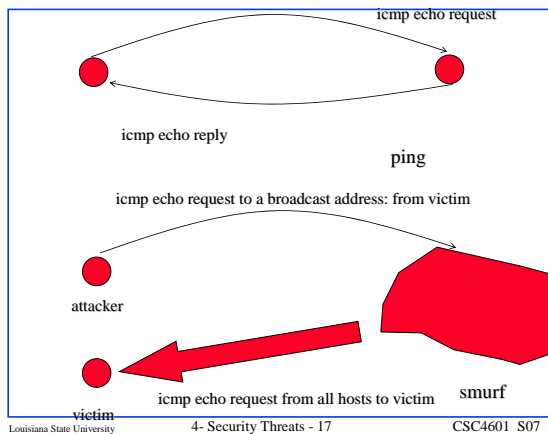
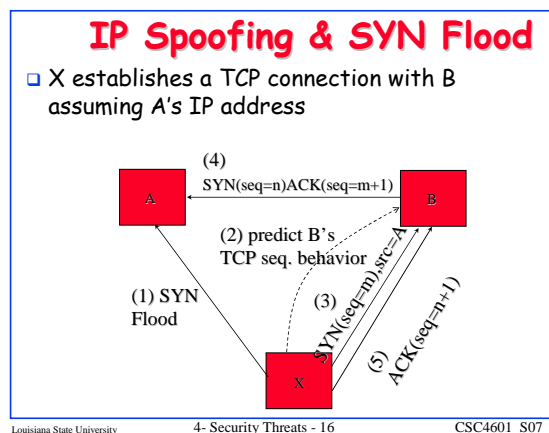
- ❑ Not standard - local policy.

## Router Filtering

- ❑ Very effective for some networks (ISP should always do that!)
  - At least be sure that this packet is from some particular subnet
- ❑ Problems:
  - Hard to handle frequent add/delete hosts/subnets or mobile IP
  - Upsets customers should legitimate packets get discarded
  - Need to trust other routers



- ### TCP Handshake
- Very effective for stopping most such attacks
  - Problems:
    - The attacker can succeed if "y" can be predicted
    - Other DoS attacks are still possible (e.g., TCP SYN-flood)
- Louisiana State University 4- Security Threats - 15 CSC4601 S07



- ### Smurf Attack
- Generate ping stream (ICMP echo request) to a network broadcast address with a spoofed source IP set to a victim host
  - Every host on the ping target network will generate a ping reply (ICMP echo reply) stream, all towards the victim host
  - Amplified ping reply stream can easily overwhelm the victim's network connection
  - Fraggle and Pingpong exploit UDP in a similar way
- Louisiana State University 4- Security Threats - 18 CSC4601 S07

## Vulnerability

- ❑ A vulnerability (or security flaw) is a specific failure of the security controls.
- ❑ Using the failure to violate the site security: exploiting the vulnerability; the person who does this: an attacker.
- ❑ It can be due to:
  - Lapses in design, implementation, and operation procedures.
  - Even security algorithms/systems are not immune!
    - ❑ We will go over some examples in this course.

## Example: IP Protocol-related Vulnerabilities

- ❑ Authentication based on IP source address
  - But no effective mechanisms against IP spoofing
- ❑ Consequences (possible exploits)
  - Denial of Service attacks on infrastructures, e.g.
    - ❑ IP Spoofing and SYN Flood
    - ❑ Smurf and Fraggle attacks
    - ❑ OSPF Max Sequence

## Summary



- ❑ Security threats.
- ❑ IP flaws.
- ❑ Attacks.