

# Network Security

M.Ramkumar

# Overview

## (Rest of the Course)

- Threats and vulnerabilities
  - Most vulnerabilities are due to inability to authenticate source.
    - Smurf attack (ICMP ping packets)
    - Fraggle (UDP echoes)
    - Pingpong (UDP servers like day-time servers)
    - Land attack (TCP stack)
  - Some potential solutions and pitfalls
- Routing Attacks

# Overview (continued)

- Denial of Service and Traceback
  - Syn flood, ping-of-death
  - DdoS
    - Attacker, Masters, Zombies
    - Trinoo, TFN, Stacheldraht
    - Prevention, traceback
- Firewalls and IDS
  - Misuse detection
  - Anomaly detection
  - Host based IDS
  - Network IDSs

# And more

- Firewalls
  - Packet filtering
  - Session filtering
  - Application gateways
  - NATs
  - Proxies, SOCKS
  - VPN

# And even more...

- IPSEC
  - VPN again
- SSL (TLS)
- DNS security
- Email Security
- Web Security
- WEP