# Introduction to Network Security

Chapter 4

Taxonomy of Network-Based Vulnerabilities



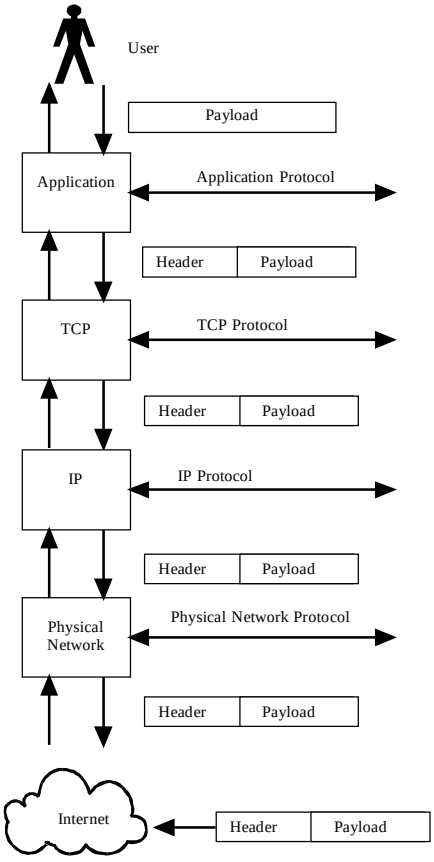
# Topics

- Network Security Model
- Header attacks
- Protocol Attacks
- Authentication Attacks
- Traffic attacks

# Network Security

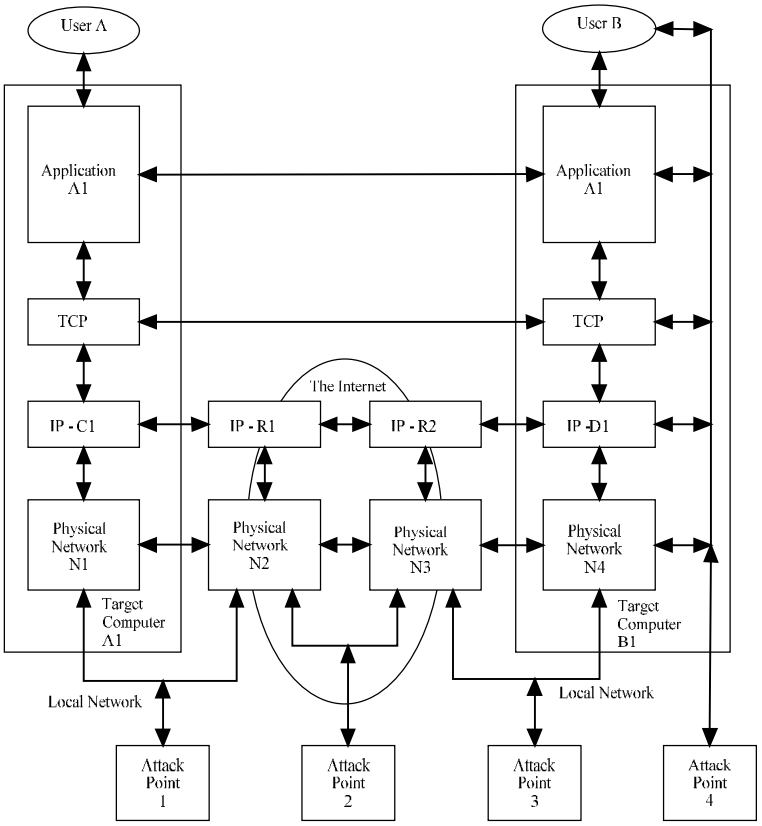
- Who (authentication)
  - Good guys
  - Bad Guys
- What to Attack
  - Protocols
  - Network connected Applications
  - Infrastructure






# Layered Model of Attack Data

- Each layer receives data from the layer below and passes data to the layer above it without looking at it
- An attacker can insert information into the payload in order to send data to a particular layer

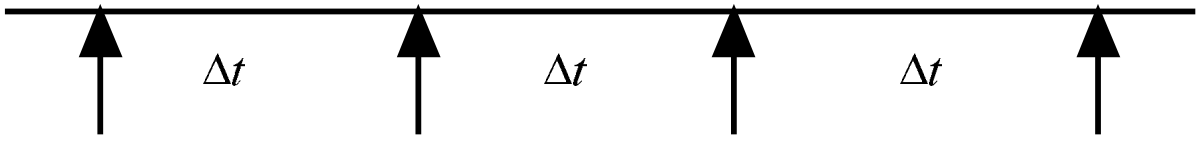



# Threat Model

- Attacker 1 & 3 can attack any layer on computers connected to the same network
- Attacker 2 can attack the TCP & Application layers of computers A1 & B1 and the IP layer of any device
- Attacker 4 has taken over the computer



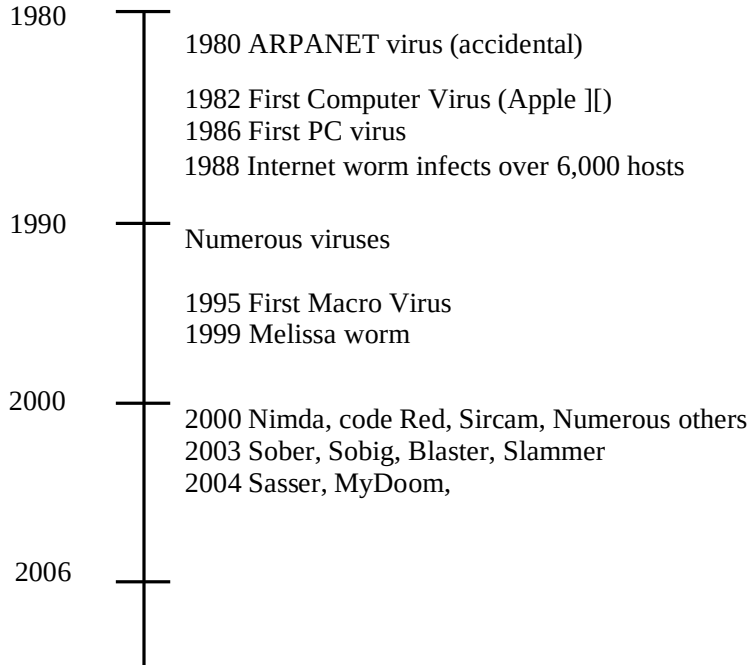
# Vulnerabilities, Exploits and Attacks




Design Vulnerability
Implementation Vulnerability
Configuration Vulnerability

# Attack Time Line

- Time between attacks has decreased and scale of attacks has increased
- Attacks now have multiple variations that can occur within hours of each other

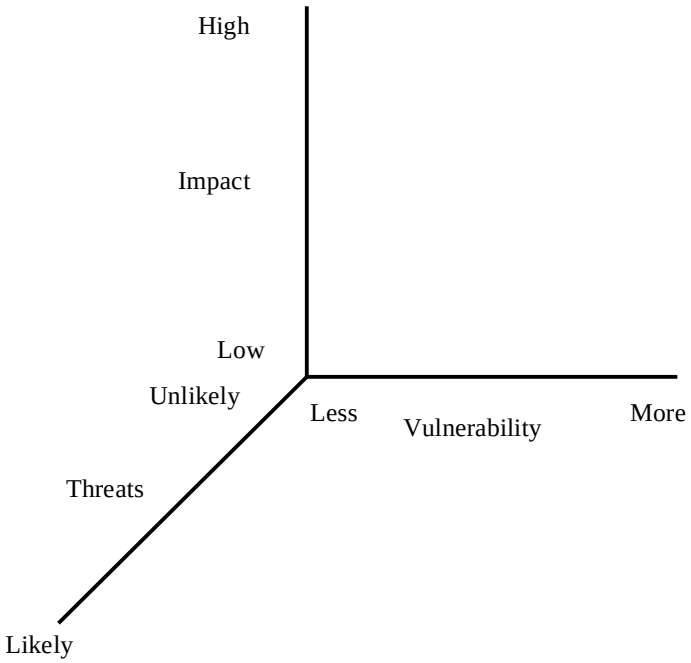





# Risk & Risk Assessment

- Risk is a measure of how critical something is and is a combination of:
  - **Threat** (How likely is it that the target will be attacked)
  - **Vulnerability** (How likely there is a weakness in the target)
  - **Impact** (What is the effect of losing the target)
- Risk assessment is the process where you decide how important something is and how hard you are going to work to protect it.

# Risk Graph






# Network Security Taxonomy

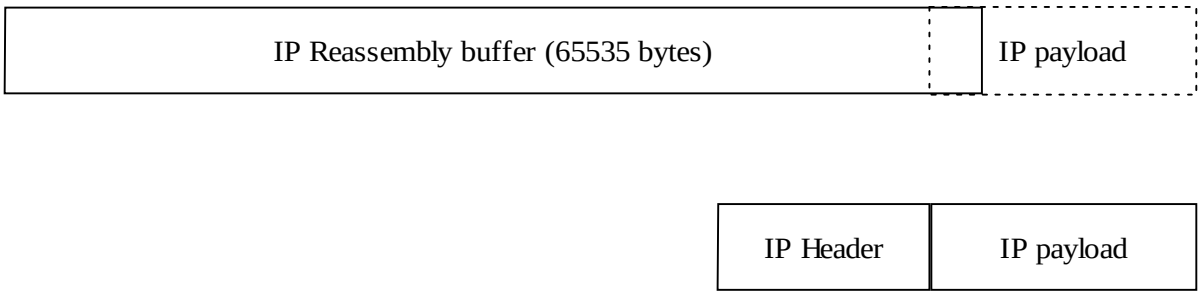
- Header based
- Protocol based
- Authentication based
- Traffic Based

# Header Based

- Creation of invalid packets, different protocols handle bad packets differently
- Source and destination address manipulation
  - Device can be confused by setting source and destination to the same address
- Setting bits in the header that should not be set
- Putting values in the header that are above or below the level specified in the standard



# Example: Ping of Death




offset = 65528 (max value)
length = 100

# Network Protocol Issues

- Timing / procedural
  - Who talks first, who says what and when
  - Think of a phone call conversations, there is a protocol, the person picking up the phone talks first
  - Attacks usually involve valid packets that are out of order, arrive too fast, or are missing packets

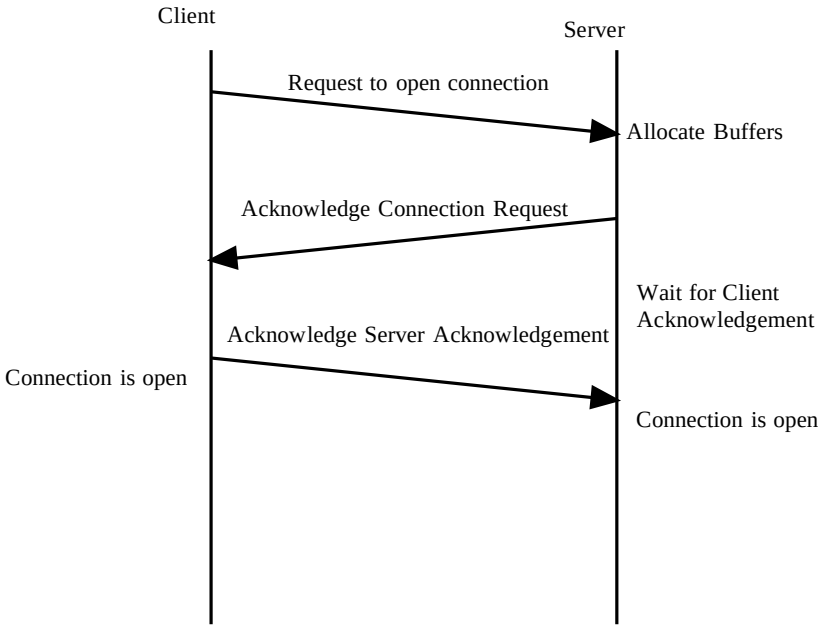


# Protocols attacks

- You can shutdown the protocol itself
- Send packets telling the device to stop talking
- For connectionless protocols you can answer as the server and tell the client the server is down.

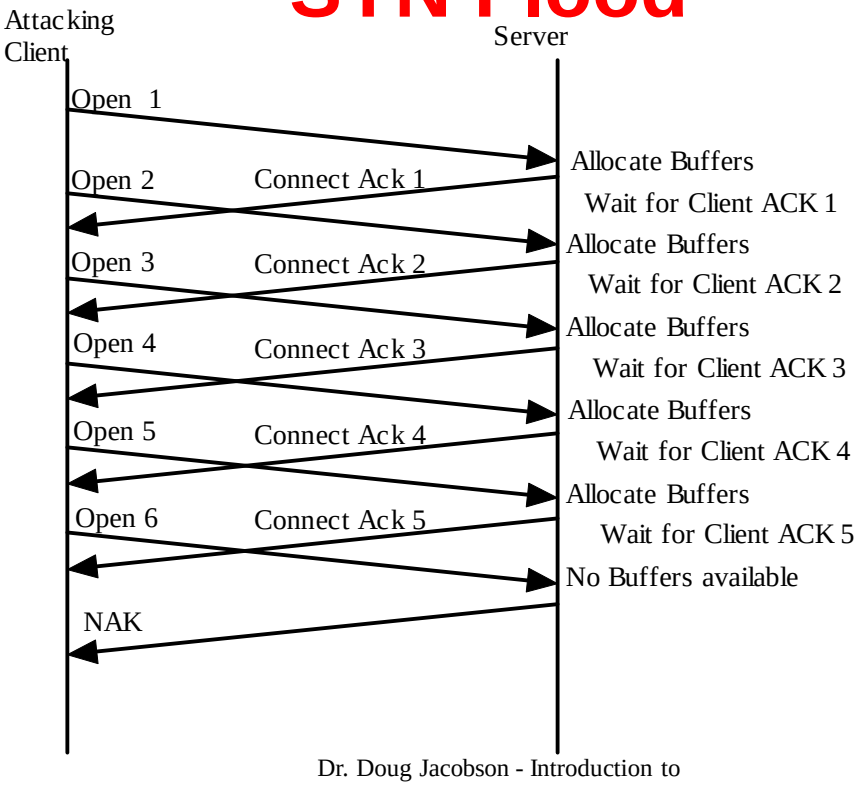
# Example: Syn Flood

- TCP 3-way Handshake





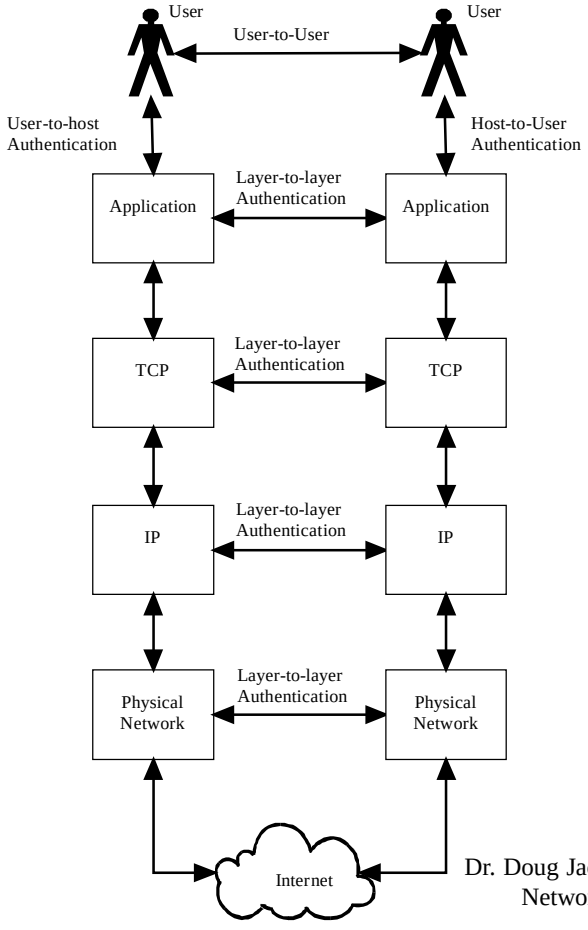

# SYN Flood



# Authentication-Based

- Authentication is the proof of one's identity to another.
- Often thought of as username & password based
- In a network addresses are often used to authenticate packets.
  - Like the 4 addresses used to identify a packet in the Internet






# Network Authentication

# Authentication

- Four different types of authentication
  - User to host
    - Person proves the identity to computer resource
    - Most prevalent
  - Host to Host
    - Work being done to strengthen this
    - In past usually done by IP address
  - User to User
    - Contracts, secure email
    - Useful for online auctions
  - Host to User
    - Server authenticating to user



# Traffic-Based

- Too much data
  - To a single:
    - Application
    - Network device
    - Protocol layer
  - From:
    - Multiple machines
    - Single attackers
- Traffic Capture (sniffing)

# Traffic Attacks

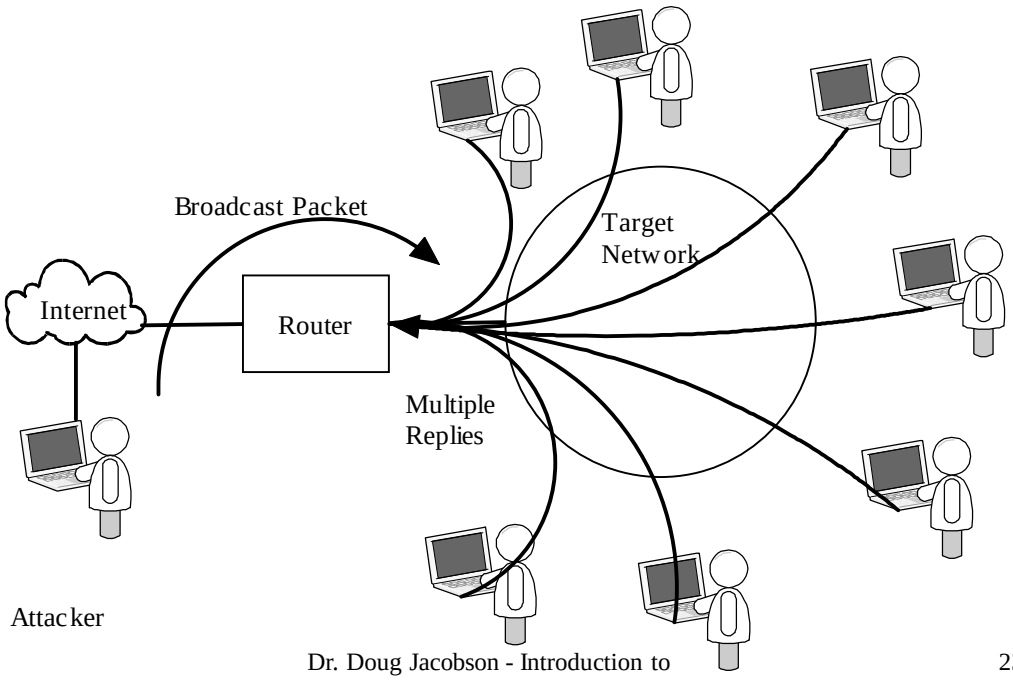
- You can shutdown a service by:
  - flooding it with packets
  - opening a large number of connections
- You can shutdown network by:
  - flooding it with a large number of packets.
  - Broadcast packets will do the most damage
- You can shutdown a machine by:
  - flooding a machine with packets on multiple services
  - Broadcast storms



# Denial of Service

- Denial of service is when a third party prevents valid network users access to services, machines, or applications
- Denial of service attacks can be difficult to detect and even harder to defend against.

# Broadcast Flood Attack






# Traffic Capture

- Packet sniffing can be played out against any layer in the network if the attacker is in a position to “see” the traffic.

# Applying the Taxonomy

- Goal versus method
- The taxonomy applies to the method
  - Breaking authentication maybe the goal, but the method maybe be header-based
- Not all attacks will be covered since not all attacks are network based.