COMP 290-040
Network Intrusion Detection

Denial of Service
Classes of Attacks & Attack Methods

Kevin Jeffay
Department of Computer Science
University of North Carolina at Chapel Hill
jeffay@cs.unc.edu

January 24, 2005

http://www.cs.unc.edu/~jeffay/courses/nidsS05

Denial of Service
The basics…

- Historically, attacks were aimed at access to information or services
  - » Steal credit card numbers
  - » Deface web pages, create/erase records, …
- Denial of service seek to… deny services to others!
  - » No data is stolen/altered
  - » *No unauthorized access of the service provider occurs!*
    - ❖ Unauthorized access occurs in creating the attack (zombie creation)
- DoS is bad because…
  - » Companies lose money
    - ❖ Direct sales, advertising revenue, loss of future revenue due to tarnished image, …
  - » End users and non-computer users can be effected
    - ❖ DNS attacks, airline operations systems, …

Denial of Service
Classes of attacks

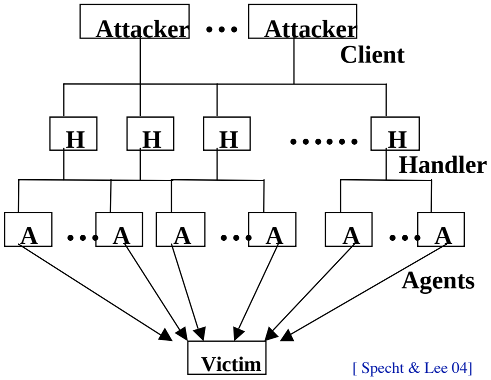
- Vulnerability attacks
  - » Send a small number of specially constructed messages to exploit a bug/feature of a system
  - » E.g., 802.11 “Hang-up” messages
  - » Exploits can be found in the OS, the network, a middleware layer, the application…
  - » The battle against vulnerability attacks is maybe winnable
- Flooding attacks
  - » Send a huge number of (seemingly) legitimate messages to overwhelm a resource
  - » Key is volume of messages not necessarily content

Denial of Service
Flooding attacks

- Flooding leads to distributed DoS
  - » To achieve required volumes, zombie armies are required
  - » Zombie creation typically relies on vulnerability exploits
    - ❖ Solve the vulnerability problem and…
- Simple attacks: Saturate a bottleneck resource
  - » Flood a victim’s network interface with bogus packets
    - ❖ Legitimate, well-formed packets for non-existent services
  - » Flood a victim’s protocol stack with bogus packets
    - ❖ Corrupted or mal-formed packets
    - ❖ Incomplete protocol control sequences
  - » Flood a victim’s machine with bogus requests for service
    - ❖ Legitimate, well-formed packets for offered services

Flooding Attacks
Orchestration

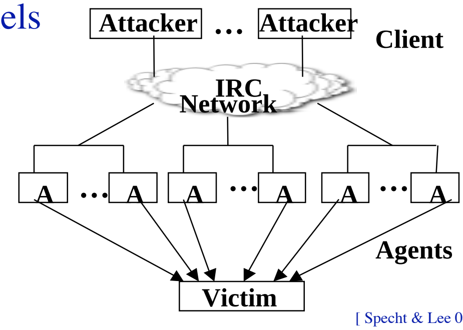
- An attacker first must gain control of a set of machines
  - An automated process
  - (More on this later)
- Hiding the identity of the attacker is key
  - Hierarchical "handler/agent" schemes are common
  - "Stepping stones" may be used to increase the levels of indirection between attacker and handler



[Specht & Lee 04]

Flooding Attacks
Orchestration

- Handler/agent traffic can be used as an identifier of DDoS activity
  - Use of encryption is becoming more common
- Use of more covert channels
  - IRC (Internet Relay Chat) channels now dominant
  - Difficult to detect without violating user's privacy



[Specht & Lee 04]

Flooding Attacks
What to do with your zombie army?

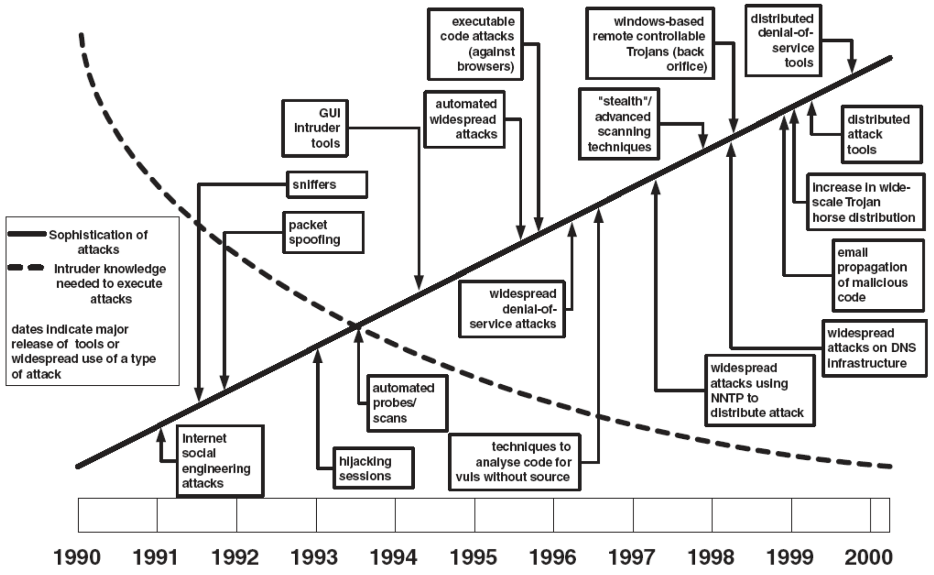
- Misusing legitimate services
- IP-spoofing-based "reflection" and "amplification" attacks
  - *ping* of death
  - friends and neighbors broadcast *ping* of death ("smurf attack")
  - DNS response flood attacks
- TCP SYN-flood attacks
- What volume of traffic is needed to be effective?
  - TCP SYN flood: 50K pps (20 Mbps)

Flooding Attacks
What's wrong with the Internet that DDoS is so easy?

- (Remember that ultimately it comes down to finding a vulnerability!)
- Network-layer connection-less protocols
  - No virtual circuits
  - No true traffic management
- No authentication
  - Probably just a minor issue give that one can amass a zombie army
  - Also required for lots of important applications!
- Packets can travel on any route between sender and receiver
- Different links have different data rates

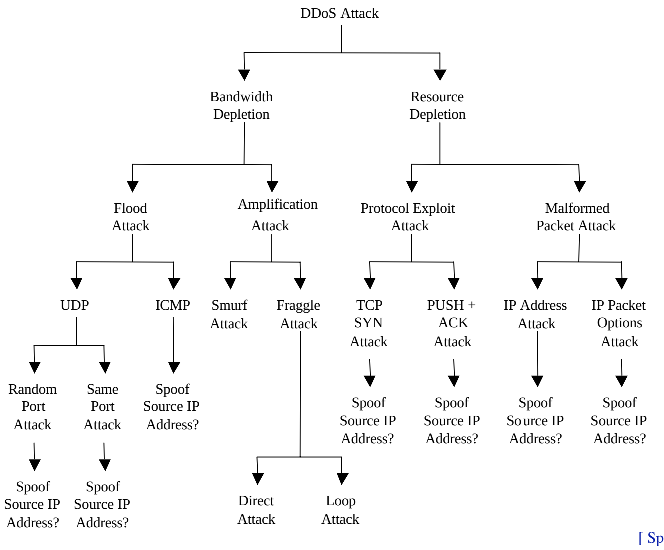
Distributed Denial-of-Service

Timeline [McHugh 01]



Distributed Denial-of-Service

Taxonomy of attacks (1)

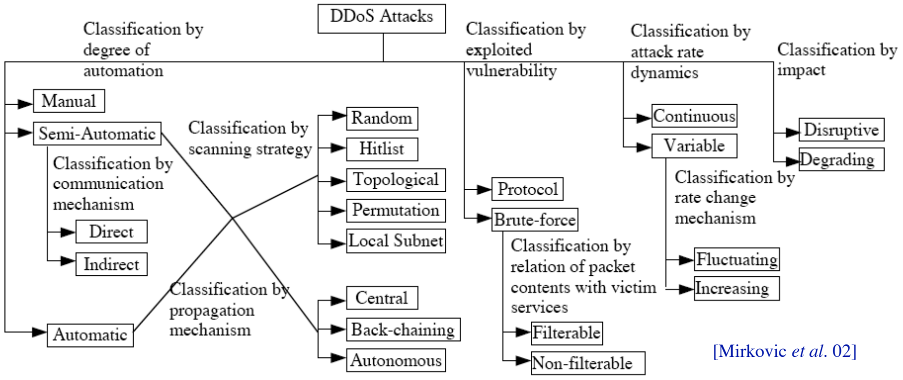


- DDoS Attack
  - Bandwidth Depletion
    - Flood Attack
      - UDP
        - Random Port Attack
          - Spoof Source IP Address?
        - Same Port Attack
          - Spoof Source IP Address?
      - ICMP
        - Spoof Source IP Address?
    - Amplification Attack
      - Smurf Attack
      - Fraggle Attack
        - Direct Attack
        - Loop Attack
  - Resource Depletion
    - Protocol Exploit Attack
      - TCP SYN Attack
        - Spoof Source IP Address?
      - PUSH + ACK Attack
        - Spoof Source IP Address?
    - Malformed Packet Attack
      - IP Address Attack
        - Spoof Source IP Address?
      - IP Packet Options Attack
        - Spoof Source IP Address?

[Specht & Lee 04]

Distributed Denial-of-Service

Taxonomy of attacks (2)

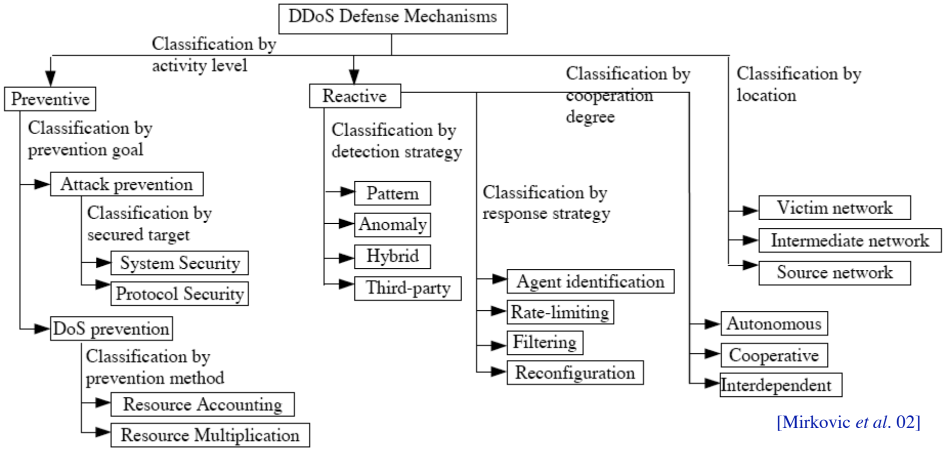


- DDoS Attacks
  - Classification by degree of automation
    - Manual
    - Semi-Automatic
      - Classification by communication mechanism
        - Direct
        - Indirect
    - Automatic
  - Classification by scanning strategy
    - Random
    - Hitlist
    - Topological
    - Permutation
    - Local Subnet
  - Classification by propagation mechanism
    - Central
    - Back-chaining
    - Autonomous
  - Classification by exploited vulnerability
    - Protocol
    - Brute-force
      - Classification by relation of packet contents with victim services
        - Filterable
        - Non-filterable
  - Classification by attack rate dynamics
    - Continuous
    - Variable
      - Classification by rate change mechanism
        - Fluctuating
        - Increasing
  - Classification by impact
    - Disruptive
    - Degrading

[Mirkovic *et al.* 02]

Distributed Denial-of-Service

Taxonomy of detection schemes



- DDoS Defense Mechanisms
  - Classification by activity level
    - Preventive
      - Classification by prevention goal
        - Attack prevention
          - Classification by secured target
            - System Security
            - Protocol Security
        - DoS prevention
          - Classification by prevention method
            - Resource Accounting
            - Resource Multiplication
    - Reactive
      - Classification by detection strategy
        - Pattern
        - Anomaly
        - Hybrid
        - Third-party
      - Classification by response strategy
        - Agent identification
        - Rate-limiting
        - Filtering
        - Reconfiguration
  - Classification by cooperation degree
    - Autonomous
    - Cooperative
    - Interdependent
  - Classification by location
    - Victim network
    - Intermediate network
    - Source network

[Mirkovic *et al.* 02]