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

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
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

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)

Distributed Denial-of-Service
Taxonomy of attacks (2)

Distributed Denial-of-Service
Taxonomy of detection schemes