

# **DENIAL-OF-SERVICE**

**Information Security in Systems & Networks  
Public Development Program**

**Sanjay Goel**

**University at Albany, SUNY**

**Fall 2006**

# Denial of Service Attacks

## Learning Objectives

- Students should be able to:
  - Recognize different techniques for launching DOS attacks
  - Identify vulnerabilities exploited to launch DOS attacks
  - Determine impact of DOS attacks on network and systems
  - Decide upon defense mechanisms to protect against DOS attacks

# Denial of Service Attacks

## Definition

- Denial of Service (DOS) is an attack on a system or network that renders it incapable of performing the function it was designed to do.
  - Aims to prevent legitimate users from authorized access to a system resource or delaying system operations and functions.
  - Attacks may be in the form of intense CPU usage, system reboots, or entire network failure
- Distributed Denial of Service (DDoS) attacks
  - DOS attacks that are amplified through coordinated attacks from several nodes simultaneously
  - Attacks are coordinated by using a framework of “handlers” and “agents”.

# Denial of Service Attacks

## Classification

- Bandwidth consumption
  - Attacks soak up the available network bandwidth
- Resource starvation
  - Attacks consume the available system resources  
e.g. CPU, memory, storage space
- Programming flaws
  - Failure of software to handle exceptions
  - E.g buffer overflow attacks
- Network Protocol Flaws
  - Weaknesses in protocols can be exploited to crash operating systems, fill buffers etc. causing DOS

# Denial of Service Attacks

## Modes of Attack

- Network connectivity attacks
  - Flooding
  - Malformed traffic
- Explicit resource consumption
  - Filling-up of data structures
  - Using storage by generating errors that are logged
  - Effect of other forms of attack, e.g.
    - SQL slammer virus
    - Account lock-out during password cracking

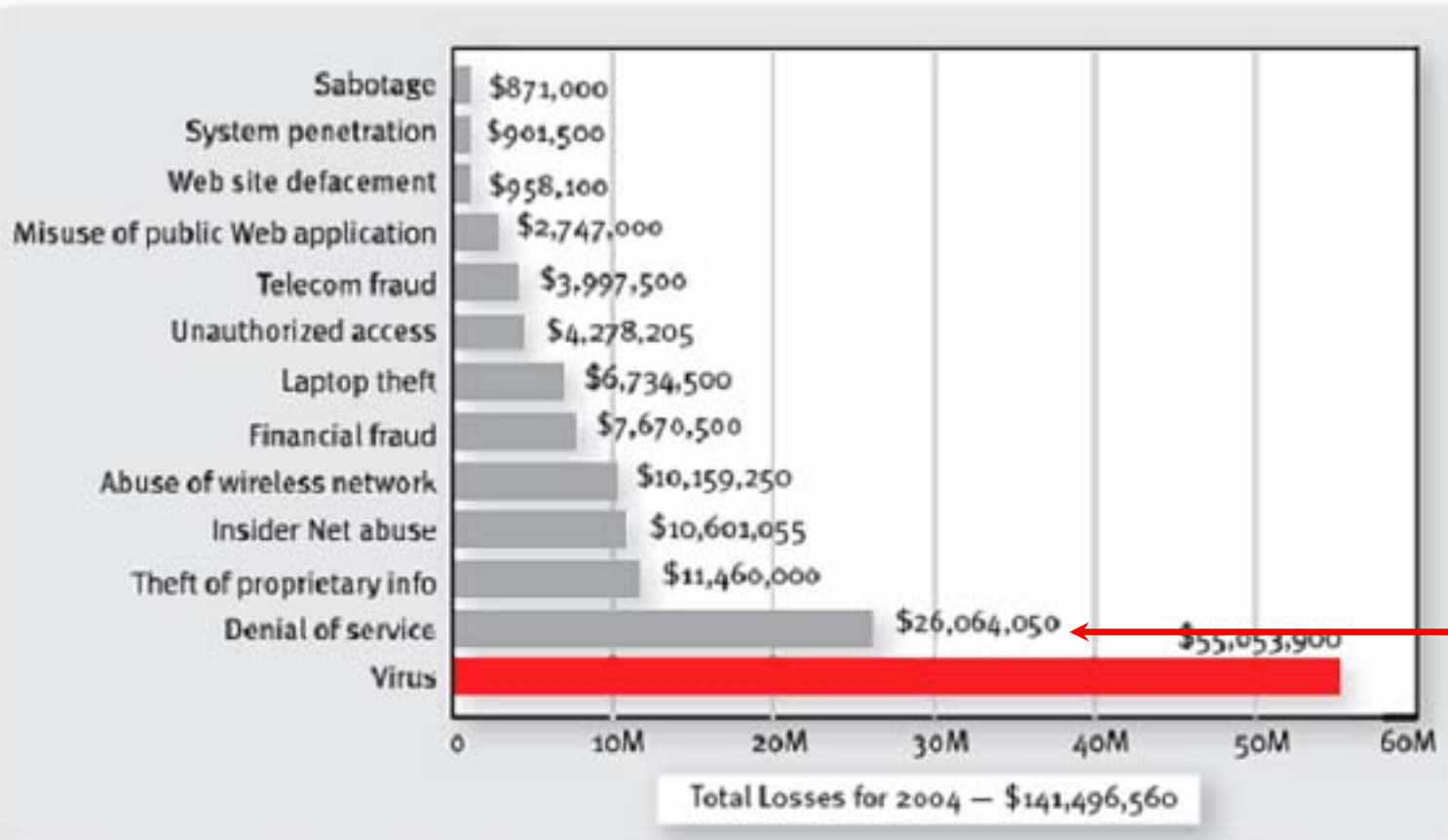
# Denial of Service Attacks

## Impact

- Critical network points stop functioning
  - e.g. Firewalls, routers, gateways, etc.
- Remote users unable to function
- Internet businesses cannot support customers
  - Customers balk and go elsewhere
- Communication slows down
  - Employee productivity suffers, delays projects
- Critical services cannot be provided, e.g.
  - SQL Slammer and 911 services
  - Coast guard computers directing shipping traffic
  - Air traffic control computers at LA airport

# Denial of Service Attacks

## Cost of Attacks



CSI/FBI 2004 Computer Crime and Security Survey  
Source: Computer Security Institute

2004: 269 Respondents

# Denial of Service Attacks

## Attacks

- SYN flooding
- DNS corruption, server corruption, RAM misuse
- ICMP attacks
- Operating system attacks  
e.g. time, memory leaks
- Mail bombing/spamming  
e.g. Avalanche
- Java Applets

# Denial of Service Attacks

## Mail Bomb

- Email bombing is characterized by hackers sending email message repeatedly to a specific address or a group of addresses at a site.
  - The message is often large and constructed from meaningless data in an effort to consume additional system and network resources.
  - Multiple accounts at the target site may be abused, increasing the denial of service impact.
- May involve mass multiple mailings to victim using intermediate bounce point
- Anonymous re-mailers makes it hard to track perpetrators
- Look for RFC compliant products (routers, firewalls, gateways)
- Problems result in larger disk usage and ultimately failure
- **Detection**
  - If your system suddenly becomes sluggish
  - If system suddenly runs out of disk space

# Denial of Service Attacks

## Mail Bomb

- **Reaction**

1. Identify source of email bomb/spam and configure your router to prevent incoming packets from that address.
2. Review email headers to determine the true origin of the email.
3. Alert the site from which email received to alert them to malicious activity.

- **Protection**

- Use a DMZ and try a not-so friendly mailer (/dev/null)
- Use mail mappings
- Learn the *signatures* of bombs and be aware
- Make sure your mail server stamps your domain on all mail

# Denial of Service Attacks

## DNS (Domain Name Service)

- DNS is critical to the operation of the Internet, thus it is a great target for attackers.
  - Cache corruption
  - Packet flooding (SYN)
  - Query overflow
- Attacks may be specific to DNS ports

# Denial of Service Attacks

## DNS: Cache Corruption

- Based on servers handling recursive queries
  - Add an 'A' record to the DNS of victim.com to resolve www.anotherhost.com to 127.0.0.1
  - Capturing dns.victim.com packets to dns.attacker.com allows retrieval of qid0 (query ID) of dns.victim.com
  - Send query to dns.victim.com asking for www.anotherhost.com using next qid
  - Flood dns.victim.com with spoofed replies from dns.anotherhost.com saying that www.anotherhost.com is 127.0.0.1
- Solution
  - Use an updated version of BIND for DNS
  - Keep caching to a minimum (set timeouts)
  - Disable unnecessary recursive queries

# Denial of Service Attacks

## ICMP

- ICMP (Internet Control Message Protocol) datagrams
  - signaling messages, encapsulated within IP datagrams, used by network layer to notify special events
    - e.g. destinations unreachable, redirection, congestion control, testing network connectivity
- Maximum datagram size is 64 KB in IP Specification
- ICMP “echo” datagrams typically used to test network connectivity.

# Denial of Service Attacks

## ICMP: Ping of Death

- A destination host is expected to respond with an icmp echo\_reply message when “pinged” with an icmp echo\_request message.
- Some systems react in an unpredictable fashion when receiving oversized (>64 KB) IP datagrams, causing systems crashing, freezing or rebooting, and resulting in a DoS.
- This is an example of a DOS attack that exploits a programming flaw
  - IP implementation is unable to deal with exceptional condition posed by the oversized datagram.

# Denial of Service Attacks

## ICMP: Ping Floods

- Attackers flood network link with icmp echo\_request messages using “ping” command
  - From DOS: ping -l 65510 victim.com
- Exploits a characteristic of the IP layer, that answers with icmp echo\_reply messages upon reception of icmp echo\_request messages
- Attack successful only if the source host and the channel between source & target have enough network bandwidth to flood the target host

# Denial of Service Attacks

## ICMP: Ping Attacks

- Solution
  - Get the fixes & updates/patches from vendors
  - Disable ICMP for your system
  - Try and set filters to watch for large ping packets and grab the time signature to block it out

# Denial of Service Attacks

## ICMP: Directed Broadcast Address

- The *directed broadcast address* is an IP address with all the host address set to 1. Used to simultaneously address all hosts within same network.
  - i.e. directed broadcast address for network class B 169.226.0.0 has IP address 169.226.255.255 and addresses simultaneously all hosts that can be within that network.
- For networks with subnets, *directed broadcast address* is an IP address with all host addresses within the same subnet set to 1.
- When a “ping” is made to a directed broadcast address all hosts in the broadcast domain answer back Network traffic “*amplification*”:
  - 1 datagram generates  $n$  datagrams in response (where  $n$  is the number of systems replying to a broadcast ICMP ECHO\_REQUEST)

# Denial of Service Attacks

## ICMP: Smurf Attack

- Attacker sends ping requests directed to broadcast address, with the source address of the IP datagram set to the address of the target system under attack (*spoofed* source address)
- All systems within broadcast domain answer back to the target address, thus flooding the target system with ICMP traffic and causing network congestion
  - Attack strength is proportional to the number of affected systems in the broadcast domain.
  - Leveraging the multiplicative effect, systems with limited network resources can generate a large amount of network traffic
- The source address of the 1st datagram (from hacker to broadcast address) corresponds to address of attacked system.

# Denial of Service Attacks

## ICMP: Directed Broadcast Address

- Prevent being used as an intermediary
  - Hosts can be configured not to respond to ICMP datagrams directed to IP broadcast addresses. Most OS's have specific network settings to enable/disable the response to a broadcast ICMP ping message
  - Disable IP-directed broadcasts at your leaf routers: to deny IP broadcast traffic onto your network from other networks (in particular from the Internet)
- Block network users from attacking other systems
  - A forged source is required for attack to succeed.
  - Routers must filter outgoing packets that contain source addresses not belonging to local sub-networks

# Denial of Service Attacks

## SYN Floods: Attack

- “Three-way handshake” is the procedure used to establish (open) a connection.
- TCP SYN flood is a DoS attack that sends a host more TCP SYN packets than the protocol implementation can handle.
  - Based on bogus TCP connection requests, created with a spoofed source IP address, sent to the attacked system.
  - Connections are not completed, thus soon it will fill up the connection request table of the attacked system, preventing it from accepting any further valid connection request.

# Denial of Service Attacks

## SYN Floods: Attack

- The source host for the attack sends a SYN packet to the target host.
- The target host replies with a SYN/ACK back to the legitimate user of the forged IP source address.
- Since the spoofed source IP address is unreachable, the attacked system will never receive the corresponding ACK packets in return, and the connection request table on the attacked system will soon be filled up.

# Denial of Service Attacks

## SYN Floods: Attack

- Attack works if spoofed source IP address is not reachable by the attacked system.
  - The legitimate owner of the source IP address would respond with a RST packet back to the target host, closing the connection and defeating the attack.
- Is a resource starvation attack because once the connection table is full, the server is unable to service legitimate requests.

# Denial of Service Attacks

## SYN Floods: Prevention & Detection

- Apply Operating System fixes:
  - Check incomplete connection requests, and randomly clear connections that have incomplete three-way handshake.
  - Reduces likelihood of a complete block due to a successful SYN attack, and allows legitimate client connections to proceed.
- Configure TCP SYN traffic
  - Increase connection queue
  - Decrease time-out wait for handshake
- Install IDS to detect TCP SYN flood attacks
  - Compare incoming log of recent packets on a regular basis

# Denial of Service Attacks

## SYN Flood: Prevention & Detection

- Filter network traffic:
  - Router/Firewall with SYN protection.
  - Use circuit level firewalls (*stateful inspection*) to monitor handshake of each new connection & maintain state of established TCP connections.
  - Filtering system must be able to distinguish harmful uses of a network service from legitimate uses.
  - Static packet filtering (*stateless*) does not protect from TCP SYN flood attacks.
- Prevent nodes from your network to initiate a SYN flood

# Denial of Service Attacks

## Rogue Applets

- Applets are a perfect avenue for DOS attacks
  - Java can execute resource consuming commands causing DOS
  - Hostile applets embedded in web pages can contain endless sound files, looping gifs, windows opening, hidden attacks
- These attacks are directed against users.
- Solution
  - Don't allow Java (ActiveX for that matter)
  - Stop the applets at the firewall

# Denial of Service Attacks

## Router Attacks

- When packet floods are sent to specific servers the routers just "upstream" from the servers are deluged with a large number of requests which they are not designed to handle.
- Once they discard packets and send status messages to other routers that the connection was full.
- Soon all paths to the servers were clogged, legitimate traffic couldn't get through the logjam, and the attackers' goals were accomplished
- Can also be initiated by sending a barrage of requests for UDP diagnostic services
  - Routers have several diagnostic ports that cause CPU usage when connected to (e.g. echo, discard)
- Configuring the router tables or shutting off router are the most effective ways of dealing with this.

# Denial of Service Attacks

## Summary

- DOS attacks is one of the most expensive attacks
- Based on the specific business there can be a different impact of the attack on the business
- Several different forms of DOS attack exist
- Security policies are critical in preventing DOS attacks.