Denial of Service (DoS)

S. Shanmuga
Senior Lecturer, Faculty of Informatics,
University of Wollongong Programs

What is Dos attack?

- DoS stands for Denial of Service
- An attacker attempts to prevent or hinder the legitimate use of a system, so they are attacks on availability.
- There are several common ways of doing this:
  - By starving the system of resources… (such as through bandwidth consumption)
  - Crashing the system
- Easy to launch and difficult to protect against, and are not restricted to internet based attacks
  - Telephone DoS to block legitimate callers.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Bandwidth consumption

- Any communication network has an upper bound on the volume of traffic at one time.
- Denial of service by bandwidth consumption occurs when this volume of traffic is reached, and further traffic cannot be transmitted.
- This could happen through legitimate interactions,
- When the limit is reached existing traffic will slow, freeze, or be disconnected.
  - Such inactivity *may* be evidence of a DoS attack

Bandwidth consumption

- Common attacks include protocol-based exploits that consume network bandwidth by sending crafted network data.
  - Attacks sometimes exploit misconfigured

- This could happen through legitimate interactions,

- When the limit is reached existing traffic will slow, freeze, or be disconnected.
  - Such inactivity *may* be evidence of a DoS attack

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Smurfs and Fraggles

- ICMP packets contain unauthenticated source and destination addresses.
  - In a **Smurf attack** the attacker generates lots of ICMP echo requests with a destination address associated with their target.
  - A single echo reply is small but enough can overwhelm a network

- Standard defense: Hosts should ignore ICMP echo requests.
  - External routers should not forward ICMP echo requests or replies.

- The **fraggle attack** uses UDP echo requests.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Resource Saturation

- Just as communication bandwidth is a DoS vulnerable resource for networks, computers also have DoS vulnerable resources; including memory, storage, and processor capacities.

- Resource saturation is when all of one or more of these resources is used up.

- The SYN flood is a popular example of an attack that uses all the available networking resources on a system.

- Web servers are common targets for a denial-of service attack

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Memory Starvation Attacks

- Consume available memory.

- With Windows NT 4 (Server Terminal Edition), for example, each connection accepted was allocated about 1 MB of memory.

- This could be used to drain the computer of memory, simply by opening lots of connections.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

System and Application Crash

- System or application crashes are generally easy to launch and difficult to protect against.

- Depending on the application, it may be as simple as sending a victim data or packets their application cannot handle

- A well-known example of these crashes is the "Ping of Death" attack, which uses oversized ICMP echo requests,
  - Such small but deadly messages are sometimes referred to as *poison packets*.
- These attacks are also commonly directed against network access devices.

System and Application Crash

- While small packets of data can be used to exploit vulnerabilities, if no such vulnerabilities are available we can still launch a Denial of Service attack, using “brute force”..
- We could flood a system or network with so much information that it cannot respond.
  - If a system can only handle 10 packets a second, and an attacker sends it 20 packets a second…
  - … the system may well fall over.
- Even if it doesn’t fall over, the processing of those illegitimate packets stops or slows down the processing of legitimate packets. This is also denial of service.

Email Bombs

- These are very simple and very annoying.
- The simplest and traditional email bomb involves sending many messages to your mailbox.
  - It could be thousands
- At some point the quota on your account will be full and you won't be able to store any mores,
- Using mail filters, which serve to provide protection against the general problem of spam, is a (somewhat) effective protection mechanism.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Email Bombing Viruses

- Email based viruses can also result in denial-of service.
- Applications are increasingly automated and integrated, within operating systems for example.
- Windows-based macro and Visual Basic Script (VBS) viruses:
  - The VBS.LoveLetter, “ I Love You”

Bandwidth consumption

- Ping packets are part of the Internet Control Message Protocol (ICMP) which are part of IP (Internet Protocol).
  - ICMP is for testing connectivity to various machines on the Internet
  - ICMP can convey status and error information
- Ping utilizes ICMP sends an ICMP echo reply.
- The response to a ping is referred to as a pong,

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Launching a “Ping of Death”

- Typically a command like the following, using a DOS window on Windows, would be used.
  - Ping –t –l 65527 IP address
  - Where 65527 corresponds to the amount of data to send to the IP address mentioned.
- Write a program to capture the active and inactive IP addresses in your network.
- Write a simple batch file to process the above.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

CPU Starvation Attack

- One specific example of a resource saturation attack is when we can put an application into a loop doing an expensive calculation or operations.

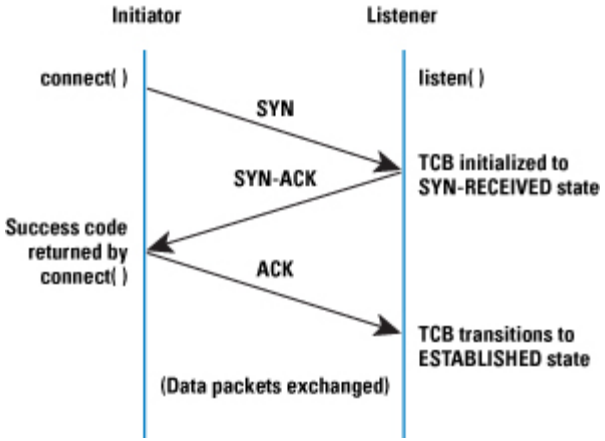
Quiz

- If you write an algorithm to run the browser infinite times, Is it memory or CPU starvation?

SYN Flood

- is a form of DoS attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

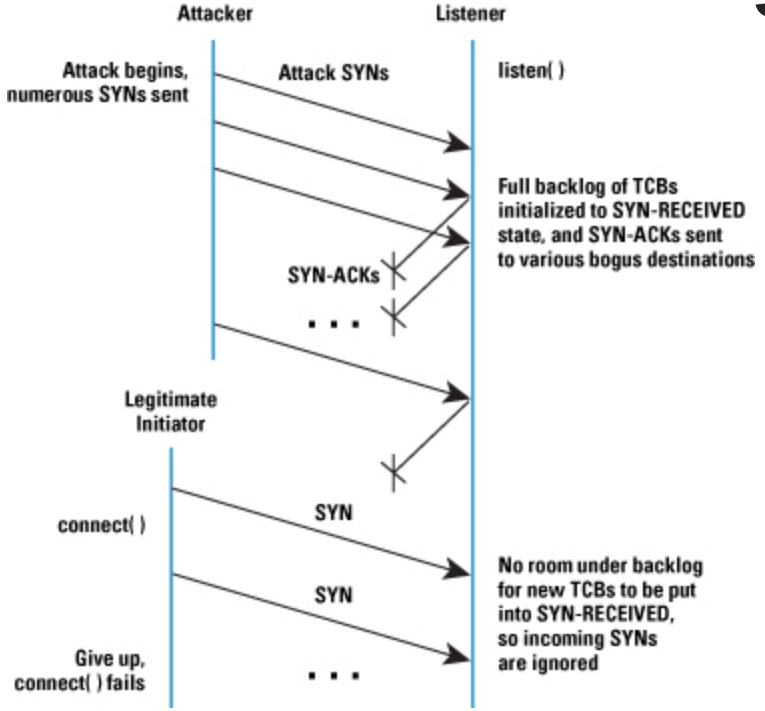
3-way TCP connection



- (1) The client requests a connection by sending SYN (*synchronize*) message to the server.
- (2) The server *acknowledges* this request by sending SYN-ACK back to the client.
- (3) The client responds with an ACK, and the connection is established.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

TCP-SYN Flooding



- The *Transmission Control Block* (TCB) is a transport protocol data structure (actually a set of structures in many operations systems) that holds all the information about a connection. The memory footprint of a single TCB depends on what TCP options and other features an implementation provides and has enabled for a connection. Usually, each TCB exceeds at least 280 bytes, and in some operating systems currently takes more than 1300 bytes. The TCP SYN-RECEIVED state is used to indicate that the connection is only half open, and that the legitimacy of the request is still in question. The important aspect to note is that the TCB is allocated based on reception of the SYN packet— before the connection is fully established or the initiator's return reachability has been verified.

Distributed DoS

- Since about 2000 the real problem for DoS is distributed attacks.
- Attacks are launched from multiple networked computers
- Difficult to defend against:
  - Hard to block multiple IP addresses

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

HTTP DoS Attack

- The most common application layer methods for launching a DDoS attack are HTTP GET and HTTP POST floods, with the GET floods significantly more “popular”.

- HTTP flood attack is an application layer DoS attack targeting websites and online services.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

HTTP DoS Attack

- The purpose of HTTP GET flood is to download large amount of data (images or scripts)
- HTTP flood attack is an application layer DoS attack targeting websites and online services.
- Multiple computers in the network are used to launch this attack, so this will prevent the legitimate user to get access to downloading files

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

HTTP DoS Attack

- The purpose of HTTP POST flood is to filling up online forms, but obviously using many computers in the network.

- This will slow down the service reply and in fact causing the legitimate users to wait.

Reflection Attack

- The attacker sends packets to a known service on the intermediary with a spoofed source address of the target system.
- The response from the intermediary is directed to the target.
- This attack uses the slave computers / serverrs to launch the attacks

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Amplification Attack

- It's a sophisticated denial of service attack using DNS servers to amplify the attack.

- Attackers use open internet services such as DNS resolvers and NTP servers to increase the amount of bandwidth sent to the victim and overwhelming their capacity.

- With no bandwidth remaining to service real customer requests, the victim's website is unable to service requests for real users.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Amplification Attack

- The reason it's called an amplification attack is because the attacker only needs a small Internet connection, while still being able to deluge the victim with traffic.

- This is done by spoofing (or faking) the source IP of the DNS request such that the response is not sent back to the computer that issued the request, but instead to the victim.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES

Amplification Attack

- This is easy since the protocol that DNS relies on is UDP and as such there is no verification that the source IP address is in fact the sender. Using very simple tools the attacker can send many thousands of spoofed requests to open resolvers and the responses, which are much larger than the request, amplify the amount of bandwidth sent to the victim.

INTI
International College Subang
LAUREATE INTERNATIONAL UNIVERSITIES