Denial of Service

Information Security – Lecture 18

Aadil Zia Khan

Denial of Service (DoS)

- A denial of service (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space

Some Famous DoS Attacks

- In February of 2020, Amazon mitigated the largest DDoS attack ever recorded
  - AWS Shield stopped a 2.3 Tbps attack
  - Previously the world record for largest recorded DDoS attack was 1.7 Tbps
- In February of 2018, 1.3 Tbps of traffic flooded Github servers with 126.9 million packets each second
  - Took GitHub's systems down for about 20 minutes
- In October, 2002 an attack lasting for approximately one hour was targeted at all 13 DNS root name servers

DoS Attack Strength Over The Years

- Due to Internet bandwidth growth, the largest attacks have increased from a modest 400 Mbps of DOS traffic in 2002 to 100 Gbps in 2010 to 2.3 Tbps in 2020
- With the an increase in IoT devices, the attack strength will only increase
- The reasons for attacks include
  - Financial extortion
  - Hacktivism
  - State-sponsored attacks on opponents
  - Attacks on systems as a diversion from the real attack on some other system

DoS Targets

- There are three main categories of resources that could be attacked
  - Network bandwidth
  - System resources
  - Application resources

Attacking Network Bandwidth

- A DoS attack targeting network bandwidth typically aims to overload an organization's access link
- Usually organization's connection to the ISP has a lower capacity than the links between ISP routers
- Thus it is possible for more traffic to arrive at the ISP's routers than can be carried over the organization's access link
    - Access router will discard some packets, delivering only as many as can be handled by the link
    - Users will experience a degraded or nonexistent service as a consequence

Attacking System Resources

- A DoS attack targeting system resources typically aims to overload or crash its network handling software
- Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system
    - Temporary buffers used to hold arriving packets
    - Tables of open connections
    - Other memory datastructures

Attacking System Resources

- Poison packet – a form of system resource attack which uses packets whose structure triggers a bug in the system's network handling software, causing it to crash
  - System can no longer communicate over the network until this software is reloaded

- E.g., of poison packet : ping of death
  - The size of a correctly-formed IPv4 packet including the IP header is 65,535 bytes
  - Many historical computer systems could not handle larger packets, and would crash if they received one
  - Since sending a ping packet larger than 65,535 bytes violates the Internet Protocol, attackers would generally send packets in fragments - when the target system attempts to reassemble the fragments and ends up with an oversized packet, memory overflow could occur and lead to various system problems including crash

Attacking Application Resources

- An attack on a specific application (e.g., Web server) involves a number of valid requests, each of which consumes significant resources
- This limits the ability of the server to respond to requests from other users
- For example, if a large, costly DB query can be constructed, then an attacker could generate a large number of these that severely load the server
    - This limits its ability to respond to valid requests from other users.

Classical DoS Attacks - Simple Network Flooding

- Attacks network bandwidth
- Suppose the attacker has a higher bandwidth link compared to the victim
- The attacker will simply send traffic at maximum rate to the victim
  - E.g., by running a massive number of ping commands targeted towards the victim
- Since packet arrival rate is more than departure rate, the queue will develop at the victims end leading to packet losses

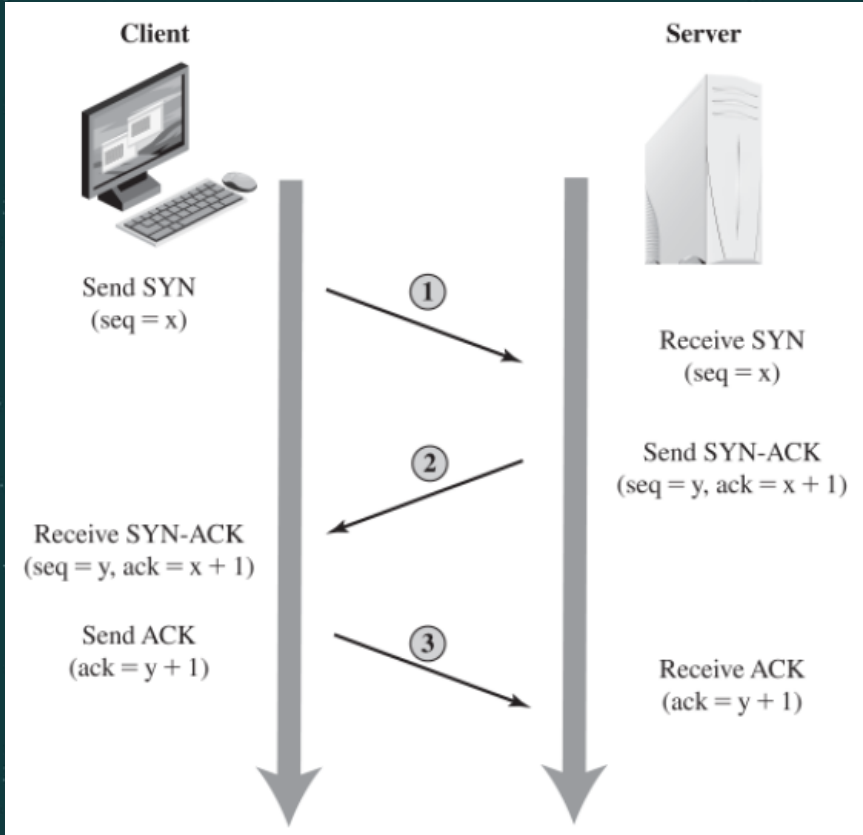
Classical DoS Attacks - Simple Network Flooding

- Network Flooding problem – attack packets will include source address
  - Attacker will be identified
  - If too much garbage traffic is coming from the same source, the network can identify it as an attack and drop it
  - Ping response packets will burden the attacker

- Solution - Source Address Spoofing
  - A common characteristic of packets used in many types of DoS attacks is the use of fake source addresses – this is called source address spoofing
  - Given sufficiently privileged access to the network handling code on a computer system, it is easy to spoof source address
    - Usually done via the *raw socket interface* on many operating systems or custom device drivers

Classical DoS Attacks - SYN Spoofing Attack

- Attacks system resources
- Recap: TCP 3way handshake
  - Client sends connection request (SYN) to server, together with required information
  - Server saves information in TCP connections table, and sends a SYNACK to the client, together with required information
  - Client replies with an ACK to complete connection setup



Classical DoS Attacks - SYN Spoofing Attack

- Attacker sends a connection request (SYN) to the server
  - But the source address is spoofed
- Server replies with a SYNACK but sends it to the spoofed address
- Spoofed client obviously doesn't ACK
  - It may or may not send a RST packet to inform the server that it did not initiate
- Server retransmits SYNACK multiple times
- Attacker will do this with multiple different addresses – thus filling up the TCP connections table, preventing other connections
- Note: Unlike the flooding attack, here the attacker does not need access to a high bandwidth link