Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

April 23, 2015

Secure networks

- Before the advent of modern telecommunication network, messages were delivered:

  – by hand – spoken over telephone or – sent via radio waves
- Security goals then were:

  – keeping the message secret (confidentiality)

  – making sure the message came from the true sender (authenticity)

  – making sure the message wasn't altered (integrity)
- Modern telecommunication systems – new security concerns

  – the means of delivering the messages could be stopped, slowed, or altered

  – messages could be redirected to false recipients

  – attackers could also gain access to communication channels

Secure networks

- Four broad goals
- Availability, confidentiality, functionality and access control

Secure networks

Availability

- Ensuring network availability means that authorized users have access to information, services, and network resources
- Denial-of-service (DoS) attacks is an attack on availability
- Attacks on network availability can prevent customers, suppliers, and employees from transacting business
- The profitability of online retailers depends on network services, such as a webserver, being continuously available

Secure networks

Confidentiality

- Has a slightly different meaning in the context of network security
- Means preventing unauthorized users from gaining information about the networks structure, data flowing across the network, network protocols used, or packet header values
- An attacker can gain valuable information by passively monitoring traffic coming into and out of a corporate network
- Even if the traffic is encrypted the attacker can still see sites urls, amount of data transmitted, and port numbers used
- The attacker might also be able to map an internal network and passively fingerprint internal hosts
- Default TTL value MS Windows: 128, Mac OS X: 64

Secure networks

Functionality

- To prevent attackers from altering the capabilities or operation of the network
- Appropriate network functionality would include properly routing packets, correctly resolving hostnames, excluding unapproved protocols, correctly assigning IP addresses
- ARP poisoning, man-in-the-middle attack

Secure networks

Access control

- In the context of network security, access control is the policy-driven control of access to systems, data, and dialogues
- To keep attackers from accessing any internal resources
- Also include limiting access to internal employees

Denial of service (DoS)

- A denial-of-service (DoS) attack attempts to make a server or network unavailable to serve legitimate users by flooding it with attack packets
- Corporations and government entities are attackers' primary targets

Denial of service ... but not a DoS attack

- All service interruptions are not DoS attacks
- Faulty coding: For example, *in 2011, Newsnet Scotland claimed to be the victim of a DoS attack by pro-Unionism political opponents. However, it turned out that the loss of service was caused by faulty coding*
- Referrals from large sites: a common occurrence with news aggregators
- The smaller news site can become overwhelmed by the dramatic increase in traffic

Denial of service ... but not a DoS attack

- All service interruptions are not DoS attacks
- Faulty coding: For example, *in 2011, Newsnet Scotland claimed to be the victim of a DoS attack by pro-Unionism political opponents. However, it turned out that the loss of service was caused by faulty coding*
- Referrals from large sites: a common occurrence with news aggregators
- The smaller news site can become overwhelmed by the dramatic increase in traffic

Goals of DoS attacks

- The ultimate goal of a DoS attack is to cause harm
- For corporations, this can come in the form of losses related to online sales, industry reputation, employee productivity, or customer loyalty
- DoS attacks can cause harm by
  - stopping a critical service or
  - slowly degrading services over time

Goals of DoS attacks

Stopping a critical service

- Web services are a popular target because of the economic damage that can be done
- Websites for Amazon, Walmart, and the Gap, were unreachable for about an hour two days before Christmas in 2009
- A DDoS attack was launched against the DNS provider (Neustar) to these large companies
- Attackers may stop employees from accessing their e-mail/file servers

Goals of DoS attacks

Degrade services

- DoS attacks against critical services are easy to identify and don't last long
- The most damaging attacks are those that cannot be identified and so they last a long time
- An attack that slowly degrades services is more difficult to detect because there isn't an abrupt change in service quality
- Network administrators cannot see a clear distinction between genuine growth in network traffic and a progressive DoS attack
- They may be forced into unnecessary capital expenditures for additional bandwidth, hardware, and software

Methods of DoS Attacks

Four main methods:

1. Direct/indirect
2. Intermediary
3. Reflected
4. Sending malformed packets

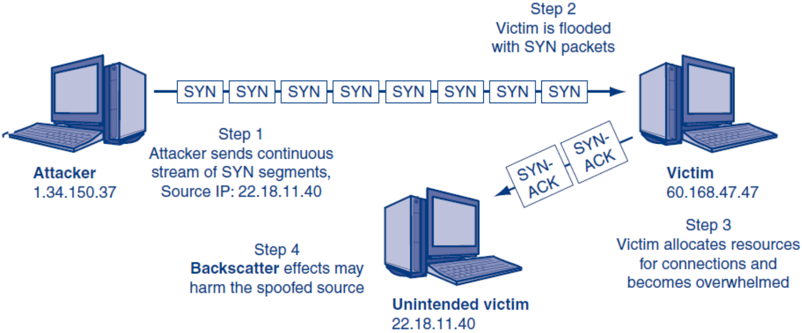
- Each method has its own advantages and disadvantages
- Simpler attacks may be easier to implement, but they are also easier to stop
- Attacks that are inherently more complex may be extremely difficult to stop without causing additional harm

Methods of DoS Attacks

Direct/indirect

- A direct attack occurs when an attacker tries to flood a victim with a stream of packets directly from the attacker's computer
- An indirect attack tries to flood the victim computer in the same way, but the attacker's IP address is spoofed (faked) so the attack appears to come from another computer

Methods of DoS Attacks: Direct/indirect



Step 2
Victim is flooded
with SYN packets

Step 1
Attacker sends continuous
stream of SYN segments,
Source IP: 22.18.11.40

Step 3
Victim allocates resources
for connections and
becomes overwhelmed

Step 4
Backscatter effects may
harm the spoofed source

Methods of DoS Attacks: Direct/indirect

Flooding

- Can only succeed if the attacker can flood the victim with more requests than the victim can handle
- The attacker must have more bandwidth, memory (RAM), and/or CPU power than the victim
- Corporate servers can handle more requests than the single attacker can generate

Methods of DoS Attacks: Direct/indirect

Spoofing

- Attackers prefer to use spoofed IP addresses that hide their IP address
- The attacker cannot get direct feedback about the attack

Backscatter

- Occurs when a victim sends responses to the spoofed IP address used by the attacker, and inadvertently floods an unintended victim

Methods of DoS Attacks: Direct/indirect

Types of packets sent

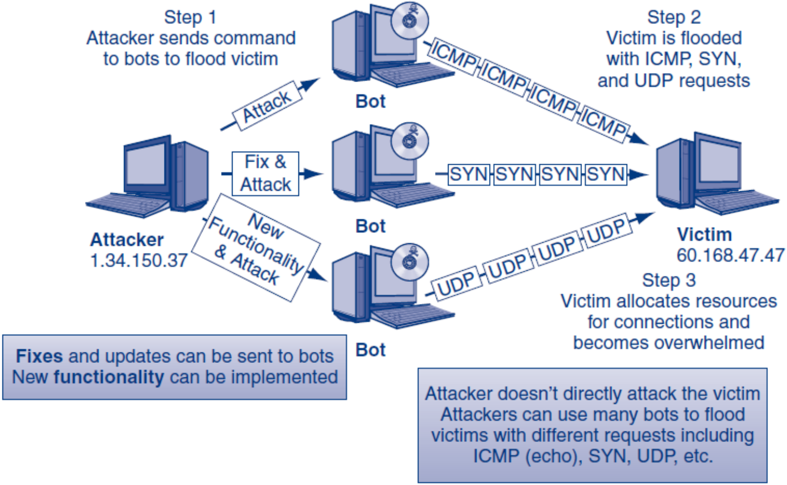
- SYN Flood: A victim is flooded with SYN packets in an attempt to make many half open TCP connections. Memory is allocated for each false connection causing the victim to run out of memory and crash
- Ping Flood: A victim is flooded with ICMP packets (also known as echo requests) that appear to be normal supervisory traffic. Bandwidth and CPU cycles are consumed to the point where the victim crashes
- HTTP Flood: A victim, typically a webserver, is flooded with application layer web requests. The webserver crashes due to insufficient memory and CPU power

Methods of DoS Attacks

Intermediary

- Intermediaries, typically referred to as bots, are actually compromised hosts running malware controlled by the attacker
- The DoS attack begins when the botmaster sends a signal for the bots to attack the victim
- An attacker controlling bots in a coordinated attack against a victim, is known as a distributed denial-of-service (DDoS) attack
- In DDoS the identity of attacker is hidden and resources are available to him

Methods of DoS Attacks: Intermediary



Step 1
Attacker sends command
to bots to flood victim

Step 2
Victim is flooded
with ICMP, SYN,
and UDP requests

Step 3
Victim allocates resources
for connections and
becomes overwhelmed

Fixes and updates can be sent to bots
New **functionality** can be implemented

Attacker doesn't directly attack the victim
Attackers can use many bots to flood
victims with different requests including
ICMP (echo), SYN, UDP, etc.

Methods of DoS Attacks

Reflected

- Uses responses from legitimate services to flood a victim
- The attacker sends spoofed requests to existing legitimate servers
- Servers then send all responses to the victim
- Servers with large capacities are chosen that can overwhelm a victim with its traffic
- Using a botnet in a reflected attack is known as a distributed reflected denial-of-service (DRDoS) attack

Methods of DoS Attacks

Smurt flood

- A variation of a reflected attack that takes advantage of an incorrectly configured network device (router) to flood a victim
- The attacker sends a spoofed ICMP echo request to a broadcast enabled network device
- The network device forwards the echo request to all internal hosts
- Internal hosts respond to the spoofed ICMP echo request and the victim is flooded
- The attacker benefits from a multiplier effect because a single ICMP request is responded to by multiple hosts
- Disabling broadcast to internal hosts will stop a Smurf flood

Methods of DoS Attacks

Sending malformed packet

- Sending malformed packets that will cause the victim to crash
- For example, ping of death is a well-known older attack that uses an illegally large IP packet to crash the victim's operating system

  – the flaw has been fixed and the attack is rarely used anymore
- Flaws in host operating systems susceptible to malformed packets will continue to surface and be exploited