Cybersecurity

Denial of Service Attacks

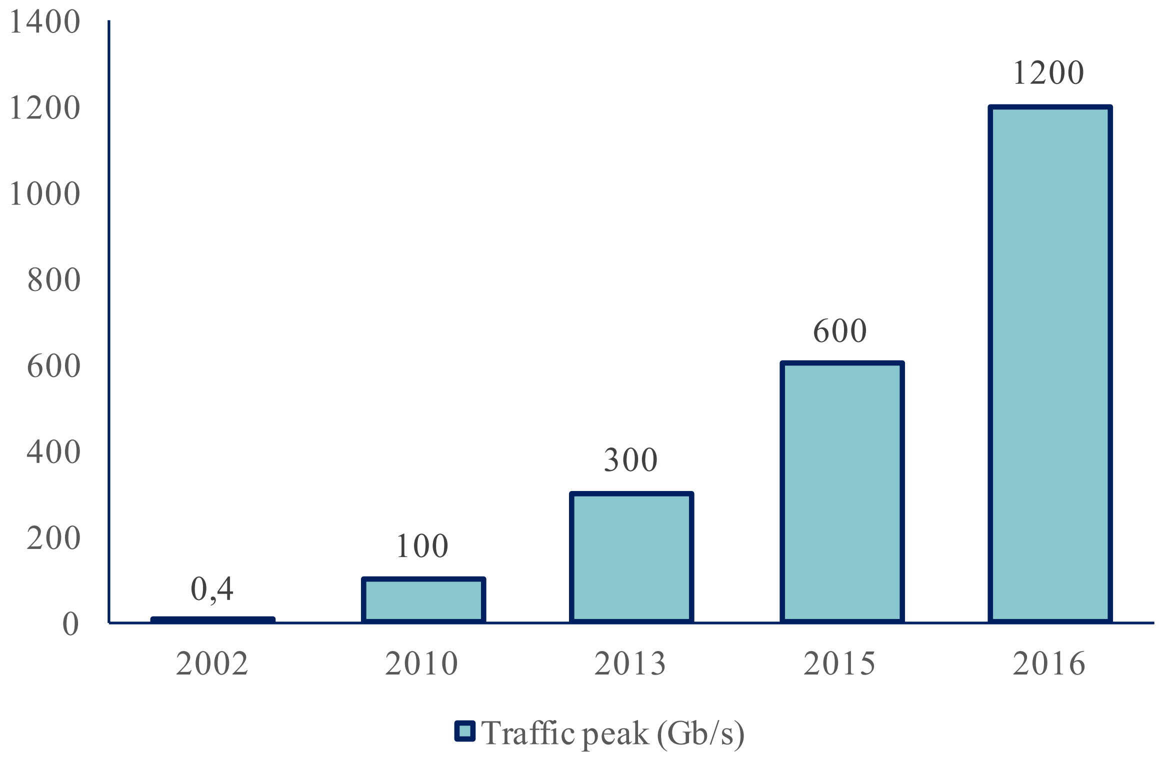
Mauro Barni

University of Siena

Denial of Service attacks

- **NIST SP 800-61:** *a denial of service (DoS) attack 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*
- Multiple reasons
  - Financial extortion
  - Hacktivism
  - State-sponsored attacks
  - Diversion

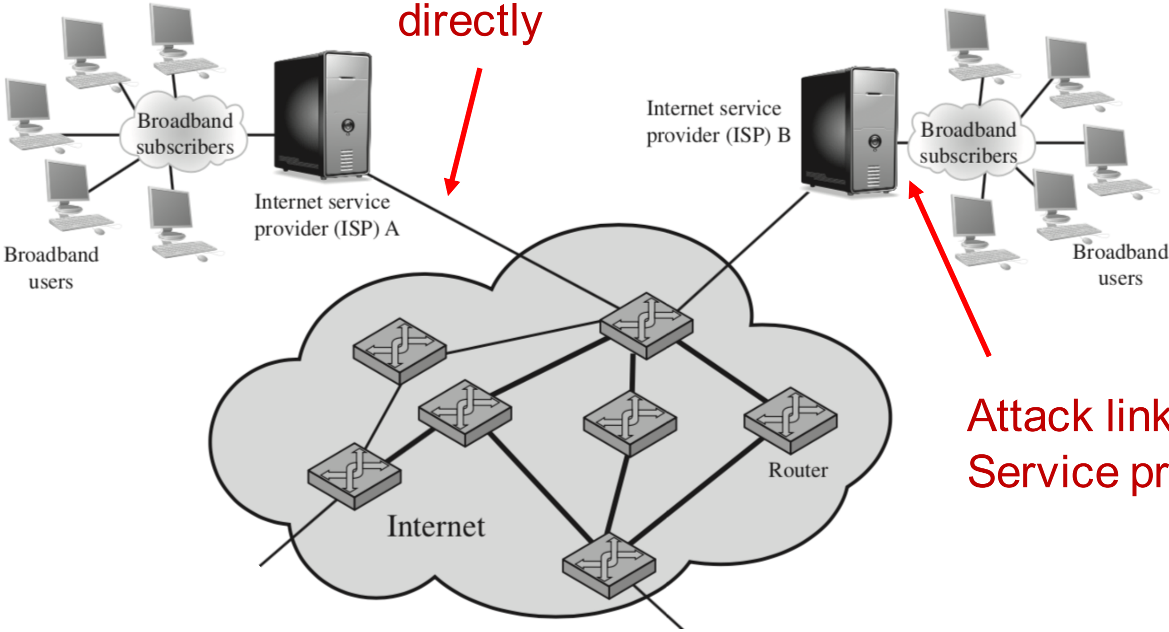
Increasing power and diffusion



A DDoS attack in October 2016 to a major DNS reached an unprecedented level with about 100,000 bots involved (including IoT devices like webcams, baby monitors …), multiple waves of attacks, a duration of several hours

Attacked resources

- DoS attacks can be classified according to the resource they are trying to exhaust
- **Attacks against network resources**



Attack ISP network directly

Attack link to Internet Service provider

Attacked resources

- **Attacks against system resources**
  - overload or crash its network handling software (example: SYN flooding attack)
  - uses packets whose structure triggers a bug in the system’s network handling software, causing it to crash (**poison packet**)

Attacked resources

- **Attacks against application resources**
  - send a massive amount of valid requests, each of which consumes significant resources.
  - design and send particularly heavy requests
  - build a request that triggers a bug in the application software to force the system to reload the service

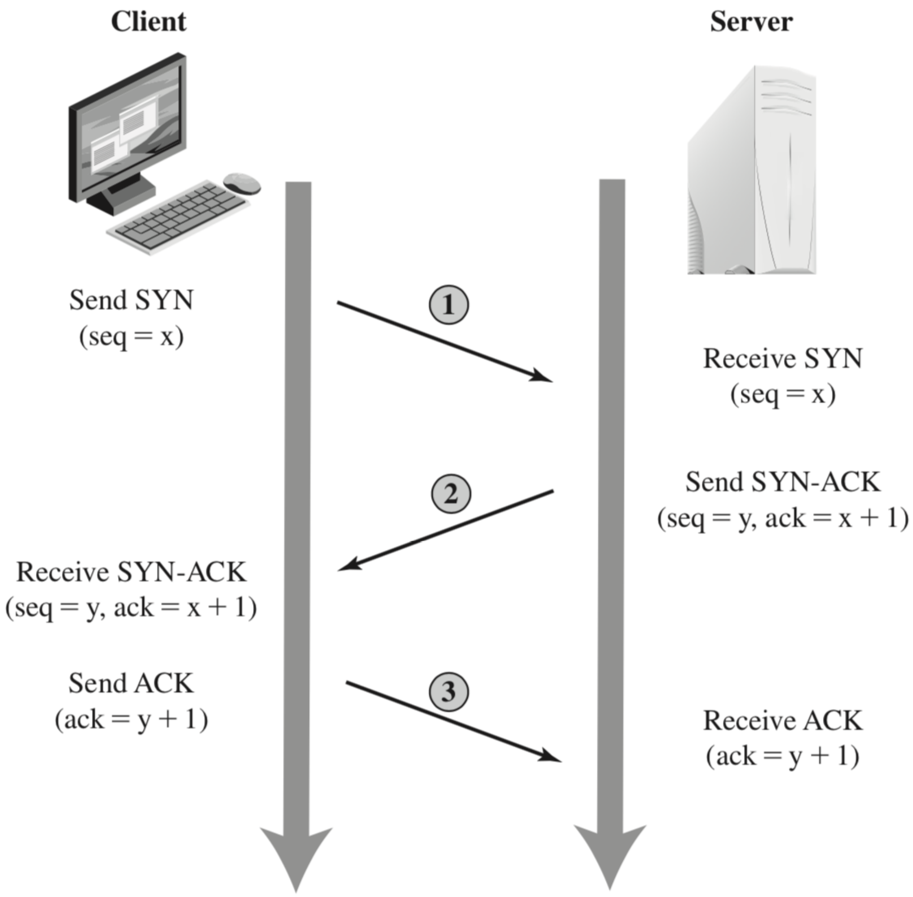
Classical network flooding attack

- Single source attacks send all packets from a single source with a high bandwidth connection (ex. ping flooding attack)
- Packets source can be traced and the attacker identified
- It also causes back-traffic problems
- Access to *raw socket interface* allows to counterfeit the source address of packets
  - *egress filtering* recommended to ISP but rarely implemented

Source address spoofing

- Source address spoofing has many advatanges for the attacker
  - makes the identification of attack source difficult (it requires the help of network engineers)
  - does not overload the bandwidth of the attacker
  - use of non-existing IP addresses increases traffic to target system
- On the other hand, backscatter traffic can be exploited to detect attacks and filter packets with non-existing source addresses

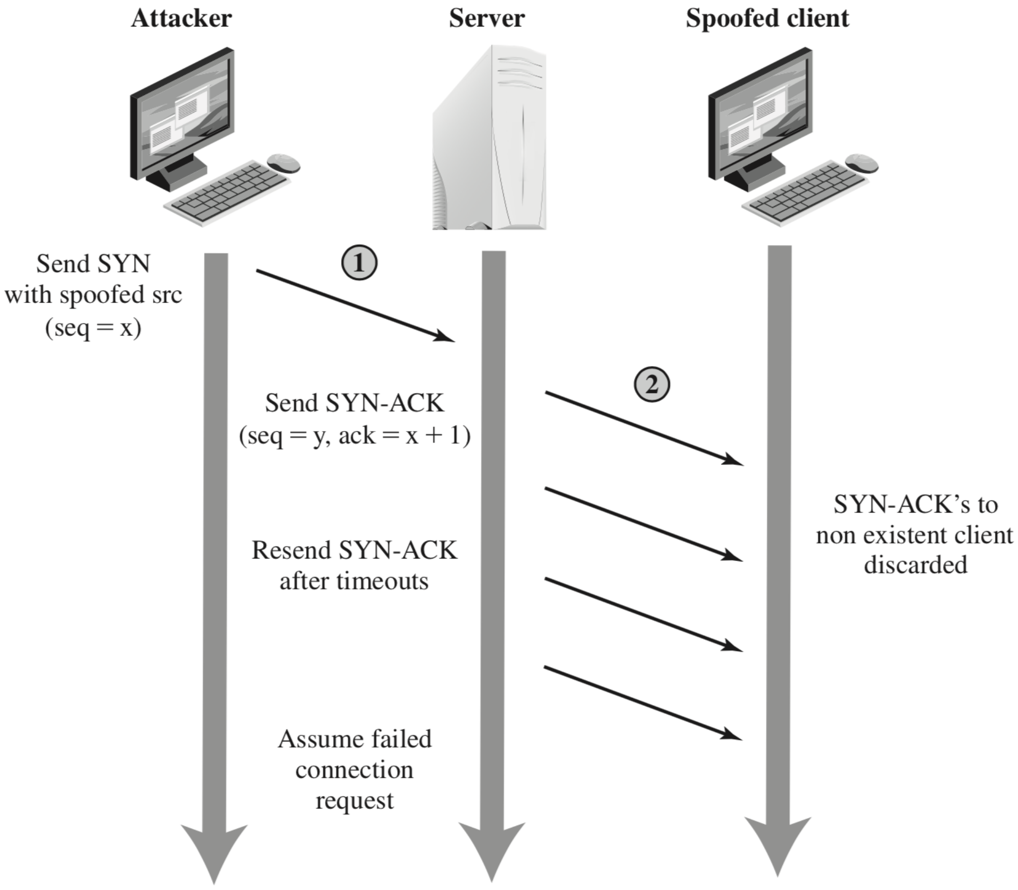
SYN spoofing attack



TCP connection handshake

- To provide a reliable transport protocol, if ACKs are not received in due time SYN-ACK is resent up to a maximum number of times
- Connection details are maintained in a TCP connection table
- Size of TCP connection table is chosen based on normal traffic assumptions

SYN spoofing attack


Attacker
Server
Spoofed client
Send SYN with spoofed src (seq = x)
1
2
Send SYN-ACK (seq = y, ack = x + 1)
Resend SYN-ACK after timeouts
Assume failed connection request
SYN-ACK's to non existent client discarded

SYN spoofing attack

- To maximize the effectiveness of the attack, non existing src addresses are used
- Valid spoofed source addresses may also be attacked to minimize the possibility that a reset command is transmitted
- SYN spoofing attack requires considerably less resources than network flooding attacks

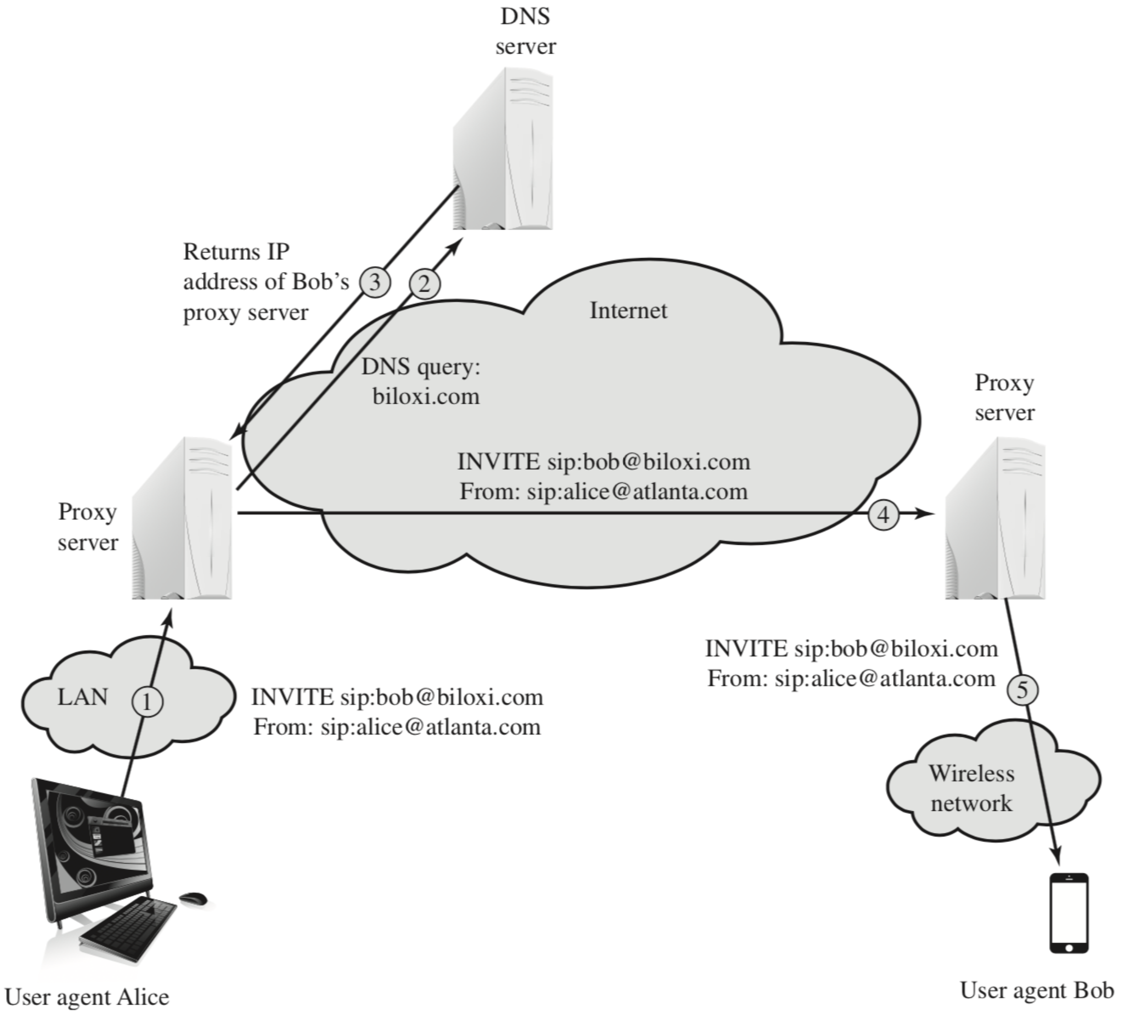
Other types of flooding attacks

- Any kind of packets can be used to mount a flooding attack
  - **ICMP** flooding attacks: ping flooding attack belongs to this category. Other kinds of packet, that can not be filtered, are commonly used. Ex: *ICMP destination unreachable*, *ICMP time exceeded*
  - **UDP** flooding attack. Can be used whenever the target system runs a service using UDP traffic
  - **TCP flooding.** SYN flooding, or just normal TCP packets.

Application-based DoS attacks

- Force the target to execute resource-consuming operations that are disproportionate to the attack effort
- Application-based network consumption attacks, consume the network resources of the server

Example 1: SIP-flood attack


DNS server
Returns IP address of Bob's proxy server
3
2
Internet
DNS query: biloxi.com
Proxy server
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
4
Proxy server
LAN
1
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
5
Wireless network
User agent Alice
User agent Bob

- Establishing a SIP connection requires quite a heavy load to the Proxy server
- Sending several requests with random addresses may consume all the resources of the proxy

Example 2: HTTP-requests attacks

- **HTTP Flood**: request to download a large file from the target causes the Web server to read the file from hard disk, store it in memory, convert it into a packet stream, then transmit the packets. This process consumes memory, processing, and transmission resources
- **Slowloris**
  - web servers uses multi threads to handle service requests
  - RFC2616 states that a blank line must be used to indicate the end of the request headers and the beginning of the payload
  - Sending incomplete requests and keeping them alive will eventually consume all the available thread resources of the server

From DoS to DDoS

- Effectiveness and stealthiness of the attack can be increased in a variety of ways:
  - Distributed denial-of-service attacks
  - Reflector attacks
  - Amplifier attacks.

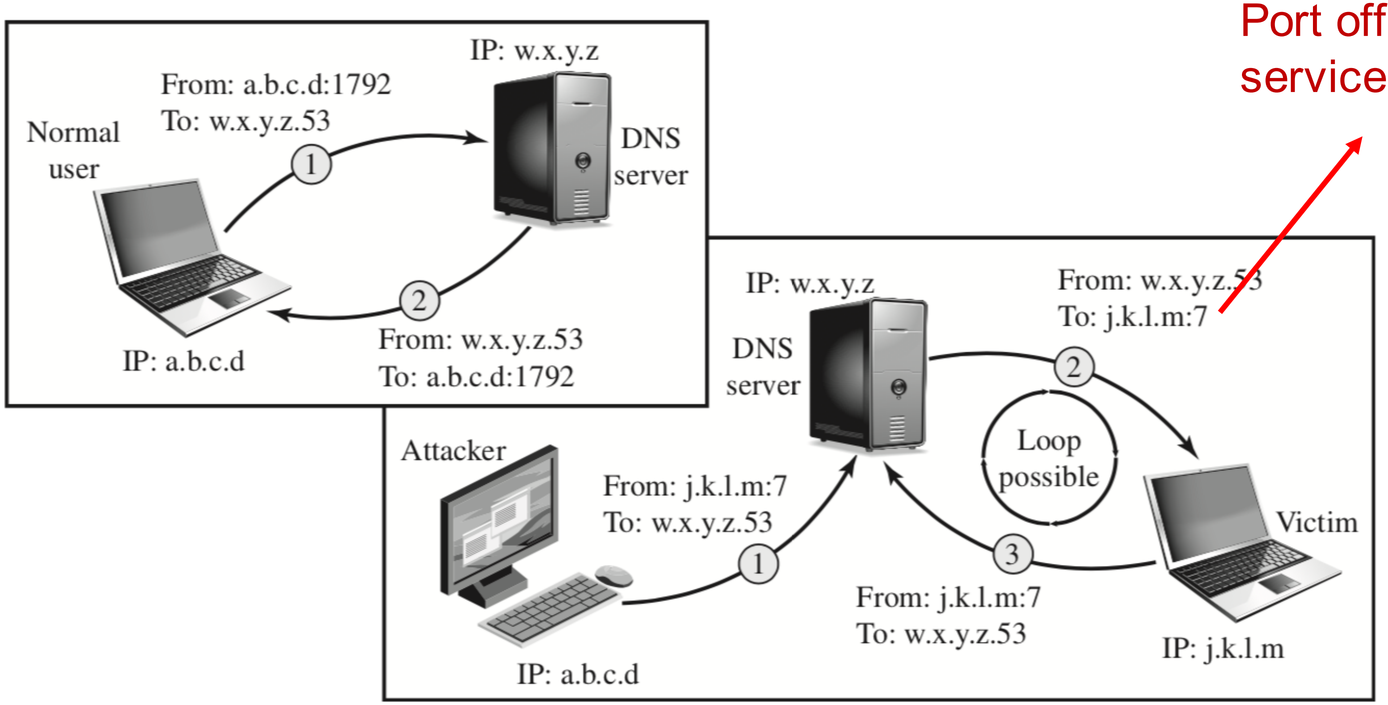
Distributed DoS

- They rely on zombies and big botnets
- There exists an underground economy that creates and hires out botnets for use in Ddos attacks
- Botnets often have a hieararchycal structure
- Several DDoS tools exist to build, handle and exploit botnets to launch DDoS attacks (e.g. Tribe Flood Network, Tribe Flood Network 2000, TFN, TFN2K)

Reflector attacks

- A reflector attack use non-corrupted systems as intermediaries for the attack
- Attacker sends packets with spoofed source address to several servers. Spoof address is the address of the target of the attack.
- The servers reply to the spoofed address and floods the target system
- Services with answers longer than requests are often chosen
- Intermediate servers, should have a high capacity to avoid that their functionality is disturbed and the attack (partially) interrupted
- A variant of SYN-FLOODING attack exploiting reflectors has been used often to create considerable damage

Reflector attacks with loops

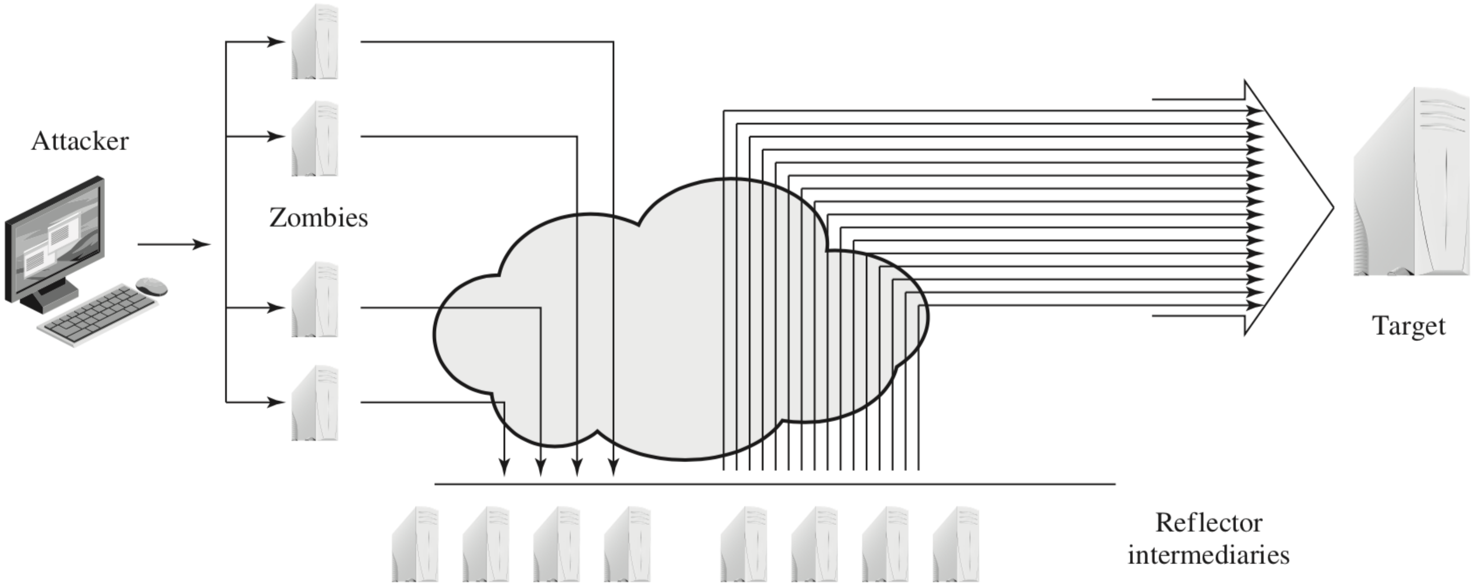


Port offering an echo service

- Flooding attacks with loops can be very dangerous and can be implemented with limited resources, but are quite easy to be filtered out

Amplification attacks

- It is a variant of the reflector attack where the packet is sent to the broadcast address of an intermediary network (ping and echo requests are common choices)



- It is recommended that broadcast address can not be used externally to the network; unfortunately this is a widely ignored recommendation

Amplification attacks

- Another variant of the amplification attack can exploit service providers (like DNS) answering packets much longer than the request
- With classic DNS protocols, a 60 bytes UDP request can result in a 512 bytes UDP response
- The extended DNS protocol (thought to provide additional services and support for IPv6, can transform a 60 butes request unto a 4000 bytes response

Defenses and responses

- DDoS can not be prevented entirely. 4 lines of defense
  - **Attack prevention (before the attack):** These mechanisms enable the victim to endure attack attempts. Techniques include enforcing policies for resource consumption and providing backup resources available on demand
  - **Attack detection and filtering (during the attack):** These mechanisms attempt to detect the attack as it begins and respond immediately. Detection involves looking for suspicious patterns of behaviour. Response involves filtering out
  - **Attack source identification (during and after the attack):**This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough to mitigate an ongoing attack
  - **Attack reaction (after the attack):** This is an attempt to eliminate or curtail the effects of an attack.

Attack prevention

- The great majority of DoS attacks use some form of source address spoofing
- Filtering packets woith spoofed source address is the primary defense line against DoS.
  - As close as possible to the packet source
  - ISP are bet positioned to do that
    - reverse path filters (e.g. in Cisco routers using the “ip verify unicast reverse-path” command)
  - Long-standing recommendation, often ignored by ISP
- Limit rates of certain class of packets (ICMP floods)
- SYN-Spoofing attack can be limited by modifying the TCP connection handling protocol (*SYN cookies, selective drop*)

Attack prevention

- The best defense against broadcast amplification attacks is to block the use of IP-directed broadcasts. This can be done either by the ISP or by any organization whose systems could be used as an intermediary.
- Long-standing security recommendations that all organizations should implement.
- Attacks against web services require modification to the service
  - Captcha or graphic puzzles are often used to avoid attacks from bots

Attack responses

- Incident response plan
  - Coordinated effort with ISP
    - attack can only be blocked upstream
    - alternative communication means with ISP
- Automated network monitoring and intrusion detection system running to immediately notify about abnormal traffic (more on this later)
- After detection, we pass to attack identification (possibly with ISP)
- After identification: packet filtering (ISP), bug removal
- Source identification useful to report the attack to the relevant law enforcement agencies
- **Last but not least: contingency plan to switch to alternative servers or rapidly commission new ones**

References

- W. Stallings, L. Brown, “*Computer security: principles and practices*”, Pearson, 4-th edition. Chapter 7
- Lectures notes (these slides)