SWINBURNE UNIVERSITY OF TECHNOLOGY

Distributed Denial of Service Attacks

Lecture sixteen

Outline of Lecture

- Distributed Denial of Service Attacks
- Classification of attacks
- Types of attacks

Learning Objectives

- At the end of this lecture you should be able to explain
  - What a DDOS attack is it
  - How DDoS attacks can be classified
  - Types of DDoS attacks
  - Reflector and Direct attacks
  - SYN Flooding
  - TCP Reset
  - UDP Flooding
  - ICMP Flooding
  - DNS Request attacks

Denial of service attacks

- Denial of Service attack
  - An incident that disables a victim from receiving or providing normal service.
- Relies on consuming limited or non-renewable system resources.
- Can be launched by using system design weaknesses, CPU intensive tasks, or flooding.
  - Examples : ping of death, teardrop, smurf.

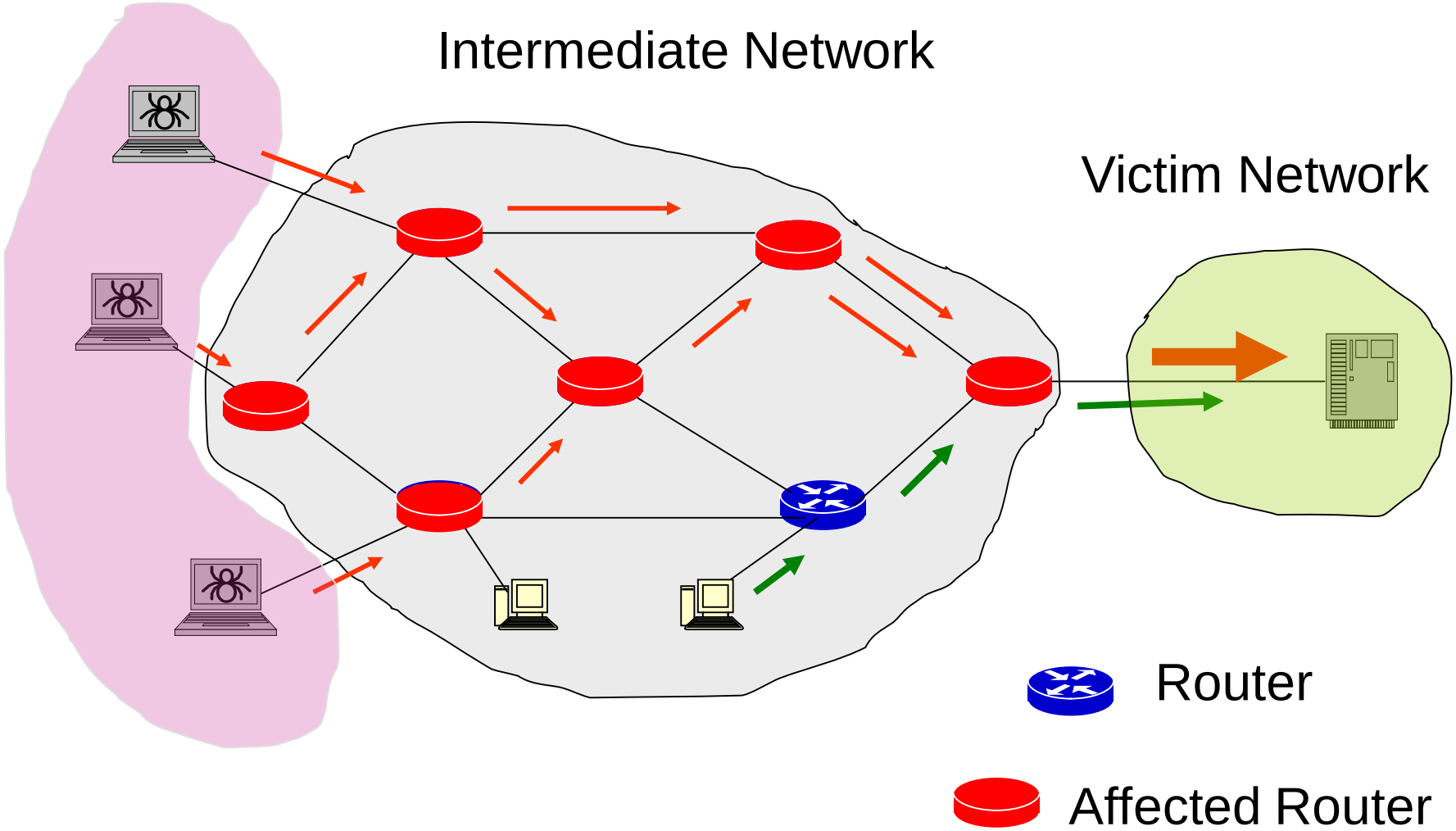
Distributed denial of service attacks (DDoS)

- Do not depend on system or protocol weaknesses.
- DDoS attacks
  - A large number of compromised hosts send overwhelming number of useless packets to jam a victim, or its Internet connection (network) or both.
  - Compromised hosts (handlers and zombies) are vulnerable machine infected by virus or worm, and are used in DDoS attack.
  - DDoS attacks exploit the resource asymmetry between the Internet and the victim
  - Biggest difficult with DDoS attacks is identifying legitimate traffic from attack traffic
- The burst of traffic generated crashes the victim or disables it.

DDoS Attacks

- Hard to detect and stop.
- Can spread within a few minutes.
- Usually period of flooding lasts for a few hours, and is sporadic.
- IP Spoofing makes it hard to identify attackers.

DoS/DDoS Attacks



Why do DDoS attacks occur?

- Target of a DDoS attack
  - Host, router, server or entire network
- The purpose of DDoS attacks is to stop a victim providing or receiving normal services in the Internet.
- DDoS can and have been used to disable strategic business, government, public utility and even military sites.
- Potential also for blackmail of companies that rely on Internet connectivity for their revenues
  - Particularly those that have high volume, relatively low value transactions
    - Amazon, eBay etc

How do DDoS attacks occur?

- DoS exploits system design weaknesses (e.g. ping-of-death) or imposes computationally intensive tasks on a victim (e.g. encryption or decryption computation).
- DDoS scan for vulnerable hosts to gain malicious control (handlers and zombies).
- Attacker uses handlers to coordinate the attack, and uses zombies to attack the victim by sending large amount of legitimate traffic to the victim network.

DDoS classification

- Can classify DDoS attacks in a number of ways
- Its architecture
  - Direct
  - Reflector
- The resource it denies
  - Bandwidth exhaustion
    - Either incoming or outgoing
  - Server resource exhaustion
    - Buffer space for SYN-ACK attacks

Direct or Reflector

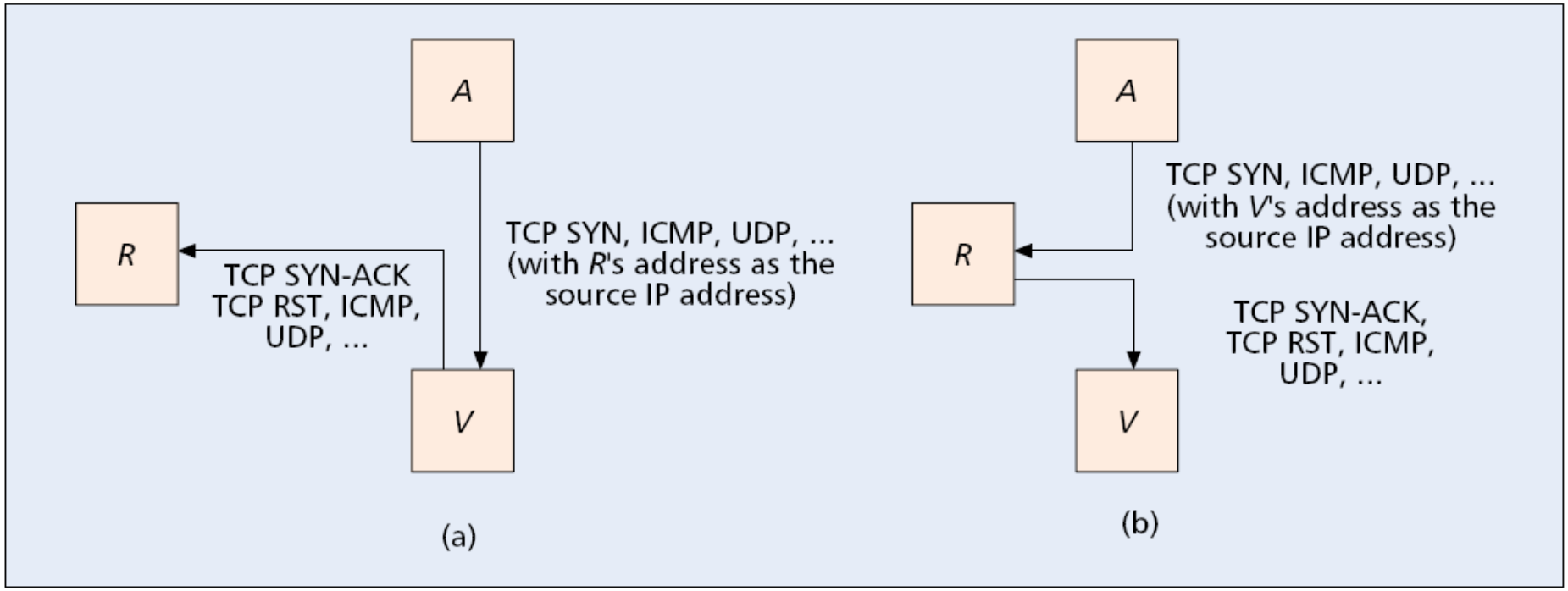


Figure 1. *Two types of flooding-based DDoS attack: a) direct; b) reflector.*

Direct or Reflector

- Direct attack
  - An attacker arranges to send a large number of attack packets directly toward the victim
  - Probably makes use of compromised hosts (zombies)
- Reflector attack
  - An indirect attack
  - Intermediary nodes are innocently used as attack launchers
  - Intermediate nodes may be servers, routers or (less often) hosts
  - Attacker sends packets to the reflector that require responses
  - Packets spoof victim's IP address as source address

DDoS Architecture

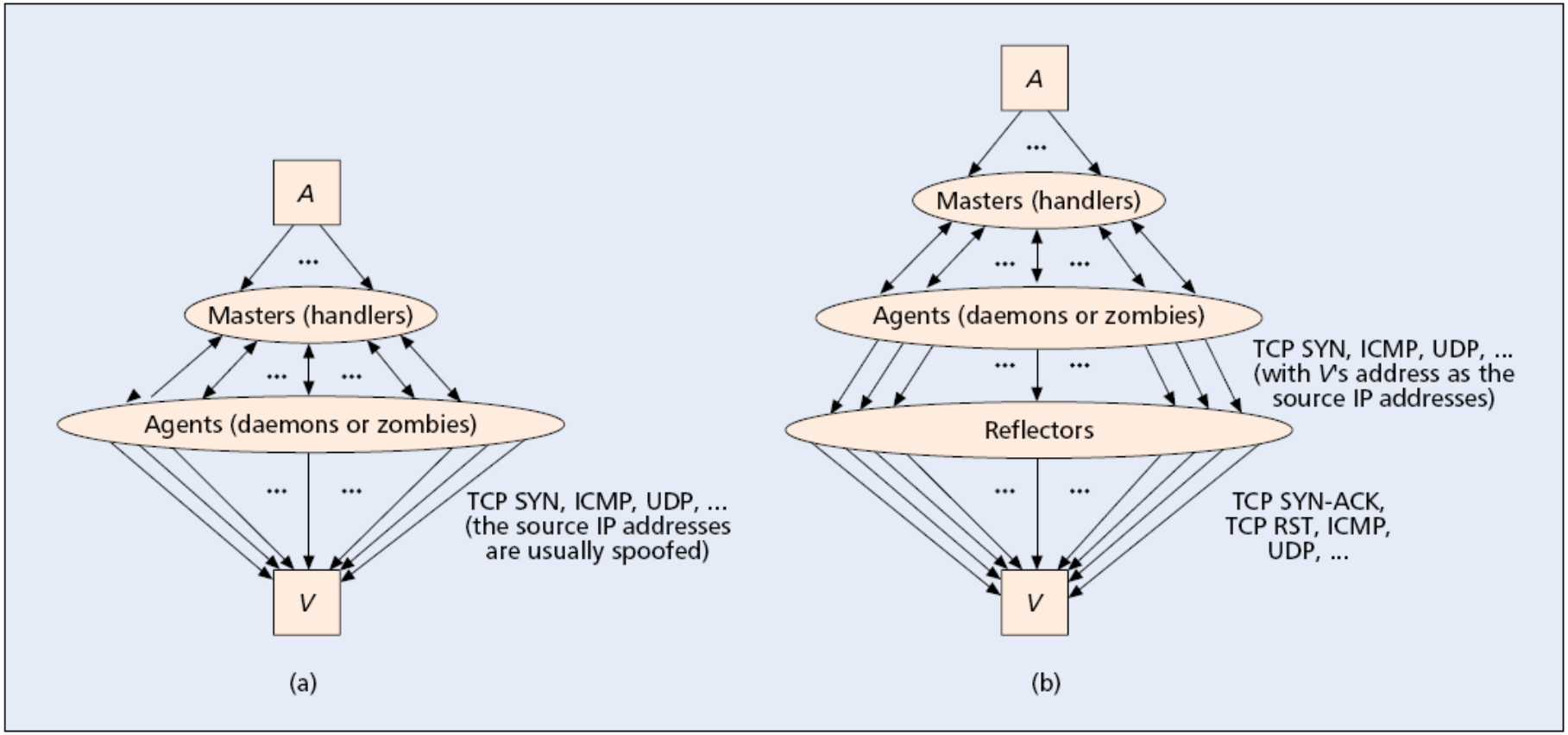


Figure 2. *DDoS attack architectures for a) direct and b) reflector attacks.*

Direct DDoS

- Direct attack contains 2 stages. First is to scan and find vulnerable host in the Internet and install attack tools in them (zombies).
- Secondly, attacker sends command to the zombies to attack through intermediate nodes (handlers).
- The attack traffic with spoofed IP addresses is sent to victim from the zombies.
- Spoofed IP to reduce the risk of tracing back via zombies,
  - Also makes it harder to filter attack traffic without affecting legitimate traffic.

Reflector DDoS

- Reflector attack contains 3 stages. The first one is similar to that of Direct attack.
- Secondly, attacker instruct zombies to send traffic to the third party with victim' spoofed IP address.
- In the third stage, the third party will reply (without knowing) to the victim with attack traffic.
- More dangerous because more distributed and has bandwidth amplification effect

Reflector

	Packets sent by an attacker to a reflector (with a victim's address as the source address)	Packets sent by the reflector to the victim in response
Smurf	ICMP echo queries to a subnet-directed broadcast address	ICMP echo replies
SYN flooding	TCP SYN packets to public TCP servers (e.g., Web servers)	TCP SYN-ACK packets
RST flooding	TCP packets to nonlistening TCP ports	TCP RST packets
ICMP flooding	• ICMP queries (usually echo queries) • UDP packets to nonlistening UDP ports • IP packets with low TTL values	• ICMP replies (usually echo replies) • ICMP port unreachable messages • ICMP time exceeded messages
DNS reply flooding	DNS (recursive) queries to DNS servers	DNS replies (usually much larger than DNS queries)

Table 1. *A summary of some reflector attack methods.*

DDoS Attack types

- Can classify based on resource it denies
  - Bandwidth exhaustion
    - Either incoming or outgoing
  - Server resource exhaustion
    - Buffer space for SYN-ACK attacks
- Bandwidth attacks
  - Aims to disable the services provided by victim or its network by sending an excessive volume of useless traffic.
- Server resource exhaustion
  - SYN-ACK attack exhausting number of connections a common attack (SYN flooding)

Flash crowds and bandwidth attacks

- One of the difficulties in recognising bandwidth attacks is that they can be confused with a flash crowd
  - Measures to prevent bandwidth attacks can affect flash crowds
  - Flash crowds need to be controlled but not eliminated
- Flash Crowds
  - Large number of legitimate users access a network or server at the same time.
- Both Bandwidth attacks and Flash Crowds cause congestion in the victim's network, and overload the victim's servers.

Flash crowds

- Any method of identification needs to be able to distinguish between flash crowds and DDoS attacks
  - May be regular and predictable
    - Stock exchange prices at opening time
  - Irregular and predictable
    - Significant sporting events
  - May be irregular and unpredictable
    - Natural disasters such as bushfires or floods
    - Terrorist attacks
- Traffic from flash crowds need to be controlled while DDoS attacks need to be eliminated

Flash crowds

- Traffic in Bandwidth attacks is unresponsive to traffic controls, while in Flash Crowds they are responsive to traffic control.
  - One way of preventing flash crowds is to get users to verify some aspect of their usage
  - Eg “Captcha”.
- Traffic in Flash Crowds is genuine, while in Bandwidth attacks it is not.
- Traffic in Flash Crowds is usually web traffic, while in Bandwidth attacks it can be anything.

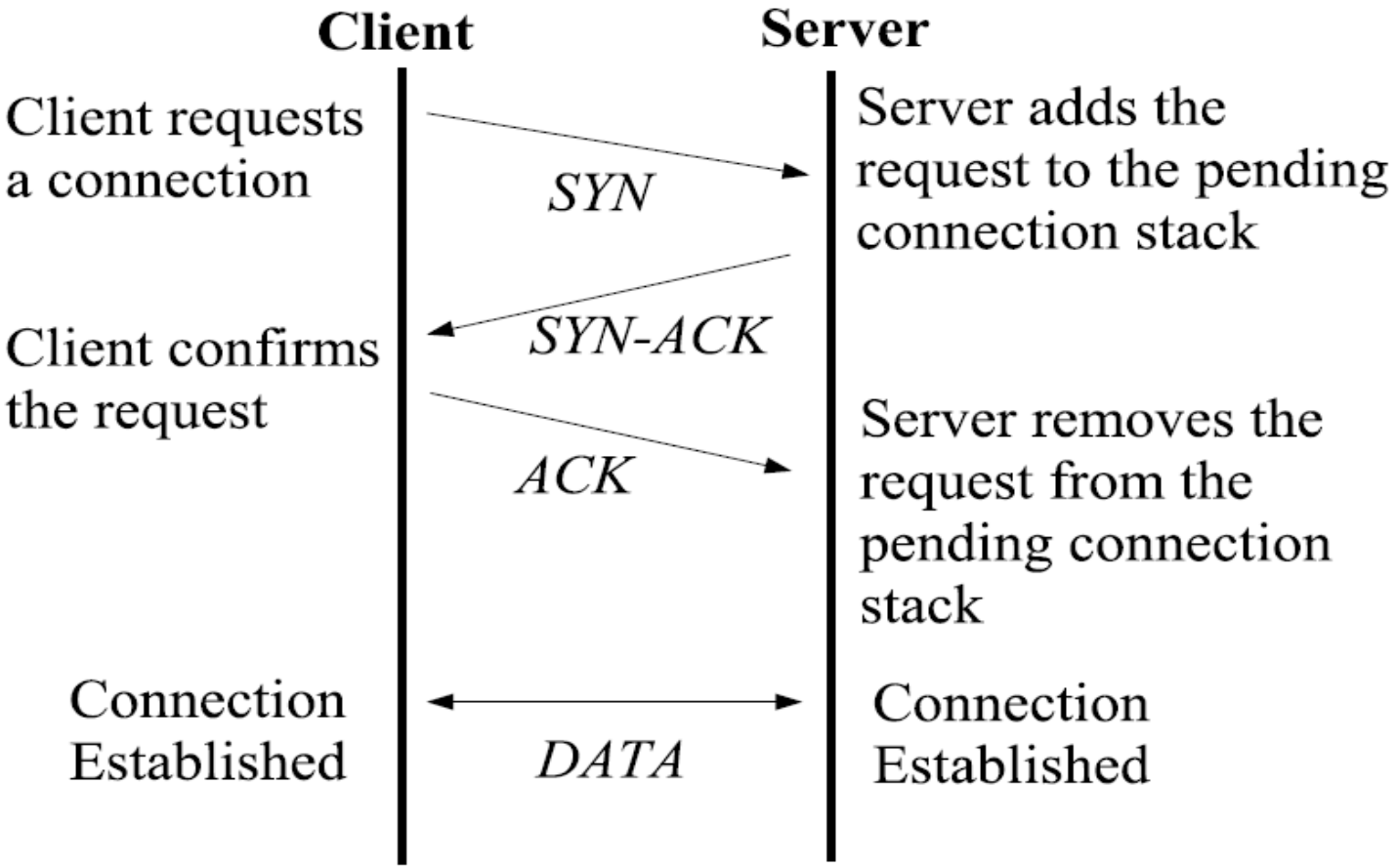
Common DDoS Attack Types

- SYN Flooding
- TCP Reset
- UDP Flooding
- ICMP Flooding
- DNS Request

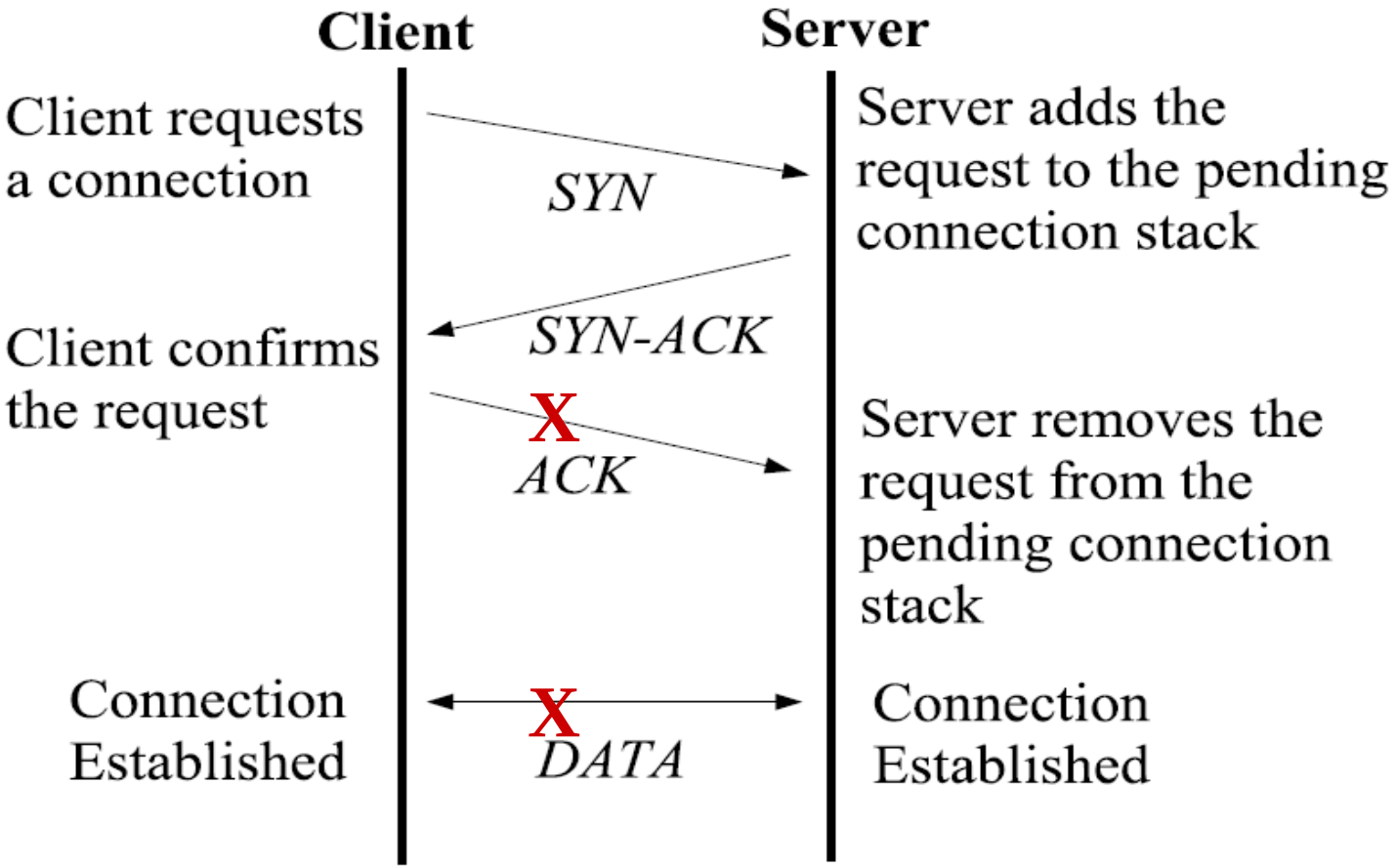
SYN Flooding

- The most common and powerful DDoS attack.
- Attackers send SYN messages with spoofed IP address causes half-open TCP connections.
- These pending connections are kept in a server's memory at the victim network.
- Once the memory is full, no new request including legitimate requests can be processed and the services of the system are disabled.

TCP Three-Way Handshake



SYN Flooding



SYN Cookies

- A cryptographic approach to dealing with SYN flooding
- Uses cryptographic techniques embedded in the ISN (initial sequence number) to deal with the problem
  - The ISN is the SYN Cookie
- Once the SYN queue fills up, new entries are dropped
- However if an acknowledgement is received there is sufficient information in the acknowledgment to reconstruct the dropped SYN message
- SYN Cookies include authentication information and sufficient information to reconstruct the original SYN request in the ISN

SYN Cookies

- Built around the ISN
  - Rather than choosing a random number the ISN sent in response to a SYN has the following structure:
    - t (time) 5 bits
    - m (maximum segment size) 3 bits
    - s (result of a cryptographic computation based on server and client IP addresses, port numbers, t and secret key)
- If the response is received the host subtracts one from the ISN and then recalculates the above computation
  - t is used to ensure request hasn't timed out and to prevent replay attacks
  - m is information needed during set up
  - s is used to ensure valid SYN cookie

SYN Cookies

- s is the authentication value
- Based on hash functions and secret (sec1)
- s is calculated as follows
  - Concatenate sec1,saddr,sport,daddr,dport,sec1
  - Do an MD5 or SHA-1 hash on concatenated value
  - Additional computations to avoid replay attacks and ISN prediction
    - Another hashed secret and counter
- SYN Cookies work by including authentication information and sufficient information to reconstruct the original SYN request in the ISN
- Implemented in Linux

TCP Reset

- Can be a direct or reflector attack
- TCP packets with spoofed source addresses sent to non-listening ports on reflector host
- Under TCP reset attacks, victim usually responds with RST (Reset) message.
- If a reflector attack causes congestion on the victim's incoming link.
- If a direct attack causes congestion on the victim's outgoing link.

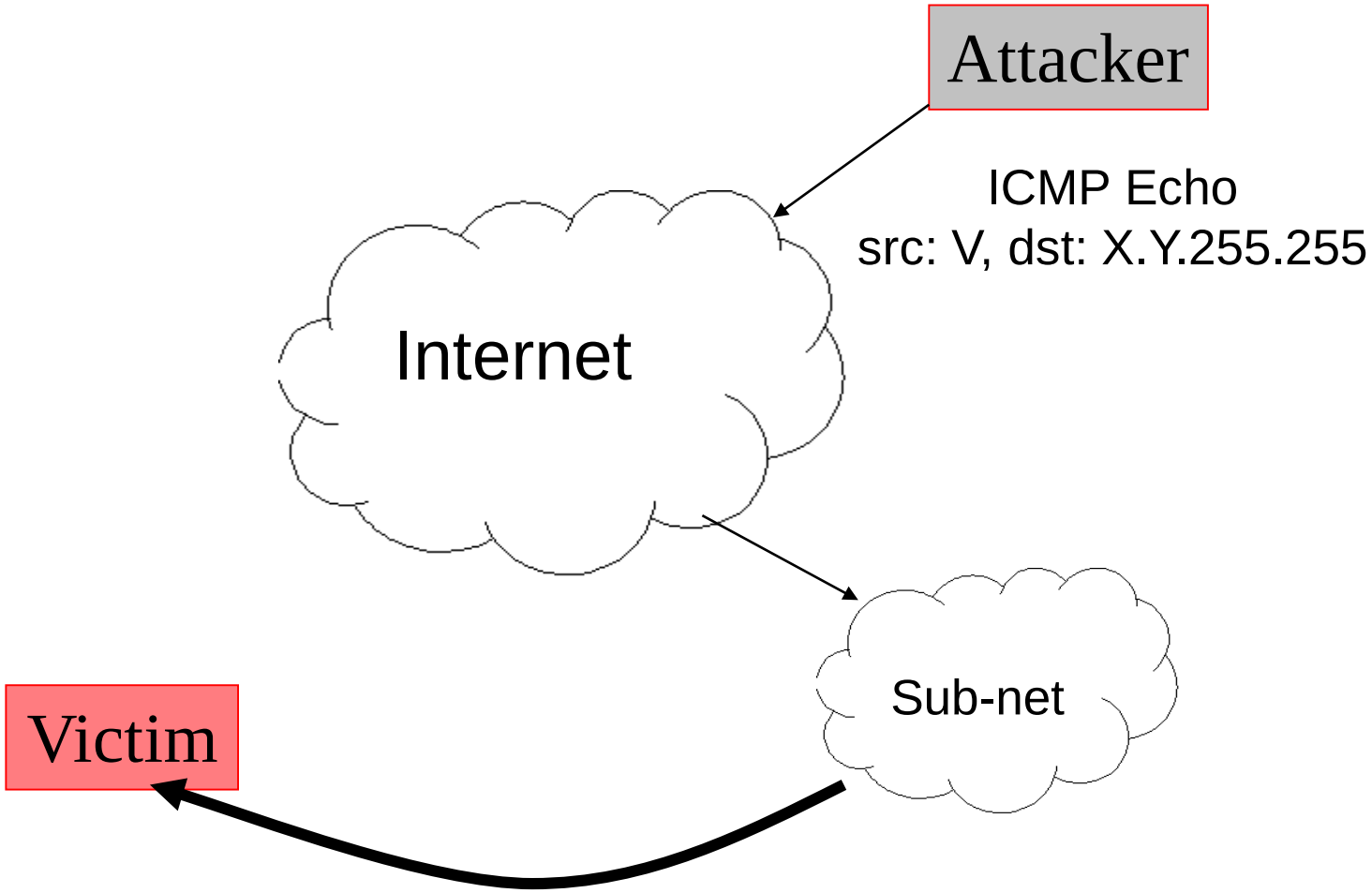
UDP Flooding

- Flood the victim with large UDP packets.
- UDP traffic does not react to the traffic flow control, and therefore difficult to recognize attacks based on the sending rate.
- Will crowd out TCP connections

ICMP Flooding

- Flood the victim with ICMP (Internet Control Message Protocol) packets.
- ICMP can be directed to an individual machine or broadcast to an entire network.
- Smurf attack is a type of ICMP flooding, where attackers use ICMP echo request directed to IP subnet-broadcast addresses
  - Smurf attacks are not DDoS attacks
    - Restricted to a single subnet
    - Easily filtered

Smurf


Attacker
ICMP Echo
src: V, dst: X.Y.255.255
Internet
Sub-net
Victim
ICMP Reply, src: X.Y.*.*, dst: V

DNS Request Attacks

- Attack sends DNS recursive queries with spoofed IP address.
- More destructive because this attack triggers a reflected packet (DNS replies) of a much larger packet size (bandwidth amplification).
- Difficult to recognize the attack and to stop it without affecting normal services.
- Can be managed with dynamic firewalls

Conclusion

- DDoS attacks
  - What they are
  - How they are carried out
  - SYN cookies
  - Classifications of DDoS attacks