General Categories of Security Attacks

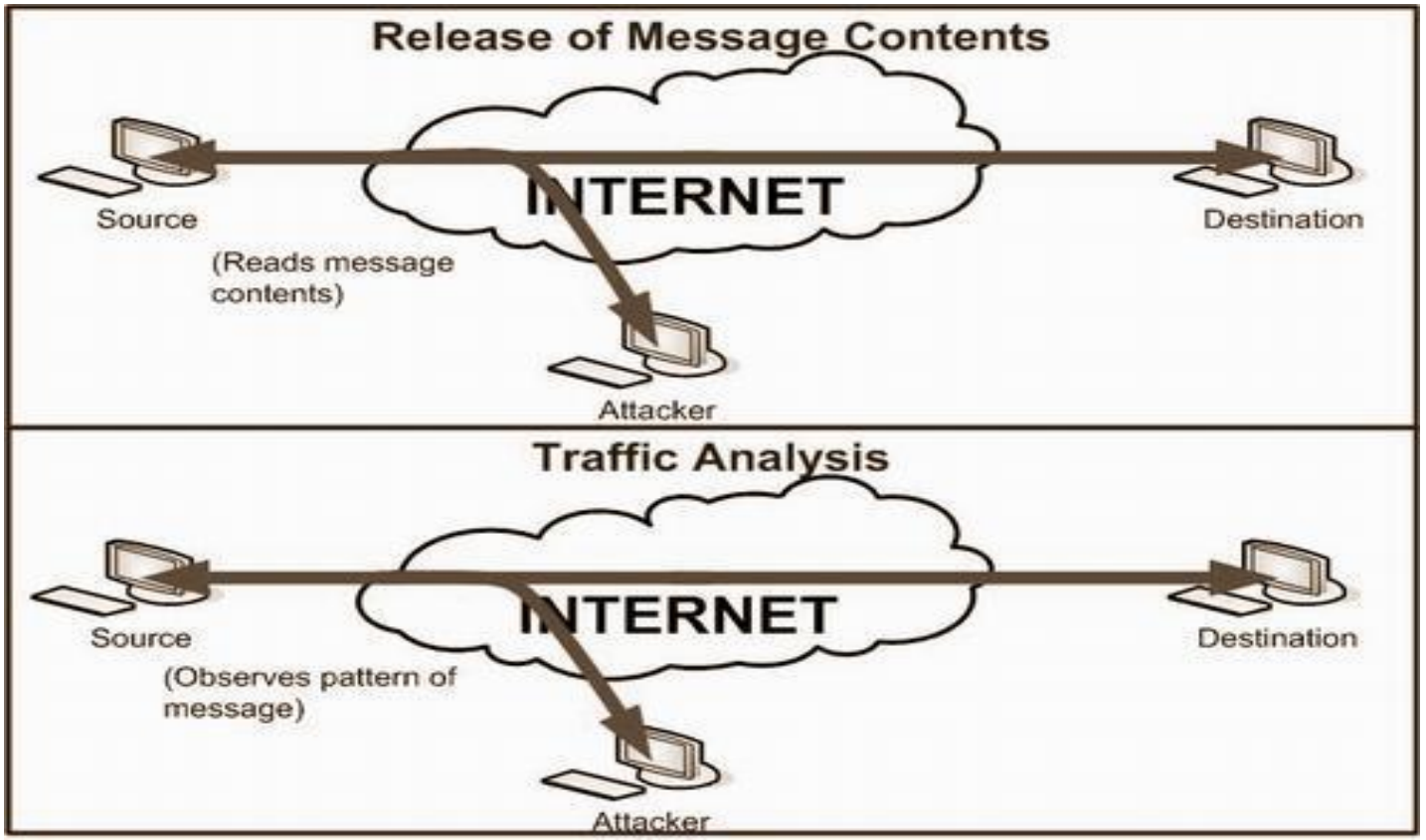
Secure system

- A system which is providing the services required by the user accurately and preventing the illegal use of system resources is called a secure system.
- Any action that compromises the security is called a security attack.

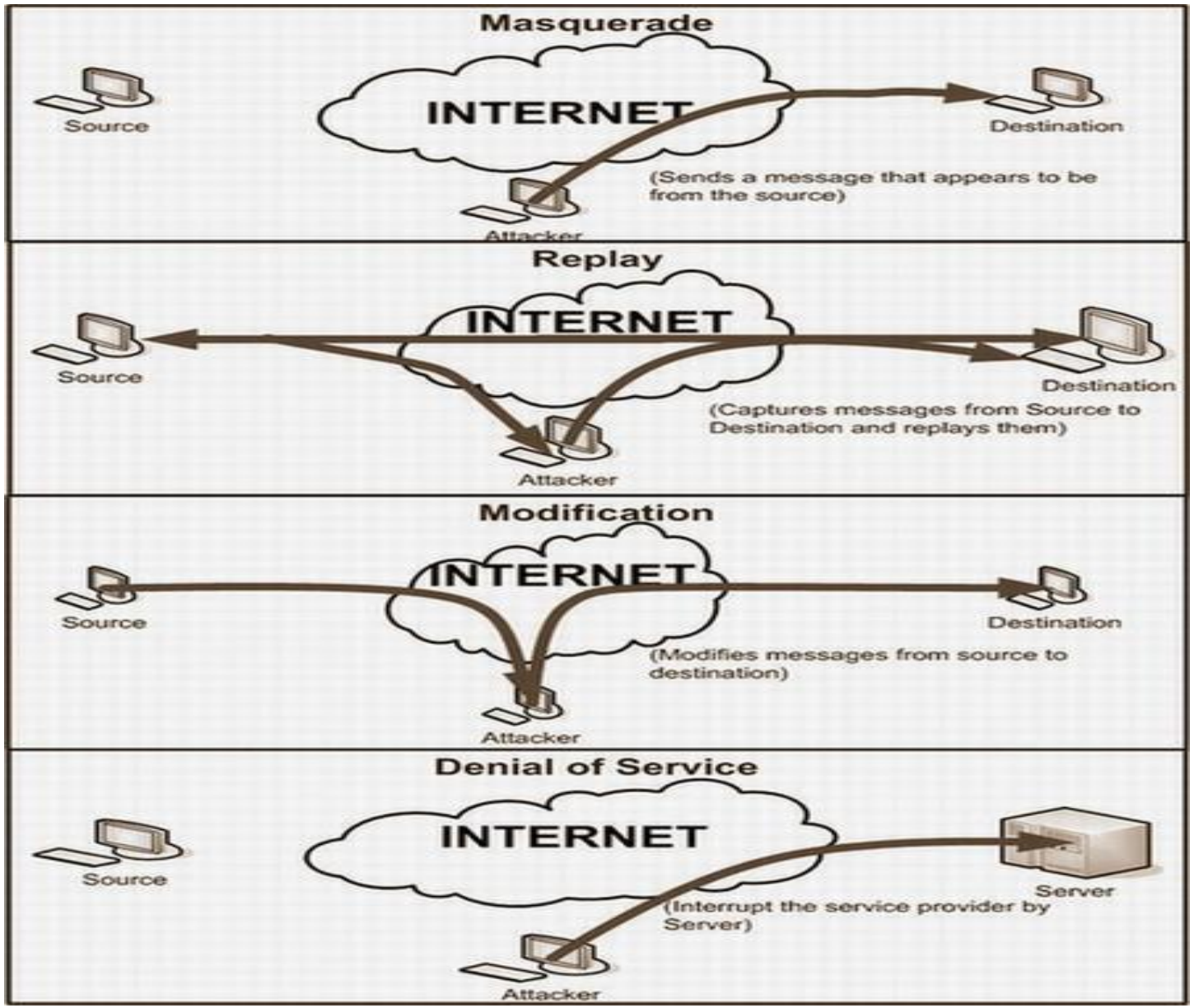
- Attacks can be categorized into following basic categories:
  - Interruption (attack on availability)
  - Interception(attack on confidentiality)
  - Modification (attack on integrity)
  - Fabrication (attack on authenticity)

- We can further classify security attacks as *passive attacks* and *active attacks*.
- Passive attacks are only involved in monitoring of the information(interception). The goal of this attack is to obtain transmitted information.

- Two types of passive attacks are
  - r*elease of message content*
  - *traffic analysis*


Release of Message Contents
INTERNET
Source
Destination
(Reads message contents)
Attacker
Traffic Analysis
INTERNET
Source
Destination
(Observes pattern of message)
Attacker

- Active attacks are involved in modification of data (interception, modification, fabrication) or creation of false data.
- These attacks are further subdivided into four categories:
  - *Masquerade*
  - *Replay*
  - *modification of data*
  - *denial of service*


Masquerade
INTERNET
Source
Destination
(Sends a message that appears to be from the source)
Attacker
Replay
INTERNET
Source
Destination
(Captures messages from Source to Destination and replays them)
Attacker
Modification
INTERNET
Source
Destination
(Modifies messages from source to destination)
Attacker
Denial of Service
INTERNET
Source
Server
(Interrupt the service provider by Server)
Attacker

Reconnaissance Attacks

- Gathering information against a targeted host or network is called reconnaissance attack.
- Attackers analyze the target host and try to discover the details:
  - alive IP addresses
  - open ports of the network
  - failure of operating system
  - types of services and protocols running

- Some basic reconnaissance attacks are:
  - Packet Sniffers
  - Port scan and ping sweep
  - Internet information queries

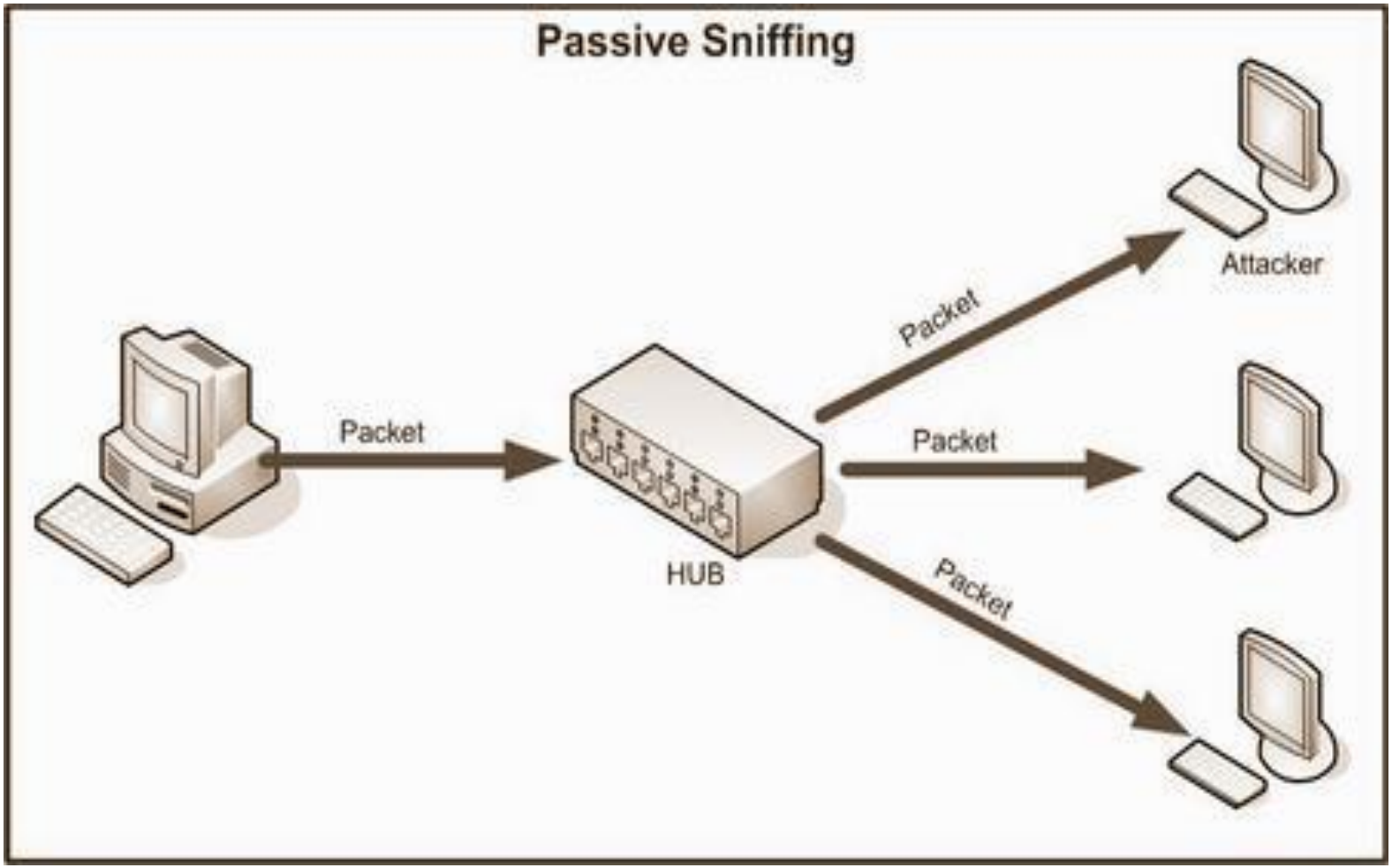
Packet Sniffers

- Packet sniffer is a tool or device that can be used for capturing the packet at data link layer.
- Can be used both by the hacker for eavesdropping and by the administrators for network monitoring and troubleshooting
- *Tcpdump, windump, wireshark* are examples of different sniffing tools.

- Sniffing can be of two types depending on the network.
  - Passive Sniffing
  - Active Sniffing

Passive Sniffing

- Passive sniffing is used in hubbed networks.
- hard to detect because it generates no traffic on network.
- To avoid passive sniffing most of the networks nowadays are using switches instead of hubs.


Passive Sniffing
Attacker
Packet
Packet
Packet
Packet
HUB

Active Sniffing

- Active sniffing is performed on switched network
- Switch worked as a central entity, rather then broadcasting
- Switches worked on the basis of MAC addresses.

- They maintain an address resolution protocol (ARP) table in a special type of memory called Content Addressable Memory (CAM).
- ARP table has all the information that which IP address is mapped to which MAC address.

- Two major attacks are possible:
  - MAC Flooding
  - ARP poisoning

MAC Flooding

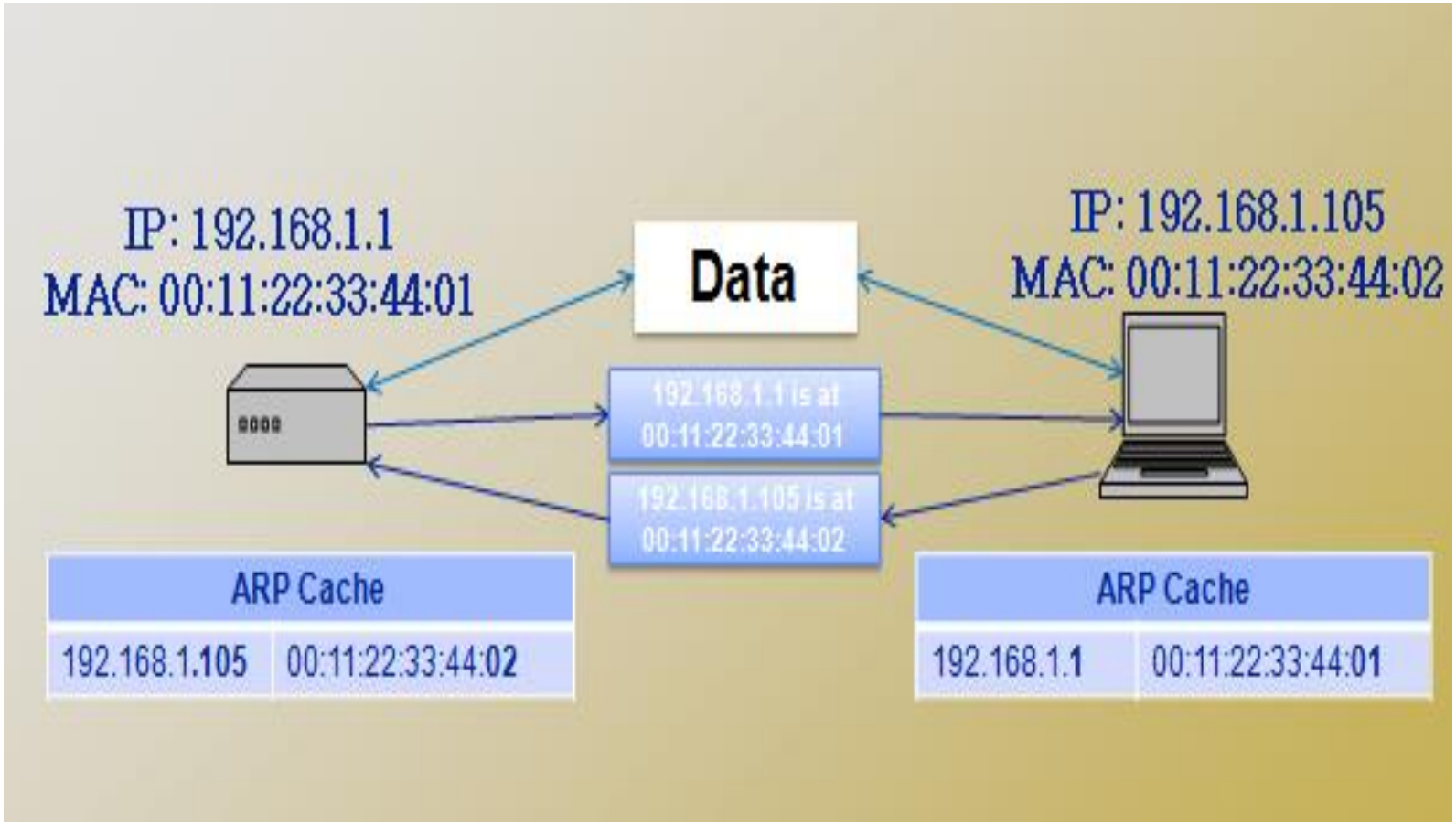
- The switch can intelligently route packets from one host to another.
- The switch has limited memory
- The act of overloading the CAM is known as MAC flooding.
- MAC flooding bombard the switch with fake MAC addresses, so that it became saturated

- The switch goes to a *failopen* mode and cannot perform IP to MAC mappings
- It starts behaving like a hub and starts transmitting the data to all machines.

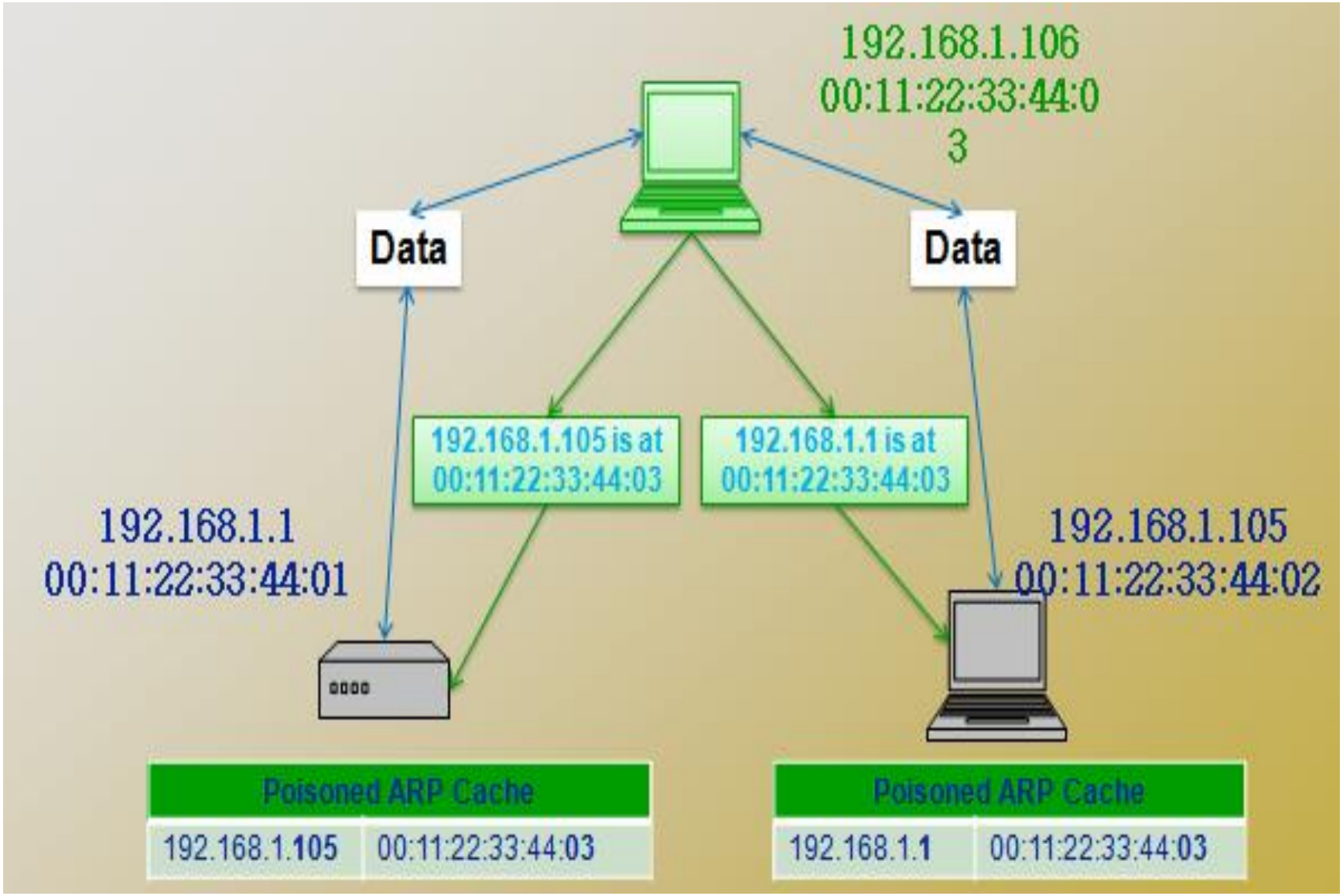
ARP poisoning

- ARP resolves IP addresses to MAC addresses.
- ARP works by broadcasting requests and caching responses for future use
- The ARP table is updated whenever an ARP response is received
- Requests are not tracked
- ARP announcements are not authenticated

- Machines trust each other, a rogue machine can spoof other machines
- An ARP cache updates every time that it receives an ARP reply, even if it did not send any ARP request
- It is possible to poison an ARP cache by sending fake ARP replies


IP: 192.168.1.1
MAC: 00:11:22:33:44:01
Data
IP: 192.168.1.105
MAC: 00:11:22:33:44:02
192.168.1.1 is at 00:11:22:33:44:01
192.168.1.105 is at 00:11:22:33:44:02
ARP Cache
192.168.1.105
00:11:22:33:44:02
ARP Cache
192.168.1.1
00:11:22:33:44:01

Poisoned ARP Caches



Port Scan and Ping Sweep

- These are two common network probes typically used to run various test against a host or device to find vulnerable services.
- They are helpful to examine the IP address and the services running on a device or host.

- The most popular probing tool is Nmap (Network Mapper)
- Different types of Nmap scans are
  - ***TCP Connect Scan***
  - ***TCP SYN Scan***
  - ***FIN Scan***
  - ***ACK Scan***

- The method of finding that which IP addresses are alive is called ping sweep.
- Attacker sends an ICMP packet to each machine (with in a range) to a targeted network.
- ICMP replies from different machines are logged into a file for future reference

Internet Information Queries

- Consists of:
  - DNS queries
  - IP queries
  - Ping sweep
- After these queries, port scan is started by the hacker
  - to find out which ports are open and which services are running on these ports.

Access Attack

- Access attacks occur when a malicious hacker exploit vulnerabilities and succeed to access the confidential information of any organization.
- Different types of attacks are:
  - Password Attacks
  - Trust Exploitation
  - Port Redirection
  - Man-in-the-middle attack

Password Attack

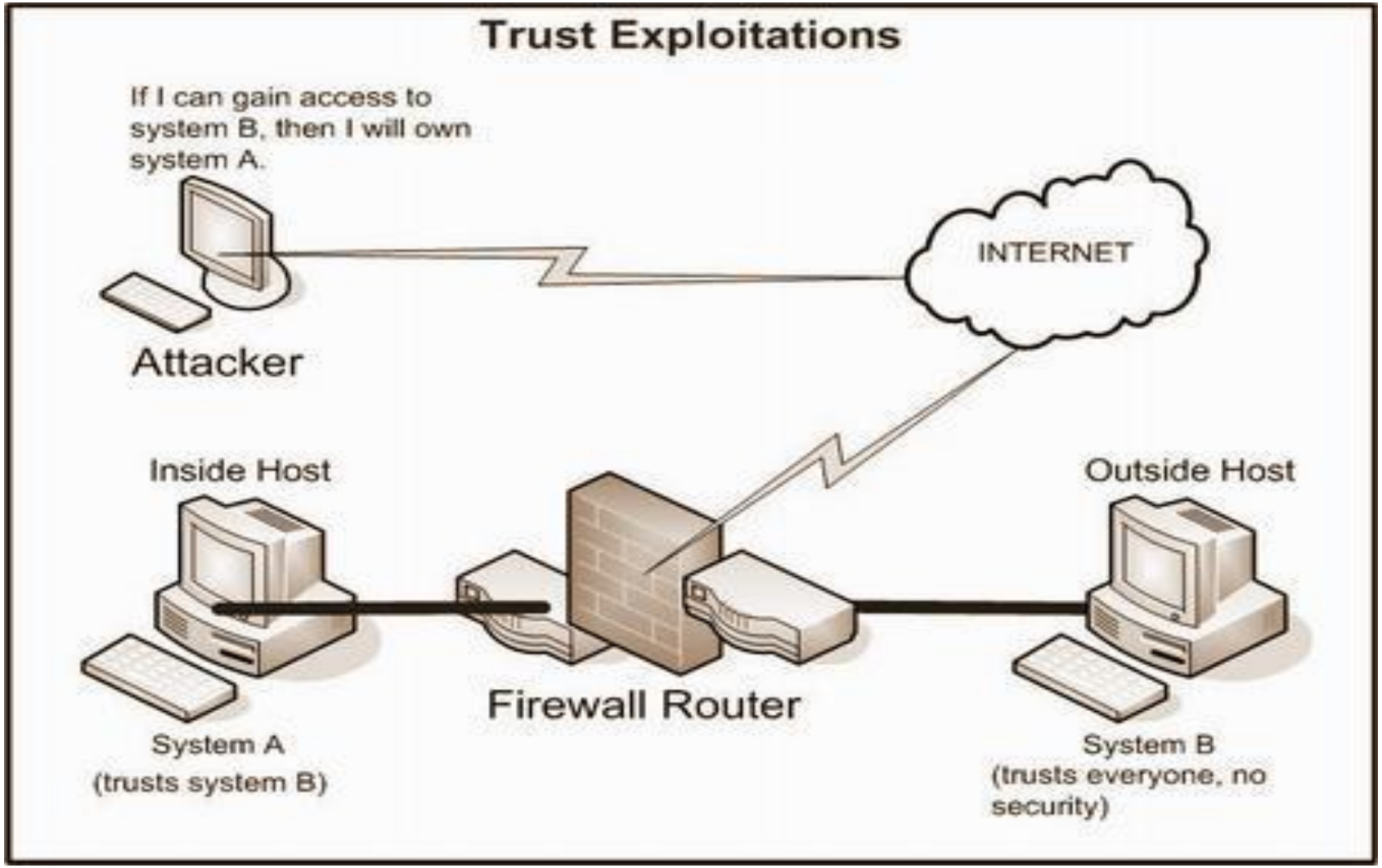
- Repeated attempts to find the user information (user name or password)
- Types of Password Attack are:
  - Dictionary Attack
  - Brute force attack
  - Hybrid Attack

Types of password Attacks

	Dictionary Attack	Brute force Attack	Hybrid Attack
Speed of the Attack	Fast	Slow	Medium
Passwords Cracked	Finds only words	Finds every password(A-Z, 0-9, special characters)	Finds only the password that have a dictionary word as the base

Trust Exploitation

- *Scenario:*
  - When a hacker attacks on a computer which is outside a firewall and that computer has a trust relationship with another computer which is inside the firewall, the hacker can exploit this trust relationship.


Trust Exploitations
If I can gain access to system B, then I will own system A.
INTERNET
Attacker
Inside Host
Outside Host
Firewall Router
System A
(trusts system B)
System B
(trusts everyone, no security)

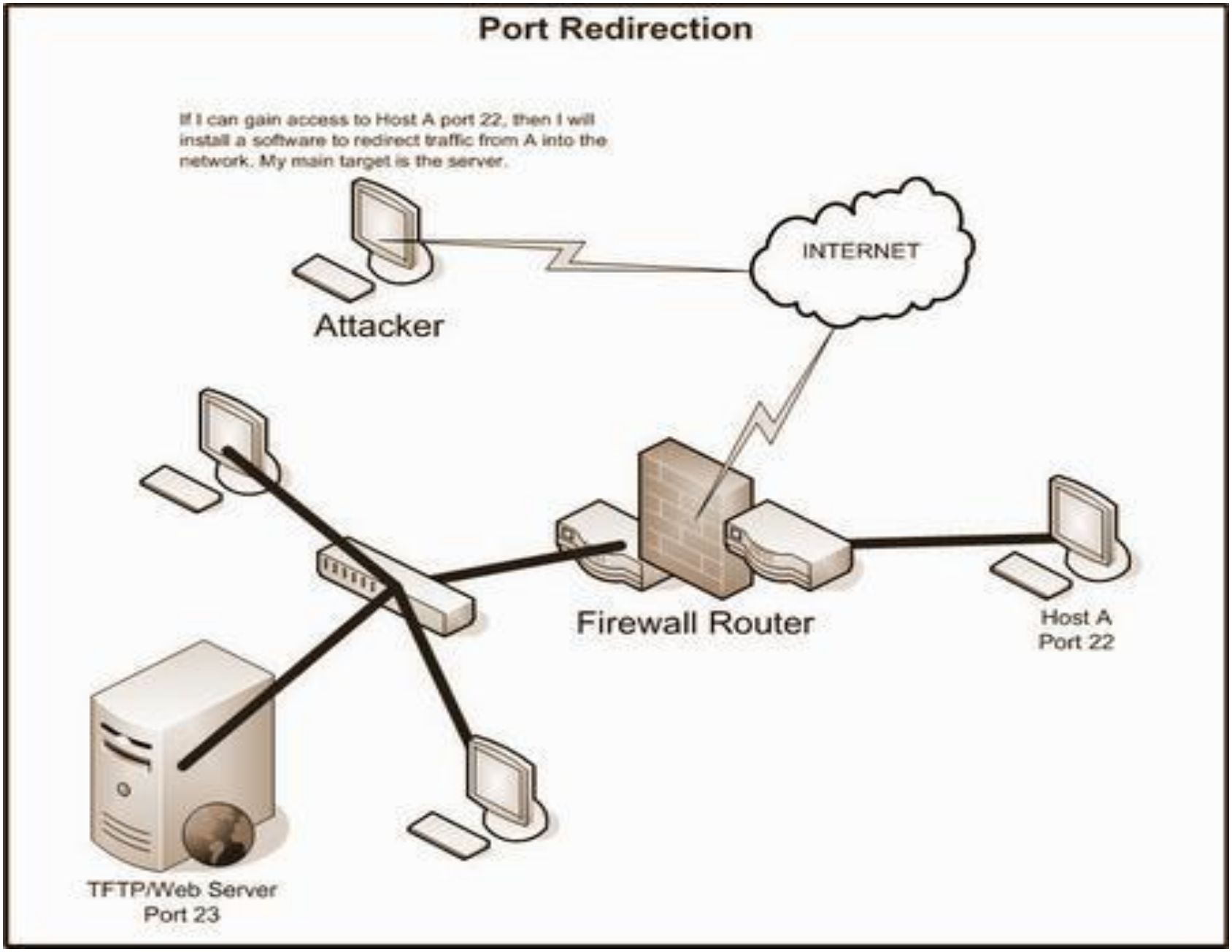
Trust Exploitation

- *Mitigated by:*
  - using private VLANs between switches
  - limiting the trust relationship between systems
  - eliminating useless trust relations between different servers

Port Redirection

- Similar to trust exploitation attack
- The attacker bypasses the security mechanism.
- The attacker installs a software that can redirect the traffic towards the attacker.

Port Redirection



Man-in-the-Middle Attack

- The attacker succeed to intrude himself between two communication parties.
- The attacker can
  - intercept data between source and destination host
  - modify data and retransmit it to the destination host
  - inject any type of false data
- MIM attack can affect on availability, confidentiality, integrity and authenticity of data.

Denial of Service (DoS) Attack

DOS Attack

- The recourses are not available even for authenticated users
- The attacker saturated the target machine with useless traffic so that it cannot respond or too slow to respond and some times unavailable.

- Denial-of service attacks can essentially disable the computer or the network. Depending on the nature of the enterprise, this can disable entire organization.
- Some denial-of-service attacks can be executed with limited resources against a large, sophisticated site. This type of attack is sometimes called an asymmetric attack.
- For example, an attacker with an old PC and a slow modem may be able to disable much faster and more sophisticated machines or network.

Classification of DOS Attacks

Attack	Affected Area	Example	Description
Network Level Device	Routers, IP Switches, Firewalls	Ascend Kill II, "Christmas Tree Packets"	Attack attempts to exhaust hardware resources using multiple duplicate packets or a software bug.
OS Level	Equipment Vendor OS, End-User Equipment.	Ping of Death, ICMP Echo Attacks, Teardrop	Attack takes advantage of the way operating systems implement protocols.
Application Level Attacks	Finger Bomb	Finger Bomb, Windows NT RealServer G2 6.0	Attack a service or machine by using an application attack to exhaust resources.
Data Flood (Amplification, Oscillation, Simple Flooding)	Host computer or network	Smurf Attack (amplifier attack) UDP Echo (oscillation attack)	Attack in which massive quantities of data are sent to a target with the intention of using up bandwidth/processing resources.
Protocol Feature Attacks	Servers, Client PC, DNS Servers	SYN (connection depletion)	Attack in which "bugs" in protocol are utilized to take down network resources. Methods of attack include: IP address spoofing, and corrupting DNS server cache.

Flooding attacks

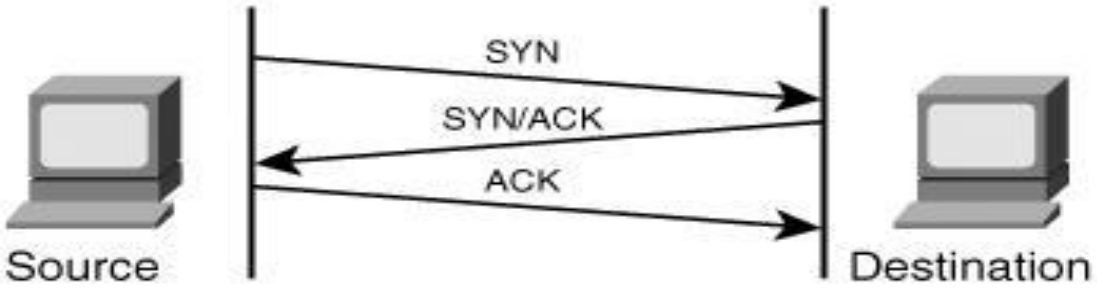
- Goal : **Bombarding large number** of malicious packets at the victim, such that processing of these packets consumes resources
- **Any type of network packet** can be used
  - Attack traffic made similar to legitimate traffic
- Valid traffic **has a low probability of surviving the discard** caused by flood and hence accessing the server
- Some ways of flooding :
  - To overload network capacity on some link to a server
  - To overload server's ability to handle and respond to this traffic
- The larger the packet, the more effective the attack

Types of flooding attacks

- Classified based on type of network protocol used to attack
  - **TCP SYN flood attack**
  - **UDP flood attack**
  - **ICMP flood attack**

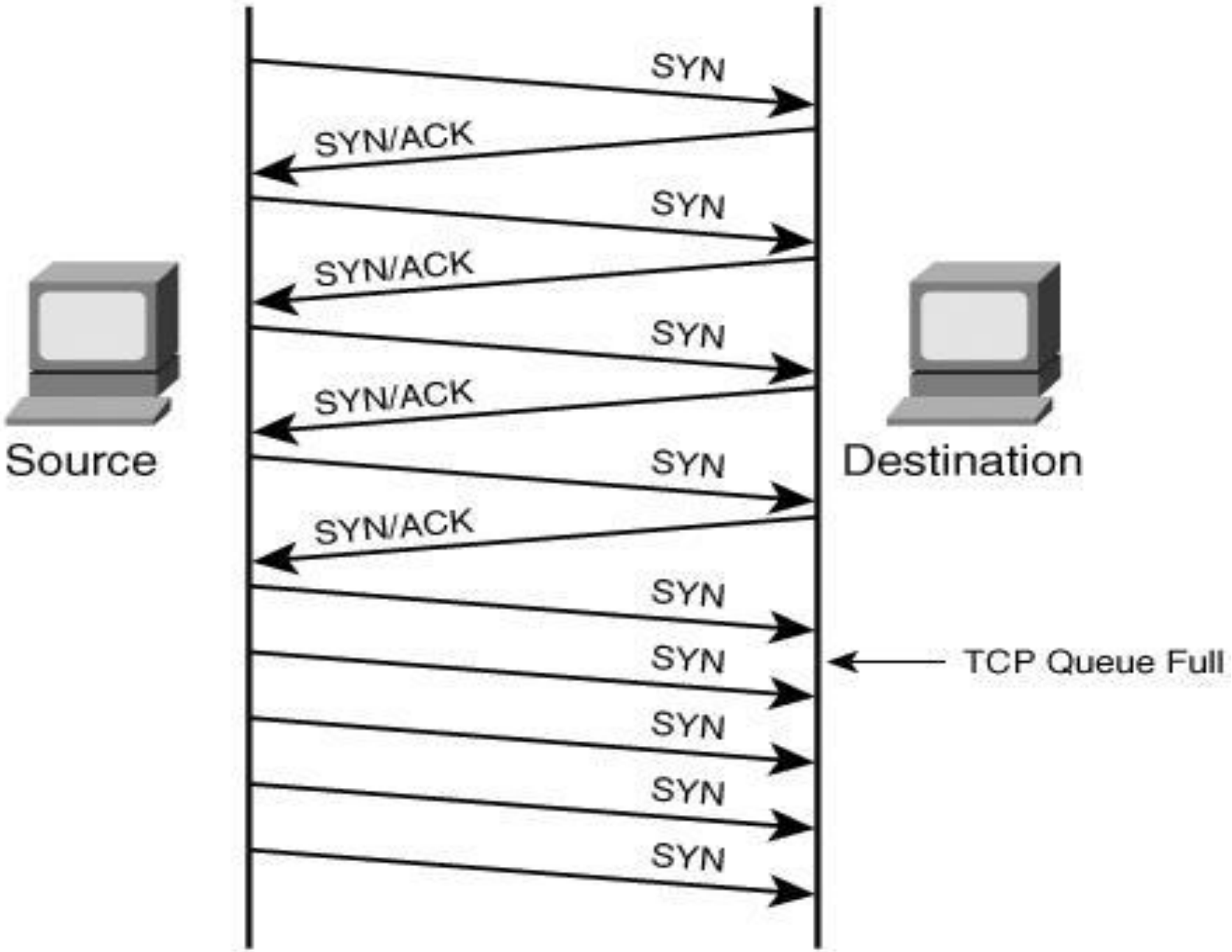
SYN flood attack

- A SYN flood is one of the oldest and yet still most effective DoS attacks.
- TCP communication begins with a SYN, a SYN-ACK response, and then an ACK response.



SYN flood attack

- An attacker sends a large number of SYN requests to a target's system
  - Target uses too much memory and CPU resources to process these fake connection requests
  - Target’s bandwidth is overwhelmed
- Usually SYN flood packets use spoofed source IPs
- Make the target very hard to decide which TCP SYN is attack and which TCP SYN is from legitimate users


SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN/ACK
SYN
SYN
SYN
SYN
SYN
TCP Queue Full
Source
Destination

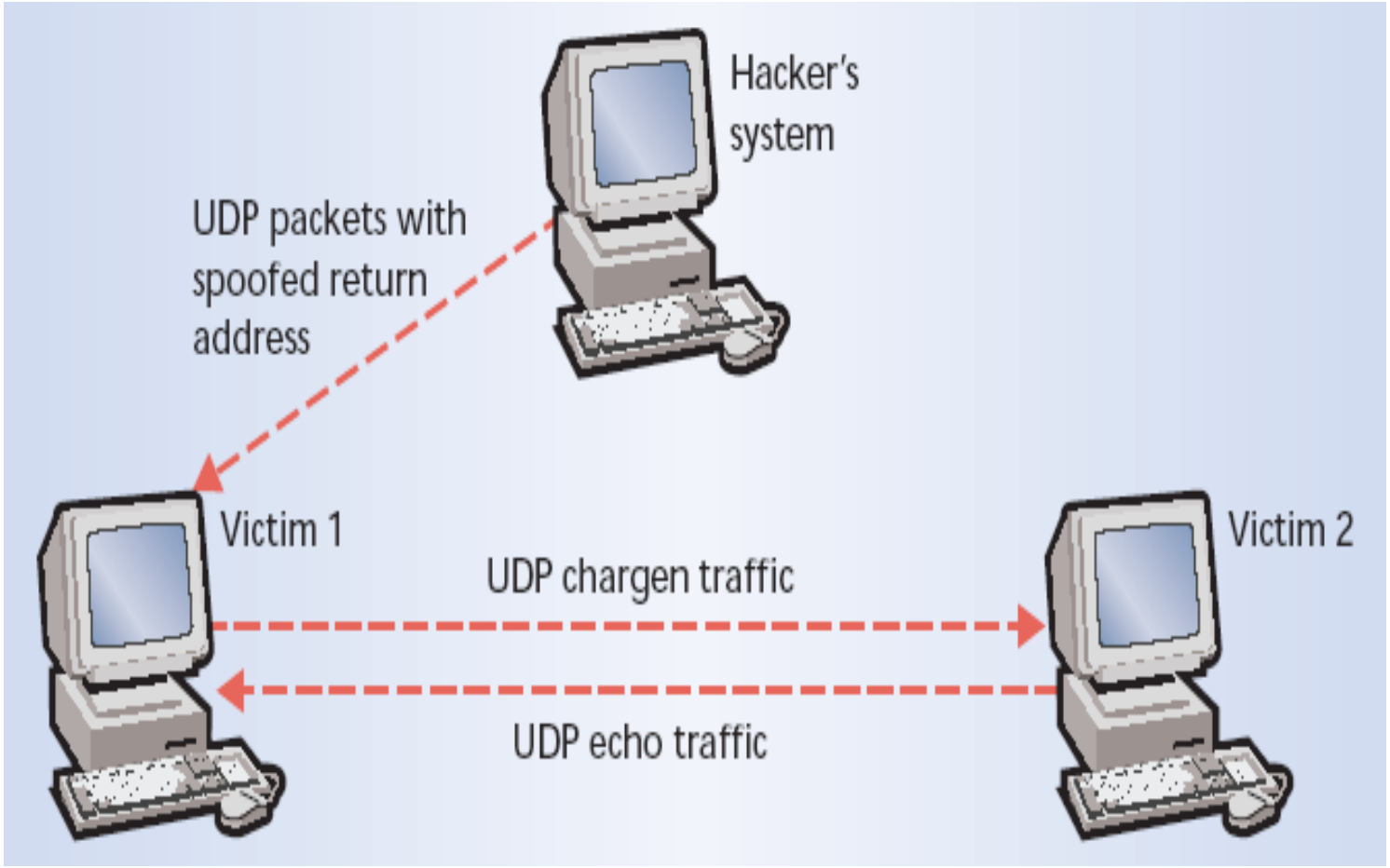
- The attacker host will send a flood of syn packet but will not respond with an ACK packet.
- The TCP/IP stack will wait a certain amount of time before dropping the connection

SYN floods are still successful today for three reasons:

- SYN packets are part of normal, everyday traffic, so it is difficult for devices to filter this type of attack.
- SYN packets do not require a lot of bandwidth to launch an attack because they are relatively small.
- SYN packets can be spoofed because no response needs to be given back to the target. As a result, attacker can choose random IP addresses to launch the attack, making filtering difficult for security administrators.

UDP flood attack

- UDP protocol is a connectionless unreliable protocol which doesn't require session negotiation between client and server application.
- UDP provides easy to use interface for producing large quantity of packets.
- UDP Flood Attacks floods the network with UDP packets destined to a victim's host.


Hacker's system
UDP packets with spoofed return address
Victim 1
Victim 2
UDP chargen traffic
UDP echo traffic

ICMP flood attack

- Also known as Ping Flood Attack
- An attacker sends a huge number of **ICMP *echo request*** packets to victim.
- The victim cannot respond promptly since the volume of request packets is high and have difficulty in processing all requests and responses rapidly.
- The attack will cause the performance degradation or system down.

Other DoS attacks

- Ping of Death Attack
- TearDrop Attack
- Land Attack

Ping of Death Attack

- Ping of Death is an attempt by an attacker to crash, reboot or freeze a system by sending an illegal ICMP packet to the host under attack.
- The TCP/IP specification allows for a maximum packet size of up to 65536 octets.
- In some TCP stack implementation, encountering packets of greater size may cause the victim's host to crash.

- In the attack, the ICMP packet is sent in the form of a fragmented message which, when reassembled is larger than the maximum legal IP packet size.

TearDrop Attacks

- Teardrop attacks target a vulnerability in the way fragmented IP packets are reassembled.
- Fragmentation is necessary when IP Datagrams are larger than the maximum transmission unit (MTU) of a network segment
- An attacker sends two fragments that cannot be reassembled properly by manipulating the offset value of packet and cause reboot or halt of victim system

Land Attacks

- An attacker sends a forged packet with the same source and destination IP address.
- The victim system will be confused and crashed or rebooted.

Countermeasures for DoS Attacks

Attack	Countermeasure Options	Example	Description
Network Level Device	Software patches, packet filtering	Ingress and Egress Filtering	Software upgrades can fix known bugs and packet filtering can prevent attacking traffic from entering a network.
OS Level	SYN Cookies, drop backlog connections, shorten timeout time	SYN Cookies	Shortening the backlog time and dropping backlog connections will free up resources. SYN cookies proactively prevent attacks.
Application Level Attacks	Intrusion Detection System	GuardDog, other vendors.	Software used to detect illicit activity.
Data Flood (Amplification, Oscillation, Simple Flooding)	Replication and Load Balancing	Akami/Digital Island provide content distribution.	Extend the volume of content under attack makes it more complicated and harder for attackers to identify services to attack and accomplish complete attacks.
Protocol Feature Attacks	Extend protocols to support security.	ITEF standard for itrace, DNSSEC	Trace source/destination packets by a means other than the IP address (blocks against IP address spoofing). DNSSEC would provide authorization and authentication on DNS information.

Defenses against DoS attacks

- DoS attacks cannot be prevented entirely
- Three lines of defense against DoS attacks
  - Attack prevention and preemption
  - Attack detection and filtering
  - Attack source traceback and identification

Attack prevention

- Limit ability of systems to send spoofed packets
  - Filtering done as close to source as possible by routers/gateways
  - Reverse-path filtering ensure that the path back to claimed source is same as the current packet's path
    - Ex: On Cisco router "ip verify unicast reverse-path" command

- Rate controls in upstream distribution nets
  - On specific packet types
  - Ex: Some ICMP, some UDP, TCP/SYN
- Use modified TCP connection handling
  - Use SYN-ACK cookies when table full
  - Or selective or random drop when table full

- Block IP broadcasts and suspicious services
- Manage application attacks with puzzles to distinguish legitimate human requests.
- Good general system security practices
- Use mirrored and replicated servers when high performance and reliability required
- Separate Client and Server Addresses.

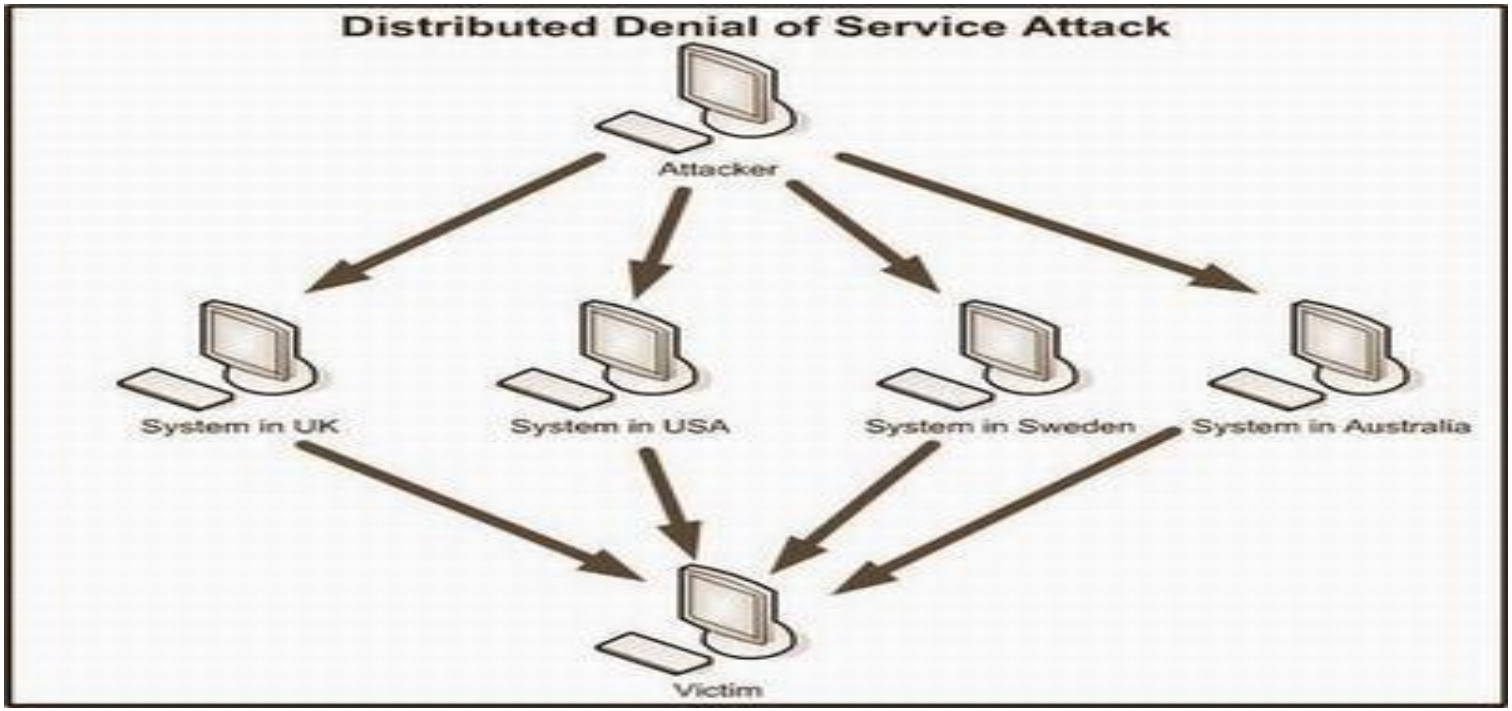
Distributed Denial of Service Attack (DDoS)

Distributed Denial of Service Attacks

- A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets.
- launched indirectly through a large number of compromised computer agents on the internet.

Distributed Denial of Service (DDOS) attack

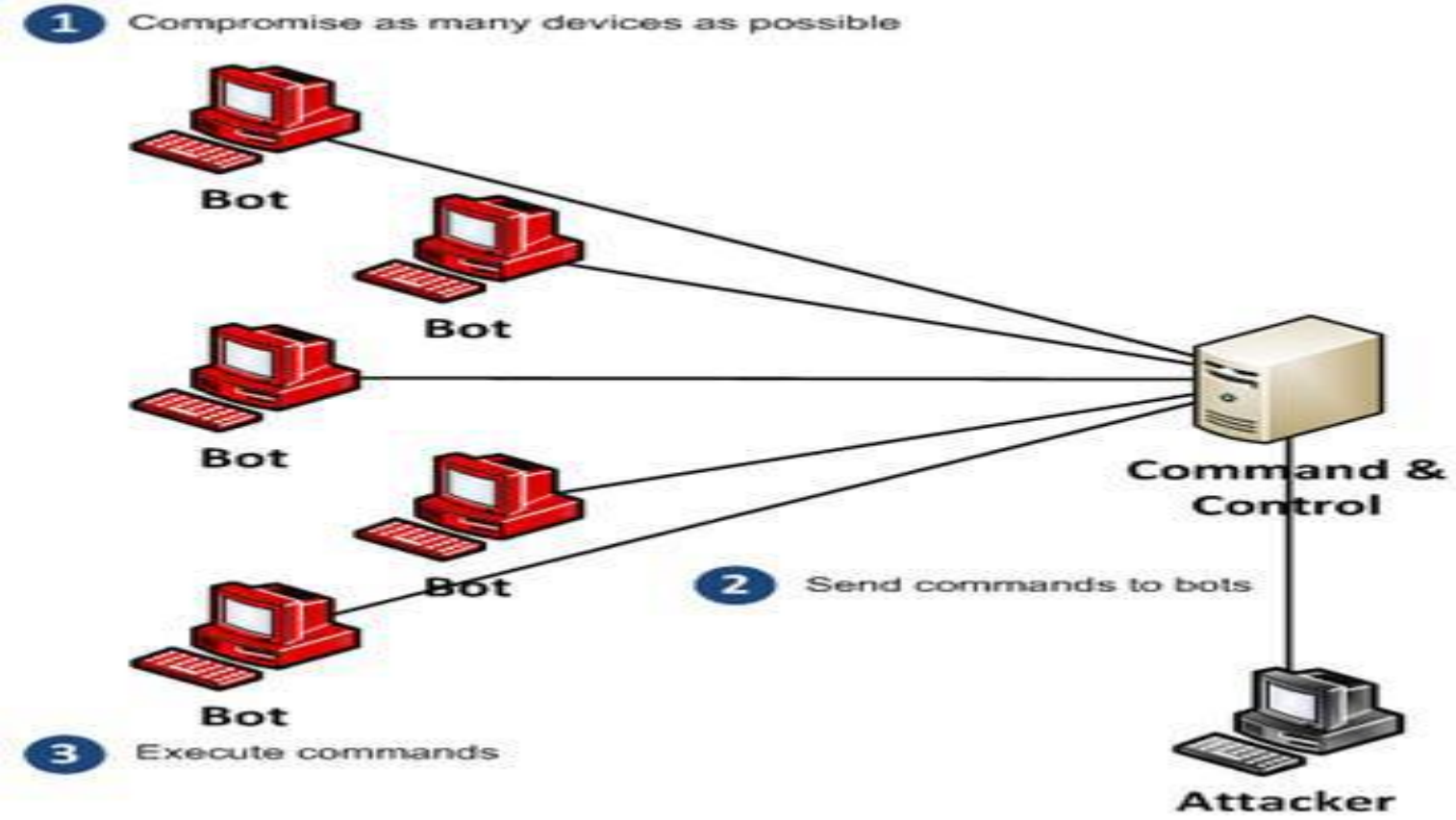
- Several compromised systems are used to launch an attack against a targeted host or network.



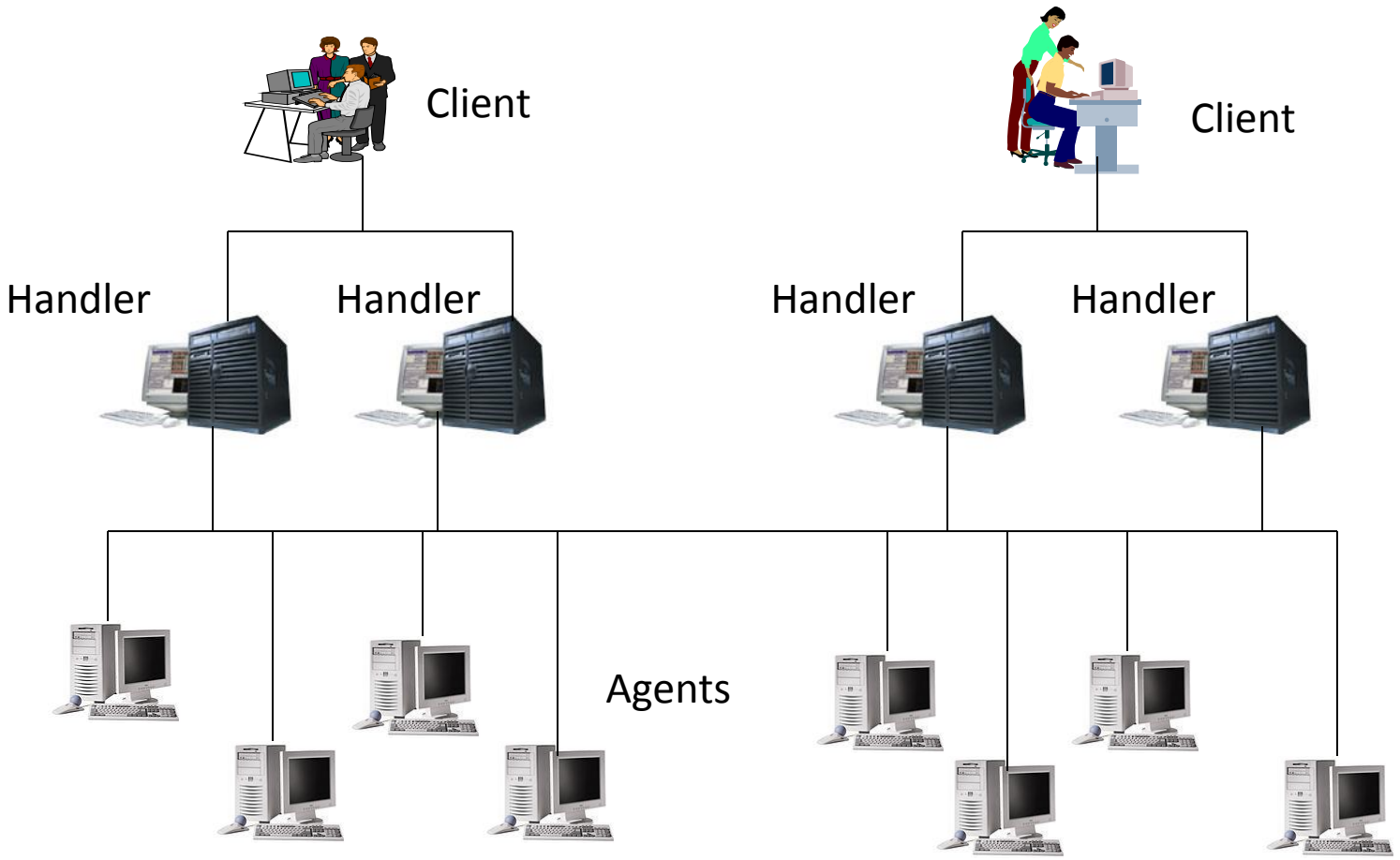
DDoS Architecture

- Basically two types:
  - IRC based architecture
  - Agent-Handler architecture

IRC-based DDoS Architecture



DDoS Architecture(Agent-Handler)



DDoS Architecture(Agent-Handler)

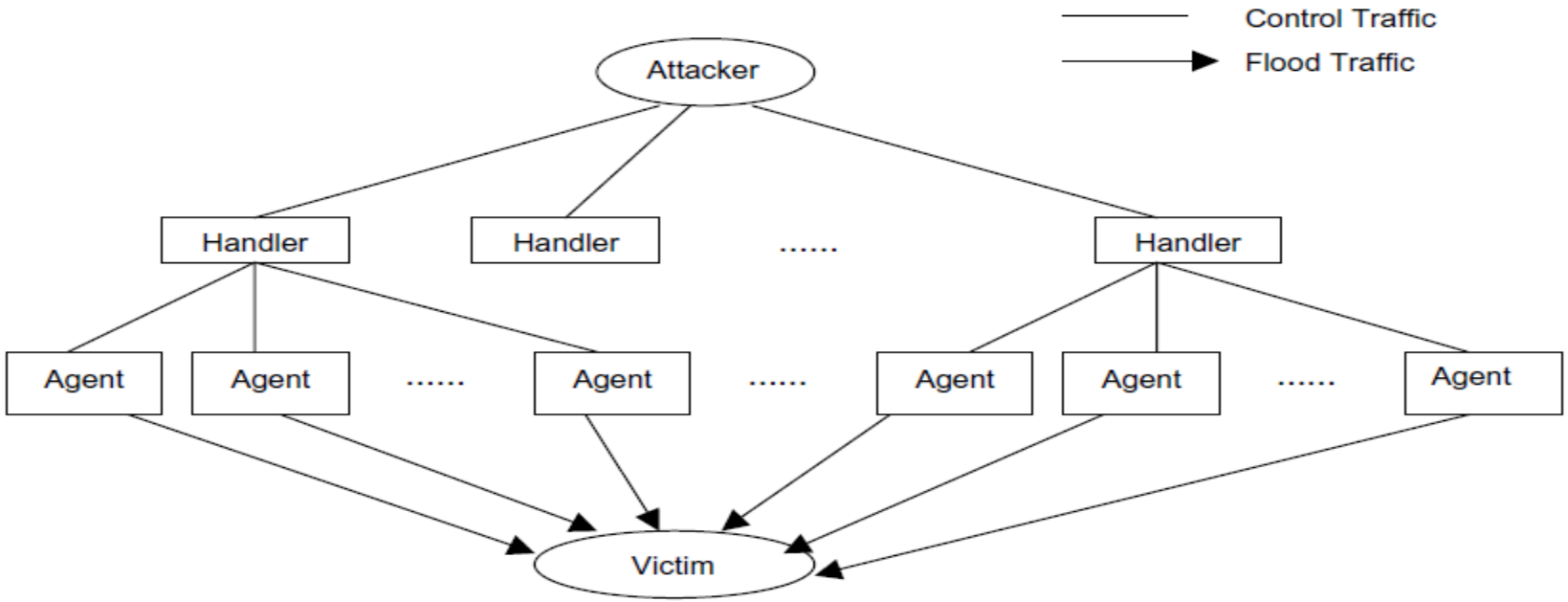
- Attacker uses multiple compromised user work stations/PCs for DoS by:
  - Utilizing vulnerabilities to gain access to these systems
  - Installing malicious backdoor programs , thereby making ***zombies***
  - Creating ***botnets***: large collection of zombies under the control of attacker

DDoS Architecture

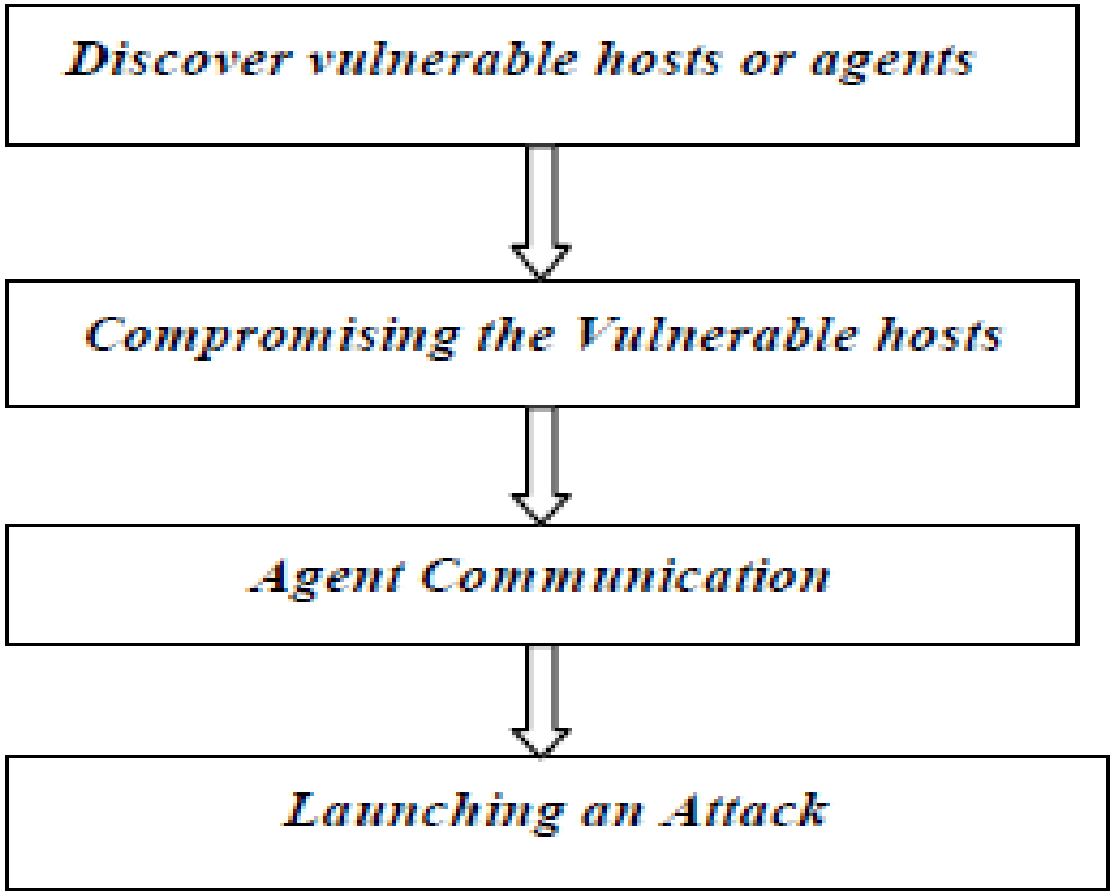
- Generally, a **control hierarchy** is used to create botnets
  - ***Handlers***: The initial layer of zombies that are directly controlled by the attacker
  - ***Agent systems***: Subordinate zombies that are controlled by handlers
- Attacker sends a single command to handler, which then automatically forwards it to all agents under its control

DDoS Architecture(Agent-Handler)

- Consists of four elements:
  - The real attacker
  - The handlers/masters
  - Attack daemon/ agents
  - A victim or target host



Phases of performing DDoS attacks



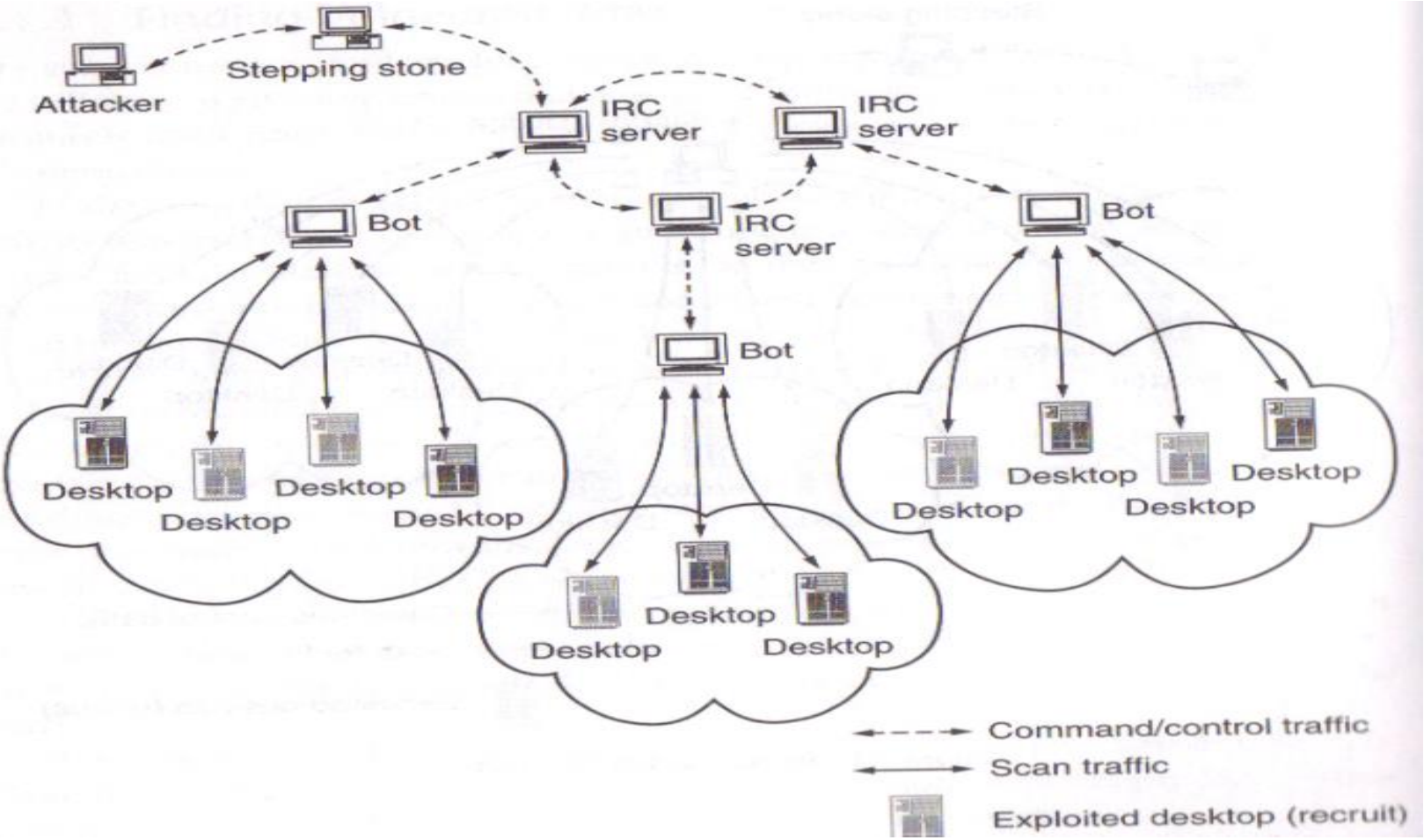
Selection of agents

- Scanning
- Breaking into vulnerable machines
  - Malware propagation

Scanning

- Find sufficiently **large number** of vulnerable machines
  - Manual or semi-automatic or completely automatic process
  - Trinoo: discovery and compromise is manual but only installation is automated
  - Slammer, MyDoom: automated process
- Recruit machines that have sufficiently **good connectivity**
- Netblock scans are initiated sometimes
  - Based on random or explicit rationale
- Examples of scanning tools : IRC bot , worms

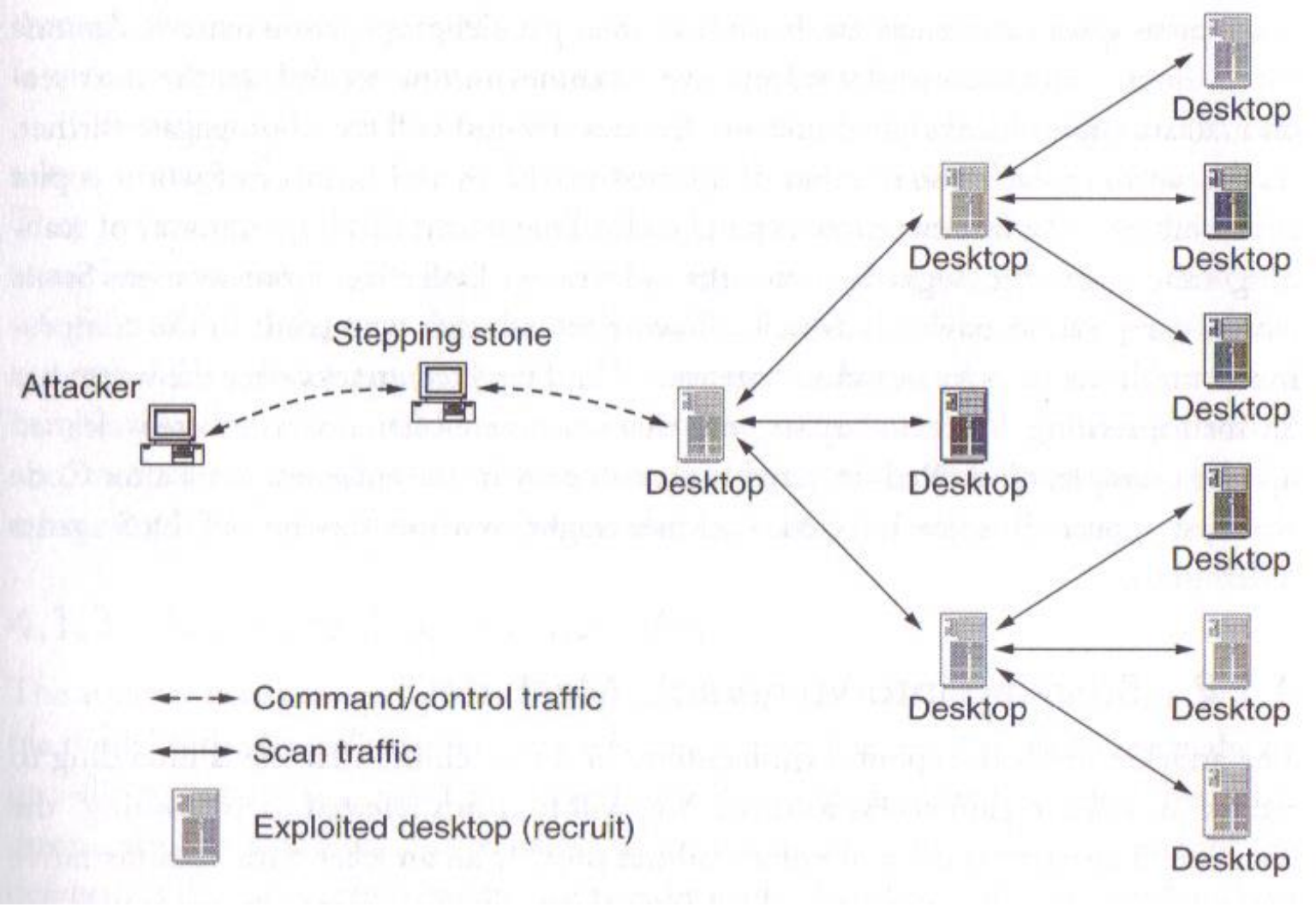
Scanning using IRC bot



Scanning using worms

- Popular method of recruiting DDoS agents
- Scan/infect cycle repeats on both the infected and infecting machines
- Worms spread extremely fast because of their **parallel propagation pattern**
- Worms choice of address for scanning
  - Random
  - Random within a specific range of addresses
  - Using hitlist
  - Using information found on infected machines
- Worms are **often not completely cleaned up**
  - Some infected machines might continue serving as DDoS agents indefinitely

Scanning using worms



Breaking into vulnerable machines

- Most vulnerabilities provide an attacker with administrative access to system
- Attacker updates his DDoS toolkit with new exploits
  - Propagation Vectors

Compromise

- The attacker exploits vulnerabilities and security holes of the agent machines and installs the attack code.

Communication

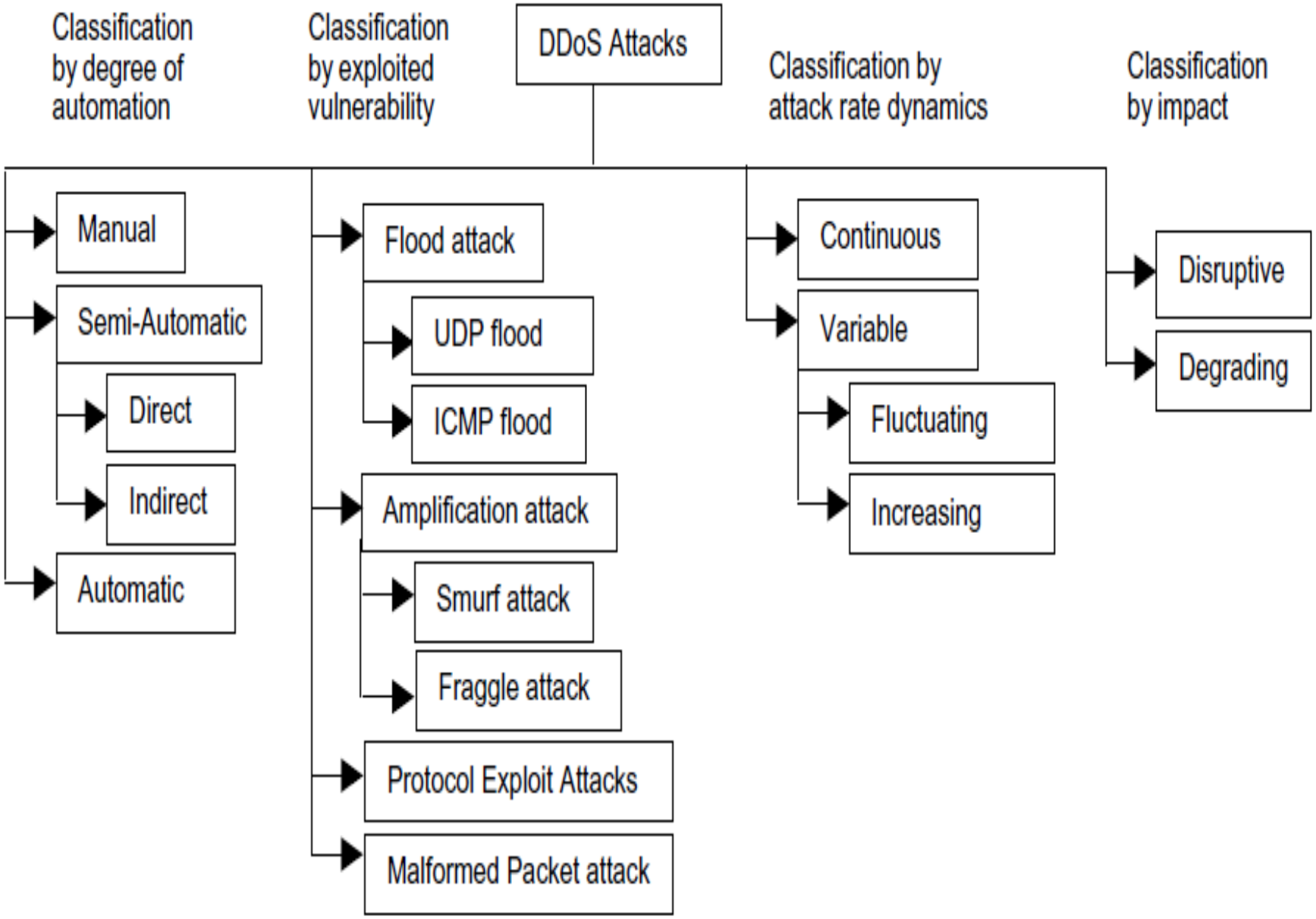
- The attacker communicates with the handlers to identify the active agents, to schedule attacks or to upgrade agents.
- The communication among the attackers and handlers can be done through various protocols such as TCP,UDP or ICMP

Launching an Attack

- The attacker launches an attack by selecting the victim system, attack duration and adjusting the features of the attack such as the type, length, Time to Live(TTL), and port numbers.

DDoS attack taxonomy

- DDoS attacks are classified according to
  - degree of automation
  - exploited vulnerability
  - attack rate dynamics
  - impact


DDoS Attacks
Classification by degree of automation
Classification by exploited vulnerability
Classification by attack rate dynamics
Classification by impact
Manual
Semi-Automatic
Direct
Indirect
Automatic
Flood attack
UDP flood
ICMP flood
Amplification attack
Smurf attack
Fraggle attack
Protocol Exploit Attacks
Malformed Packet attack
Continuous
Variable
Fluctuating
Increasing
Disruptive
Degrading

Classification by degree of automation

- Based on the degree of automation, DDoS attacks can be classified into
  - manual
  - semiautomatic
  - automatic

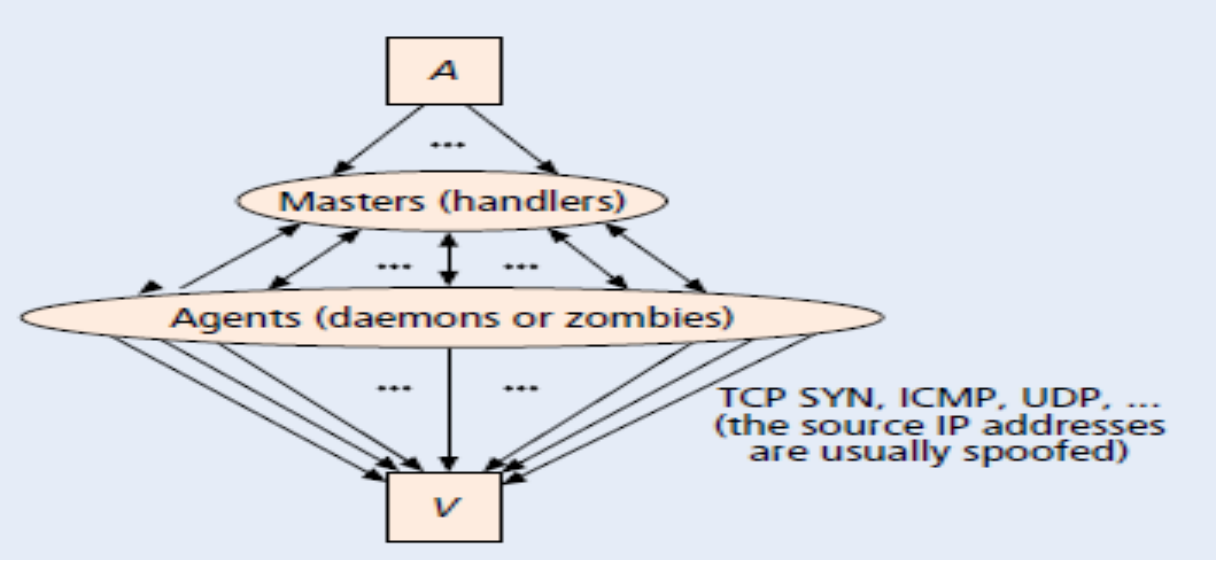
- The early DDoS attacks were manual.
  - scanning of remote machines for vulnerabilities
  - breaking into remote machines
  - installing the attack code.

- In semi-automatic attacks, the DDoS attack belongs in the agent–handler attack model.
  - attacker scans and compromises the handlers and agents by using automated scripts
  - can be divided further to attacks with direct communication and attacks with indirect communication.

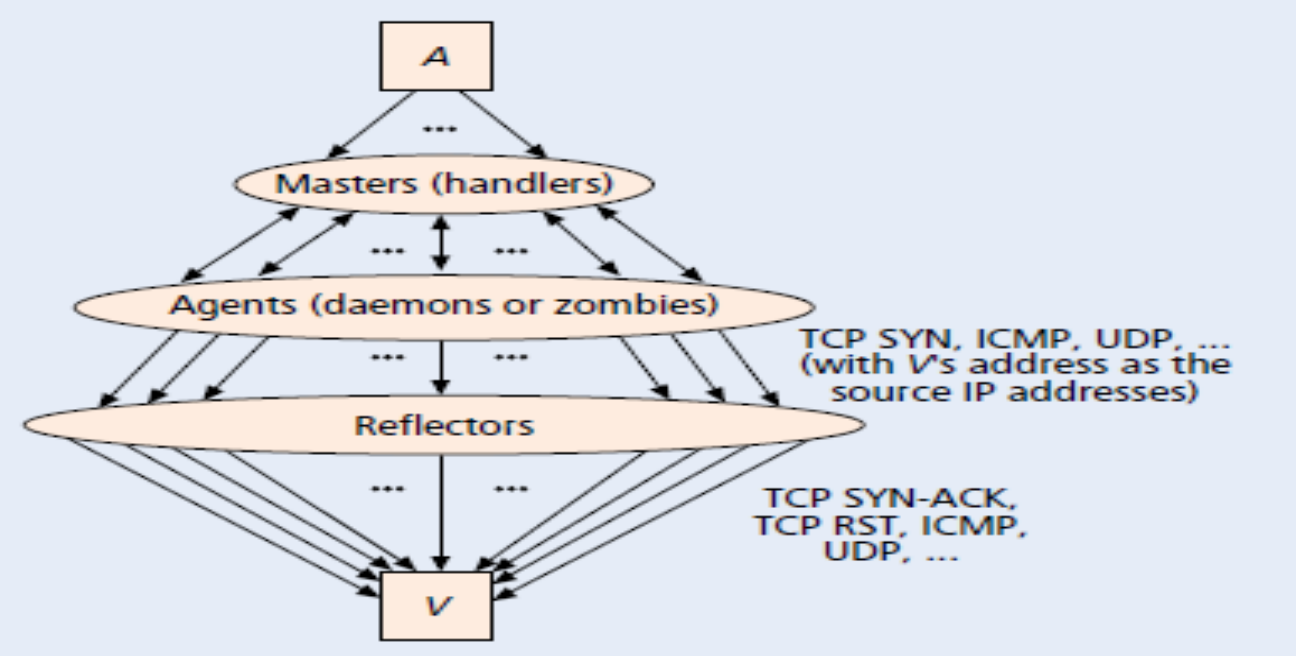
Widely Used DDoS Programs

- Trinoo
- Tribe Flood Network (TFN)
- TFN2K
- Shaft
- Trinity
- Knight

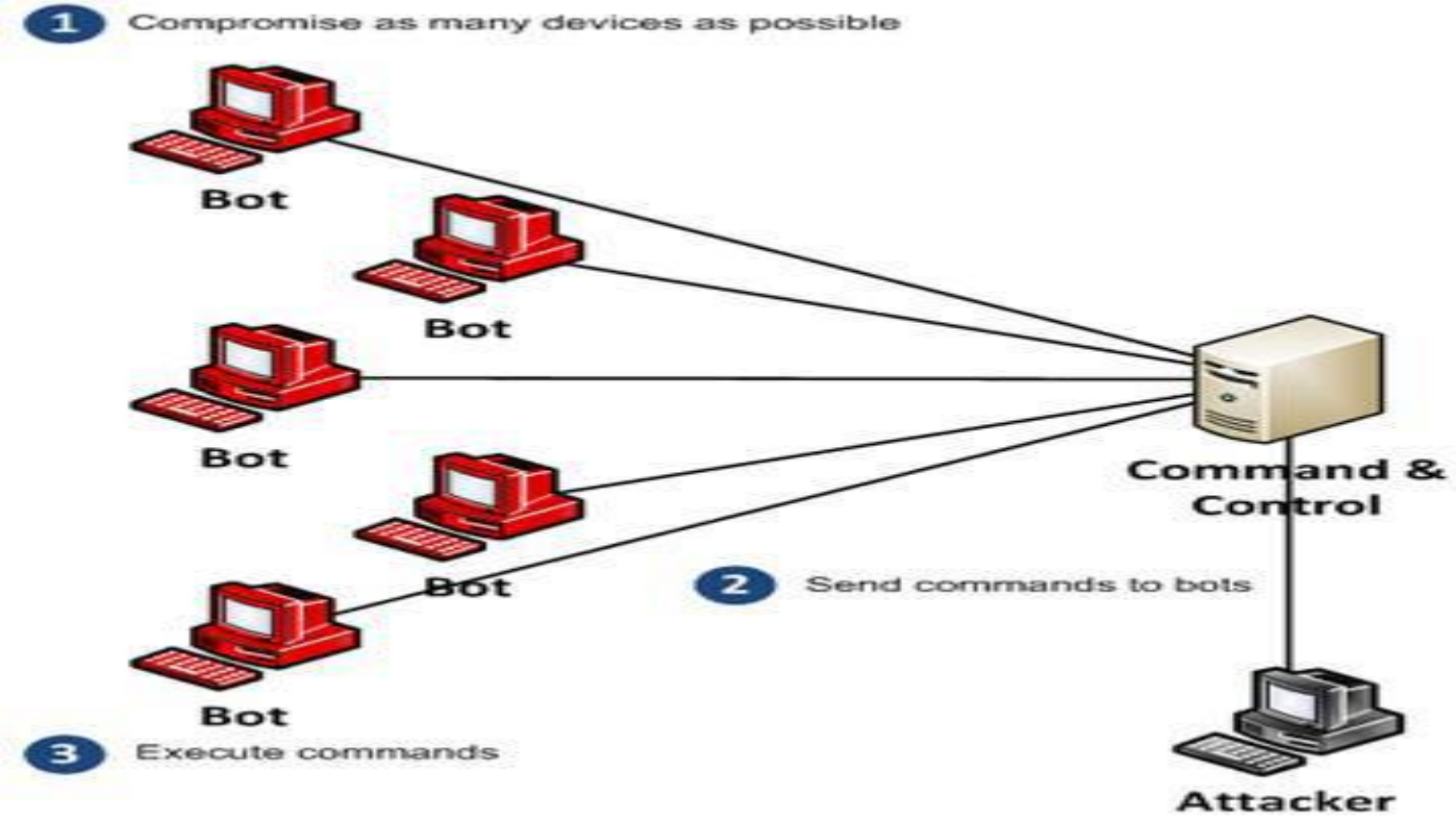
- Direct attack
  - The agent and handler need to know each others identity in order to communicate.
  - main drawback of this approach is that the discovery of one compromised machine can expose the whole DDoS network



- Indirect attack
  - Offers greater survivability of DDoS attacks
  - Example: IRC-based DDoS attacks



IRC-based DDoS attacks



- In automatic DDoS attacks, the communication between attacker and agent machines is completely avoided.
  - All the features of the attack are preprogrammed in the attack code.
  - The possibility of revealing attacker's identity is small.
  - Propagation mechanisms usually leave the backdoor to the compromised machine open, making possible future access and modification of the attack code.

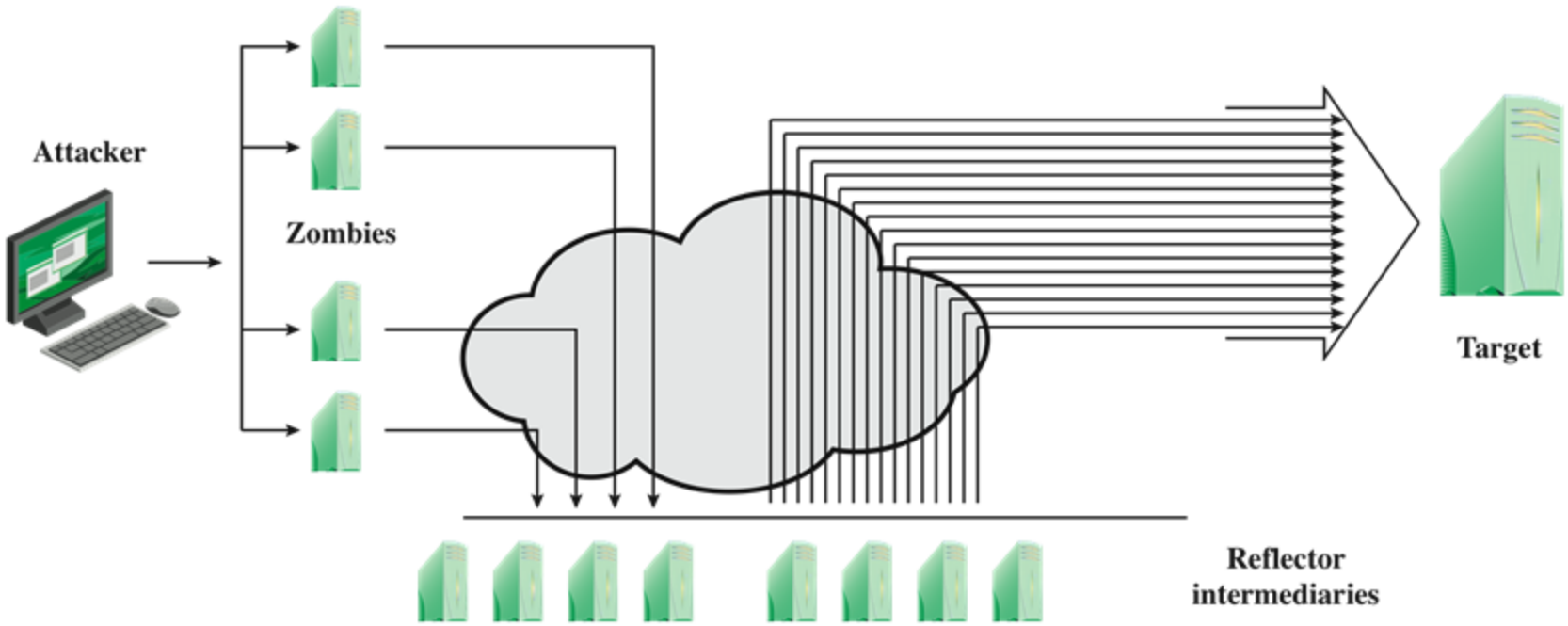
Classification by exploited vulnerability

- DDoS attacks can be divided in to the following categories:
  - flood attacks
  - amplification attacks
  - protocol exploit attacks
  - malformed packet attacks.

- In a flood attack, the compromised machines send large volumes of IP traffic to a victim system in order to congest the victim systems bandwidth.
  - SYN flood
  - ICMP flood
  - UDP flood

- In amplification attacks, the attacker makes a relatively small request, that generates a significantly larger response.
- Attackers spoof IP address of victim as source and send queries to open proxies or resolvers that then send answers to the victim.
- Answers may be amplified if the response is bigger
- Some well known amplification attacks, are Smurf and Fraggle attacks.

- Amplified DDoS attacks aim to generate multiple reflector packets for each original packet set
- Can be achieved by directing original requests to a broadcast address of a large LAN



- Protocol exploit attacks exploit a specific feature or implementation bug of some protocol installed at the victim in order to consume excess amounts of its resources.
- An example of protocol exploit attacks is TCP SYN attack.

- Malformed packet attacks rely on incorrectly formed IP packets that are sent from agents to the victim in order to crash the victim system.
- Can be divided in two types of attacks
  - IP address attack
    - packet contains the same source and destination IP addresses
  - IP packet options attack
    - malformed packet may randomize the optional fields within an IP packet

Classification by attack rate dynamics

- DDoS attacks can be divided in to
  - continuous rate attacks
    - impact of such an attack is very quick
  - Variable rate attacks
    - they avoid detection and immediate response

Classification by impact

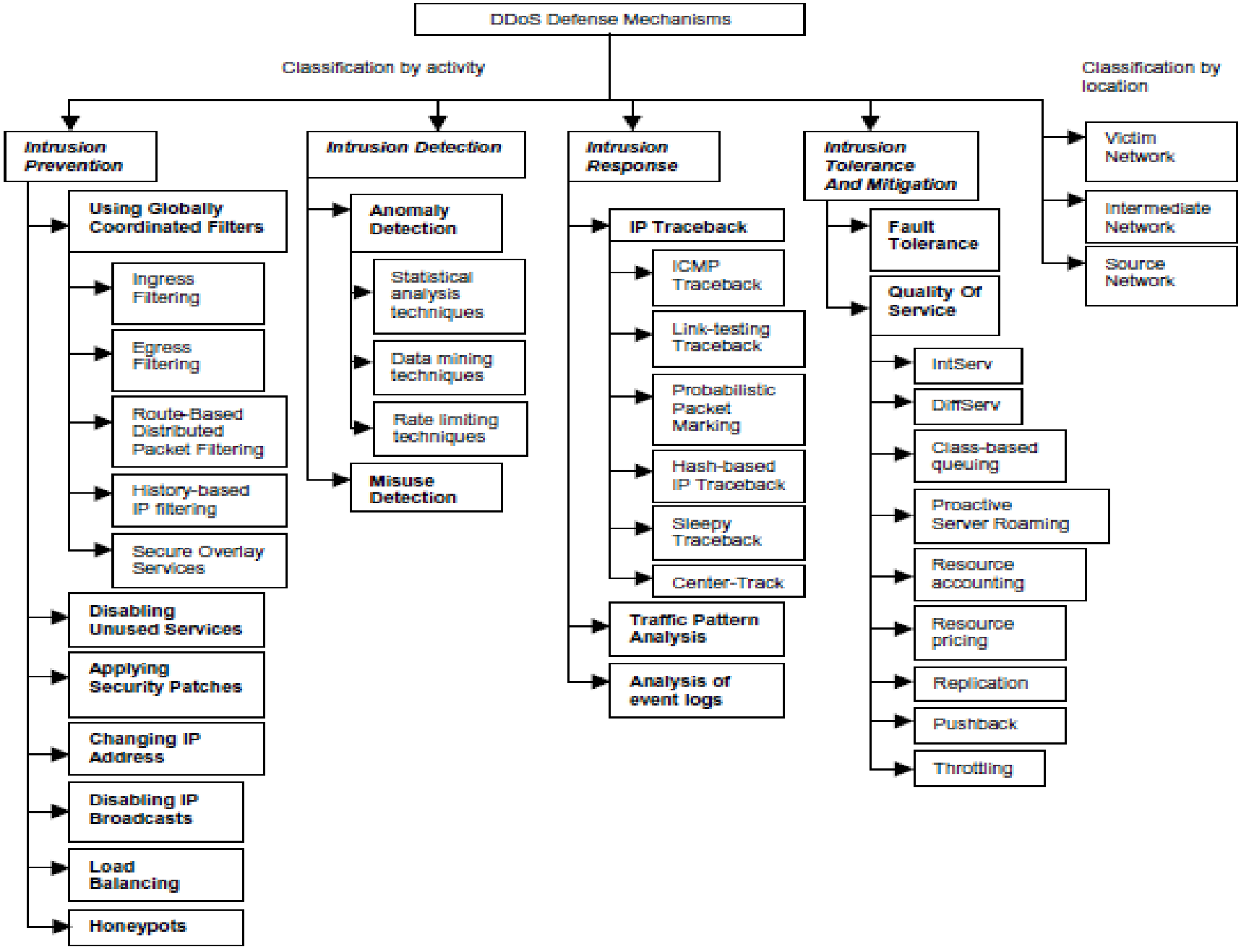
- Disruptive attacks lead to the complete denial of the victims service to its clients.
- The degrading attacks consume some portion of a victims resources.
  - Causes delay of the detection of the attack and at the same time an immense damage on the victim.

DDoS defense

- DDoS attacks blocks a lot of resources such as CPU power, bandwidth, memory, processing time
- The main goal of any DDoS defense mechanism is to detect DDoS attacks as soon as possible and stop them *as near as possible to their sources*.

Classification of DDoS defense mechanisms

- Classification by activity
  - Intrusion Prevention
  - Intrusion Detection
  - Intrusion Tolerance and Mitigation
  - Intrusion Response
- Classification by deployment location
  - Victim Network
  - Intermediate Network
  - Source Network


DDoS Defense Mechanisms
Classification by activity
Classification by location
Intrusion Prevention
Using Globally Coordinated Filters
Ingress Filtering
Egress Filtering
Route-Based Distributed Packet Filtering
History-based IP filtering
Secure Overlay Services
Disabling Unused Services
Applying Security Patches
Changing IP Address
Disabling IP Broadcasts
Load Balancing
Honeypots
Intrusion Detection
Anomaly Detection
Statistical analysis techniques
Data mining techniques
Rate limiting techniques
Misuse Detection
Intrusion Response
IP Traceback
ICMP Traceback
Link-testing Traceback
Probabilistic Packet Marking
Hash-based IP Traceback
Sleepy Traceback
Center-Track
Traffic Pattern Analysis
Analysis of event logs
Intrusion Tolerance And Mitigation
Fault Tolerance
Quality Of Service
IntServ
DiffServ
Class-based queuing
Proactive Server Roaming
Resource accounting
Resource pricing
Replication
Pushback
Throttling
Victim Network
Intermediate Network
Source Network

Intrusion prevention

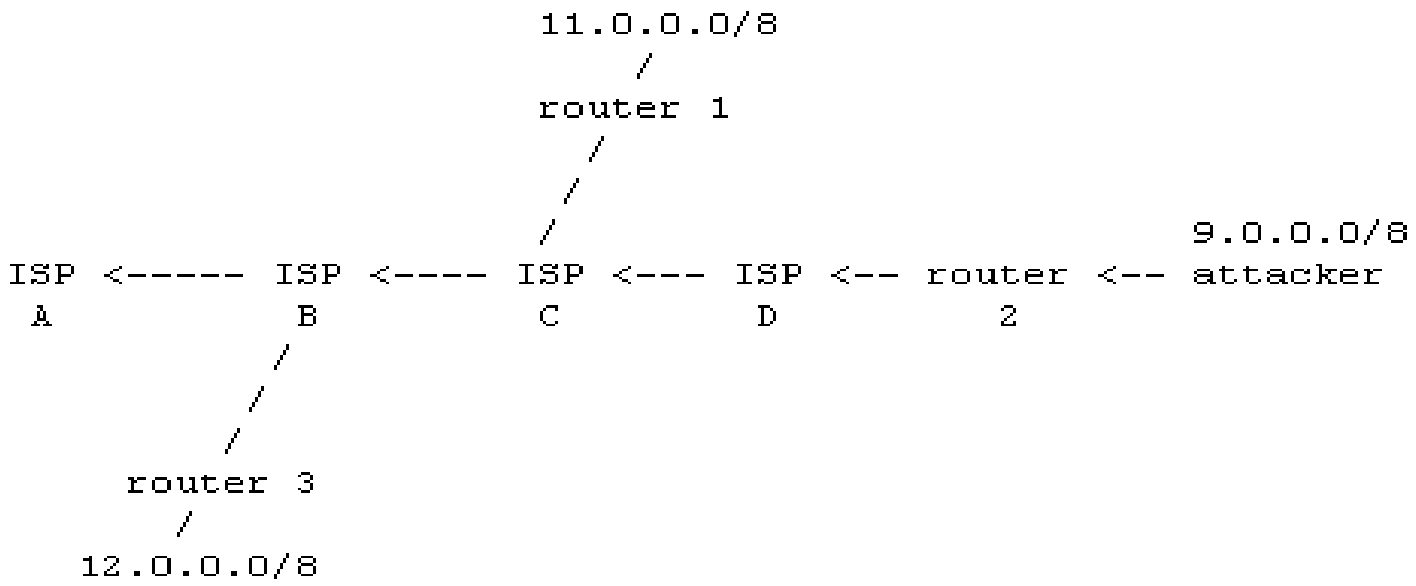
- Mitigation strategies to prevent the attack from being launched are:
  - Using globally coordinated filters
  - Secure Overlay Services (SOS)

Globally coordinated filters

- Ingress filtering
- Egress filtering
- Route-based distributed packet filtering
- History-based IP filtering (HIP)

Ingress filtering

- Ingress filtering is an approach to set up a router such that to disallow incoming packets with illegitimate source addresses into the network
- Routers block packets that arrive with illegitimate sources addresses
  - Requires the interface to be configured with a range of valid IPs
  - Quite feasible at for small network, unsuitable for larger ones.



An ingress filter on router 2 restricts traffic to allow only source addresses within the 9.0.0.0/8 prefix.

- Not all routers can look at every packets source address
- Spoofed addresses are all to often found
  - NAT
  - Mobile IP
  - Hybrid satellite architectures

- Egress filtering is an outbound filter, which ensures that only assigned or allocated IP address space leaves the network.

- Route-based distributed packet filtering is capable of filtering out a large portion of spoofed IP packets and preventing attack packets from reaching their targets as well as to help in IP traceback.

- In History-based IP filtering (HIP), the edge router allows the incoming packets according to a pre-built IP address database.
  - The IP address database is based on the edge routers previous connection history.
  - This scheme is robust, is applicable to a wide variety of traffic types and requires little configuration.

Secure Overlay Services (SOS)

- Proactively prevent DoS to allow legitimate users to communicate with critical target.

- Secure Overlay Services (SOS) is an architecture in which only packets coming from a small number of nodes (servlets), are assumed to be legitimate client traffic.
- To gain access to the overlay network, a client has to authenticate itself with one of the replicated access points (SOAPs)
- Not suitable for protection of public servers.

- Disabling unused services prevents DDoS attacks.
- Applying security patches minimize the effect of DDoS attack
- Changing IP address is another simple solution to a DDoS attack in order to invalidate the victim computers IP address by changing it with a new one.

- By disabling IP broadcasts, host computers can no longer be used as amplifiers in ICMP Flood and Smurf attacks.
- Load balancing can be applied, that enables network providers to increase the provided bandwidth on critical connections and prevents them from going down in the event of an attack.

- Honeypots can also be used to prevent DDoS attacks.
  - Honeypots are systems that are set up with limited security
  - can be used to trick the attacker to attack the honeypot and not the actual system

Intrusion detection

- Intrusion detection systems detect DDoS attacks by using
  - the database of known signatures
  - Recognition of anomalies in system behaviors

Intrusion response

- To response to DDoS attacks, the following methods can be used.
  - IP traceback
  - ICMP traceback
  - link-testing traceback
  - Probabilistic packet marking
  - Hash based IP traceback
  - Sleepy Traceback
  - Traffic Pattern Analysis

The Need for Traceback

- Internet Protocol permits anonymity
  - Attackers can "spoof" source address
  - IP forwarding maintains no audit trails

- Need a *traceback* facility
  - For a given packet, find the path to source

IP Traceback

- To identify the address of the true source of the packets causing DOS attacks(by spoofed address).
- *Ingress filtering* prevents IP address manipulation
- Some ISPs refuse to install inbound filters to prevent source-address spoofing.

Evaluation Metrics for IP Trace back Techniques

- ISP involvement.
- Number of Packets needed for Trace back.
- Effect of Partial Deployment.
- Processing Overhead.
- Bandwidth Overhead.
- Memory Requirements.
- Number of Functions needed to implement.

- Some Assumptions:
  - Packets may be Multi- or broadcast
    - Tracing system must be prepared for multiple packets
  - Attackers can get into routers
    - Tracing must not be confounded by a motivated attacker
  - Routing behavior of network can be unstable
    - Tracing must be prepared to handle divergent information
  - Packet Size Should not grow due to Tracing
  - End hosts may be resource constrained
  - Tracing is an infrequent operation

IP traceback approaches

- Reactive IP traceback : initiate the traceback process in response to an attack
  - Two Popular methods are:
    - Input debugging
    - controlled flooding
- Proactive IP traceback
  - Traceback data used for attack path reconstruction and subsequent attacker identification.
  - Techniques:
    - *Logging*
    - *Packet-marking*

Input debugging

- Input debugging allows operators to filter particular packets (with some kind of signature) on some egress port and determine which ingress port they come from.
  - Manually: call the upstream router operator
  - Automatically: some ISPs have tools to do this
- Drawbacks:
  - Often too slow
  - Management overhead
  - Coordination with other ISPs is difficult, and very slow

Controlled Flooding

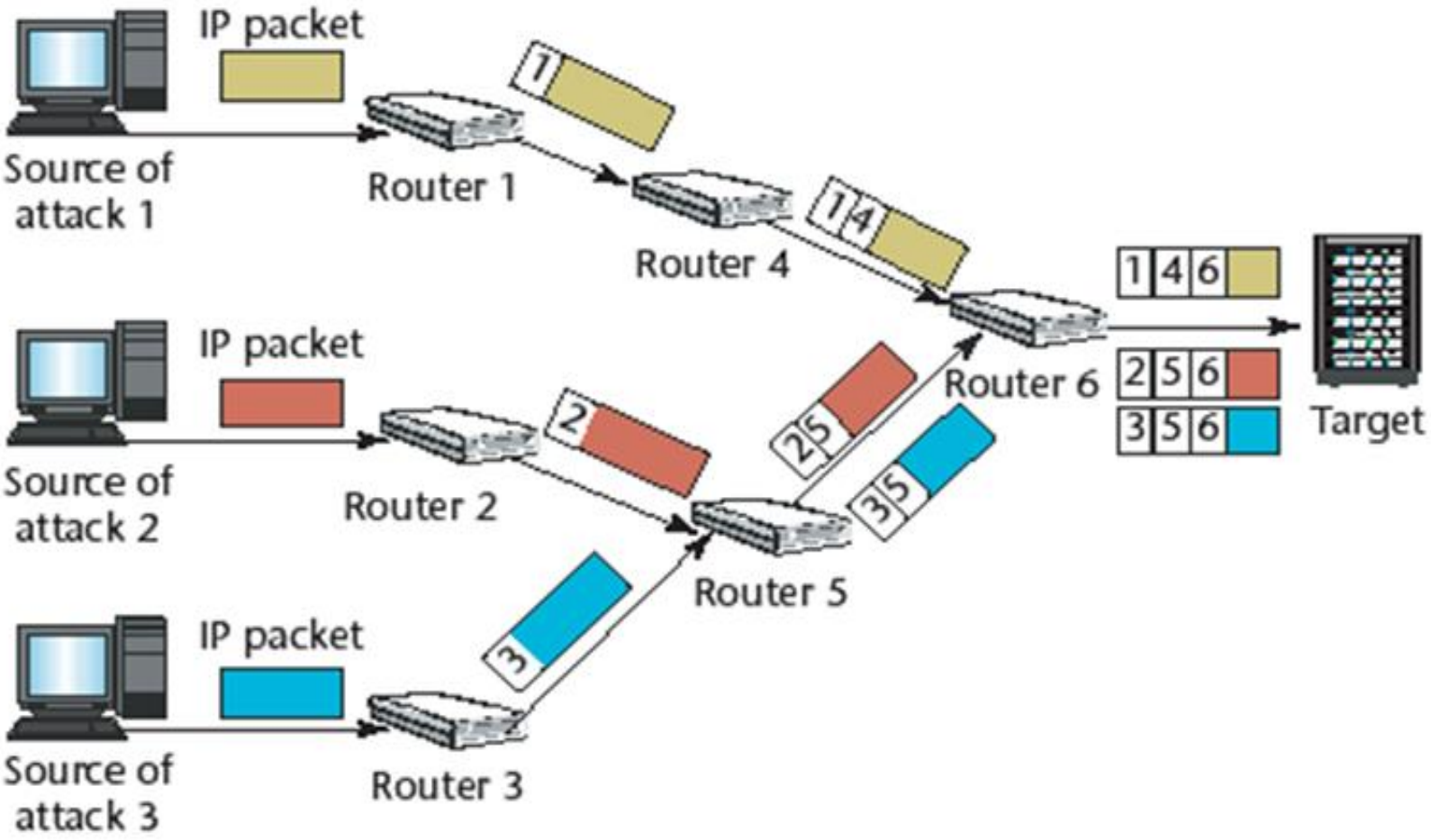
- Selectively flood a link to observe attack traffic, with the help of some Internet map
- This does not require intermediate operator intervention
- Drawbacks
  - This is a form of DoS itself
  - Requires the map, which itself is non-trivial
  - Poorly suited for DDoS
  - Only effective for on-going attacks, cannot be use for post-mortem analysis

Logging

- Log packets at key routers throughout the Internet and then use data-mining techniques to extract information about attack traffic's source.
- Huge amount of processing and storage power needed to store the logs.
- Need to save and share information among ISPs : logistical and legal problems, as well as privacy concerns.

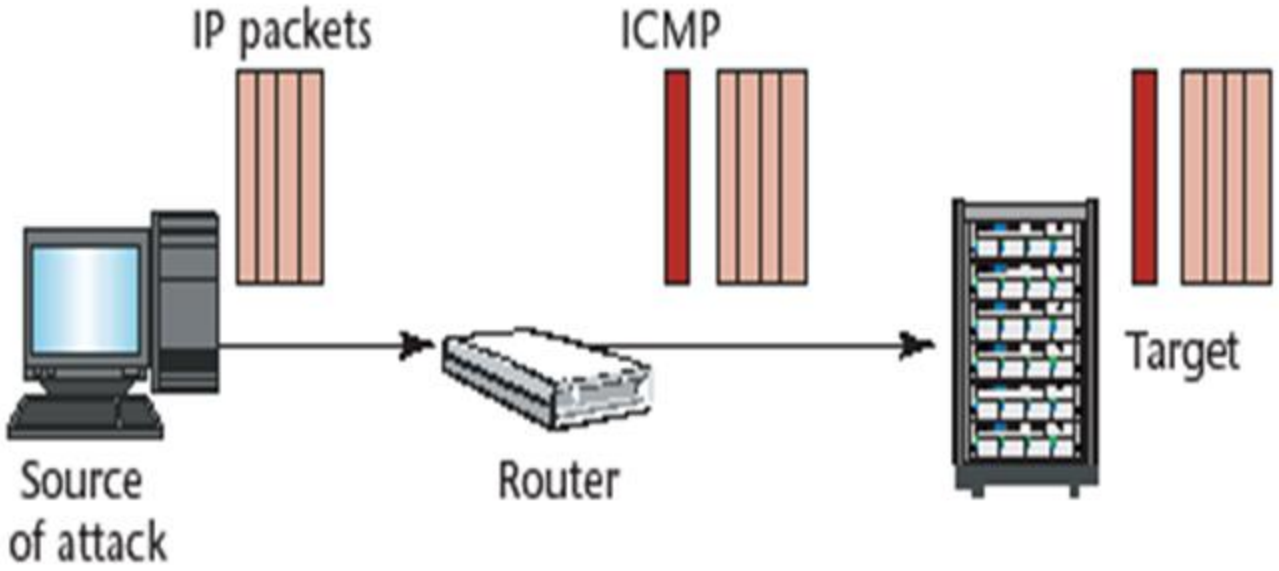
Packet Marking

- Each router marks packets as they travel through it.
- The marking process depends on the method adapted.


IP packet
Source of attack 1
Router 1
1
Router 4
14
IP packet
Source of attack 2
Router 2
2
25
Router 6
1 4 6
2 5 6
3 5 6
Target
Router 5
35
IP packet
Source of attack 3
Router 3
3

ICMP traceback

- Every router samples with low probability (1/20K) one of the packets it's forwarding
- Copy the content into a special ICMP traceback along the path to the destination, containing
  - Back link, forward link, authentication,
- Destination then use this info to do traceback


IP packets
ICMP
Target
Source
of attack
Router

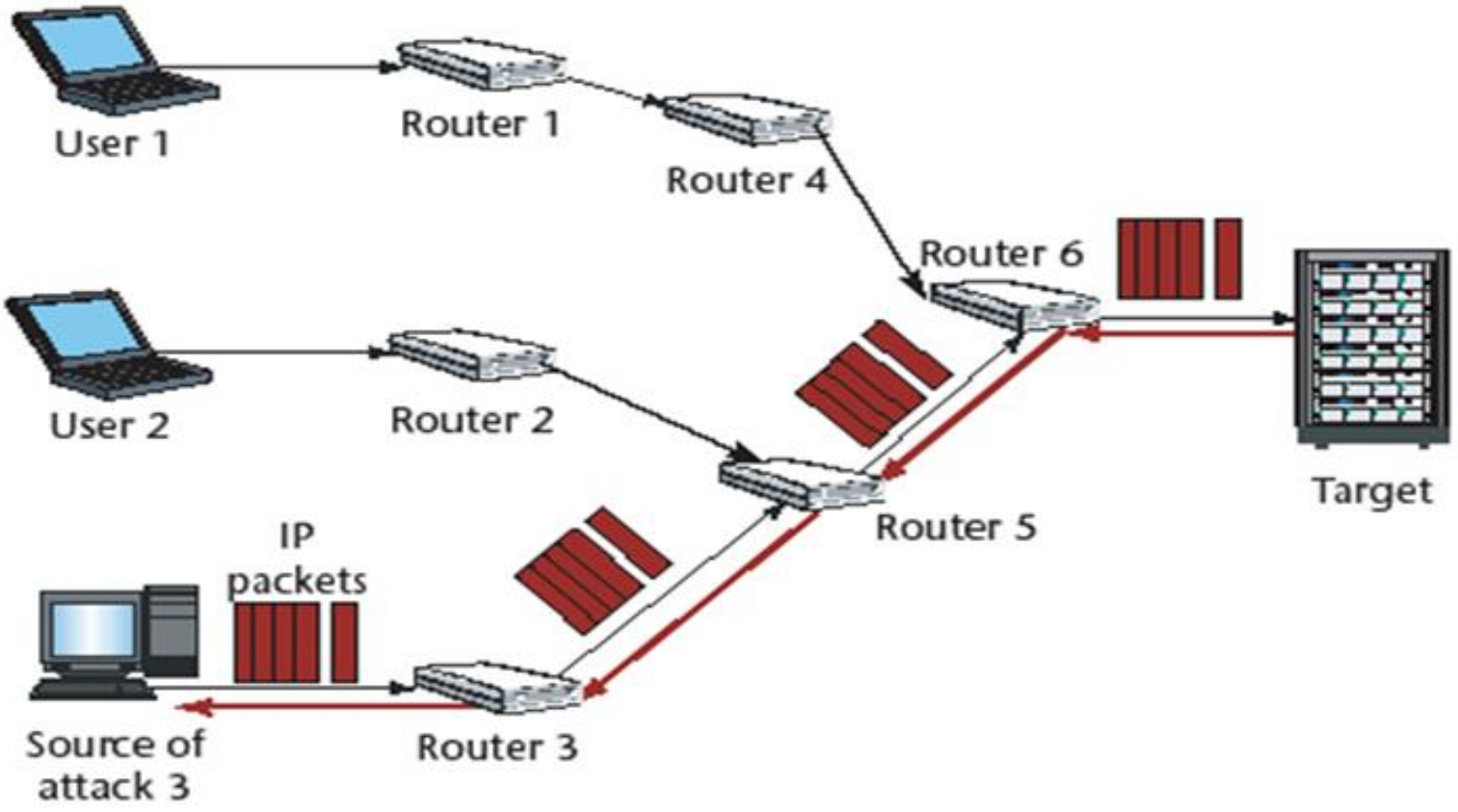
Packet Marking

- To be effective, packet marking should not increase the packets' size (to avoid additional downstream fragmentation, thus increasing network traffic).
- Secure enough to prevent attackers from generating false markings.
- Must work within the existing IP specifications : the specified order and length of fields in an IP header.
- Packet-marking algorithms and associated routers must be fast enough to allow real-time packet marking.
  - Probabilistic Packet Marking
  - Received widespread attention; active area of research

Link-testing traceback

- The victim/target determines the attack signature.
- Traceback starts from the router close to the victim.
- It interactively tests the upstream links to determine which one carries the attack traffic.

Link-testing traceback



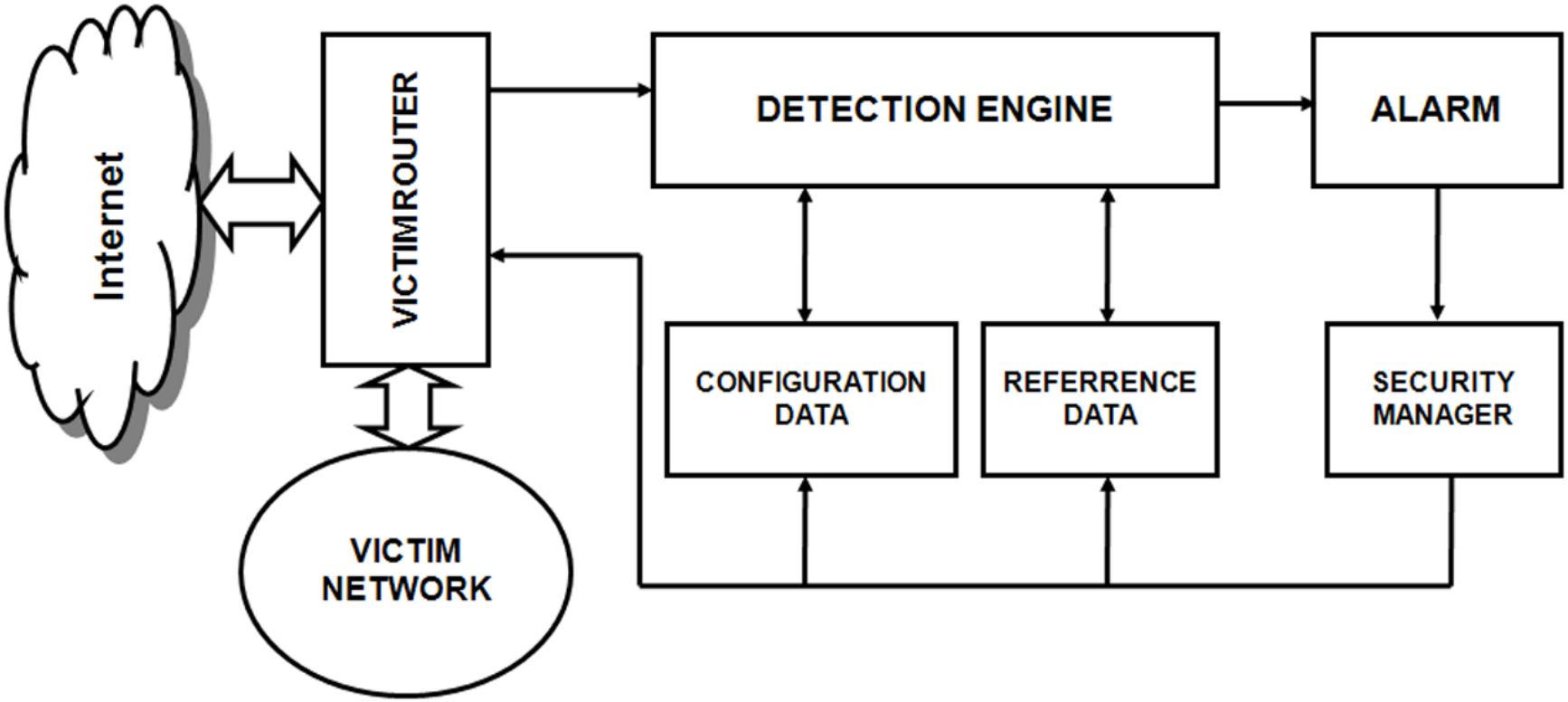
DDoS Defense based on deployment

- Victim-end defense mechanism
- Sourse-end defense mechanism
- Intermediate defense mechanism

Victim-end defense mechanism

- Generally employed in the routers of victim networks.
- The detection engine is used to detect intrusion either online or offline, using either misuse based intrusion detection or anomaly based intrusion detection.
- The reference data stores information about known intrusion signatures or profiles of normal behavior.

Generic architecture for victim-end DDoS defense mechanism

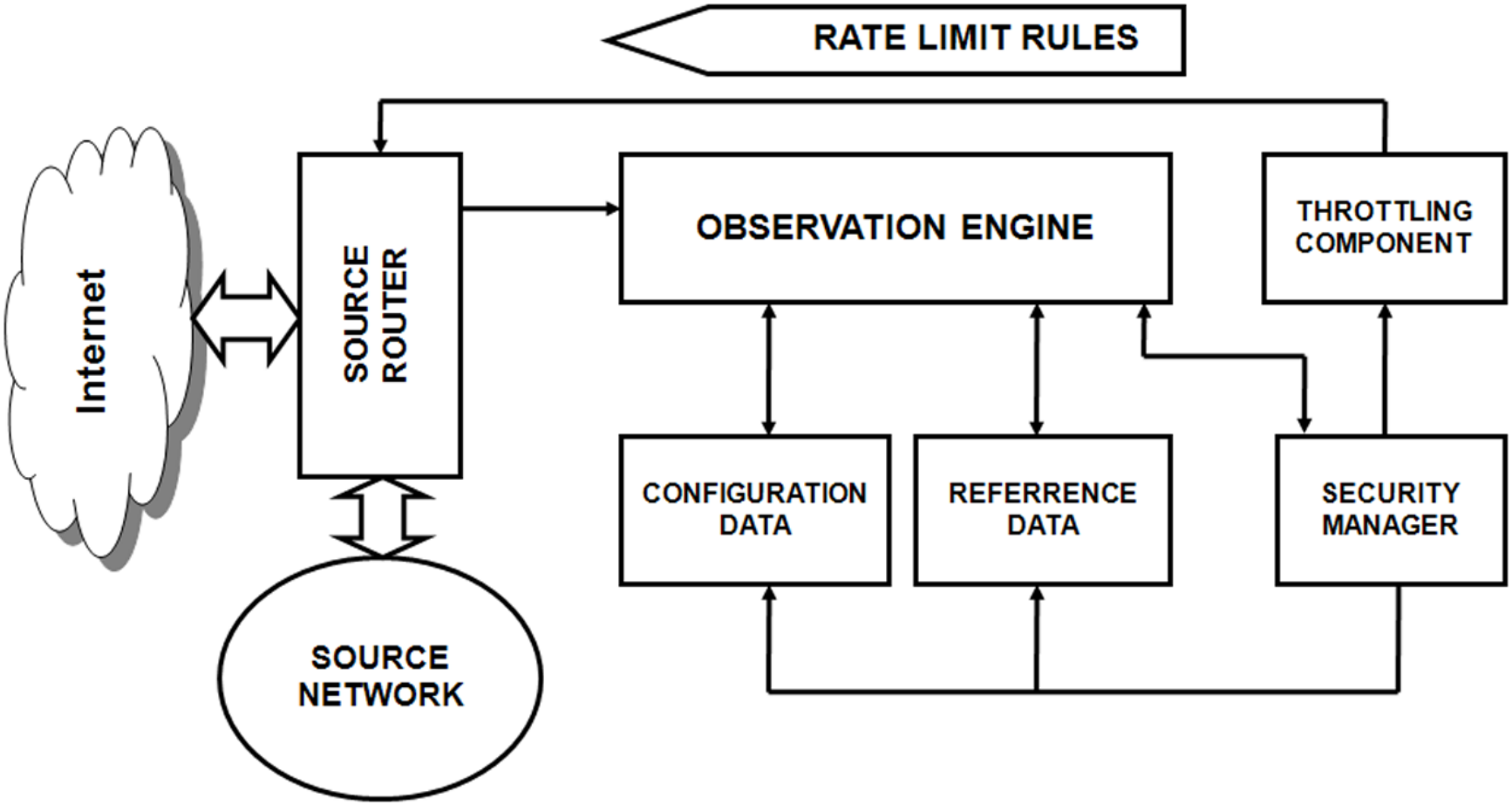


- The security manager often updates the stored intrusion signatures and also checks for other critical events such as false alarms.

Source-end defense mechanism

- Similar to the victim-end detection architecture.
- Here a throttling component is added to impose rate limit on outgoing connections.
- The observation engine compares both incoming and outgoing traffic statistics with some predefined normal profiles.

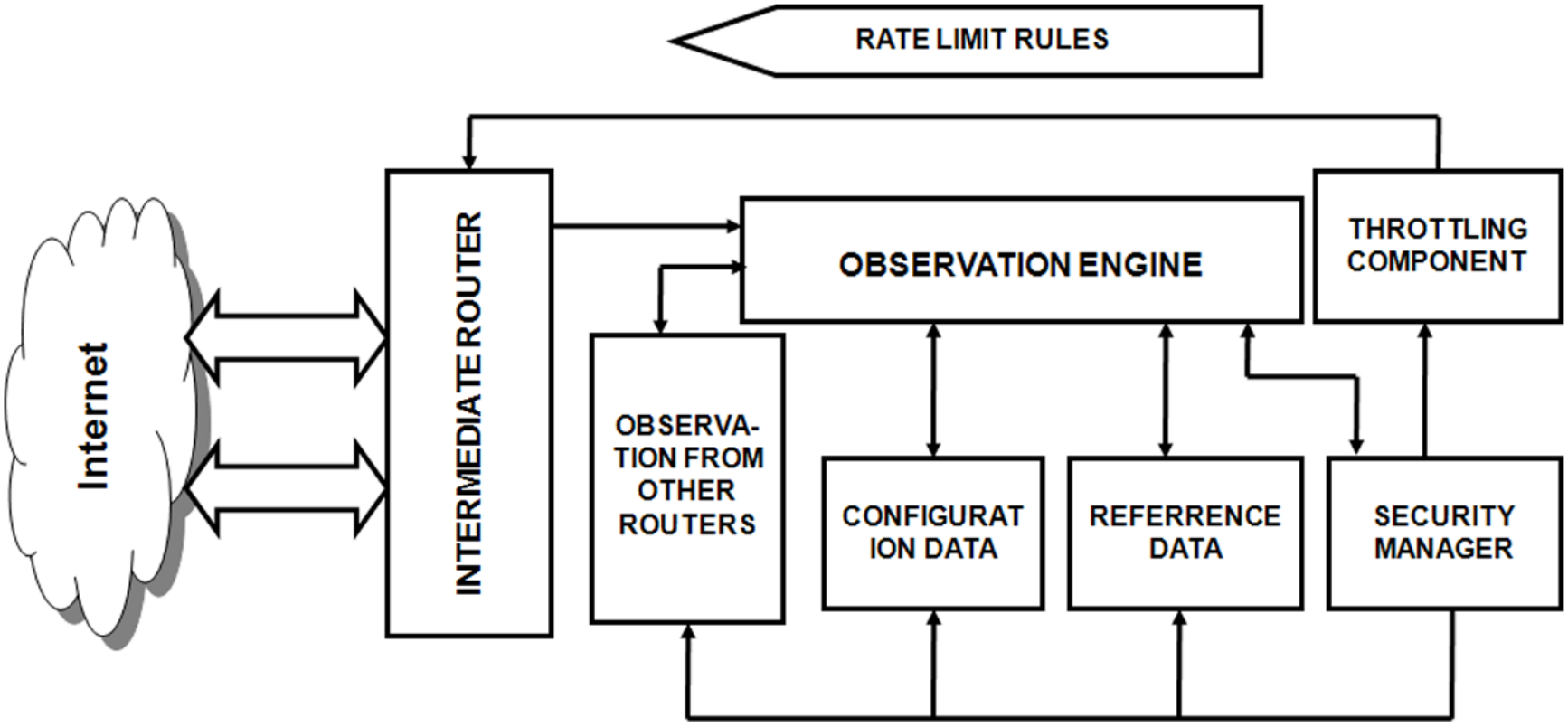
Generic architecture for source-end based DDoS defense mechanism



Intermediate defense mechanism

- Such scheme is generally collaborative in nature and the routers share their observations with other routers.
- Detection and traceback of attack sources are easy in this approach due to collaborative operation
- The main difficulty with this approach is deployability.

Generic architecture for intermediate network based DDoS defense

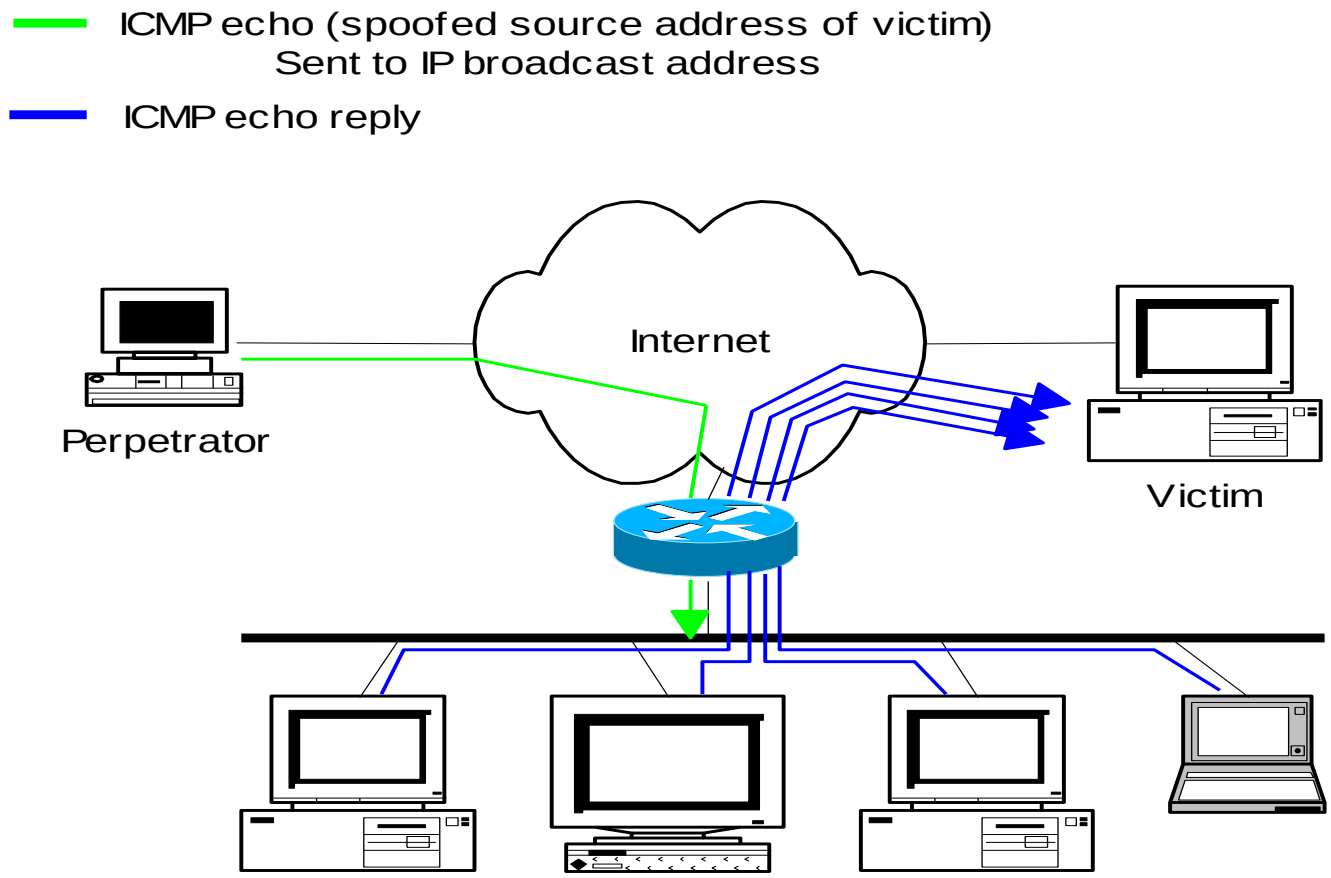


Smurf Attack

- ICMP is used for routing *error* messages
  - TTL expired
  - Host unreachable
  - Echo request
- Also used by default routers to redirect along quicker path.

Smurf Attack

- Sends ICMP ping packet with spoofed IP source address to a LAN which will broadcast to all hosts on the LAN
- Each host will send a reply packet to the spoofed IP address leading to denial of service


ICMP echo (spoofed source address of victim)
Sent to IP broadcast address
ICMP echo reply
Internet
Perpetrator
Victim