**Propagation Mechanism**

- *Attacks using central source propagation*: The attack code remains on a central server or set of servers and is downloaded to a target machine after successful infection.

- *Attacks using back-chaining propagation*: The attack code is downloaded from the attacker’s machine to the infected machine, and then the program in the infected machine is used for further propagation.

- *Attacks using autonomous propagation*: The malicious program is directly inserted into the target machine by the attacker.

**Exploited Vulnerability**

- *Protocol attacks*: Attackers exploit the vulnerabilities present in the communication protocol implementations in target machines. The TCP SYN attack, the CGI request attack, and the authentication server attack are a few examples of protocol attacks.

- *Brute-force attacks*: Attackers generate huge amounts of seemingly legitimate transactions that the target system cannot handle.
  - Filterable attacks generate bogus traffic that can be filtered by most firewalls.
  - Nonfilterable attacks use legitimate packets from the infected target to flood the network and cannot be filtered.

**Attack-Rate Dynamics**

- *Continuous-rate attacks*: The rate of propagation of attacking code is continuous and static.

- *Variable-rate attacks*: The rate of propagation of attacking code varies throughout propagation.
  - *Increasing-rate attacks*: The rate of propagation of attacking code increases with time.
  - *Fluctuating-rate attacks*: The rate of propagation of attacking code fluctuates with time.

**Impact**

- Disruptive attacks completely prevent legitimate users from using network services.
- Degrading attacks degrade the quality of services available to legitimate network users.

---

**DoS Attack Modes**

A DoS attack is known as an asymmetric attack when an attacker with limited resources attacks a large and advanced site. An attacker who is using a consumer-grade computer and a comparatively slow Internet connection may successfully attack powerful servers.

Denial-of-service attacks come in a variety of forms and target a variety of services. The attacks may cause the following:

- Consumption of resources
- Destruction or alteration of information regarding the configuration of the network
- Destruction of programming and files in a computer system

**Network Connectivity**

Denial-of-service attacks are most commonly executed against network connectivity. The goal is to stop hosts or networks from communicating on the network or to disrupt network traffic. An example of this type of attack is the SYN flood, where an attacker begins the process of establishing a connection to the victim’s machine, but does it in a way that ultimately prevents completion of the connection. An analogy would be to think of someone dialing your telephone and every time you answered, he or she would hang up and dial again. No one would ever be able to call you. Now automate it. In this case, an intruder uses the kernel data structures used in building a network connection, the three-way handshake of a TCP/IP connection model. This vulnerability enables an attack using a slower connection against a machine on a fast network.