DENIAL OF SERVICE AND INTRUSION DETECTION

DENIAL OF SERVICE

- DoS attack is an attack on the availability of network resources.
- DoS attack can be initiated in many ways, including:

- Transmission failure

-physical interference between asset and user

- Traffic redirection

- manipulation of routing table

- DNS attack

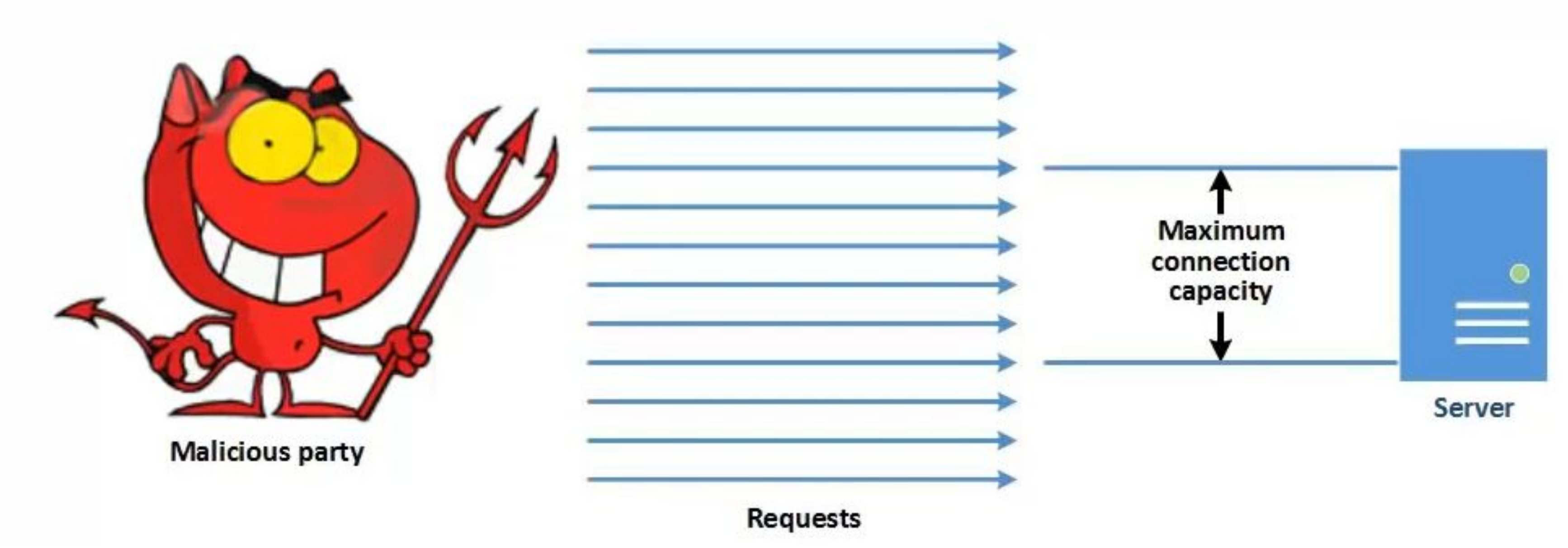
- Altering a DNS table

- Connection flooding

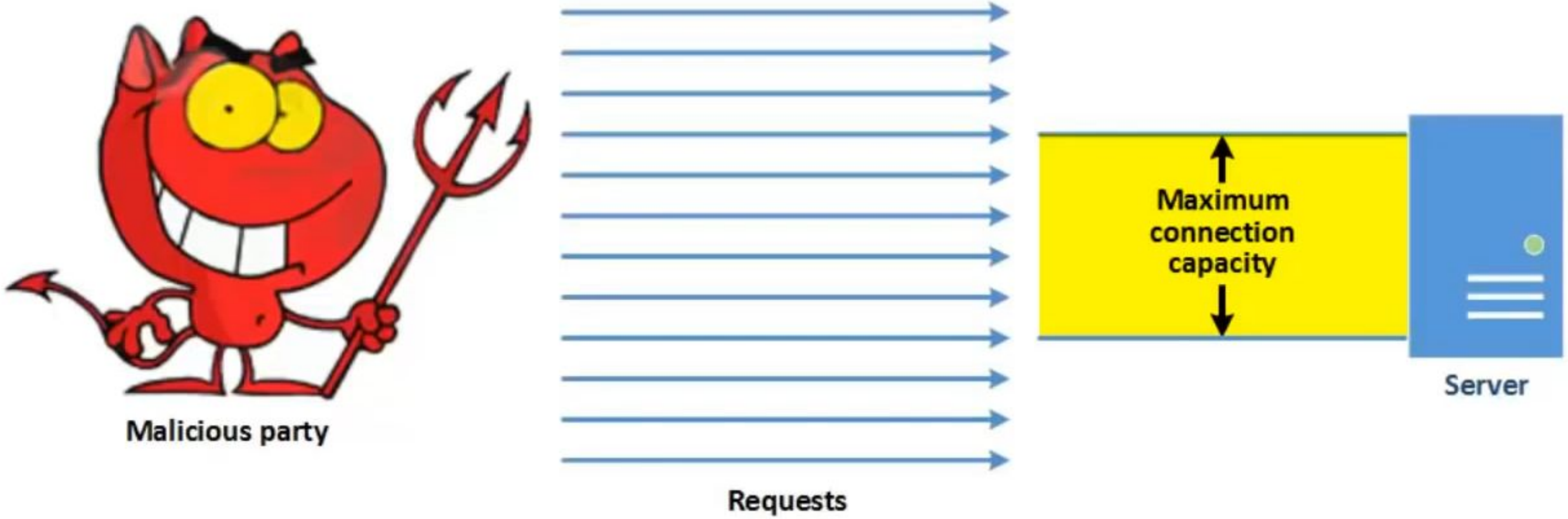
- flooding a server beyond a threshold

CONNECTION FLOODING

- Connection flooding attack seeks to negatively affect the availability of a network resource by exhausting or overwhelming the capacity of a communications channels.



CONNECTION FLOODING



TYPES OF CONNECTION FLOODING

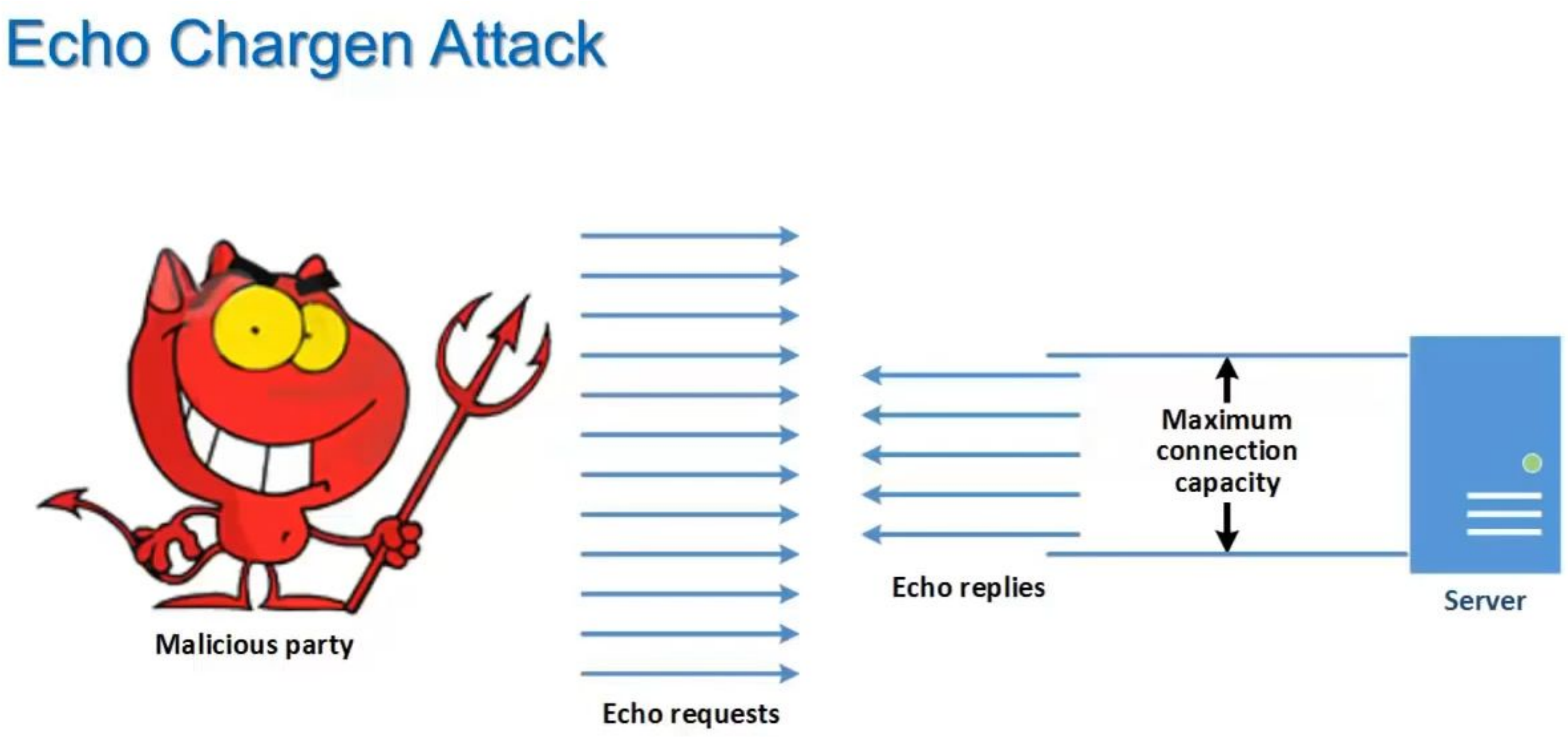
- There are many types of Connection flooding attacks, including:

1. Echo Chargen (Character Generator Protocol)
2. Ping of Death
3. Smurf attack
4. SYN flood
5. teardrop

Echo Chargen

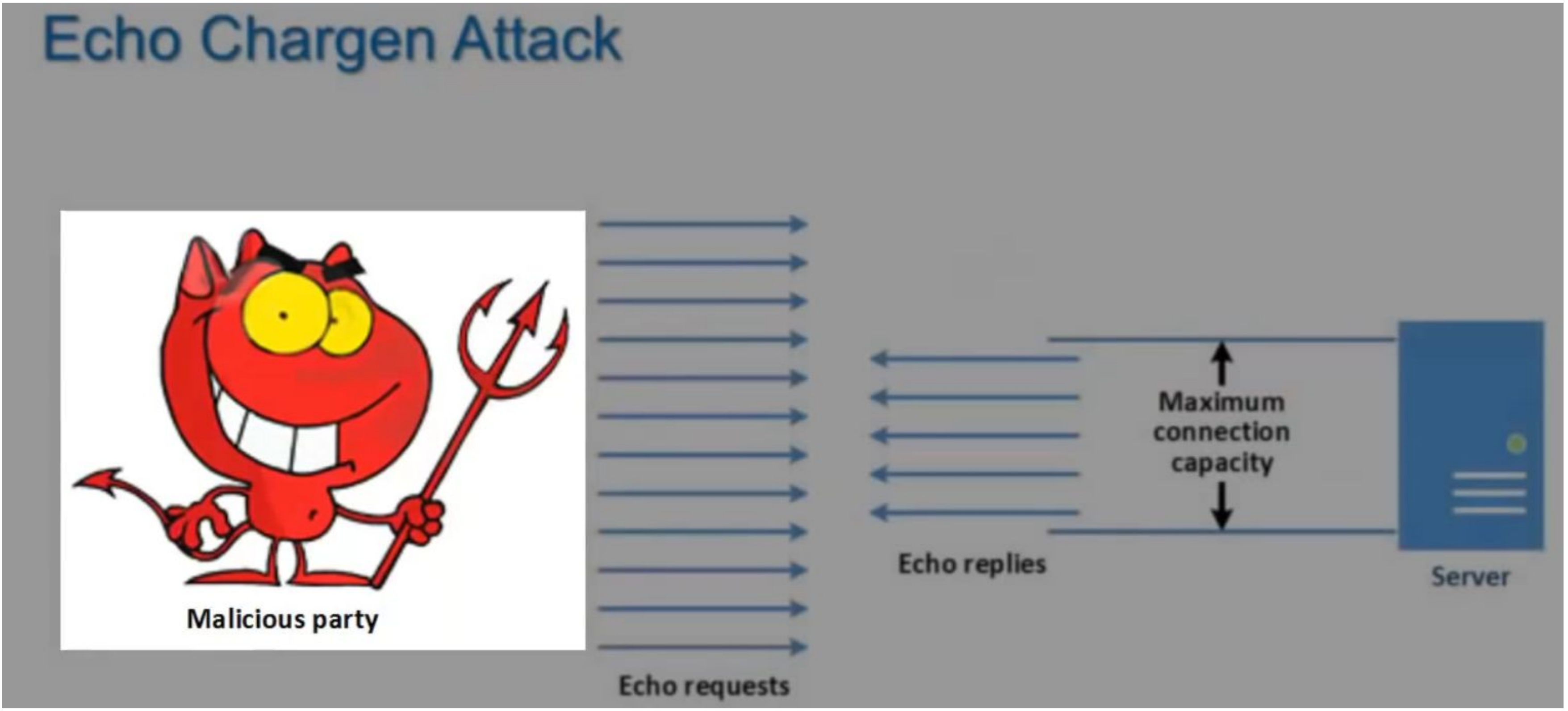
- It capitalizes on the echo commands within the character generator protocol.
- generator protocol it is a component of the broader internet protocol.
- It is designed to support debugging, testing and evaluating the performance of internet performance.
- this command simply instruct the server to send an identical copy of the data is has received back to the source server.

CONNECTION FLOODING



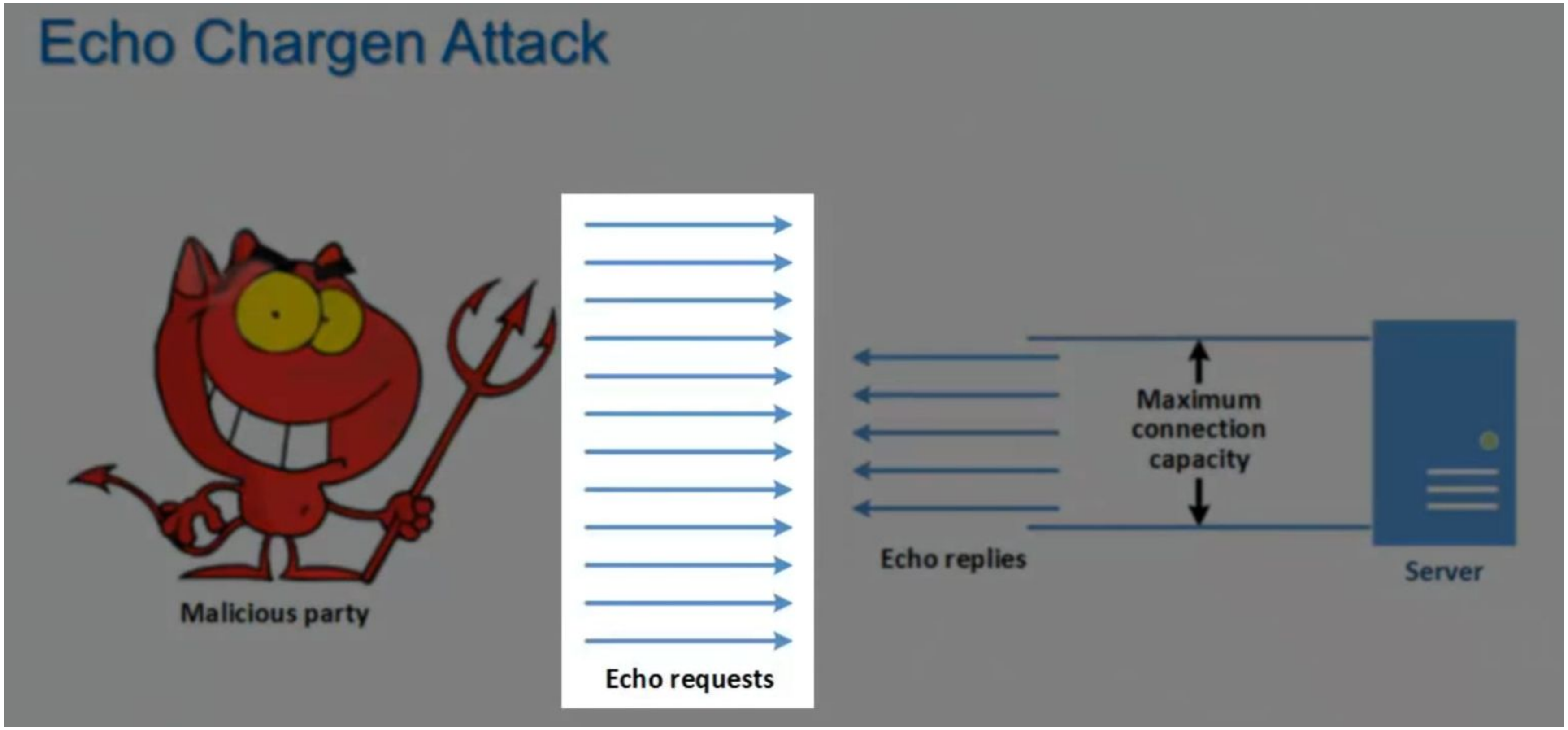
Echo Chargen Attack

CONNECTION FLOODING



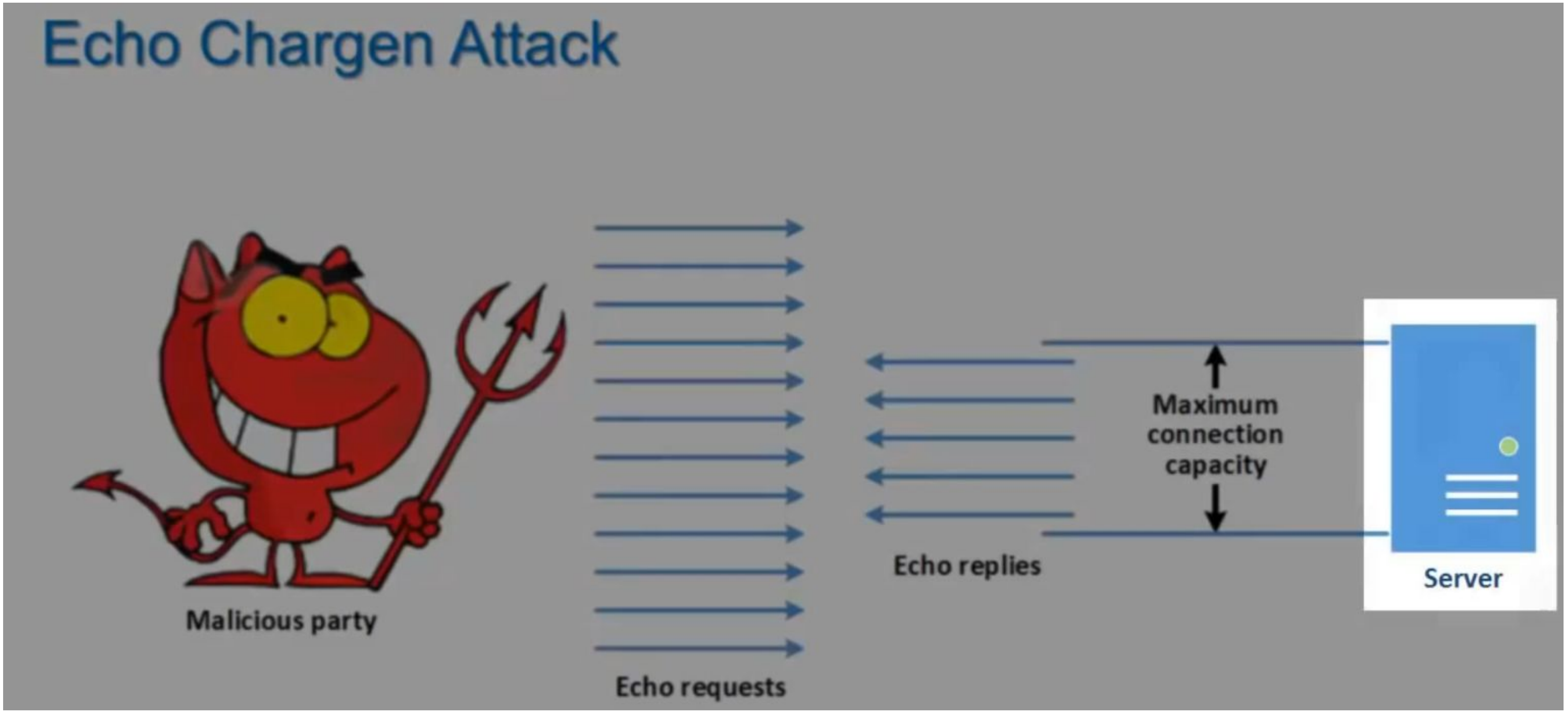
Echo Chargen Attack

CONNECTION FLOODING



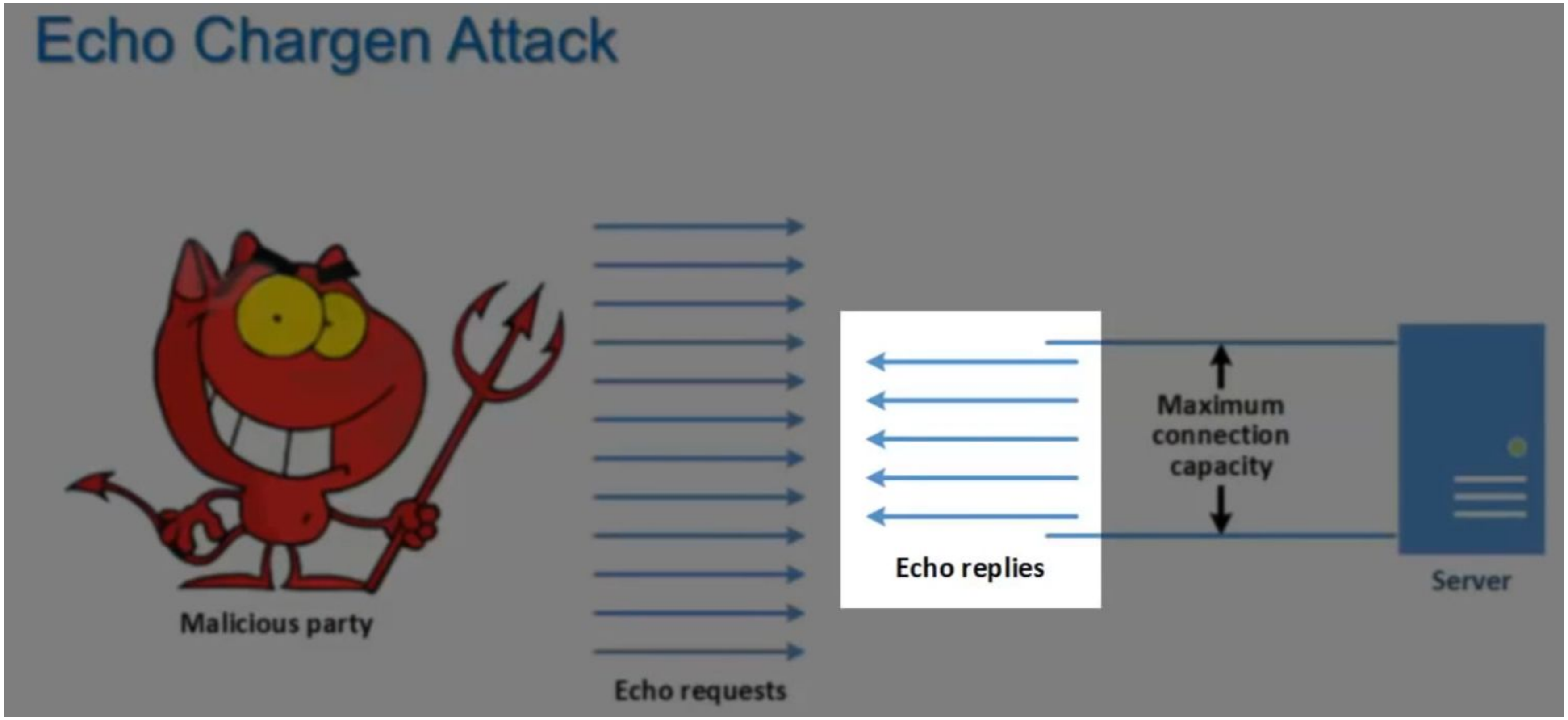
Echo Chargen Attack

CONNECTION FLOODING

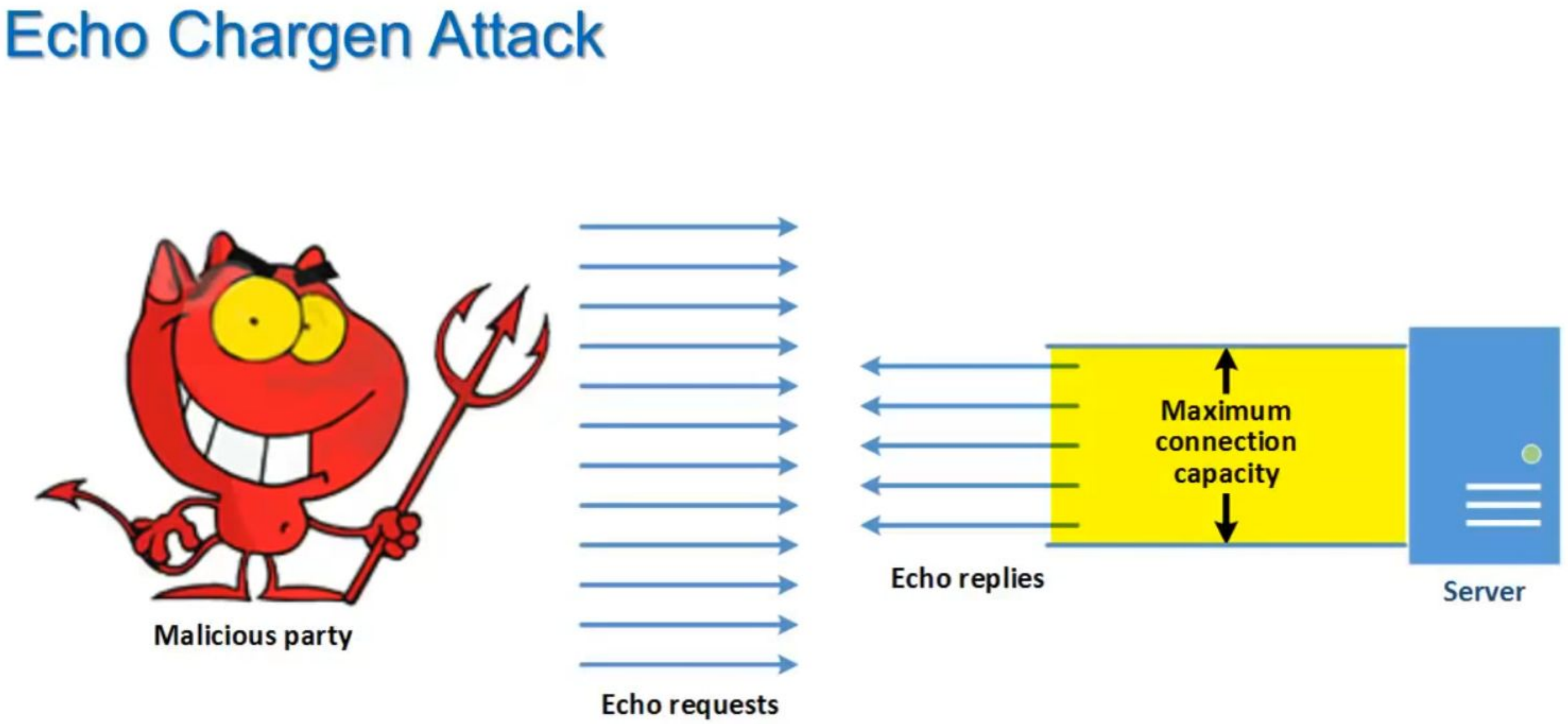


Echo Chargen Attack

CONNECTION FLOODING



CONNECTION FLOODING



Echo Chargen Attack

PING OF DEATH

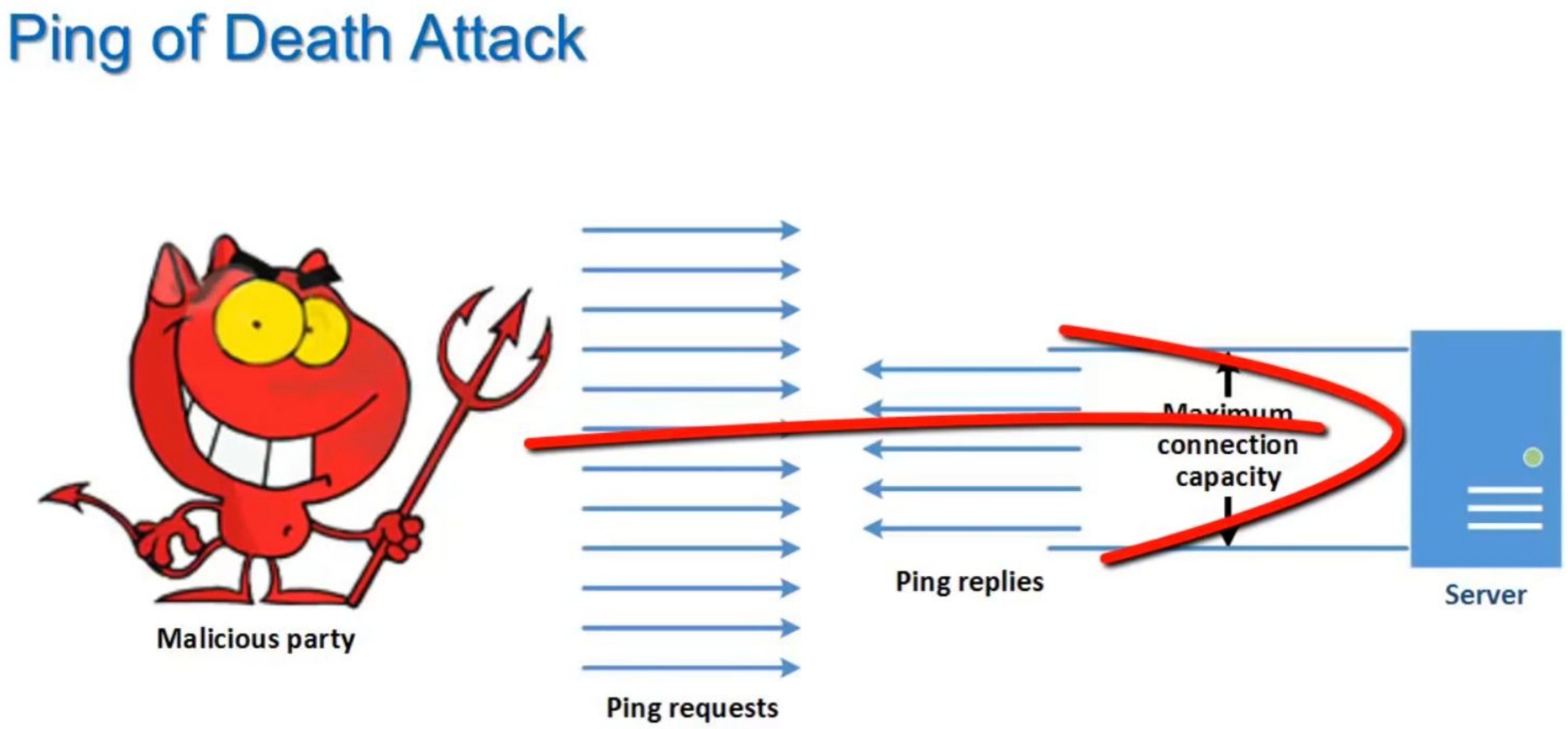
- It was created for :

  - diagnosing and solving problems with connections between host and a network that relies upon internet protocol addressing.

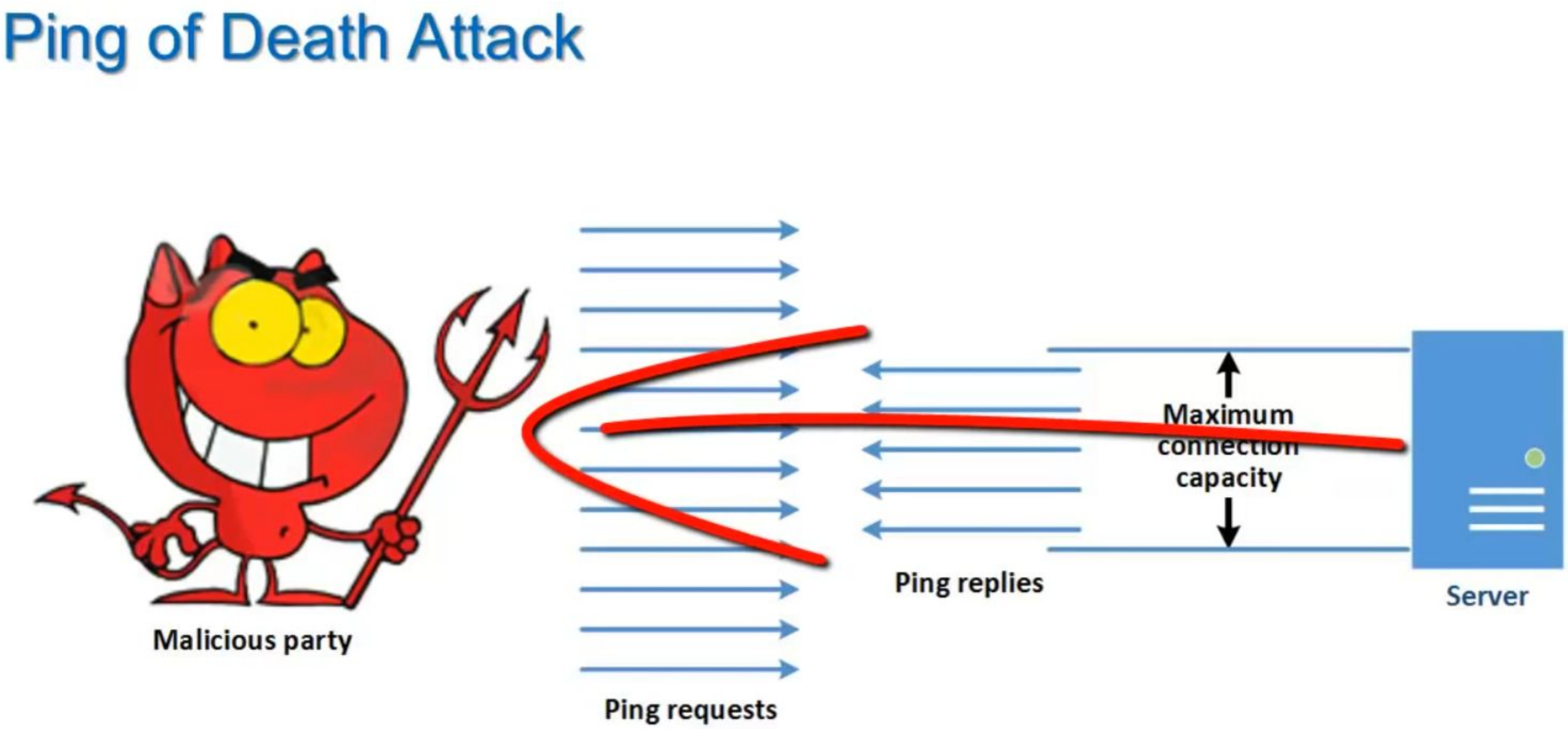
- Specifically the ping utility uses the Internet Control Message Protocol (ICMP) to send ping request to a target server.

- it measures the round trip time for each packet and track instances of packet loss

ICMP PING

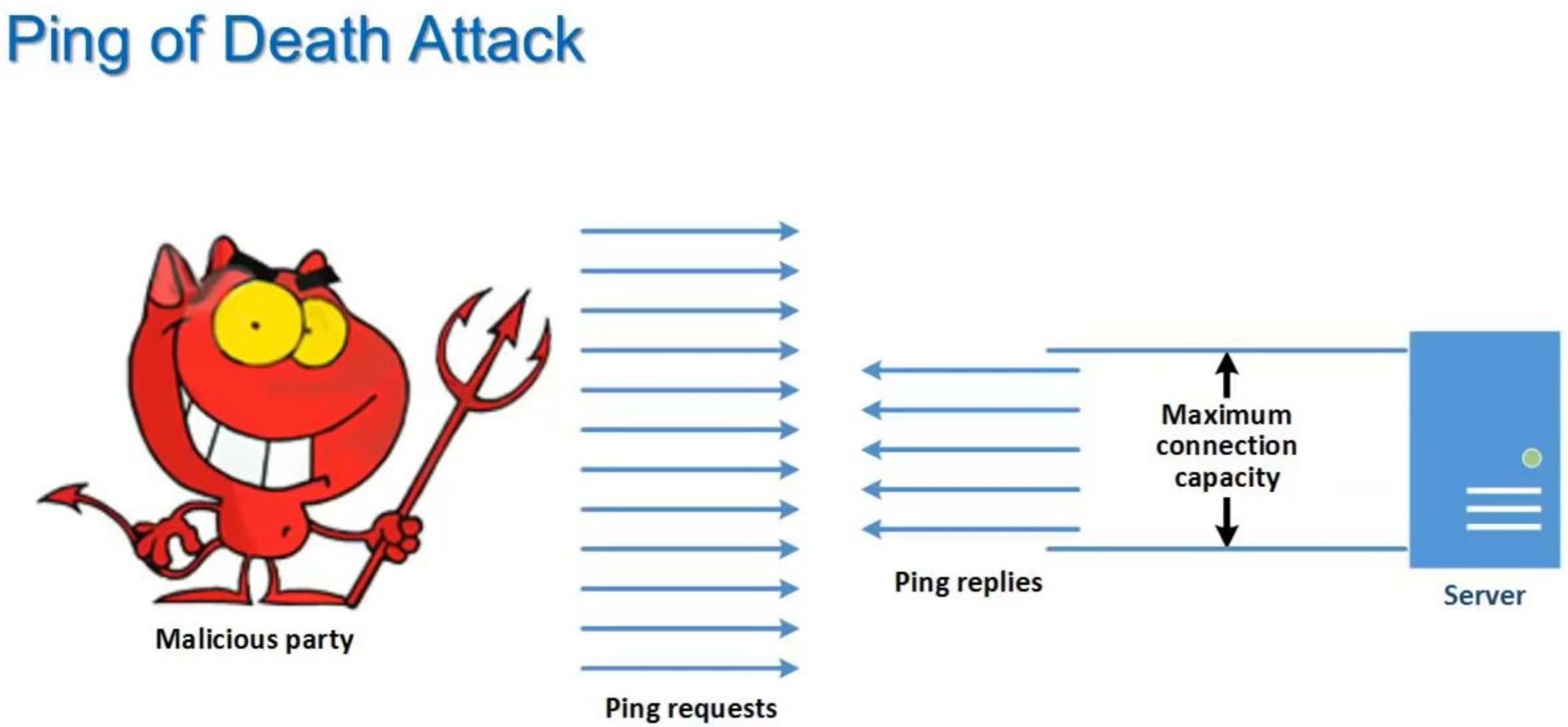

Ping of Death Attack
Malicious party
Ping requests
Ping replies
Maximum connection capacity
Server

ICMP PING



Ping of Death Attack

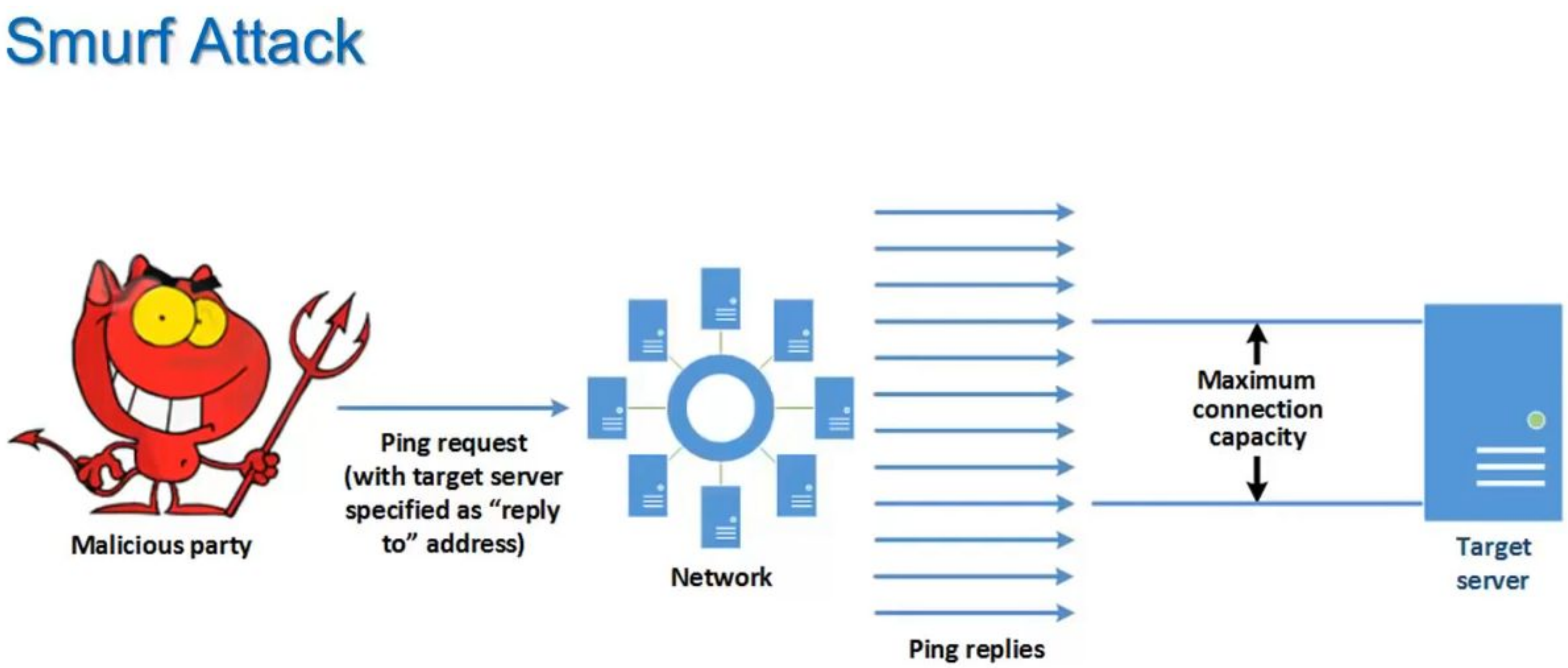
PING OF DEATH



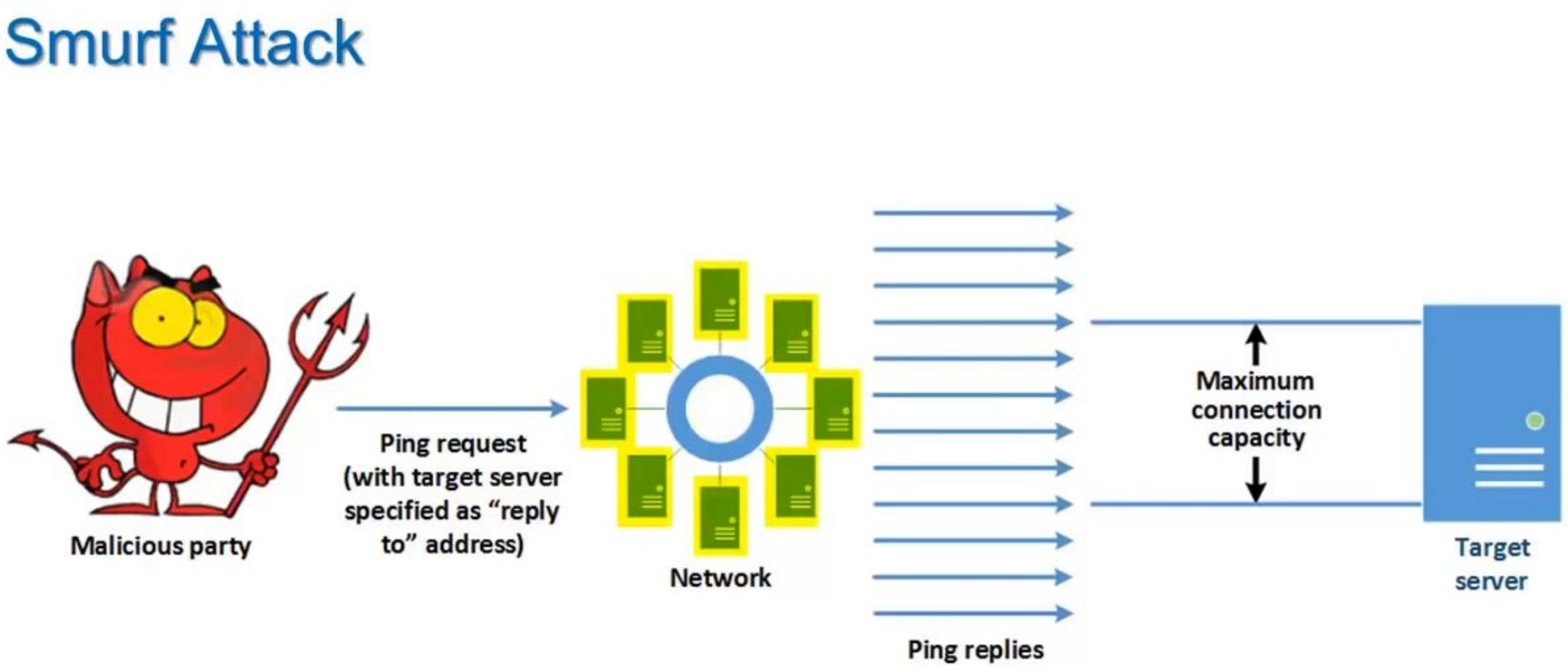
SMURF ATTACK

- It is similar to the above mentioned .
- Malicious attacker sends a request to the broadcast address and it is relayed to the host on the network.
- The host then sends the reply to the ping request that is the malicious party/attacker but it is sent back to the target server.
- Both echo chargen and ping of death need a great deal of bandwidth.

SMURF ATTACK


Smurf Attack
Malicious party
Ping request (with target server specified as "reply to" address)
Network
Ping replies
Maximum connection capacity
Target server

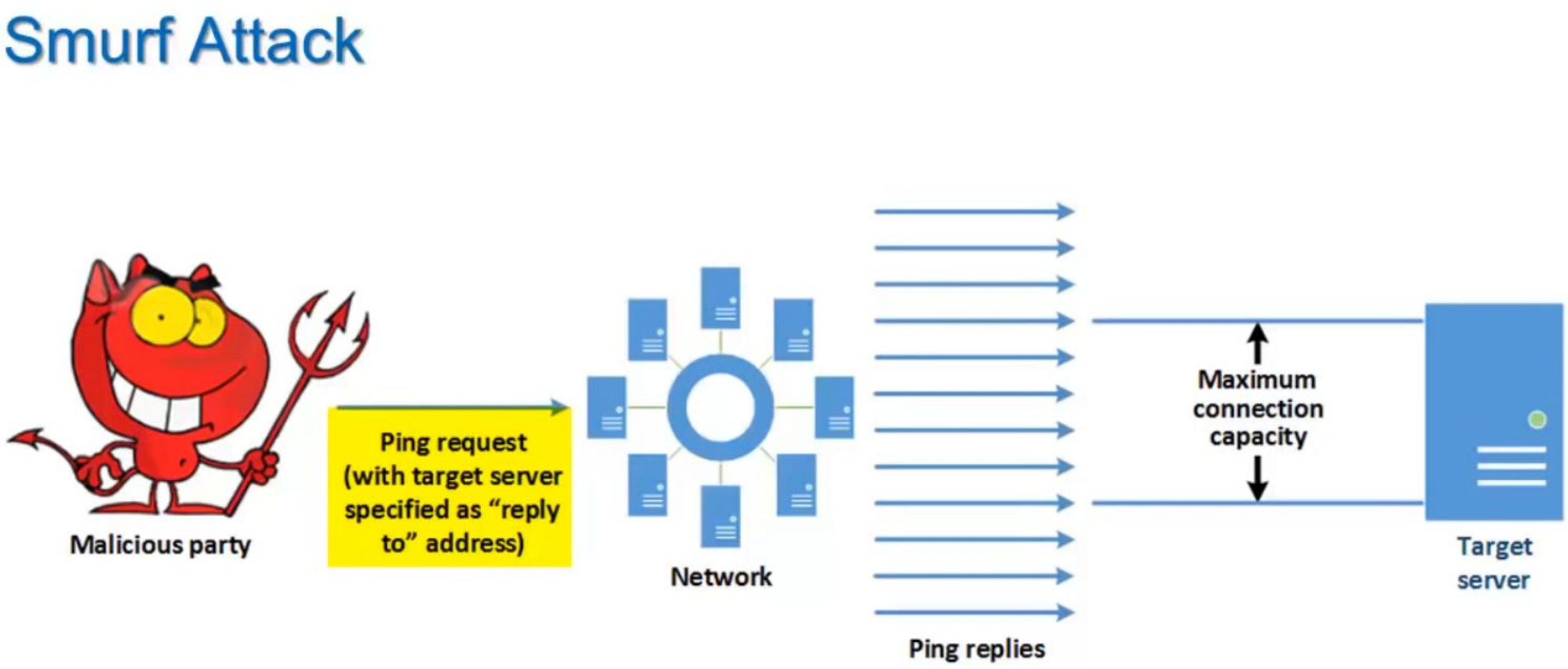
SMURF ATTACK



Smurf Attack

Malicious party
Ping request (with target server specified as "reply to" address)
Network
Ping replies
Maximum connection capacity
Target server

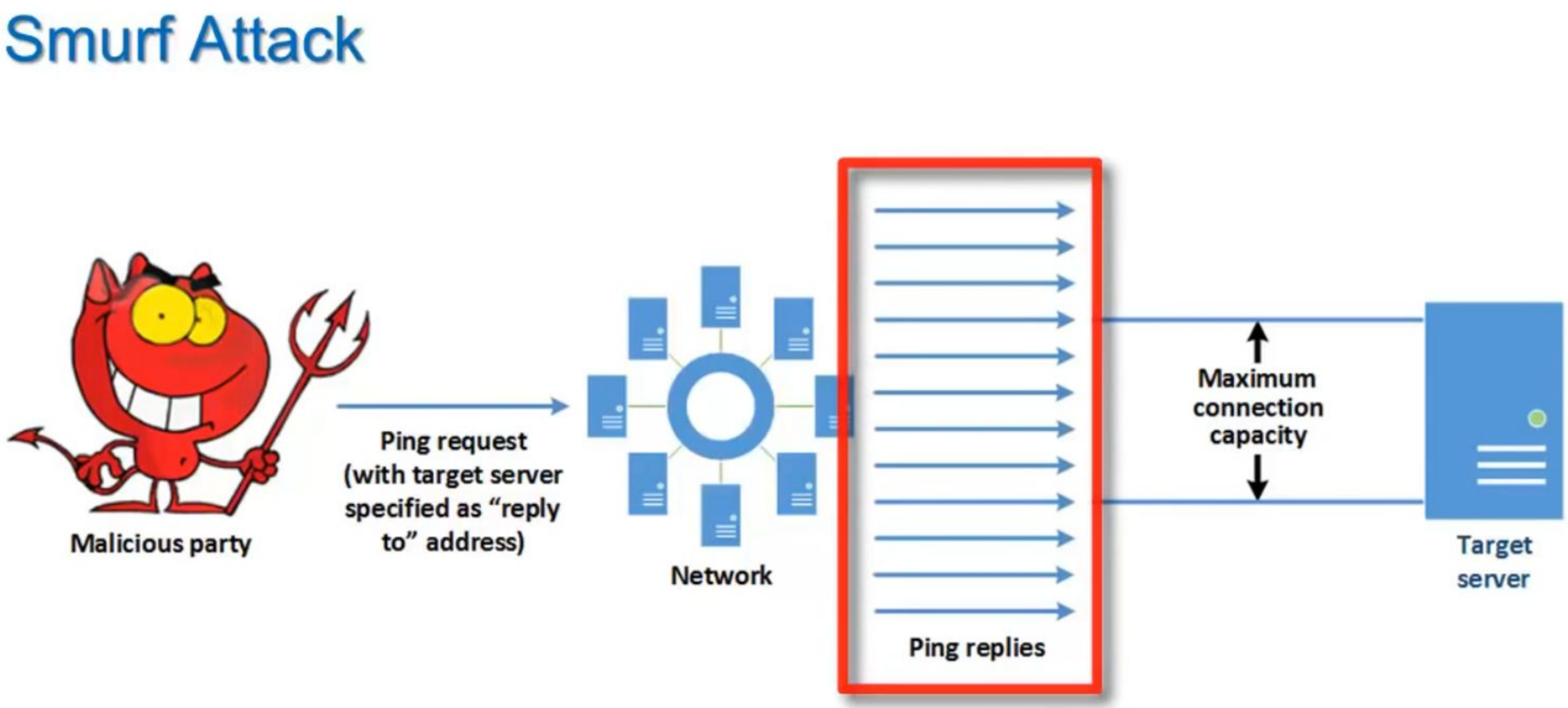
SMURF ATTACK



Smurf Attack

Malicious party
Ping request (with target server specified as "reply to" address)
Network
Ping replies
Maximum connection capacity
Target server

SMURF ATTACK



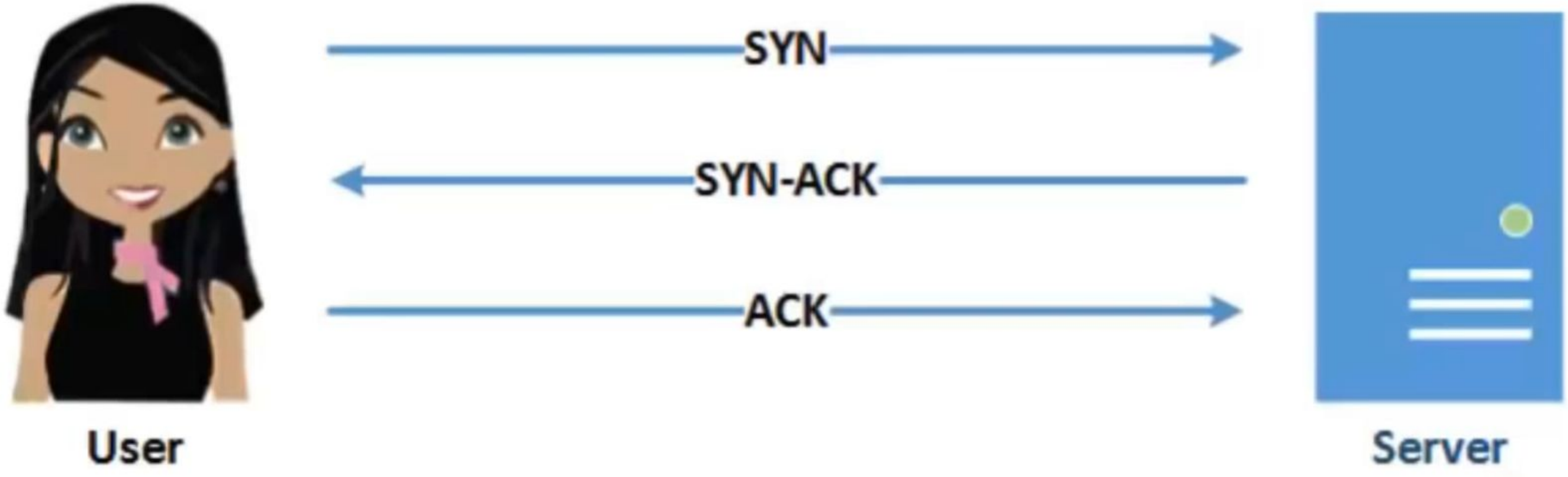
Smurf Attack

Malicious party
Ping request (with target server specified as "reply to" address)
Network
Ping replies
Maximum connection capacity
Target server

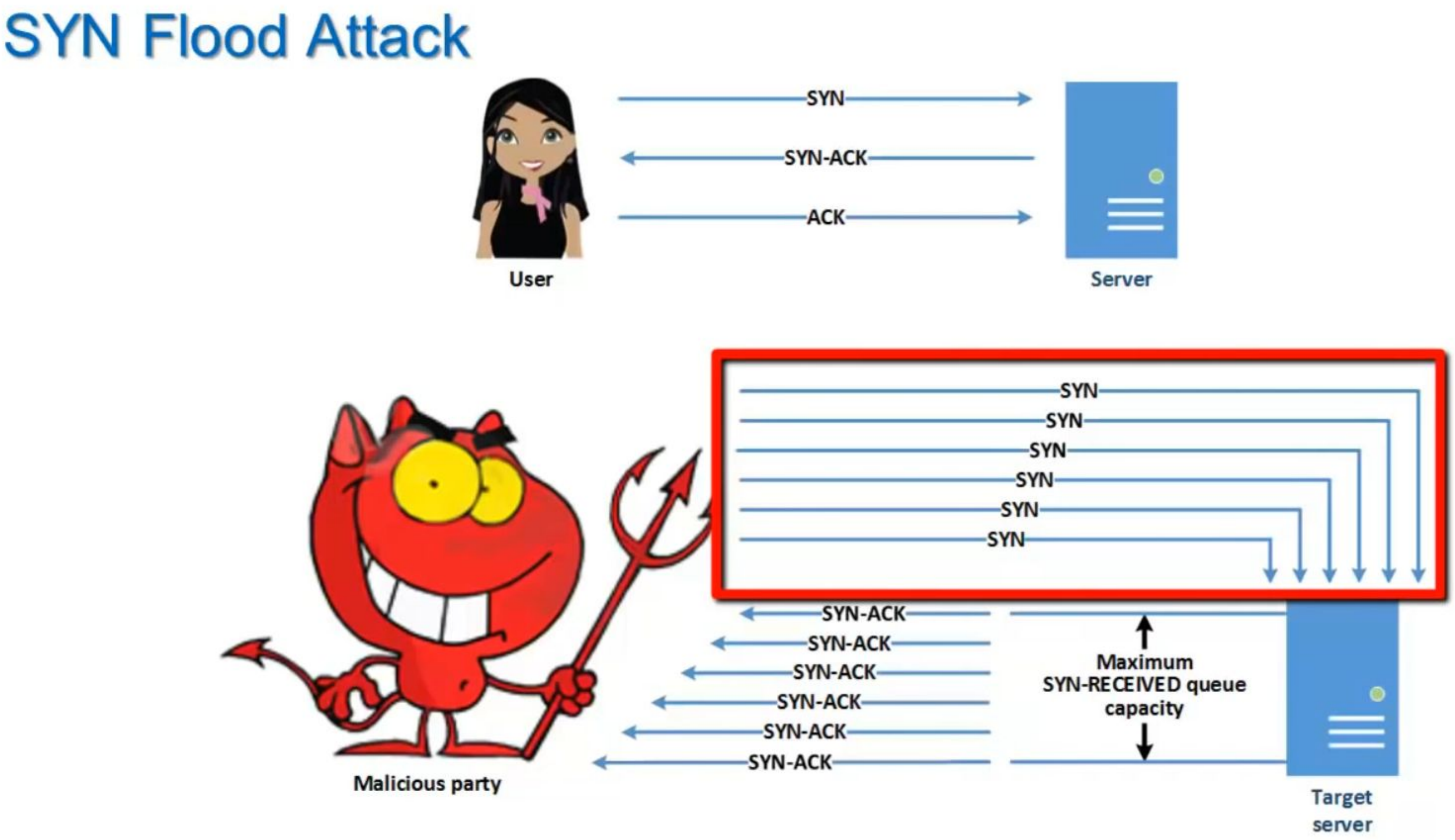
SYN FLOOD ATTACK

TCP/IP CONNECTION

- It is a three-way-handshake to establish a connection
- Syn request are stored in a syn receive queue for a limited time befor the ack from the user is received and a connection is established.
- Syn request queue has a maximum amount of unacknowledged request it can hold. When the queue is filled up it is not able to accept legitimate request from users

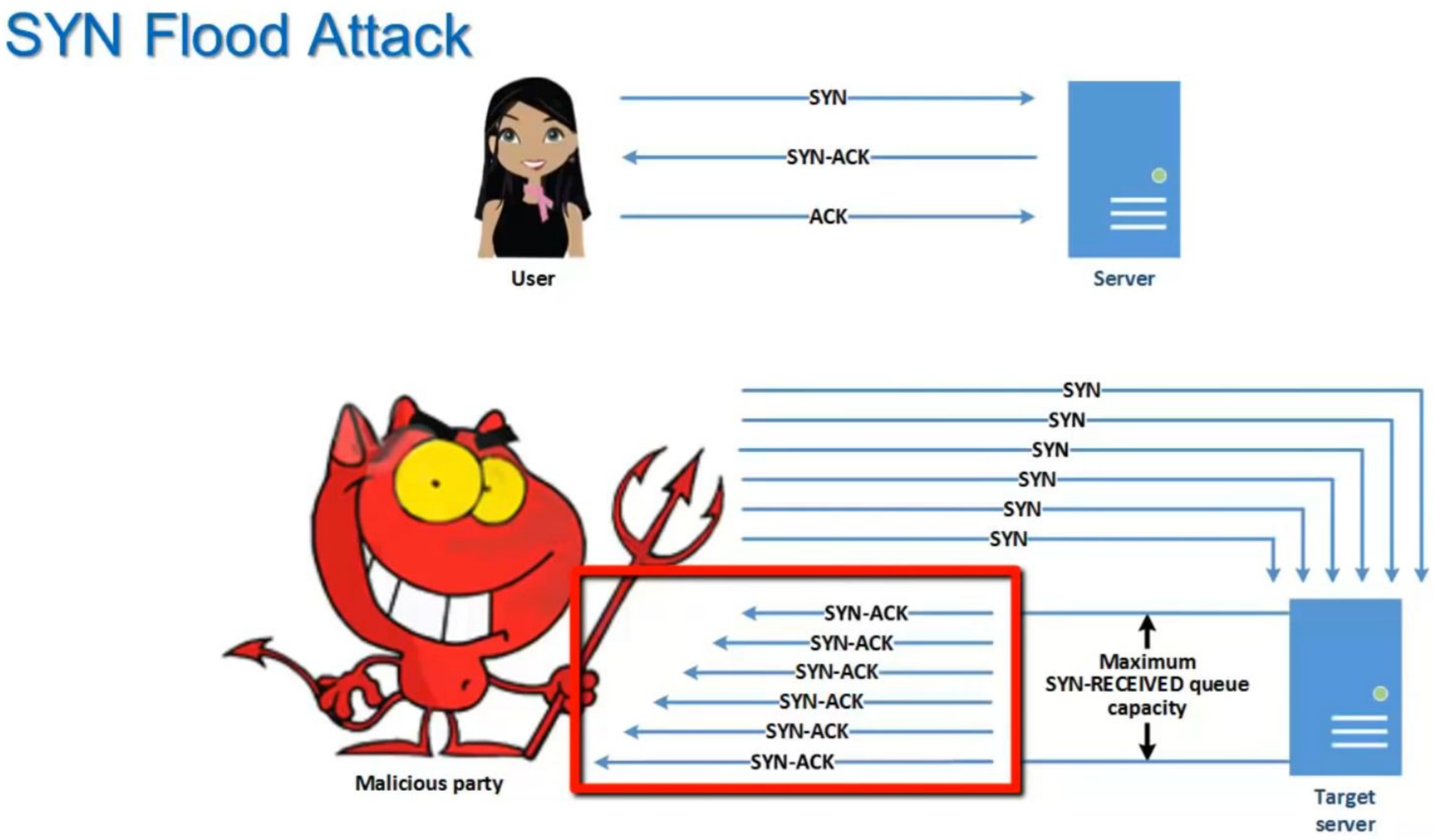


SYN FLOOD ATTACK

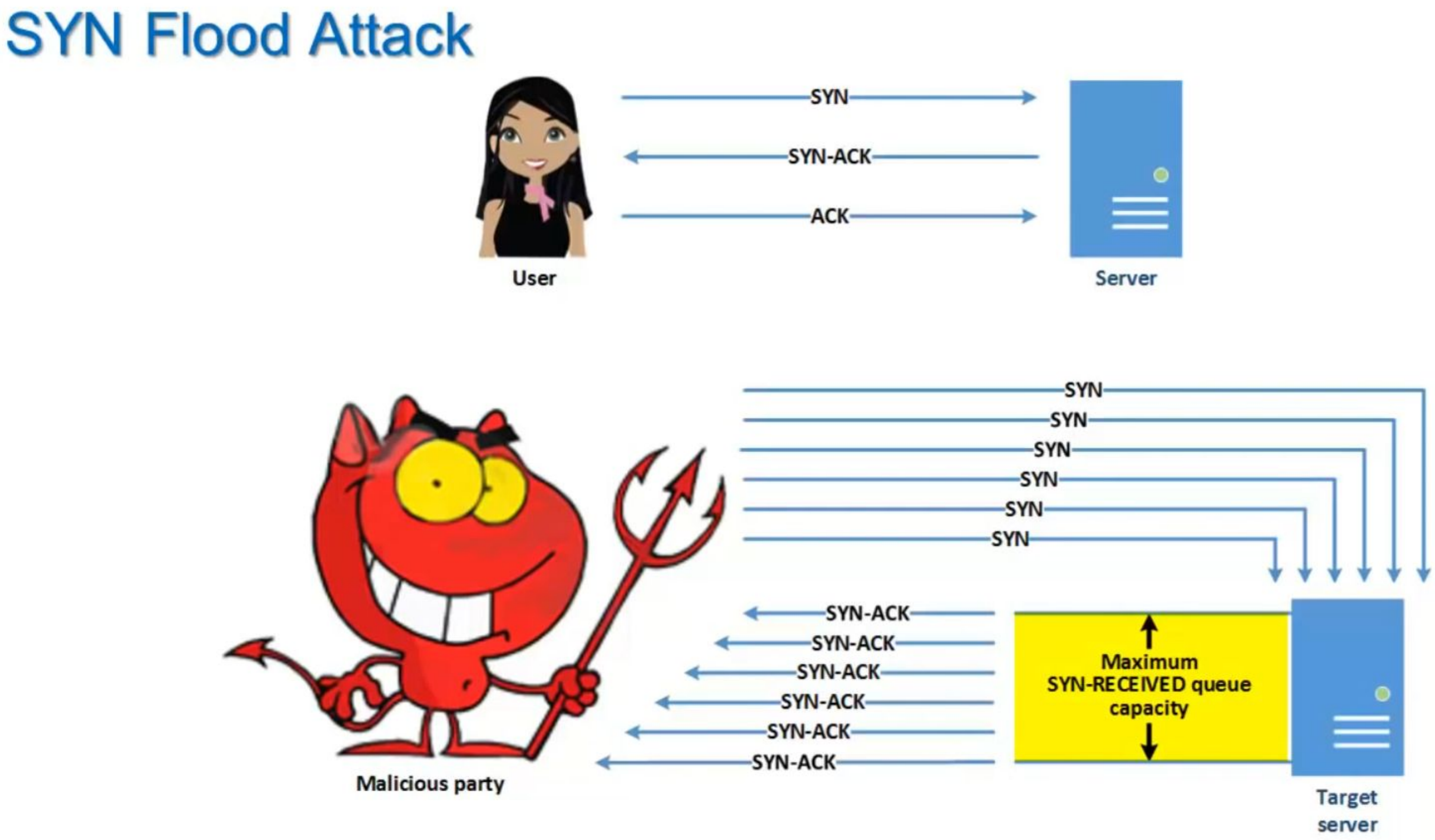


SYN Flood Attack

SYN FLOOD ATTACK

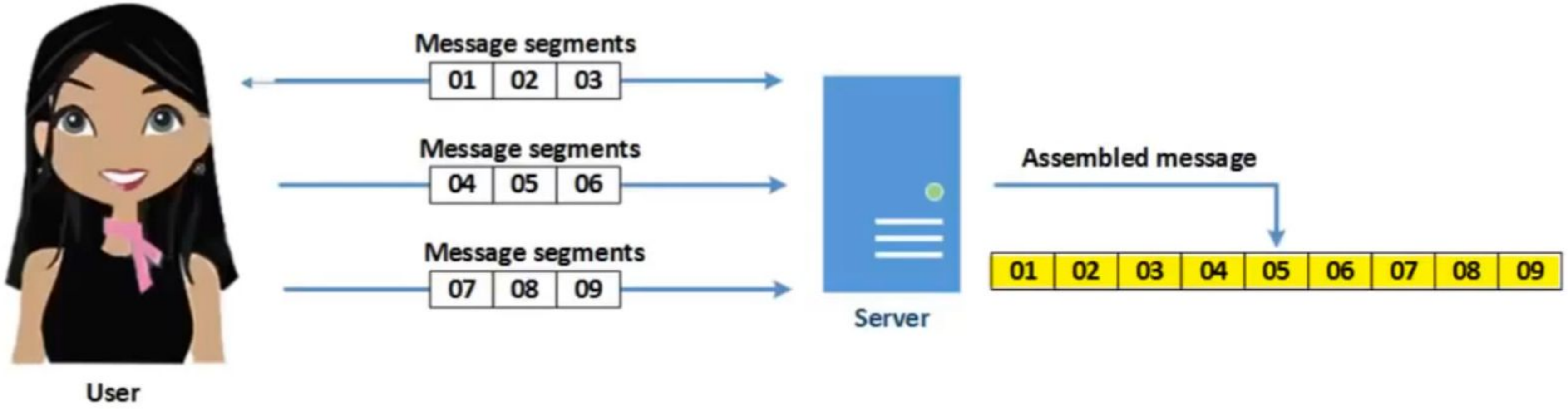


SYN FLOOD ATTACK



NETWORK COMMUNICATION

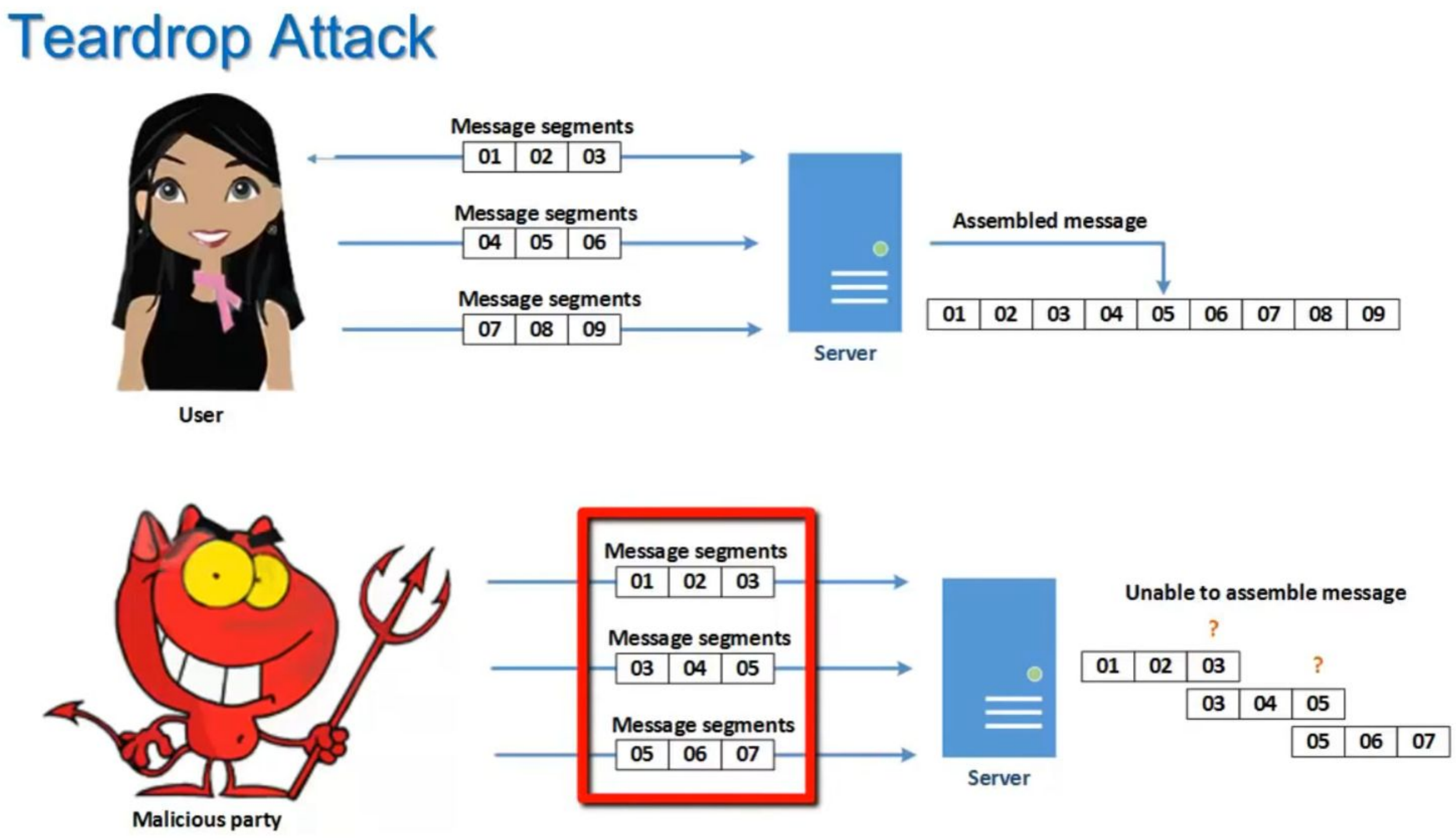
- In ordinary network communication across the internet messages between users and servers are broken apart into segment of various length which are sent independently over the network.
- Due to the network, segments arrive out of order.
- Therefore the server must hold income segment until they all arrive after which the message can be reassembled.



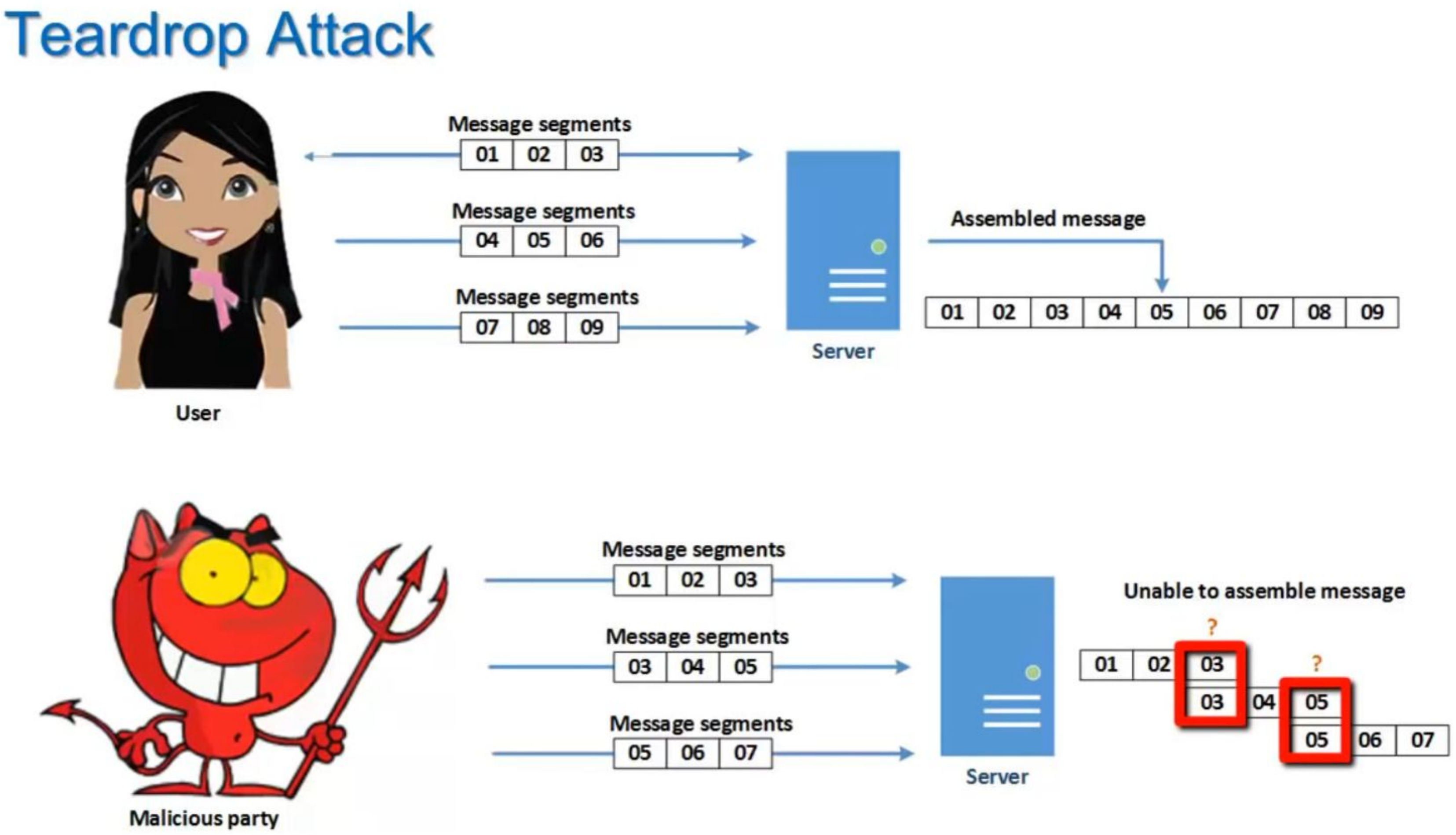
TEARDROP ATTACK

- An attacker manipulates the segment of the message in way that they overlap.
- When the manipulated segment arrives at the target server, the server is confused because the situation is out of control and it cannot find a way of reassembling the incoming message.
- If the server is not intentionally designed to handle the situation, the tear drop attack can cause the server to crash.
- Therefore disrupting legitimate user from accessing the server

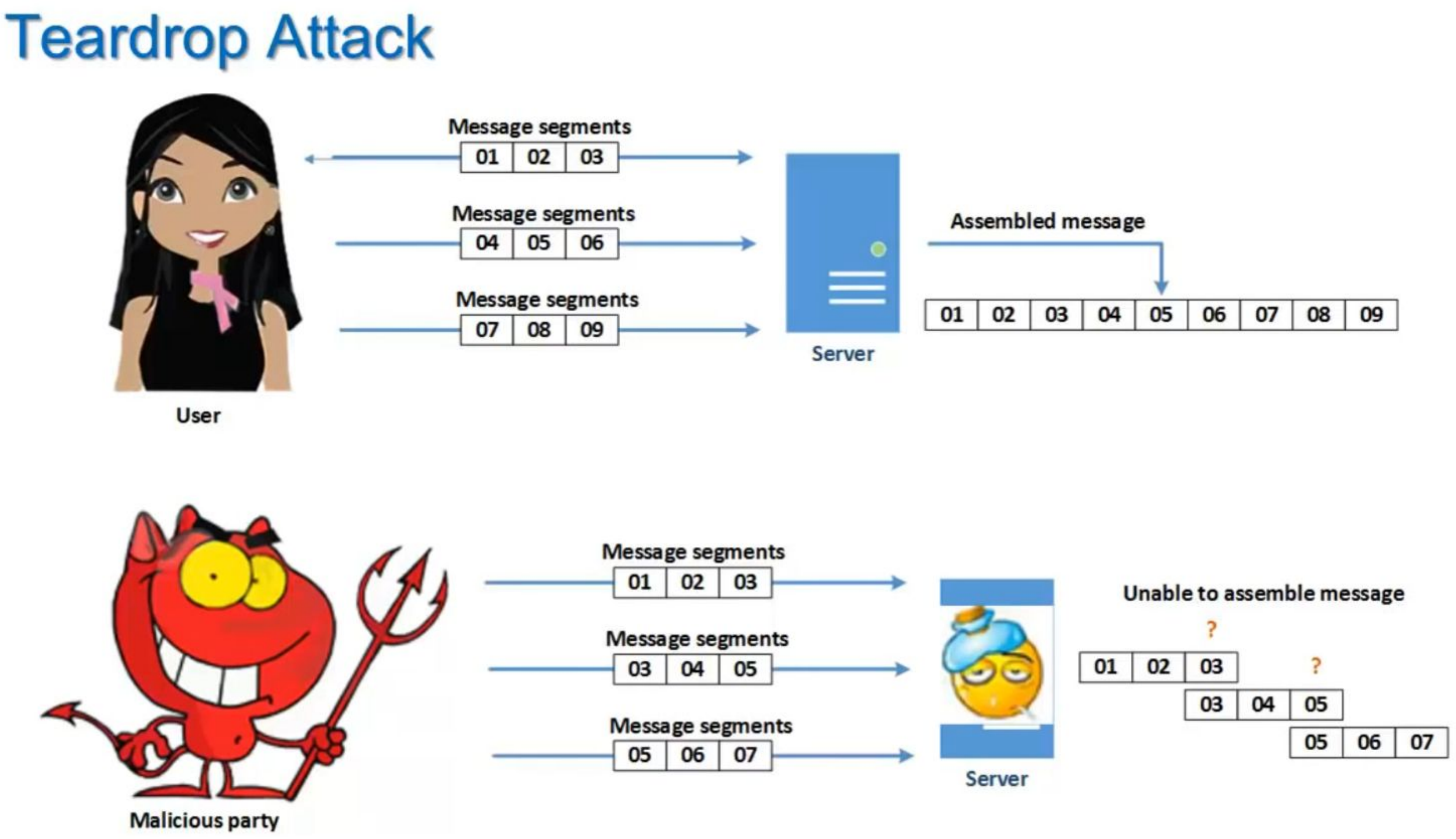
TEARDROP ATTACK



TEARDROP ATTACK



TEARDROP ATTACK



END

THANK YOU