

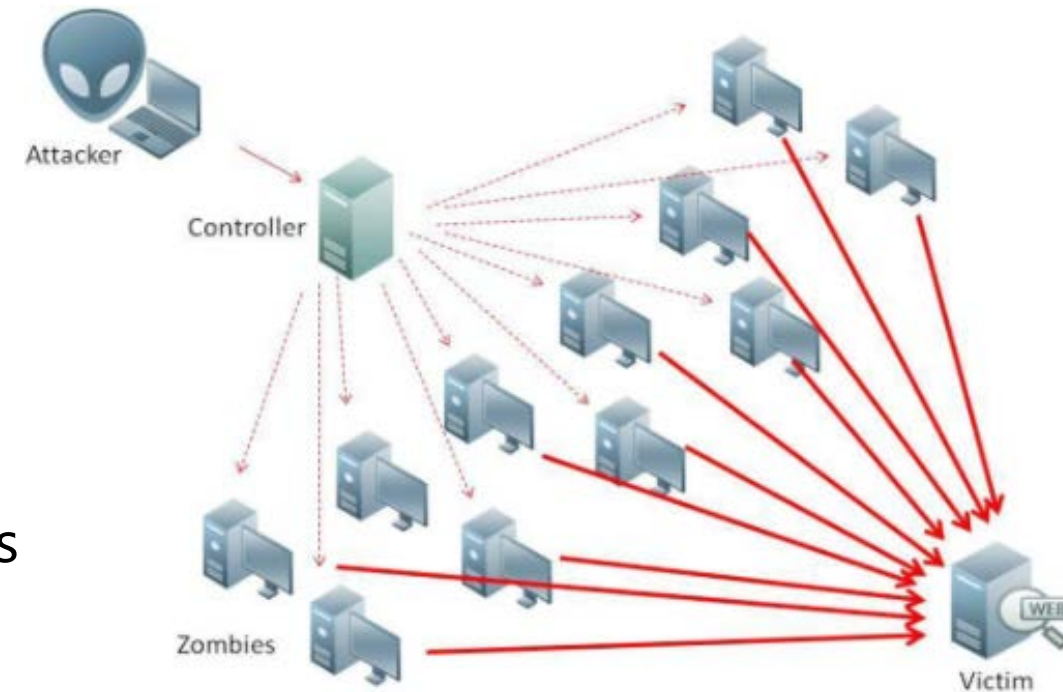
# Bots and botnets (DDOS Attack)

Dr. Shahzada Khurram

# Security Attacks

## Bots and botnets (short for robot):

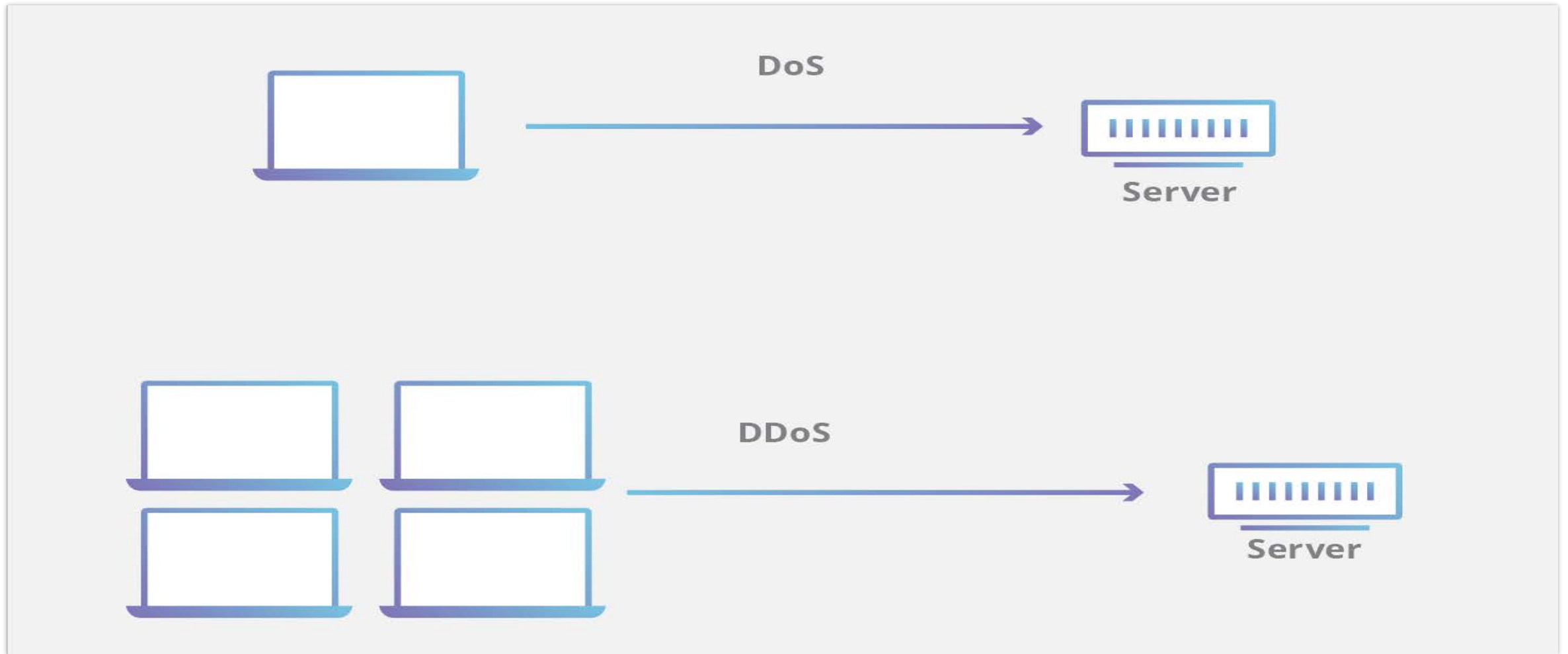
- Bots are a system with malware controlled by a botnet.
  - The system is compromised by an attack or the user installing a remote access trojan (game or application with a hidden payload).
  - They often use IRC, HTTP or HTTPS.
  - Some are dormant until activated.
  - Others are actively sending data from the system (Credit card/bank information for instance).
  - Active bots can also be used to send spam emails.
- **Botnets** is a C&C (Command and Control) network, controlled by people (bot-herders).
  - There can often be 1,000's or even 100,000's of bots in a botnet.



DDOS Attack

# DoS Attack

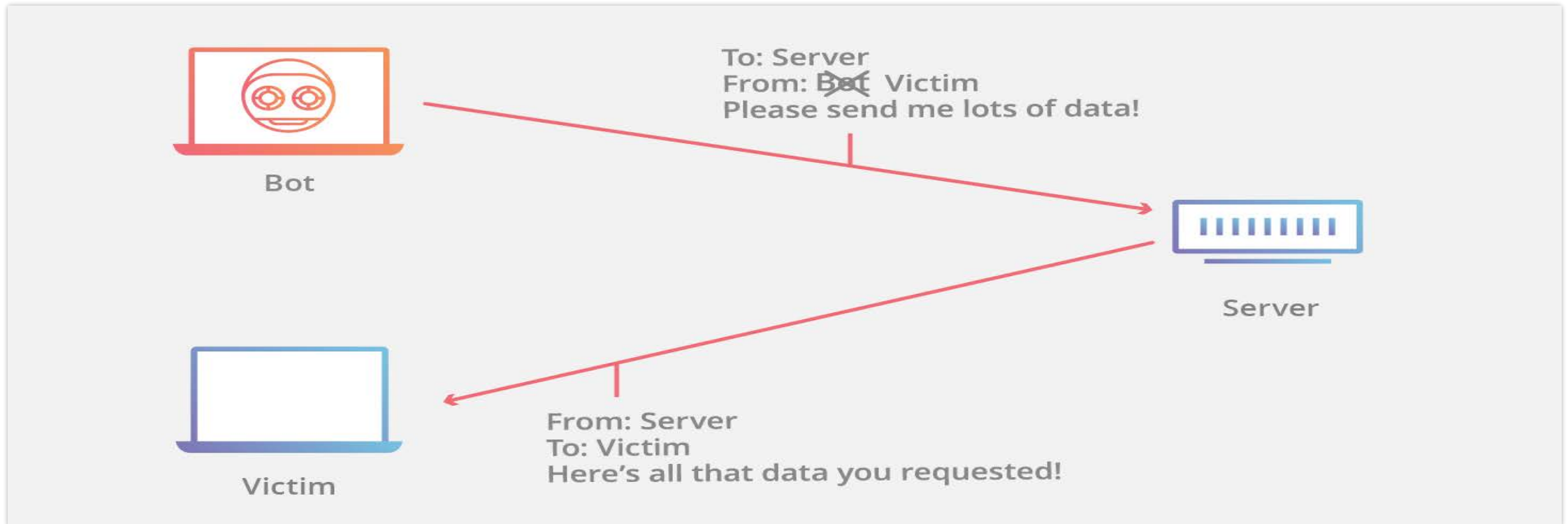
The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests



# IP spoofing

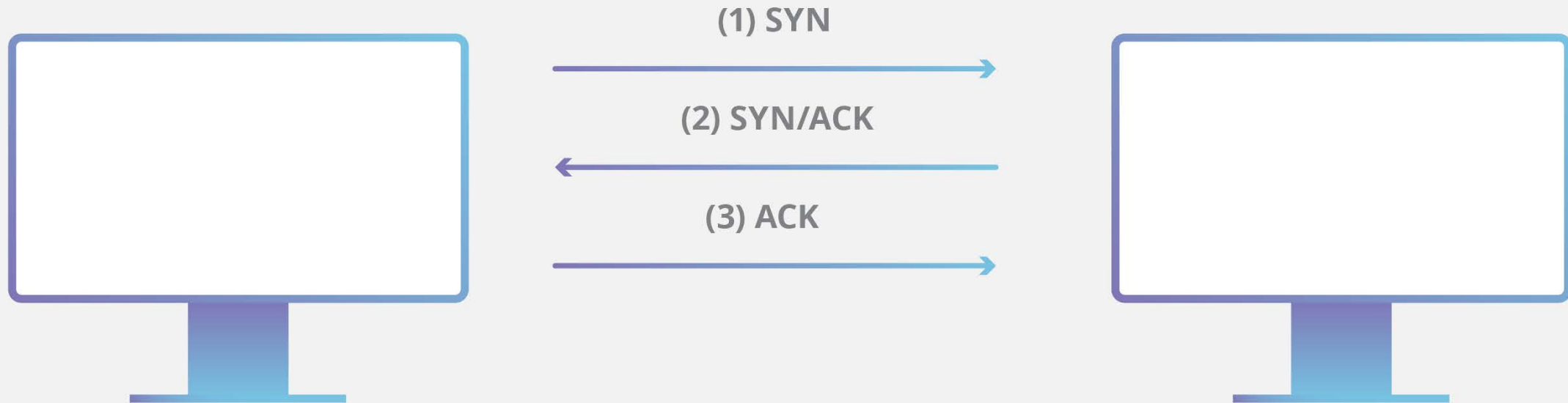
IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender. It is a technique often used by bad actors to invoke DDOS attack against a target device or the surrounding infrastructure.

In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.



# SYN Flood

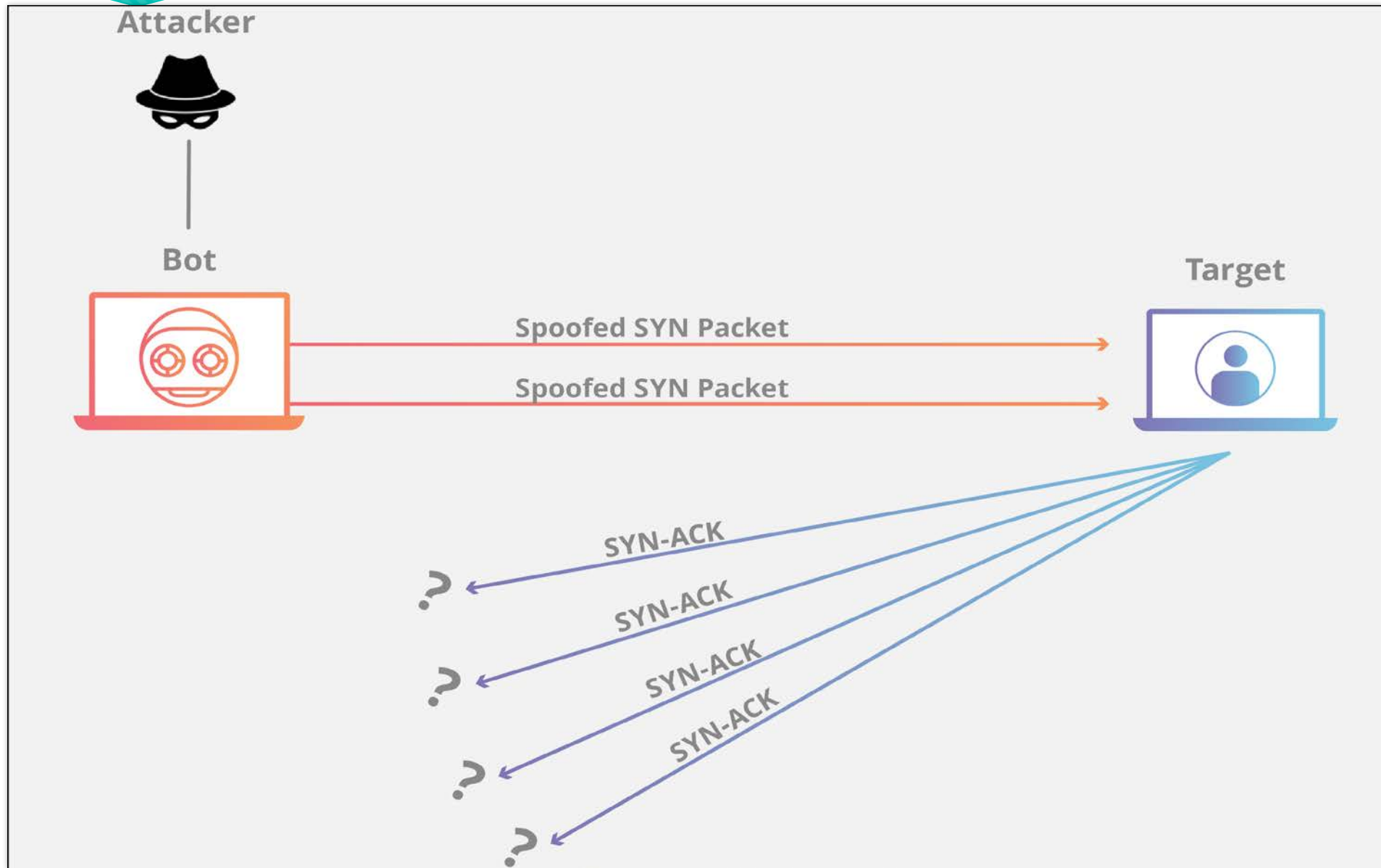
## THREE - WAY HANDSHAKE (TCP)

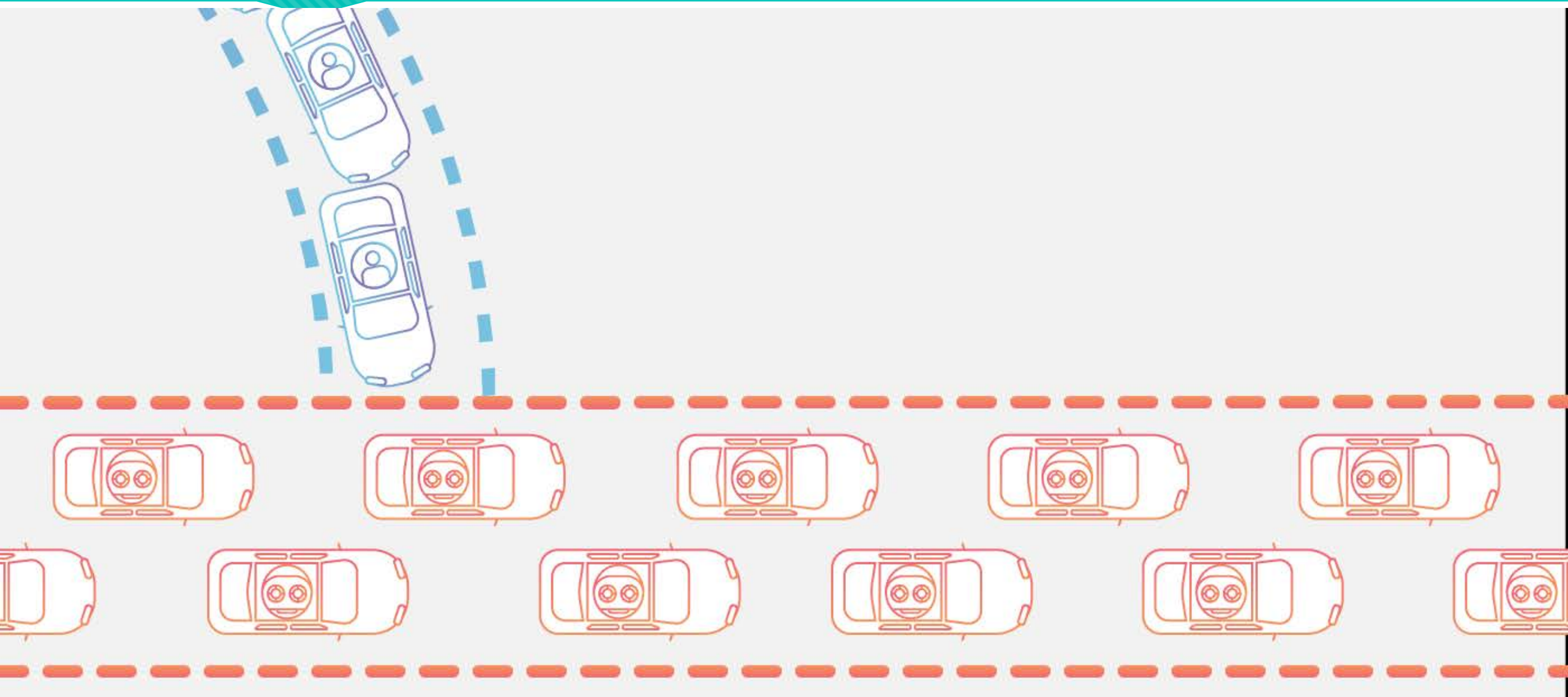
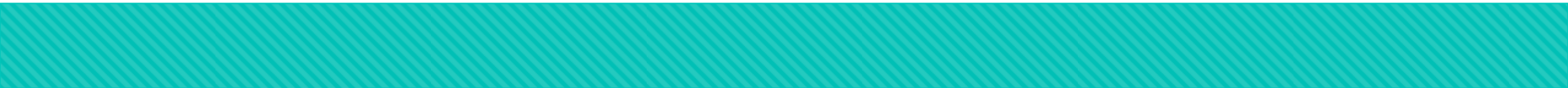


SYN = SYNCHRONIZATION

ACK = ACKNOWLEDGEMENT

# SYN Flood







Thank you