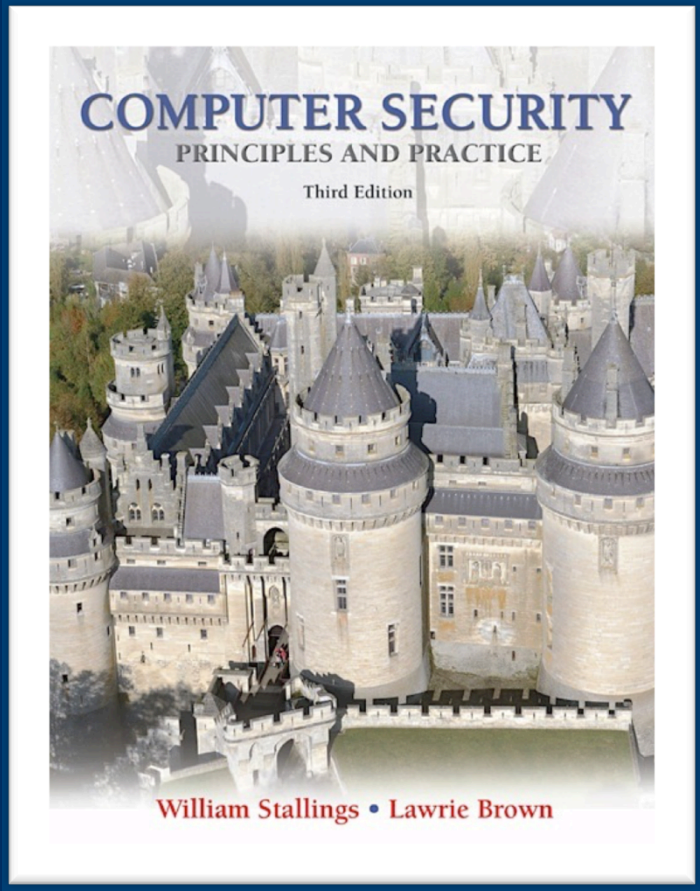
Lecture 17
Denial of Service Attacks



modified from slides of Lawrie Brown

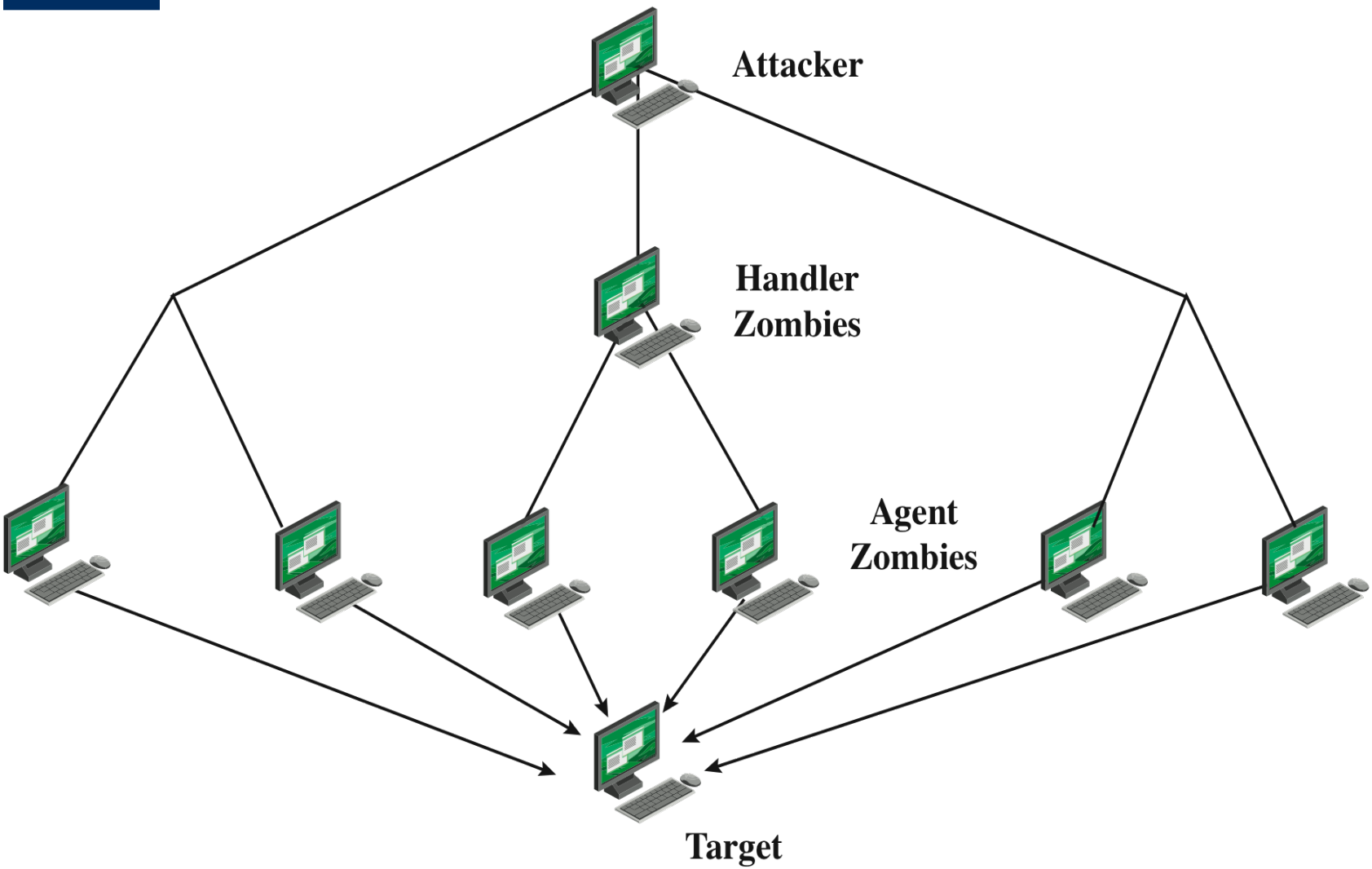
Distributed Denial of Service (DDoS) Attacks

- The attack source is more than one-and often thousands of unique IP addresses
- Use of multiple systems to generate attacks
- Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)
  - Backdoor program

Distributed Denial of Service (DDoS) Attacks

- Botnet
  - robot+network—a number of Internet-connected computers communicating with other similar machines in an effort to complete certain tasks
  - Large collections of such systems under the control of one attacker's control can be created
- Botnet is a powerful tool to conduct DDoS attack

DDoS Attack Architecture



DDoS Attack Architecture

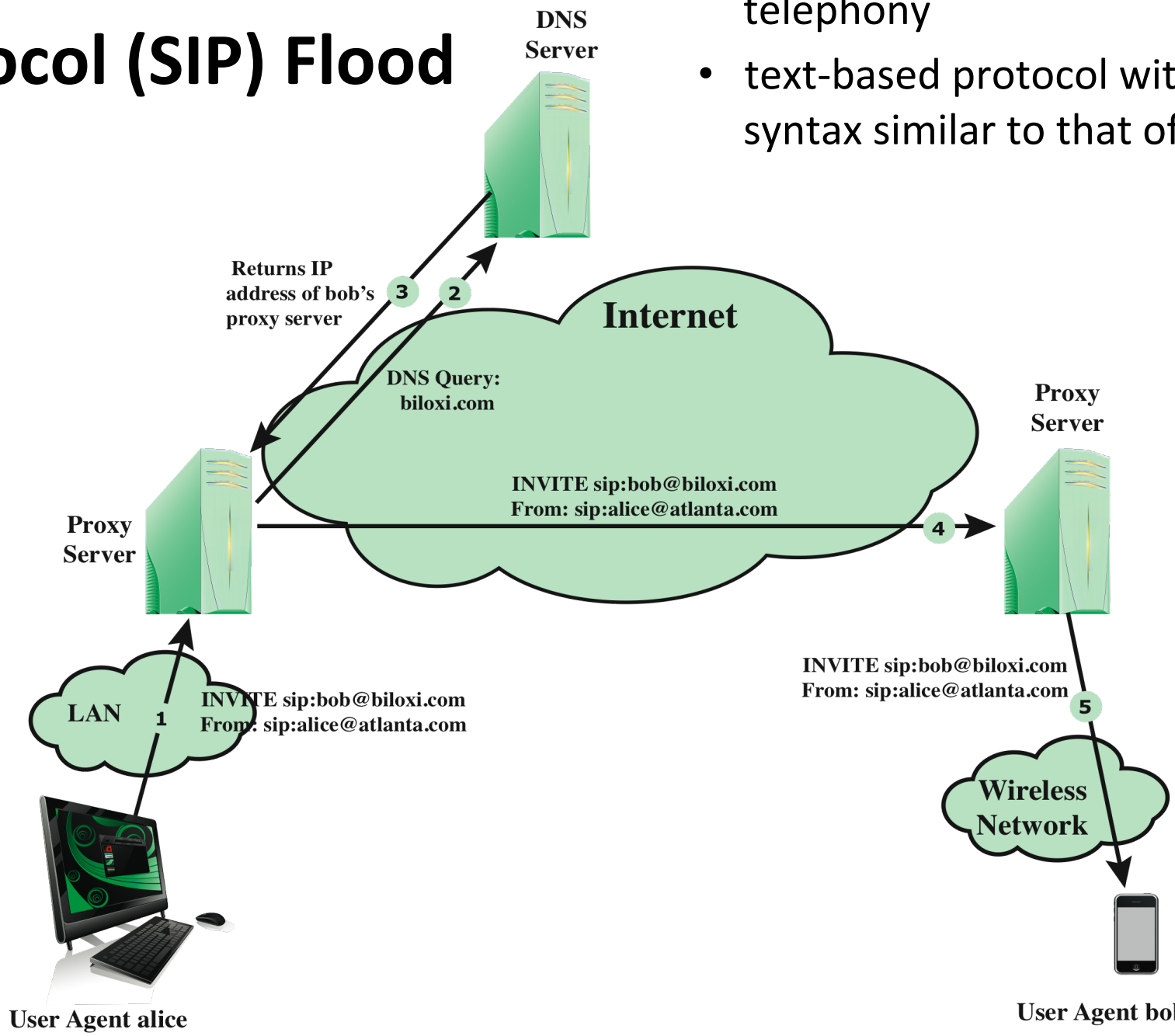
- **Advantage of hierarchical DDoS attack structure**
  - The attacker can send a single command to a handler, which then automatically forwards it to all the agents under its control
  - Lower physical capacity requirement
  - More difficult to identify the attacker

Application-based Bandwidth Attack

- To force the target to execute resource-consuming operations
- Two protocols for this kind of attack
  - SIP flood
  - HTTP based attack

Session Initiation Protocol (SIP) Flood

- standard protocol for VoIP telephony
- text-based protocol with a syntax similar to that of HTTP



SIP Flood

- A single INVITE request triggers considerable resource consumption
- The attacker can flood a SIP proxy with numerous INVITE requests with spoofed IP addresses
  - The proxy server resources are depleted in processing the INVITE requests
  - The server's network capacity is consumed

HTTP based Attack-Slowlories

- A common server uses multiple threads to support multiple requests to the same server application
- Basic idea
  - It consumes all of the available request handling threads on the Web server by sending HTTP requests that never complete
  - Since each request consumes a thread, the Slowloris attack eventually consumes all of the Web server's connection capacity, effectively denying access to legitimate users

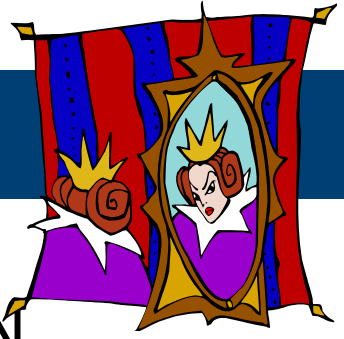
Countermeasures of Slowlories

- Limit the rate of incoming connections from a particular host
- Adjust the timeout on connections as a function of the number of connections

Reflection Attacks

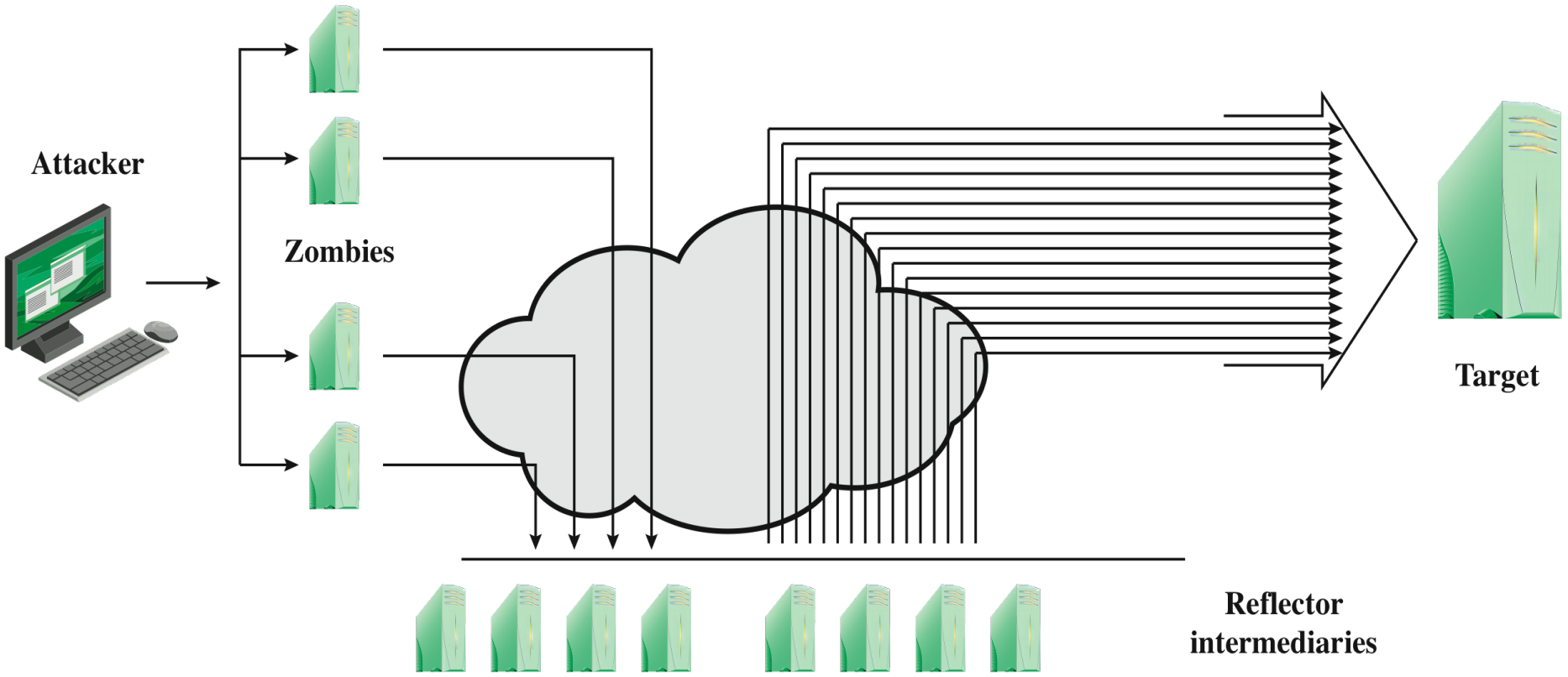
- attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- when intermediary responds, the response is sent to the target
- goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary

Reflection Attacks



- How to design reflection attack using TCP SYN packets?
  - a number of SYN packets with spoofed source addressing to the chosen intermediaries
  - the intermediaries respond with a SYN-ACK packet to the spoofed source address, which is actually the target system

Amplification Attacks



DNS Amplification Attacks

- attacker creates a series of DNS requests containing the spoofed source address of the target system
- exploit DNS behavior to convert a small request to a much larger response (amplification)
- target is flooded with responses
- basic defense against this attack is to prevent the use of spoofed source addresses

DoS Attack Defenses

- these attacks cannot be prevented entirely
- high traffic volumes may be legitimate
  - high publicity about a specific site
  - activity on a very popular site
  - described as slashdotted, flash crowd, or flash event

Defense against DoS attacks

- attack prevention and preemption
  - before attack
- attack detection and filtering
  - during the attack
- attack source traceback and identification
  - during and after the attack
- attack reaction
  - after the attack

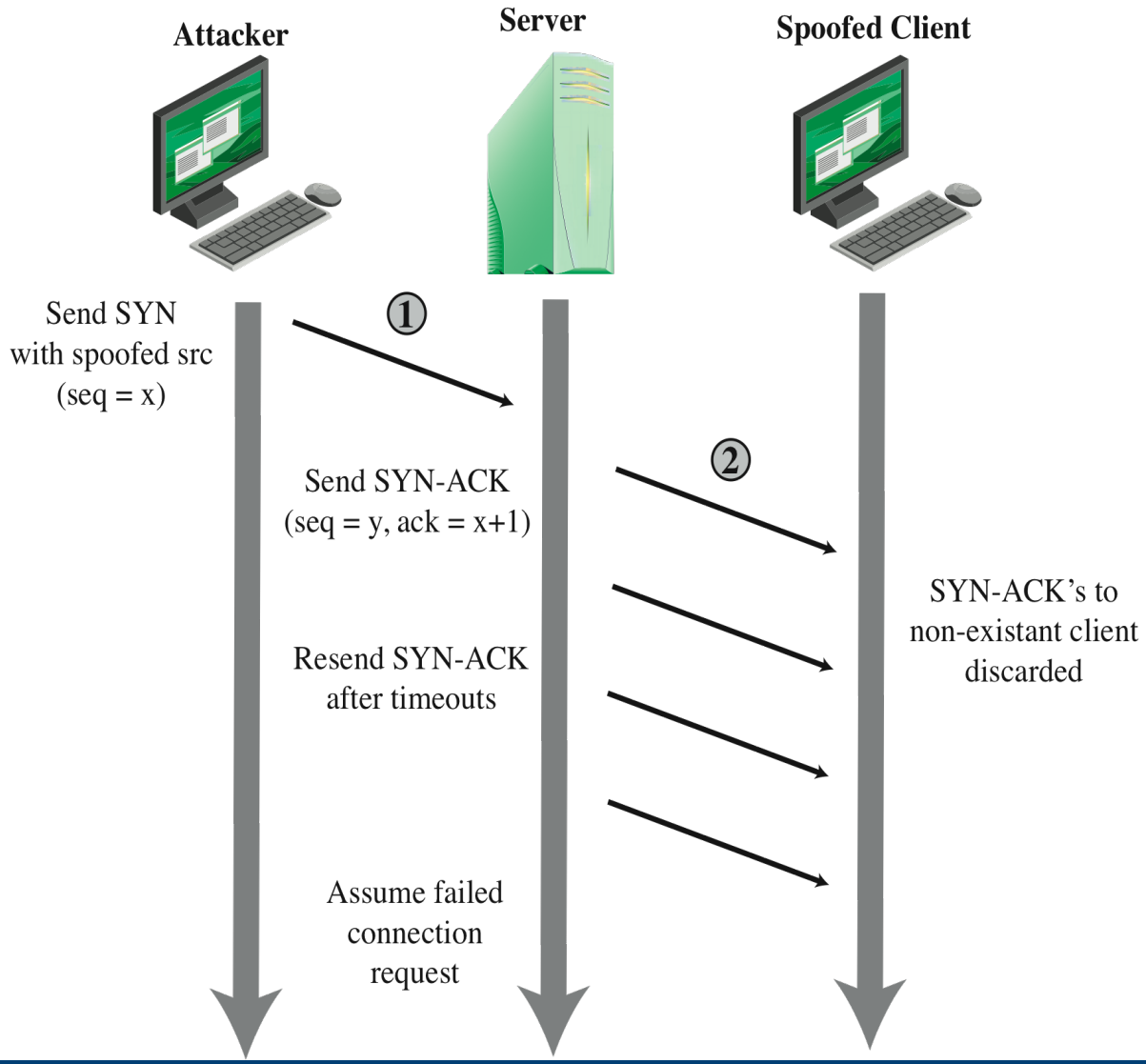
DoS Attack Prevention

- The use of spoofed source addresses
- Filter
  - As close to the source as possible
  - Routers or gateways (ISP providing the network connection for an organization or home user)
  - An ISP knows which addresses are allocated to all its customers

DoS Attack Prevention

- Defend against SYN spoofing attack
- use modified TCP connection protocol
  - The connection info is encrypted (why?) and sent to the client (rather than keeping in the server) in SYN-ACK (cookie)
  - The connection info is sent back to the server in ACK

TCP SYN Spoofing Attack



DoS Attack Prevention

- It has the advantage of not consuming any memory resources at the server
- Disadvantages
  - It takes computation resources at the server to obtain the encrypted information
  - Since the cookie size is limited, full connection information cannot be maintained