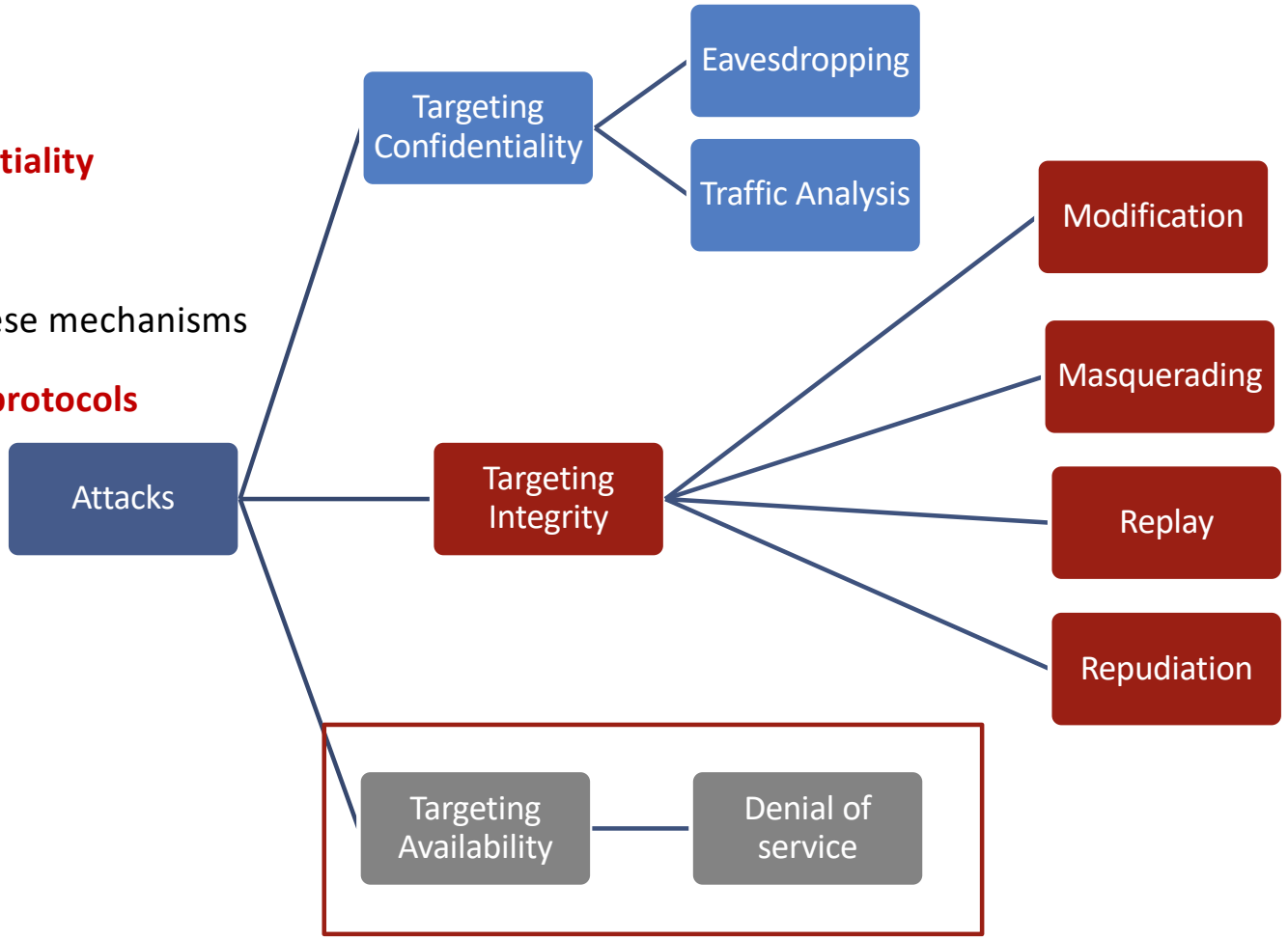
IT-Security

Chapter 8: Denial-of-Services Attacks

Prof. Dr.-Ing. Ulrike Meyer

Overall Lecture Context

- **So far, we focused on**
  - Mechanisms to **protect confidentiality**
  - Mechanisms to **protect Integrity**
  - **Key distribution** methods for these mechanisms
  - Using them to **protect network protocols**
    - on IP, TCP, and application layer
- **Not covered yet**
  - **Availability**



Overview

- **Definition of Denial-of-Service Attacks**
- **Types of attacks and simple examples targeting**
  - Network bandwidth
  - System resources
  - Application resources

- **DoS Defenses**
  - Incident response cycle
  - Examples for preventive measures

- **More Advanced Techniques**
  - Source address spoofing
  - DDoS with compromised machines
  - Reflection Attacks
    - Basic principle
    - Amplification attacks as subtype of reflection attacks

Definition and Classification

Definition

A **denial of service** (DoS) is an action that prevents or impairs the authorized use of networks, systems, or applications by **exhausting resources** such as central processing units, bandwidth, and disk space.

Classification according to type of resources targeted

Network Bandwidth

- Targets **capacity** of network link connecting victim server to the Internet

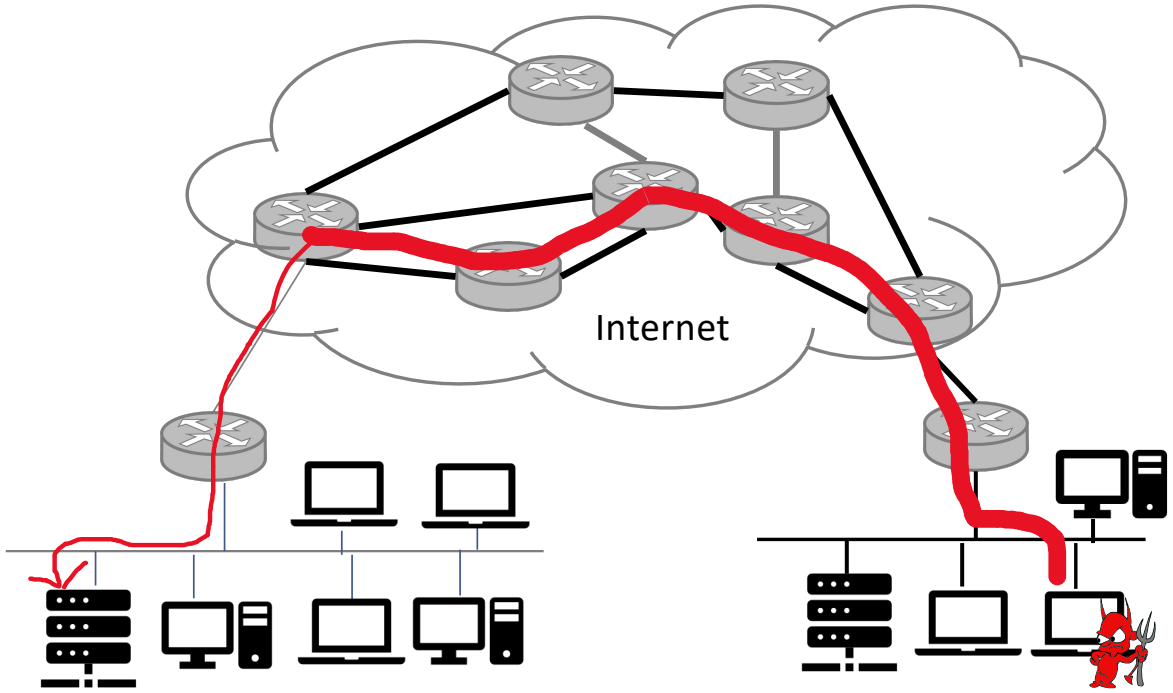
System Resources

- Targets **overloading** or **crashing** network handling software of the OS installed on the victim machine

Application Resources

- Targets a **specific application** such as a Web server or a DNS Server and overloads it with many resource consuming valid-looking requests

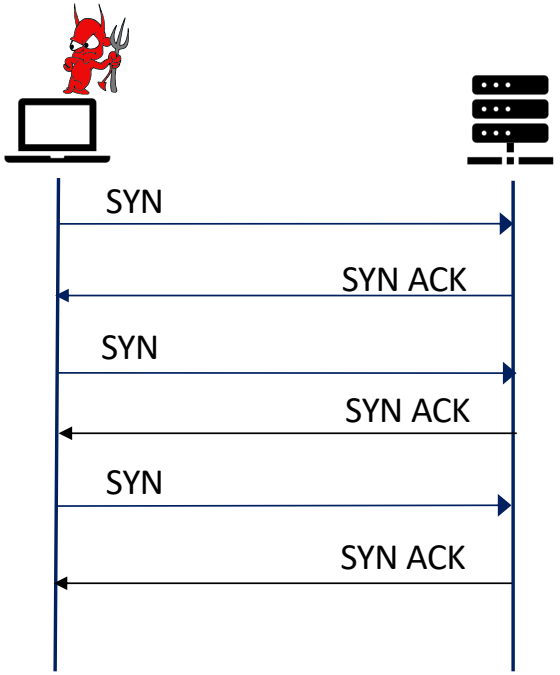
Example: Classic Flooding Attack targeting Network Capacity



- Attacker floods target network with requests
  - E.g., ICMP echo requests aka ”ping”
- Router connecting target network to the ISP starts dropping IP packets
- Consequently, legitimate packets are dropped as well
- Works well if attacker’s connection has higher bandwidth than target’s

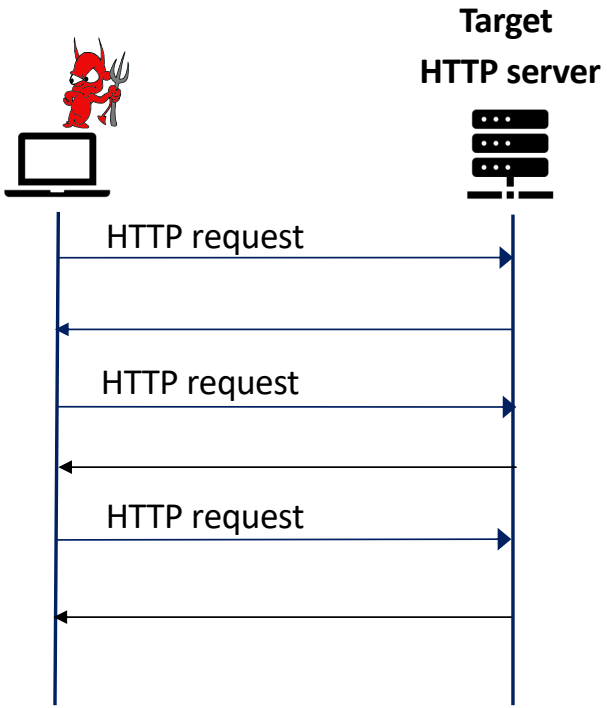
Example: Classic SYN Flooding Attack targeting System Resources

- **Targets system resources of a target server**
  - Namely, table of open TCP connections
- **Flood server with TCP SYN messages**
  - Fills up table of open TCP connections
- **Future request from legitimate users fail**
  - Server unavailable for legitimate requests



Example: HTTP Flood targeting Application Resources

- **Bombard web server with HTTP requests**
- **Request crafted to consume considerable resources**
  - E.g., request to download a large file from the target
    - Causes the web server to read the file from hard disk
    - Store it in memory
    - Convert it into a packet stream
    - Transmit the packets
    - Thus, consumes memory, processing, and transmission resources
  - Another example: recursive HTTP flood
    - Attacker starts from a given HTTP link to the server, then follows all links on the provided website recursively
    - Also called spidering



Overview

- **Definition of Denial-of-Service Attacks**
- **Types of attacks and simple examples targeting**
  - Network bandwidth
  - System resources
  - Application resources

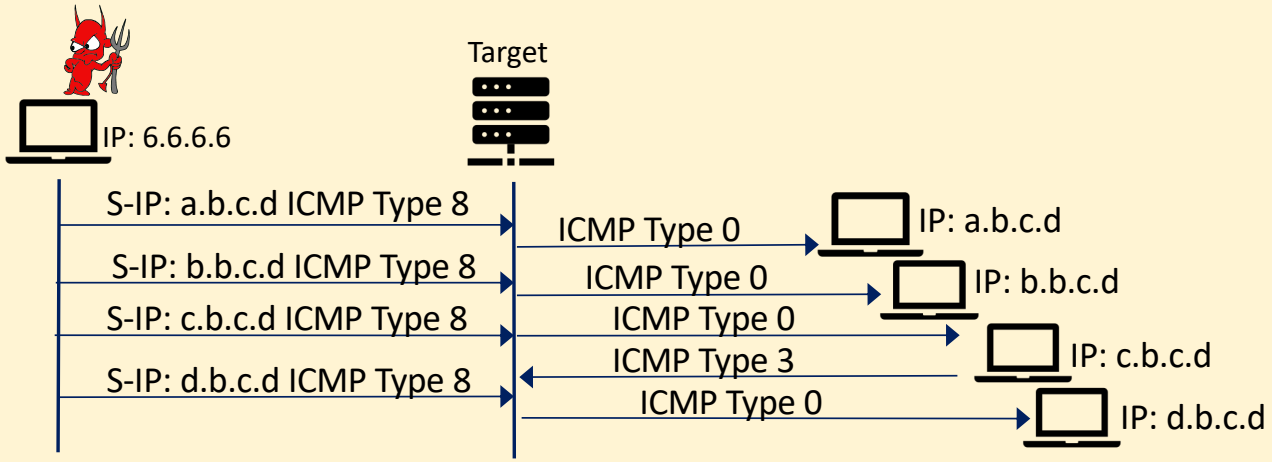
- **DoS Defenses**
  - Incident response cycle
  - Examples for preventive measures

- **More Advanced Techniques**
  - Source address spoofing
  - DDoS with compromised machines
  - Reflection Attacks
    - Basic principle
    - Amplification attacks as subtype of reflection attacks

Source Address Spoofing Directly

- **Attack from single IP can easily be blocked**
- **Attackers often use spoofed IP addresses**
  - Attacker will not be hit by the responses!

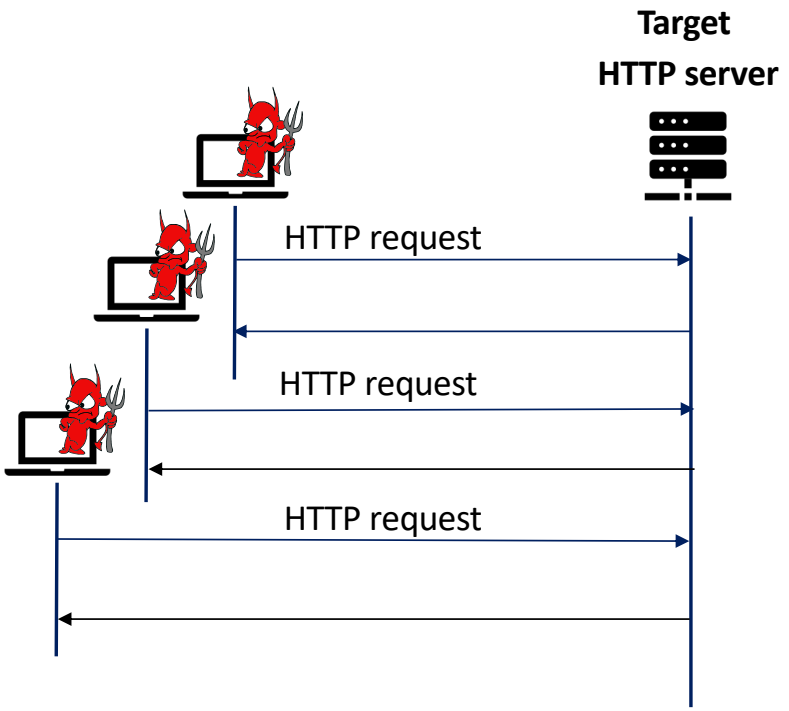
ICMP-food with IP address spoofing



- **Thwarting spoofing**
  - Block packets with topologically invalid IP
  - Needs to be applied close to the on on the subnet the attacker acts from
  - Unfortunately, there are still ISPs that do not implement such filtering
    - Too costly?

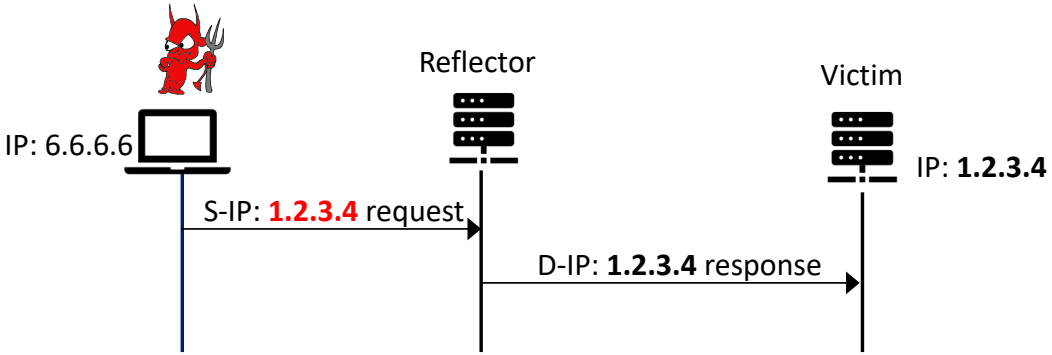
Distributed Denial of Service Attacks

- Also known as **DDoS** attacks
- Attacker makes many compromised devices send requests to the target
  - Compromised machines often infected with a bot malware
  - Remotely controllable by the attacker
  - May attack multiple targets over time
  - Owners of compromised devices unaware of the fact that their devices participate in attacks



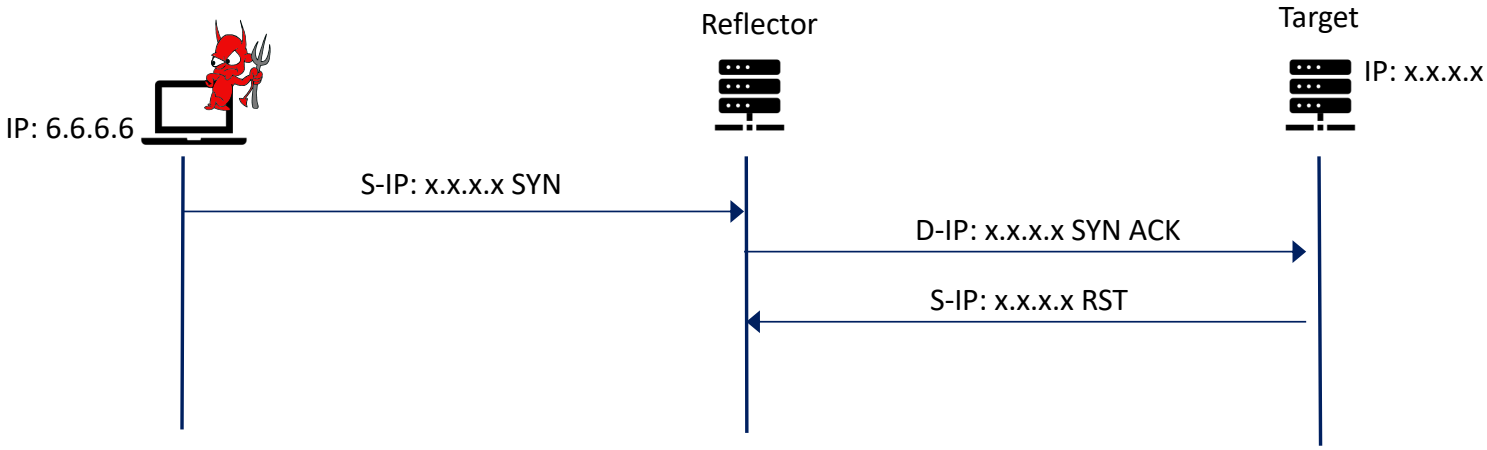
Principle of Reflection Attacks

- **Spoof source address to victim's address in requests sent to multiple reflectors**
- **Overwhelm victim with replies sent out by the reflectors to these faked requests**
- **Reflectors attack the victim, not the attacker himself**
  - Each reflector may see only one request -> not suspicious
  - Victim is hit by lots of unsolicited responses



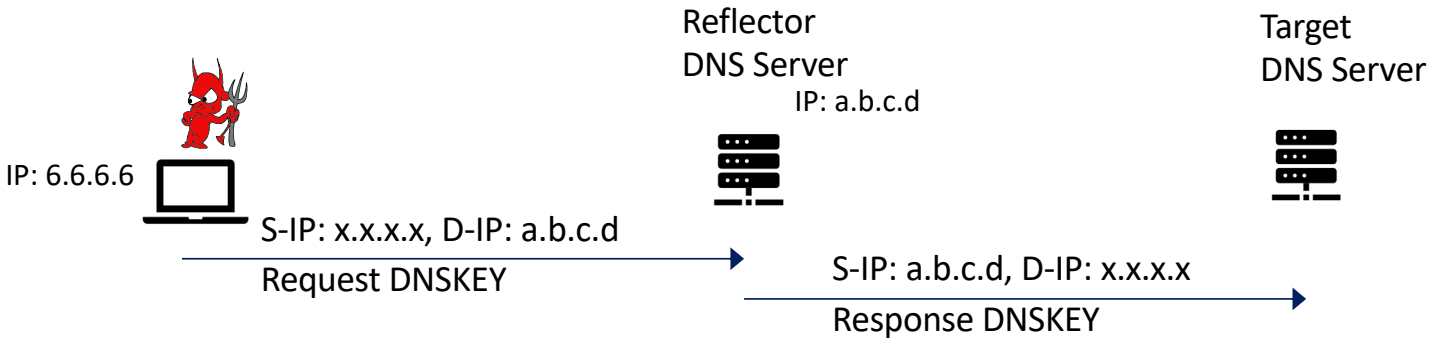
Reflection Attack

- **Simple example: SYN/ACK flooding attack using reflection**
  - Attacker sends SYN to refelctors using the target‘s IP address as source address
  - Refectors respond to target with SYN ACK
  - Target is flooded with unsolicited SYN ACKs send by many reflectors



Amplification Attacks

- **Variant of reflection attacks**
  - Each original packet sent by the attacker generates multiple or large response packets sent to the target
- **Example DNS amplification attack**
  - Uses DNS servers as reflectors
  - Attacker sends fake DNS requests to reflectors spoofing the target DNS servers IP
  - Small DNS requests may lead to huge responses especially due to DNSSec
    - DNSKEY RRs ware particularly large



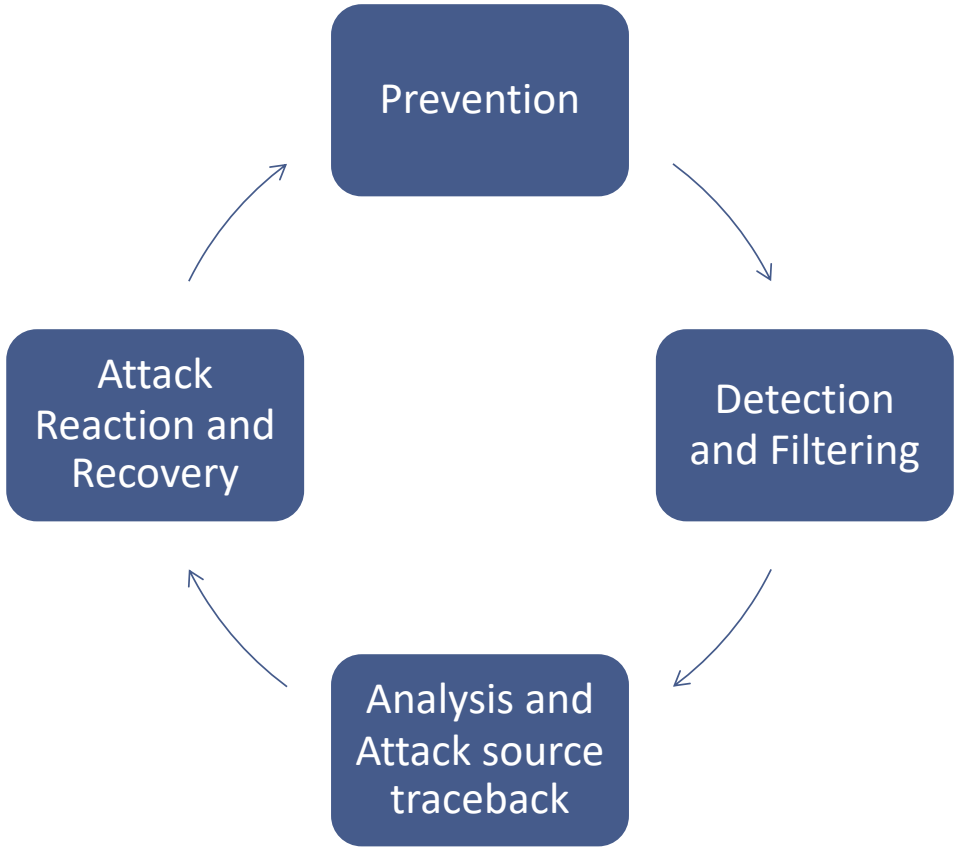
Overview

- **Definition of Denial-of-Service Attacks**
- **Types of attacks and simple examples targeting**
  - Network bandwidth
  - System resources
  - Application resources
- **DoS Defenses**
  - Incident response cycle
  - Examples for preventive measures
- **More Advanced Techniques**
  - Source address spoofing
  - DDoS with compromised machines
  - Reflection Attacks
    - Basic principle
    - Amplification attacks as subtype of reflection attacks

Defense Against DoS Attacks

Incident response cycle for DoS attacks

- Take measures to prevent DoS attacks
- Take measures to detect and filter DoS attacks
  - **Intrusion detection systems**
- Log traffic to analyze after or during attack
  - Can enable attack attribution
  - Can be used to derive new preventive measures
  - Can be used to generate new detection rules
- Take measures to react to and recover from attack



Examples for Preventive Measures

Protocol Design	• Modify protocols to minimize DoS potential • E.g., use cookies stored on client side instead of state kept on server side
Disable IP address spoofing	• Does not prevent attack against own infrastructure but helps others • Filter IP packets with source addresses that do not belong to subnet they egress from
Throttle specific Packets	• Throttle IP packets known to be used as part of flooding attacks • E.g., ICMP messages of type 8 (echo requests)
Lift resource limitations	• Increase the size of TCP connection tables • Modify time-out behavior of server

Summary

- **Denial of Service Attacks can target**
  - Network resources like the network bandwidth
  - System resources of the operating system of hosts
  - Application specific resources
- **Attackers try to hide their location by**
  - using spoofed source IP addresses in attack attack packets
  - using compromised machines of unsuspecting users
  - Also shield the attacker from response traffic
- **Reflection attacks allow an attacker to indirectly attack a target**
  - Attacker sends requests to reflectors with target's IP address as source
  - Reflectors then flood target with reply messages

Summary

- **An amplification attack is a special form of a reflection attack**
  - Small requests sent out by attacker on behalf of target
  - Each lead to multiple response or a single large response sent by the reflectors
  - Attack is thus amplified
- **Defenses against DoS attacks try to**
  - Prevent DoS attacks in the first place
  - At least detect DoS attack if prevention is not possible
  - Filter and block attack-related traffic
  - Log attack traffic to derive future preventive and detection measures

References

- **W. Stallings, Cryptography and Network Security: Principles and Practice, 8th edition, Pearson 2022**
  - Chapter 21: Network Endpoint Security
    - 21.4 Denial of Service Attacks