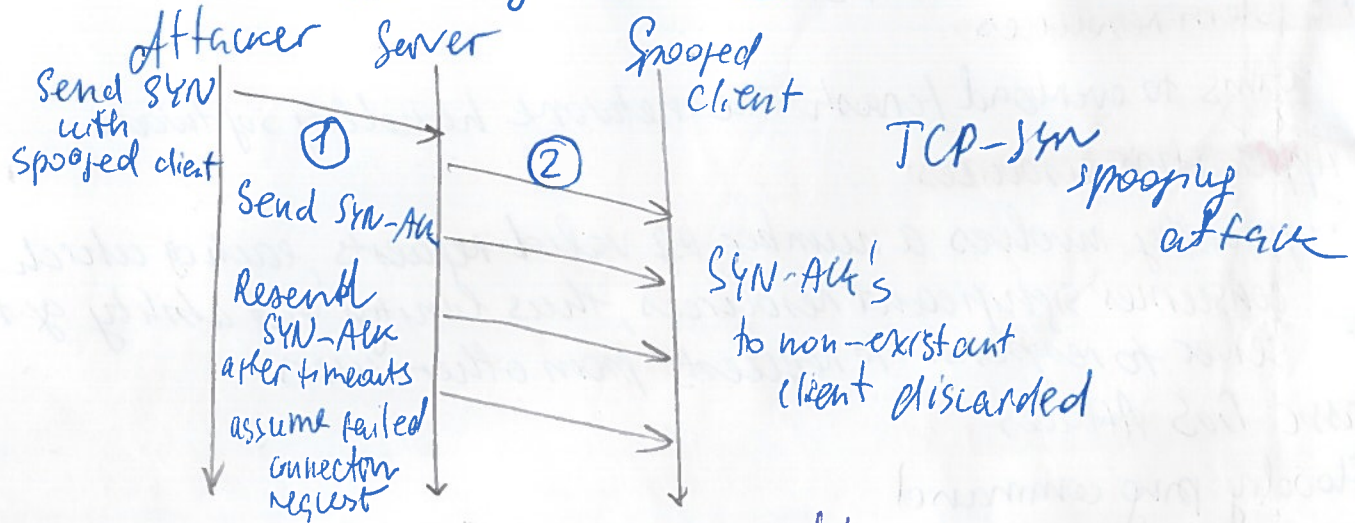
~~lecture 15~~ lecture 16

- Denial-of-Service (DoS)
  - A form of attack on the availability of some service
    - Network bandwidth
      - capacity of the network links connecting a server to the Internet or ISP
    - System resources
      - aims to overload / crash the network handling software
    - Application resources
      - typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users
  - Classic DoS Attacks
    - Flooding ping command
      - aim: overwhelm the capacity of the network connection to the target organization
      - packets are discarded as capacity decreases even when traffic by higher capacity links on the path
      - Source of the attack is clearly identified unless a spoofed address is used
      - Network performance is noticeably affected
    - Source address spoofing
      - Use forged src addr
        - usually via the raw socket interface on OS
        - makes attacking systems harder to identify
      - Attacker generates large volumes of pkts that have the target system as the dest addr
      - Congestion would result in the router connected to the final, lower capacity link
      - Requires network engineers to specifically query flow info from their routers
    - Backscatter traffic
      - Advertise routes to unused IP addr to monitor attack traffic

SYN Spoofing

system resources

- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in OS



TCP-SYN spoofing attack

Flooding Attacks

system network bandwidth

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used

ICMP Flood

- Ping flood using ICMP echo request packets
- Traditionally network admins allow such packets because ping is useful network diagnostic tool

UDP Flood

- Uses UDP packets directed to some port number on the target system

TCP SYN Flood

- Sends TCP packets to the target system
- Total volume of packets is the aim of the attack rather than the system code

Distributed DoS (DDoS)

- Use of multiple systems to generate attacks
- Attacker uses a flaw in OS/App to gain access and installs their program on it (zombie)
- Large collections of such systems under the attacker's control can be created, forming botnet

HTTP Based Attacks

HTTP Flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources system resources
- Spidering!
  - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

Slowloris

- Attempts to monopolize by sending HTTP requests that never complete
- Eventually consumes Web server's connection capacity network bandwidth
- Utilizes legitimate HTTP traffic
- Generally not recognizable

Reflection Attacks

Attacker sends packets to a known service on the intermediary with a spoofed src addr of the actual target system

When intermediary responds, the response is sent to target

"Reflects" the attack off the intermediary

Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary

Basic defense: block spoofed-src packets

DNS Amplification Attacks

- Use pkts directed at a legitimate DNS server as the intermediate system
- Attacker creates a series of DNS requests containing the spoofed src addr of the target system
- Exploit DNS behaviour 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 src addr

DoS Attack Defences

- Four lines of defense against DDoS attacks
  - Before attack: Attack prevention and preemption
  - During attack: Attack detection and filtering
  - ~~Attack src~~ During ss after: Attack src traceback and identification
  - After: Attack reaction
- Cannot be prevented entirely
- High traffic volumes may be legimate
  - High publicity about specific site
  - Activity on a very popular site
  - Described as slashdotted, flash crowd, or flash event

DoS Attack Prevention

Block spoofed src addr
- On routers as close to src as possible

Filters may be used to ensure path back to the claimed src addr is the one being used by the current pkt
- Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network

Use modified TCP connection handeling code
- Cryptographically encode critical information in a cookie
- Sent as the server's initial seq num
  - ~~Big~~ Legitimate client responds with an ACK pkt containing incr seq num cookie
- Drop an entry for an incomplete connection from the TCP connections table when it overflows

---

Block IP ~~addr~~ directed broadcasts

Block suspicious services and combinations

Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests

Good general system security practices

Use mirrored and replicated servers when high-performance and reliability is required

- Responding to DoS Attacks
  - Good Incident Response Plan
  - Identify type of attack
    - Capture and analyze pkts
    - Design filters to block attack traffic upstream
    - Or Identify and correct system/app bug
  - Have ISP trace pkt flow back to src
    - May be difficult and time consuming
    - Necessary if planning legal action
  - Implement contingency plan
    - Switch to alternate backup servers
    - Commission new servers at a new site with new addr
  - Update incident response plan
    - Analyze the attack and the response for future handling