Computer Security

Lecture 6

Denial-of-Service Attacks

Erland Jonsson
(based on material from Lawrie Brown)

Department of Computer Science and Engineering

Chalmers University of Technology

Sweden

Denial of Service

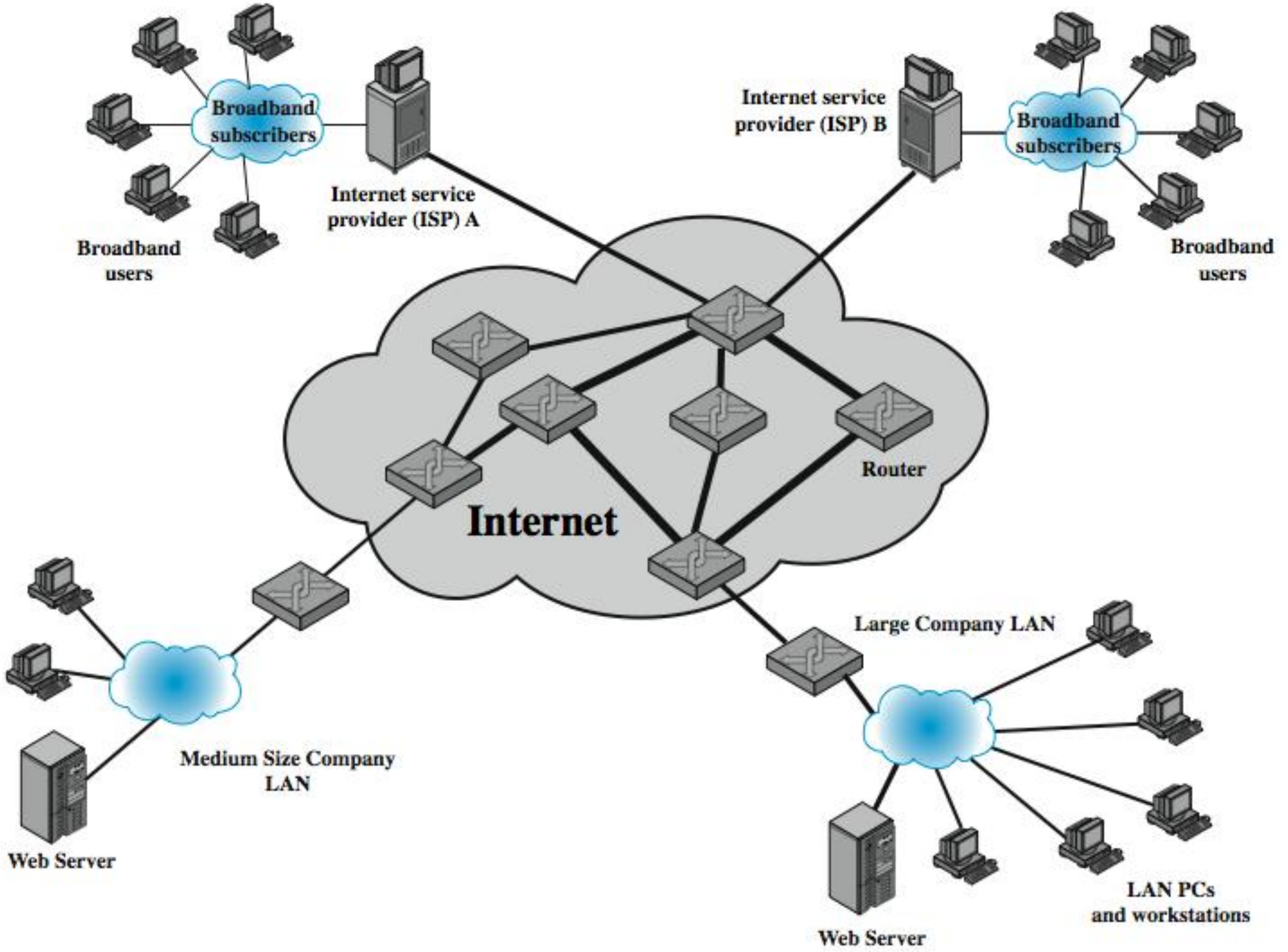
- **denial of service** (DoS) an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space
- attacks
    - network bandwidth
    - system resources
    - application resources
- have been an issue for some time
- DoS can also be accomplished by "killing" the server

Classic Denial of Service Attacks

- Flooding
  - can use simple *flooding ping*
  - from higher capacity link to lower
  - causing loss of traffic
  - source of flood traffic easily identified

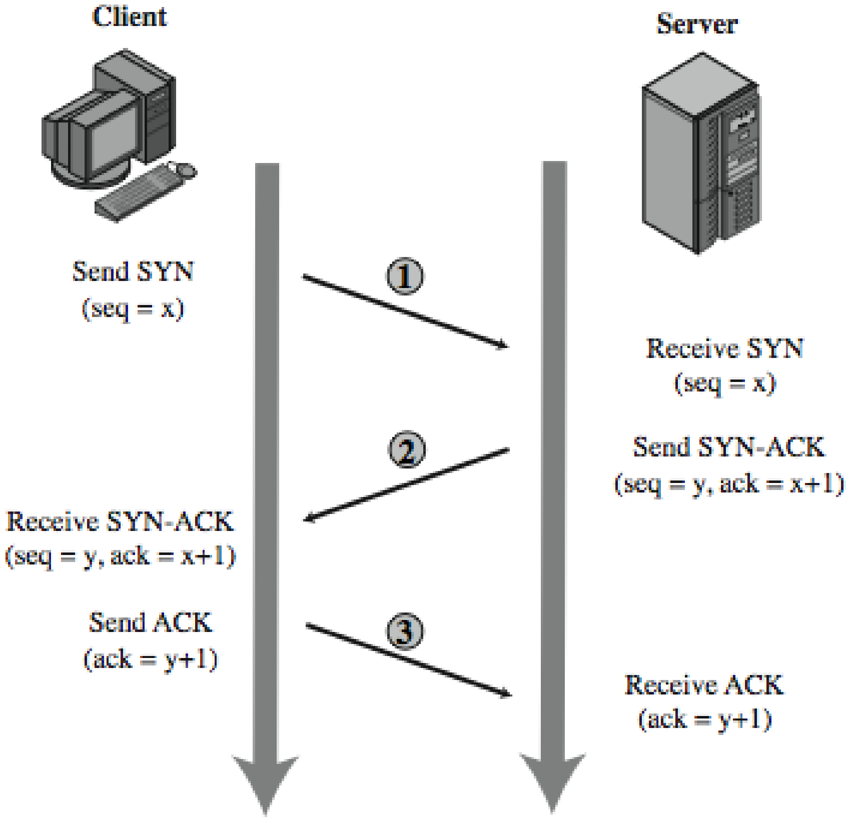
- Trigger bug in system (poison packet)
  - Ping-of-death

Classic Denial of Service Attacks

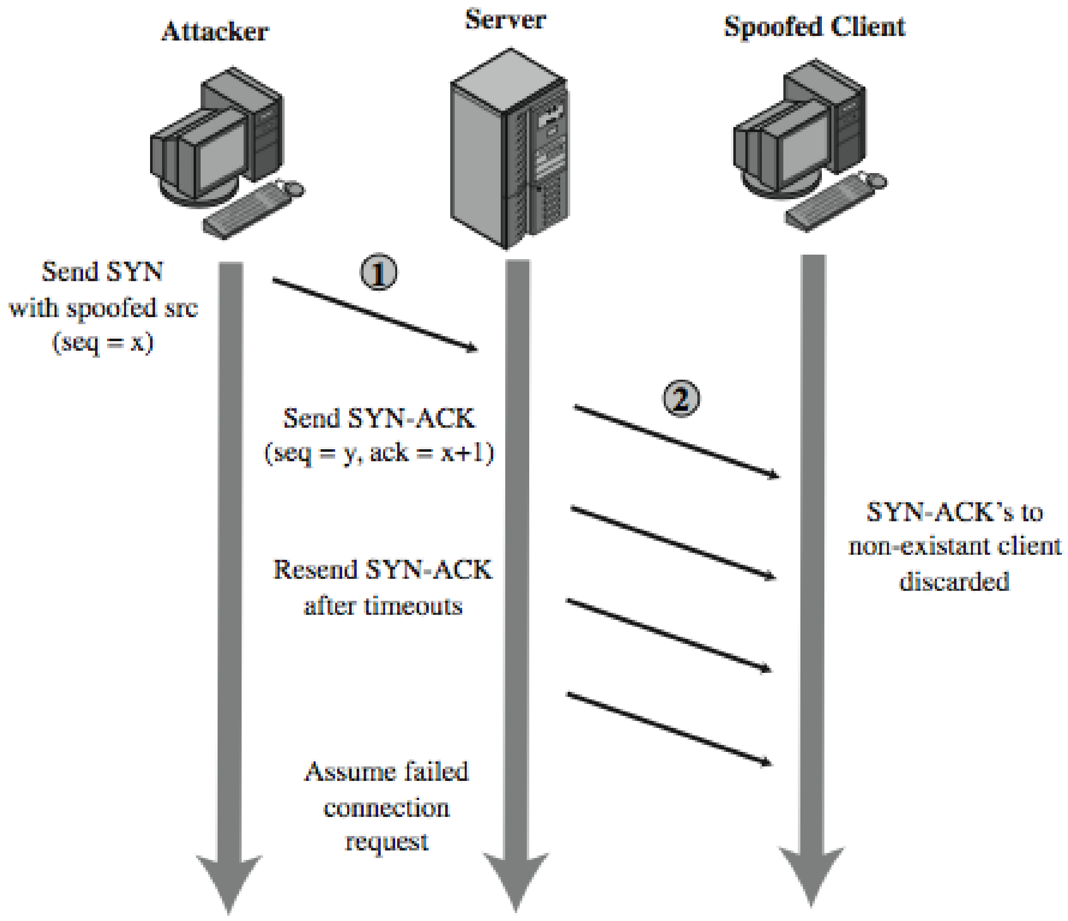


SYN Spoofing Attack

TCP Connection Handshake



SYN Spoofing Attack



SYN Spoofing Attack

- attacker often uses either
  - random source addresses
  - or that of an overloaded server
  - to block return of (most) reset packets
- has much lower traffic volume
  - attacker can be on a much lower capacity link

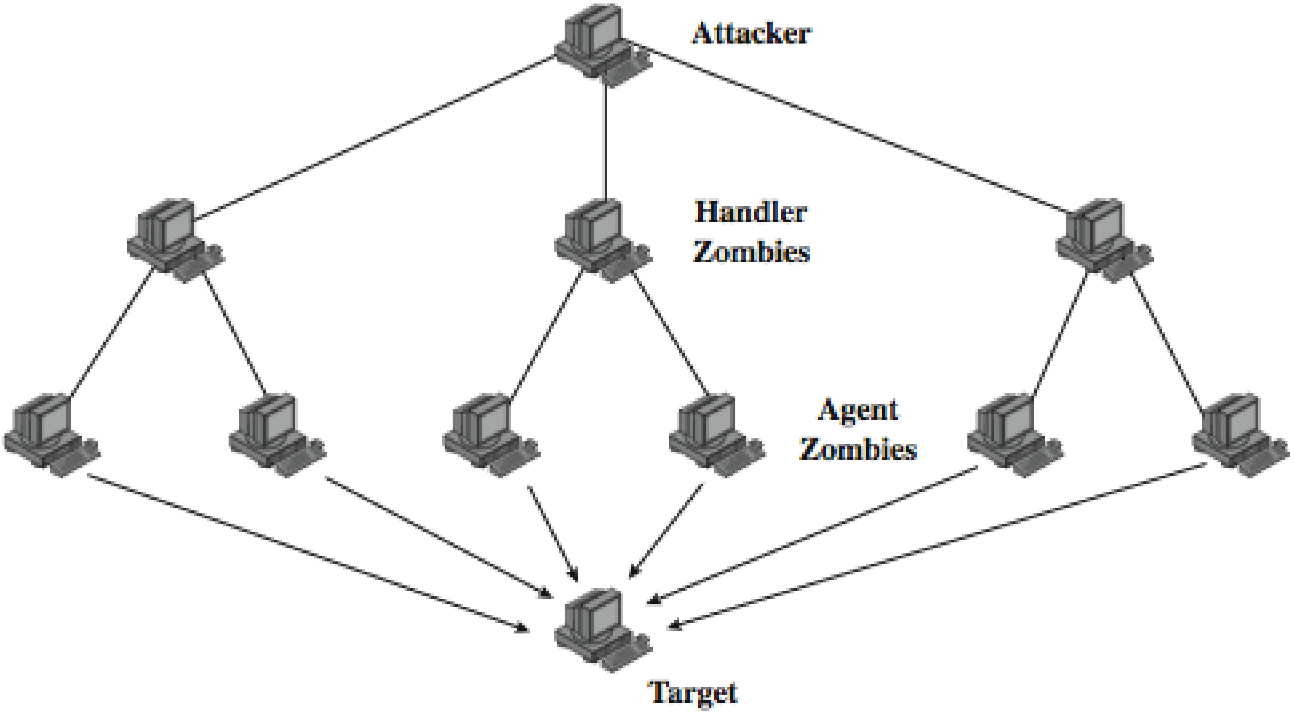
Types of Flooding Attacks

- classified based on network protocol used
- ICMP Flood
  - uses ICMP packets, eg echo request
  - typically allowed through, some required
- UDP Flood
  - alternative uses UDP packets to some port
- TCP SYN Flood
  - use TCP SYN (connection request) packets
  - but for volume attack

Distributed Denial of Service Attacks

- multiple systems allow much higher traffic volumes to form a Distributed Denial of Service (DDoS) Attack
- often compromised PC's / workstations
  - zombies with backdoor programs installed
  - forming a botnet
- e.g. Tribe Flood Network (TFN), TFN2K

DDoS Control Hierarchy

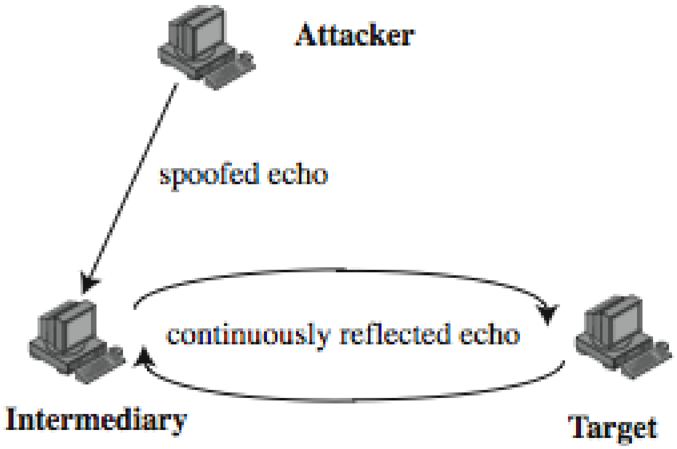


Reflection Attacks

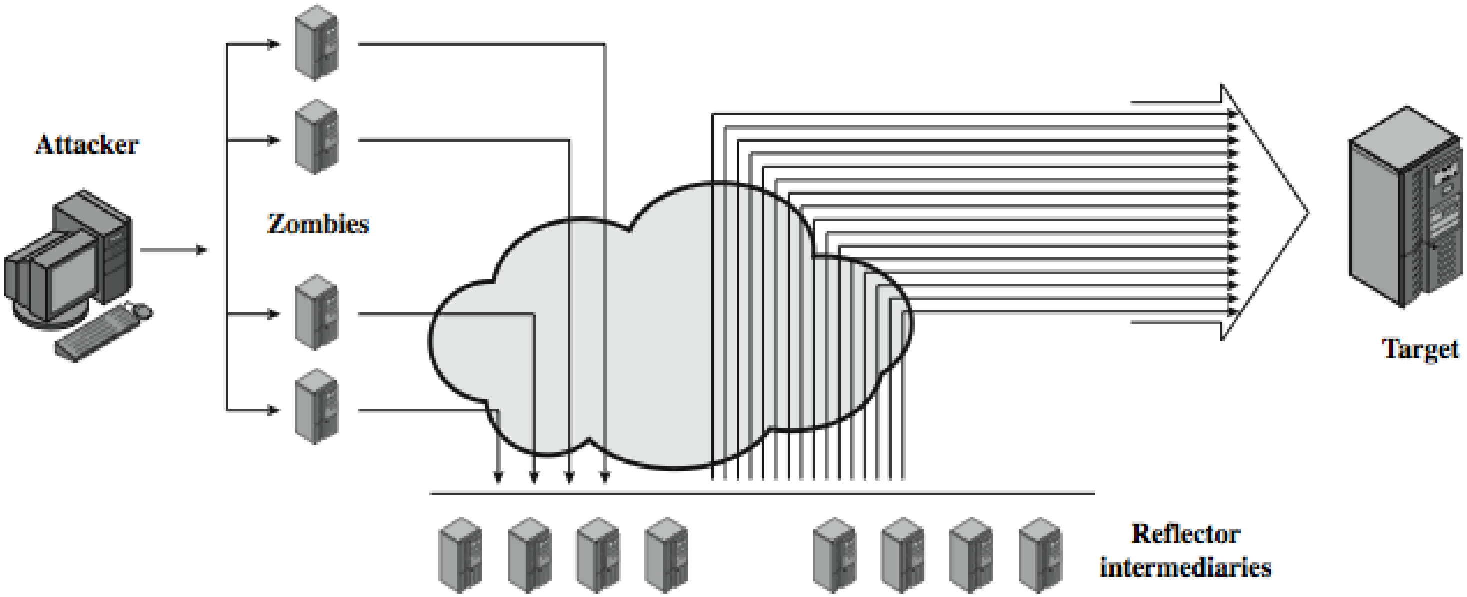
- use normal behavior of network
- attacker sends packet with spoofed source address being that of target to a server
- server response is directed at target
- if send many requests to multiple servers, response can flood target
- various protocols e.g. UDP or TCP/SYN

Reflection Attacks

- further variation creates a self-contained loop between intermediary and target
- fairly easy to filter and block



Amplification Attacks



DoS Attack Defenses

- high traffic volumes may be legitimate
  - result of high publicity
  - or to a very popular site, e.g. Olympics etc
- four lines of defense against (D)DoS:
  - attack prevention and preemption
  - attack detection and filtering
  - attack source traceback and identification
  - attack reaction (after attack) to curtail effects of ar attack

Attack Prevention

- block spoofed source addresses
  - on routers as close to source as possible
  - still far too rarely implemented
- rate controls in upstream distribution nets
  - on specific packets types
  - e.g. some ICMP, some UDP, TCP/SYN
- use modified TCP connection handling
  - use SYN cookies when table full
  - or selective or random drop when table full

Attack Prevention

- block IP directed broadcasts
- block suspicious services & combinations
- manage application attacks with “puzzles” to distinguish legitimate human requests
- good general system security practices
- use mirrored and replicated servers when high-performance and reliability required

Responding to Attacks

- identify type of attack
  - capture and analyze packets
  - design filters to block attack traffic upstream
  - or identify and correct system/application bug
- have ISP trace packet flow back to source
  - may be difficult and time consuming
  - necessary if legal action desired
- implement contingency plan
- update incident response plan