Chap 7.
Denial of Service Attack

연세대학교

Denial-of-Service (DoS) Attack

- 서비스거부(DoS) 공격
  - 중앙 처리 장치(CPU), 메모리, 대역폭 및 디스크 공간과 같은 자원을 소모하여 네트워크, 시스템 또는 응용 프로그램의 허가된 사용을 방해하거나 막는 작업
    [The NIST Computer Security Incident Handling Guide]
- 서비스에 대한 **가용성(availability) 공격**의 한 형태
- 공격받을 수 있는 자원 분류
  - network bandwidth
    - 서버를 인터넷에 연결하는 네트워크 링크의 용량
    - 대부분의 기관에서는 ISP(인터넷서비스공급자)와의 연결임
  - system resource
    - 네트워크 처리 소프트웨어에 대한 과부하 또는 실패가 목표
  - application resource
    - 많은 수의 요청을 하여 다른 사용자의 요청에 응답하는 능력을 제한하게 함

연세대학교

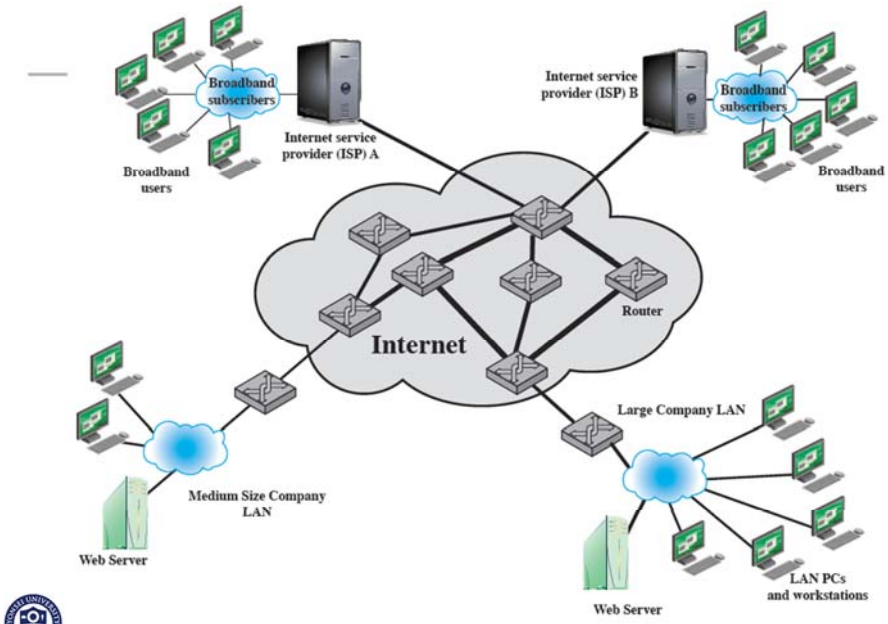


Figure 7.1 Example Network to Illustrate DoS Attacks

연세대학교

Classic Denial-of-Service Attacks

- ping (**p**acket **in**ternet **g**roper) 명령어
  - 상대 컴퓨터의 작동여부 또는 상대 컴퓨터와의 네트워크 연결 상태 확인을 위한 명령어
  - ICMP echo request를 보내고, ICMP echo reply를 받아서 확인
- ping 명령어 flooding (ICMP flooding)
  - 공격 대상 기관에 대해서 네트워크 연결 용량을 훨씬 넘어서게 하려고 ping 명령어를 과도하게 사용함
  - 트래픽은 네트워크 경로의 용량이 크면 처리 할 수 있지만 용량이 작으면 처리되지 않은 패킷은 폐기됨
  - spoof된 주소가 사용되지 않으면 공격 출처가 명확하게 식별됨
  - 네트워크 성능이 현저하게 영향을 받음

연세대학교

Source Address Spoofing

- use forged source addresses
  - 운영체제의 raw socket interface를 통하여 source 주소를 위조하여 공격 시스템을 식별하기 힘들게 함
- congestion은 라우터의 처리용량이 트래픽보다 낮아지게 함

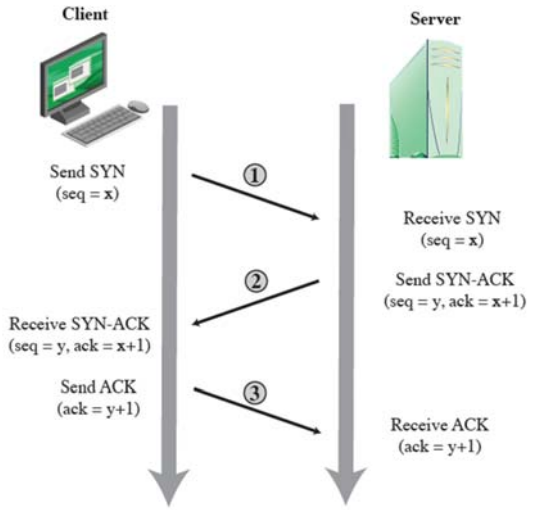
- backscatter traffic
  - 공격 트래픽을 모니터하기 위하여 사용하지 않는 IP주소들에 대한 route를 광고함 → Honeynet Project

SYN Spoofing

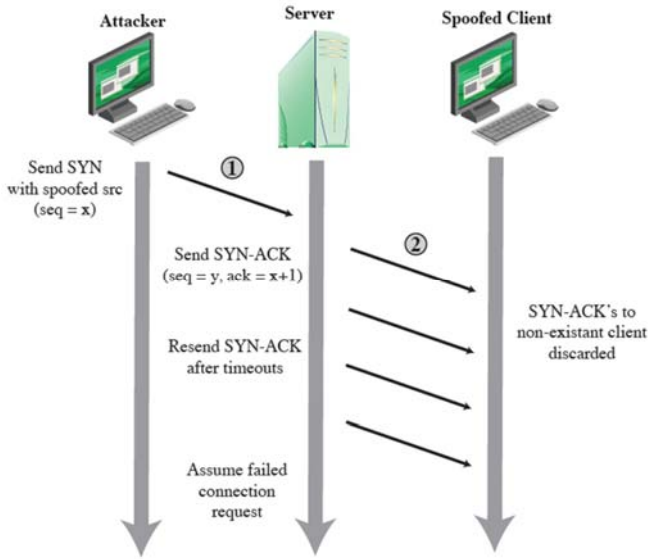
- 일반적인 DoS attack

- 연결 관리에 사용되는 테이블(TCP connection table)을 overflow시켜서 이후의 연결 요청에 응답하는 서버의 기능을 공격함
- 합법적인 사용자는 서버에 대한 접근이 거부됨
- 시스템 자원(특히 OS의 네트워크 처리코드)에 대한 공격

TCP Three-Way Connection Handshake



TCP SYN Spoofing Attack



Flooding Attacks

- 사용된 네트워크 프로토콜에 따라서 분류됨
- 서버로 가는 네트워크 링크에 대해서 과부하 하려는 의도
- 거의 모든 유형의 네트워크 패킷 사용 가능

- ICMP flood
  - (예) ping flooding
- UDP flood
  - UDP 포트로 전송
  - (예) diagnostic echo 서비스
- TCP SYN flood
  - 공격대상에 TCP 패킷을 보냄
  - SYN spoofing 공격과의 차이점은 코드(네트워크 처리코드)가 아니라 전체 패킷 양이 공격의 목표라는 것임

연세대학교

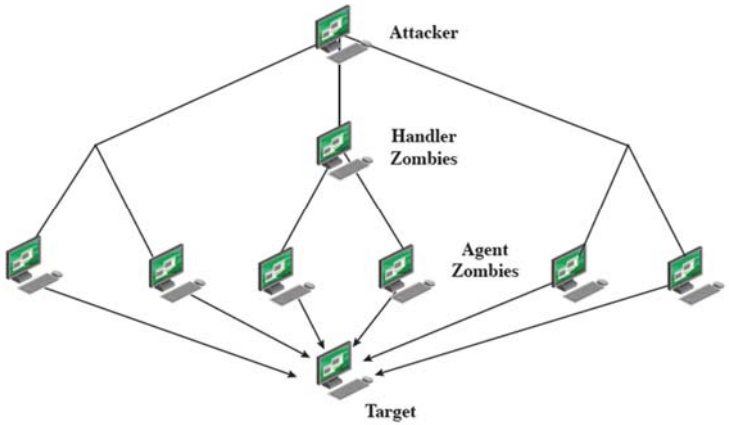
Distributed Denial of Service Attacks

- 분산서비스거부 (DDoS) 공격
  - 여러 시스템을 사용하여 서비스 거부 공격 생성

- 공격자는 운영체제나 응용 프로그램의 결함을 이용하여 Zombie 프로그램을 설치하여 DDoS 공격에 사용
  - 한 명의 공격자가 제어할 수 있는 대규모 시스템 집합을 만들 수 있음 → botnet 형성

연세대학교

DDoS Attack Architecture



연세대학교

Application-Based Bandwidth Attacks

- SIP flood
  - **Session Initiation Protocol (SIP)**
    - Voice over IP (VoIP) 전화에서 call setup에 사용되는 표준 프로토콜
    - HTTP와 유사하게 text-based 프로토콜임
  - single INVITE 요청이 상당한 자원 소비를 하는 사실을 이용하여 공격
- HTTP-based attack
  - HTTP flood
    - 과도한 HTTP요청을 사용한 웹서버에 대한 공격
  - Slowloris 공격
    - HTTP 프로토콜에서 request header의 끝을 나타내기 위해서 blank line이 와야 함. 일부 웹서버는 blank line 입력이 될 때까지 header 입력 종료를 기다림
    - 이러한 동작을 이용하여 공격

연세대학교

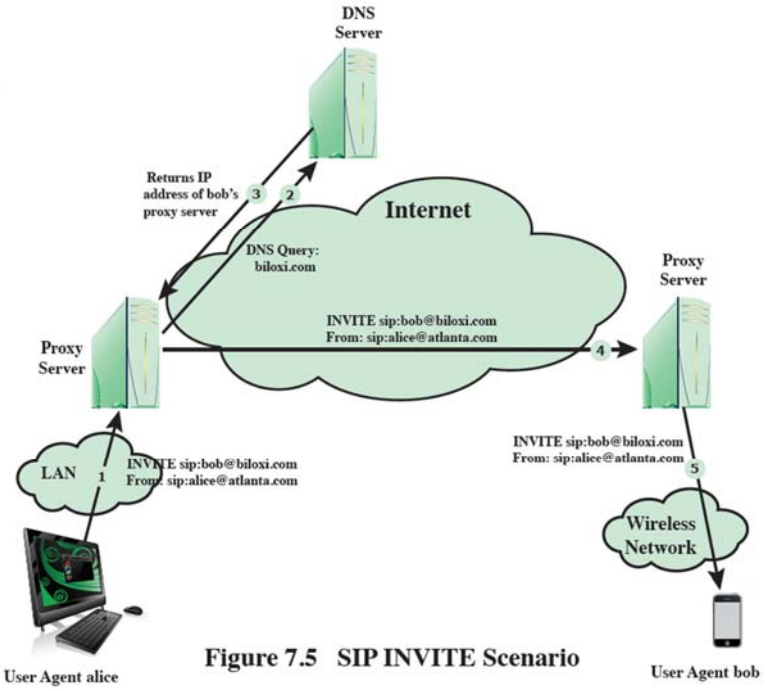


Figure 7.5 SIP INVITE Scenario

연세대학교

HTTP-Based Attacks

HTTP flood

- HTTP 요청을 사용하여 웹서버를 공격
- 상당한 자원을 소비
- spidering
  - 주어진 HTTP 링크에서 시작하여 웹사이트의 모든 링크를 따라서 반복적으로 연결하는 Bot

Slowloris

- 완료되지 않은 HTTP 요청을 보내서 웹서버 독점을 시도
- 합법적인 HTTP 트래픽 이용
- 궁극적으로 웹서버 연결 용량을 완전히 소모하게 됨
- 서명 기반의 기존 침입탐지 및 예방 방법은 Slowloris를 인식하지 못함.

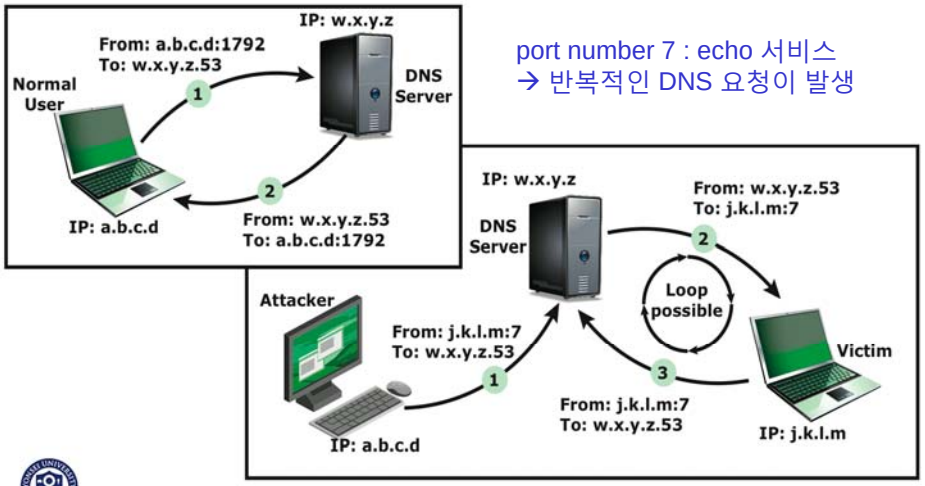
연세대학교

Reflection Attacks

- 공격자는 실제 target 시스템으로 위조된 source address를 사용하여 **중개자**(intermediary)의 알려진 서비스에 패킷을 보냅니다.
- 중개자가 응답하면, 응답이 target에게 전송됩니다.
  - 중개자가 공격을 반사하게 함
- 목표는 중개자에게 알리지 않고 target 시스템에 대한 링크를 과도하게 하기 위하여 대량의 패킷을 생성하는 것
- Defense : 위조된(spoofed) 소스 주소의 패킷을 차단

연세대학교

DNS Reflection Attacks

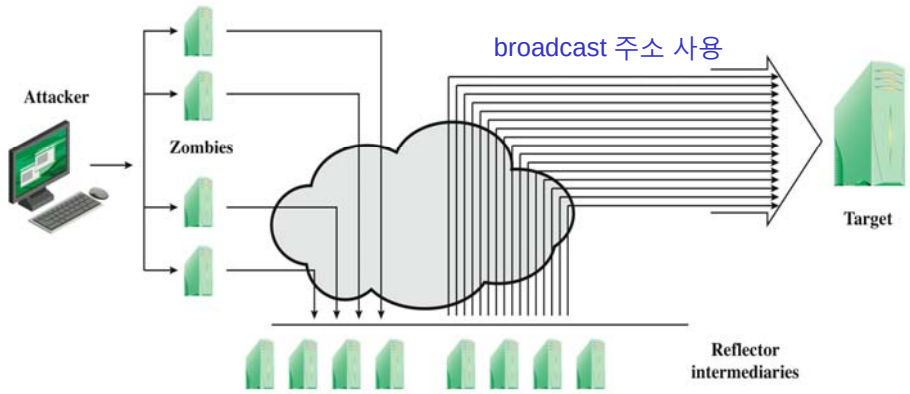


port number 7 : echo 서비스
→ 반복적인 DNS 요청이 발생

연세대학교

Amplification Attacks

- reflection을 다수의 시스템에 보내도록 하여 증폭시킴



연세대학교

DoS Attack Defenses

- 이 공격은 완전하게 막을 수는 없음
- 대용량 트래픽이 합법적일 수 있음
  - 특정 사이트에 대한 높은 광고
  - 매우 인기있는 사이트에 대한 활동
  - 일시적으로 방문자가 증가하는 것
    - slashdotted, flash crowd, flash event

연세대학교

Defense against DDoS 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

연세대학교

DoS Attack Prevention

- spoofed source address 차단
  - 가능한 한 source와 가까운 라우터에서 차단
- 주장하는 source address가 현재 패킷이 사용하는 것임을 보장하기 위해 filter를 사용할 수 있음
  - ISP의 네트워크를 떠나기 전이나, 진입지점에서 적용해야 함

연세대학교

DoS Attack Prevention

- 수정한 TCP connection handling code 사용
  - 서버의 초기 sequence number로 보내지는 cookie에 있는 중요한 정보를 암호화하여 전송
    - 합법적인 client만이 증가된 seq no.를 갖는 ACK 패킷 응답
  - TCP 연결 테이블이 overflow 될 때에 연결이 완료되지 않은 entry를 제거함

DoS Attack Prevention

- IP directed broadcast 차단
  - 특정 네트워크 상의 모든 호스트에 패킷을 전송하는 것
  - IP 주소 : x.y.z.255
- 의심스러운 서비스와 source/destination의 조합을 차단
- 실제 사람의 요청인지를 구분하기 위해 그래픽 퍼즐(captcha) 형식을 사용하여 application attack을 관리
- 좋은 일반적인 시스템 보안 습관
- 고성능 및 신뢰성이 필요할 때에는 미러링/복제 서버 사용

Responding to DoS Attacks

- Antispoofing, directed broadcast 및 rate limiting 필터가 구현되어야 함
- 네트워크 모니터와 IDS(intrusion detection system)을 사용
  - 비정상 트래픽 패턴을 탐지하고 통지함
- 공격 유형 식별
  - 패킷 캡쳐 및 분석
  - upstream 공격 트래픽을 차단하는 필터 설계
  - system/application의 버그를 찾아서 고침
- source 식별을 위한 packet flow 추적을 ISP에 요청
- 비상계획 이행
- 사고 대응 계획 업데이트