

# 정보보호

(5111041)

# 7장

서비스 거부 공격

# 서비스 거부 공격(DoS)

NIST 컴퓨터 보안 사고 처리 가이드는 DoS공격을 다음과 같이 정의:

“중앙 처리 장치(CPU), 메모리, 대역폭 및 디스크 공간 등의 자원을 소진시켜서 네트워크, 시스템 또는 응용프로그램에 대한 정상적인 사용자의 접근을 힘들게 하거나 봉쇄하는 공격”

# 서비스 거부 (DoS)

- 일부 서비스 이용의 공격 형태
- 공격받을 수 있는 자원의 분류:

## 네트워크 대역폭

인터넷에 서버를  
연결시키는 네트워크  
링크의  
수용성(capability)과 연관

대부분의 조직들은  
그들의 인터넷 접속  
서비스(ISP)에 연결

## 시스템 자원

소프트웨어를 다루는  
네트워크 과부화 또는  
충돌이 목적

## 응용프로그램 자원

일반적으로 대다수의  
유료한 요청을 포함하며,  
이들 중 각각은 상당한  
자원을 소비하고 있음.  
그러므로 다른 유저의  
요청에 서버가 응답하는  
것을 제한

# 전통적 DoS 공격

## ● Ping flooding

- 대상 조직에 대해 네트워크 연결 기능을 제압하는 것이 공격의 목적
- 트래픽은 경로상의 수용력이 더 큰 링크를 통해 처리 될 수 있지만, 패킷은 수용력이 감소할 때 삭제 됨
- 스푸핑 주소가 사용되지 않을 경우 공격 소스가 명확하게 식별 될 수 있음
- 네트워크 성능에 큰 영향을 미침

# 시작 주소 스푸핑 (Source Address Spoofing)

- 위조된 소스 주소 사용
  - 대체로 운영 체제의 원시 소켓 인터페이스를 통함  
→ 연구용으로 개발되었으나 아직도 많은 시스템에서 해당 인터페이스 지원
  - 시스템이 공격을 식별하기 어렵게 함
- 공격자는 목적지 주소로 대상 시스템에 대량의 패킷을 발생시킴, 이때 소스 주소를 무작위로 변경
  - 대표적인 예 : ICMP echo request 메시지
  - 이를 수신 받은 공격 대상은 ICMP echo response 메시지를 받은 메시지의 소스의 주소로 보답하게 되어 있음
  - 핵심만 이미 잊은 주소는 가짜 주소이며, 몇몇 주소는 실제 어떤 시스템에 존재한다고 하더 라도 예상치 못한 패킷에 와서 혼란을 일으키고, 링크 수용력을 낮춤
- 최종 목적지와 연결된 라우터에 혼란을 일으키고, 링크 수용력을 낮춤
- 네트워크 엔지니어에게 라우터에서 흘러나오는 정보를 명확하게 쿼리할 것을 요청
- 후방 산란(backscatter) 트래픽
  - 공격 트래픽을 모니터링 하기 위해 사용되지 않은 IP주소 루트를 유입 알림

# SYN 스푸핑

- Flooding과는 다르지만 일반적인 DoS 공격
- TCP 프로토콜의 취약점과 성질을 이용한 네트워크 공격임
- 공격자의 시작주소를 조작하여 SYN 메시지를 보내면, 공격 대상은 이 정보를 TCP 테이블에 저장하고 SYN-ACK를 조작된 주소로 보냄
  - 만약 실제 시스템에 존재한다면 RTS(reset)패킷이 전달되고 테이블에서 삭제
  - 존재하지 않는다면 공격대상은 요청 실패 한도까지 계속해서 SYN-ACK을 보내다가, 특정한 횟수 이상 혹은 특정 시간 이상이 지나야만 테이블에서 삭제
  - 공격자는 RTS으로 반응하지 않는 시작주소를 쓰려고 노력함 – WHY?
- 연결을 관리하는 TCP 테이블을 오버플로우 시킴으로써 연결 요청에 응답하게 될 서버의 기능을 공격
- 합법적인 사용자가 서버에 접근이 거부됨
- 운영 체제 자원 중에서도 특히 운영체제에 있는 코드를 처리하는 네트워크를 공격

# TCP 연결 3-Way Handshaking

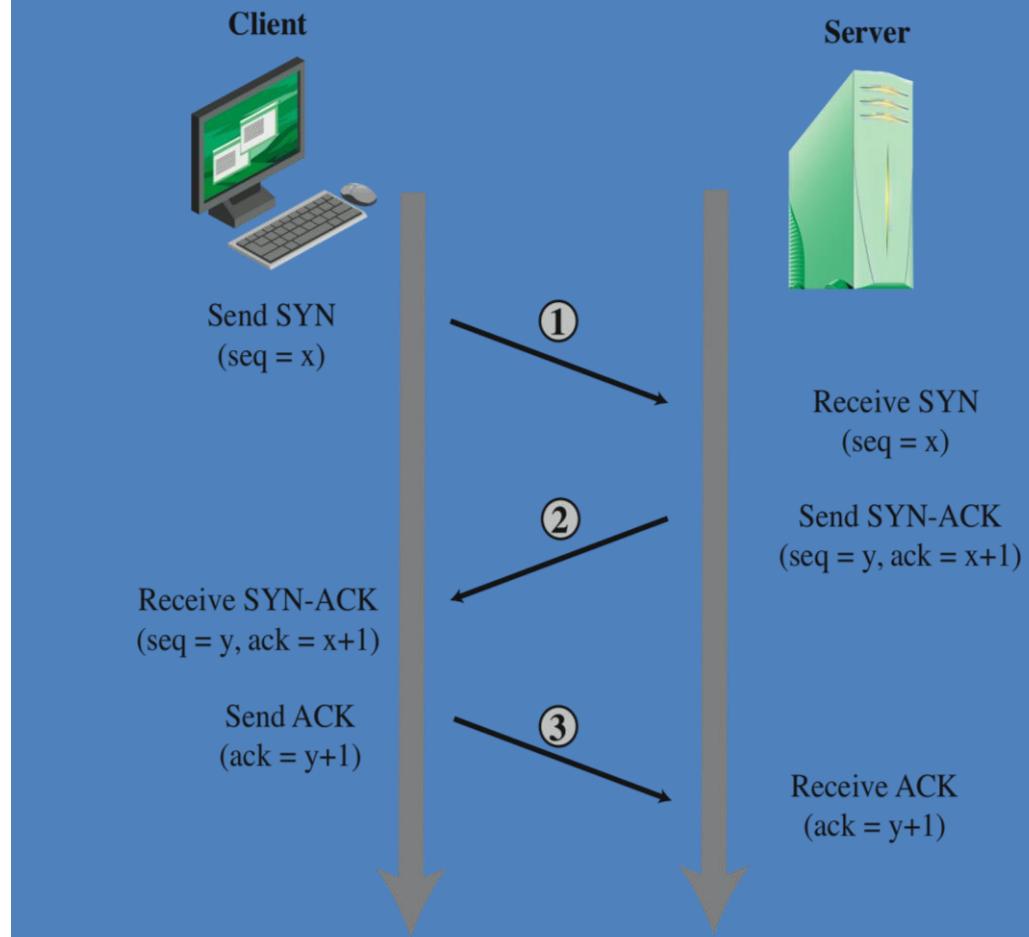


Figure 7.2 TCP Three-Way Connection Handshake

# TCP SYN 스 푸핑 공격

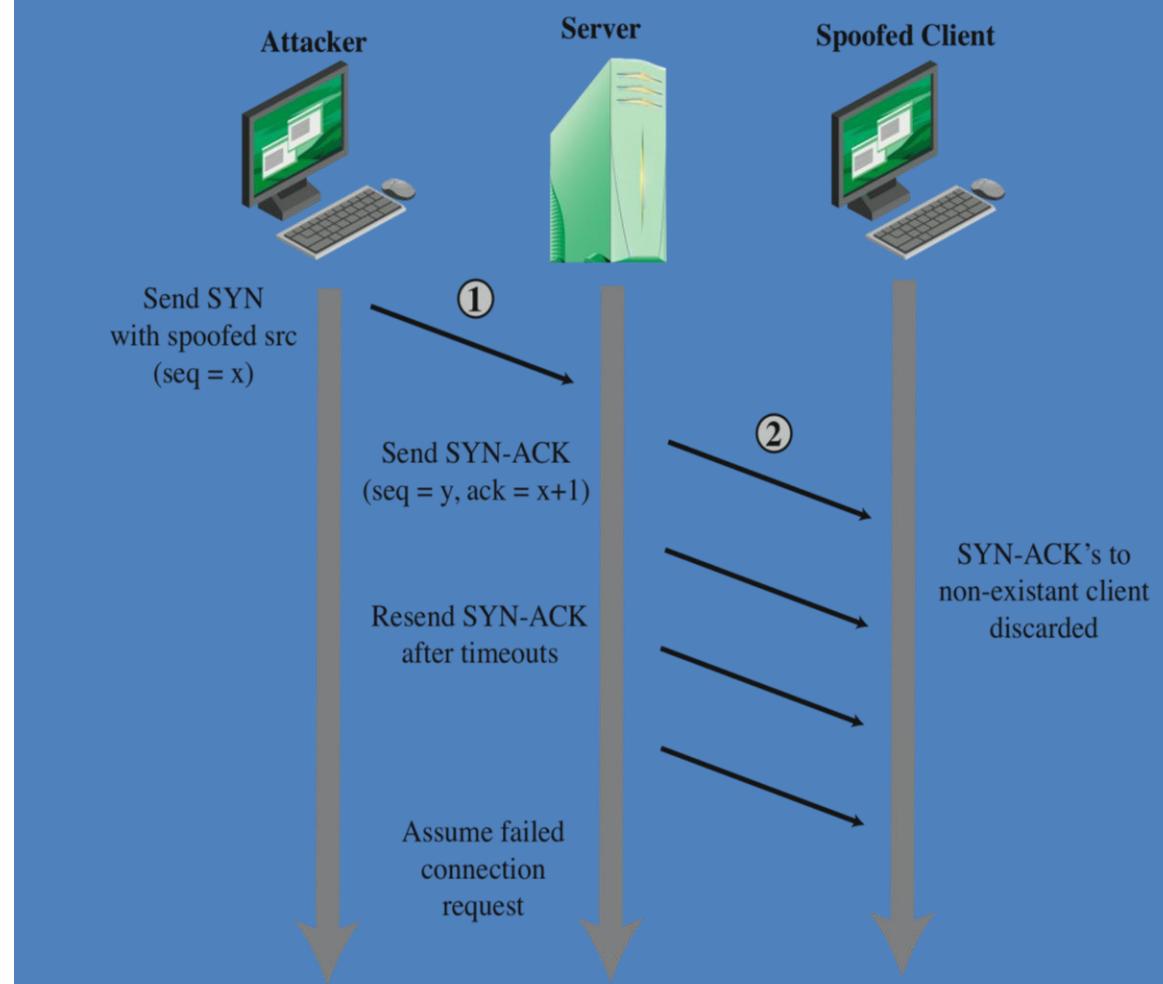


Figure7.3 TCP SYN Spoofing Attack

# 플러딩 공격 (Flooding Attacks)

- 사용되는 네트워크 프로토콜을 기반으로 분류됨
- 서버에 대한 일부 링크의 네트워크 용량을 과부하 시키는 것이 목적
- 실제로 모든 네트워크 패킷 타입이 사용 가능

## ICMP 플러드

- ICMP 에코(echo)를 이용하는 핑 플러딩이 패킷을 요청
- 일반적으로 네트워크 관리자는 핑이 유용한 네트워크 진단 도구이기 때문에, 그러한 패킷이 네트워크로 유입되도록 허가 함

## UDP 플러드

- 대상 시스템의 포트 숫자에 연결된 UDP 패킷 사용

## TCP SYN 플러드

- TCP 패킷을 대상 시스템에 전송
- 시스템 코드를 견啷하기보다는 총체적인 패킷의 양이 공격의 대상
- SYN spoofing과 비슷한 효과

# 플러딩 공격 (Flooding Attacks)

- 기존 Flooding 공격의 한계
  - 하나의 시스템만 사용했을 시에는 패킷의 양에 한계가 있음
  - 또한, 하나의 시스템을 공격하면 트래픽 패턴이 분석되어 발각이 쉬움
  - 시스템 용량이 더 작은 네트워크에서는 공격이 어려움
- 여러 시스템을 이용한 공격
  - 훨씬 대규모의 트래픽 생성이 가능
  - 직접 공격하지 않고 한단계 물러서서 공격하기 때문에 추적이 어려움
  - 공격 시스템은 특별히 성능이 좋거나 대용량의 네트워크 링크가 필요 없음
- 여러 시스템을 이용한 공격의 종류
  - 분산 DoS 공격
  - Reflector 공격
  - Amplifier 공격

# 분산 서비스 거부(DDoS) 공격

공격에 다양한  
시스템을 사용

공격자는 운영체제  
또는 시스템에  
프로그램을  
설치하거나  
접근권을 얻을 수  
있는 공용  
어플리케이션의  
결함을 악용(좀비)

한 공격자의 통제  
하에 제어되는  
많은 시스템  
집합이 형성되어,  
봇넷을 구성할 수  
있음

# 분산 DoS 공격 아키텍쳐

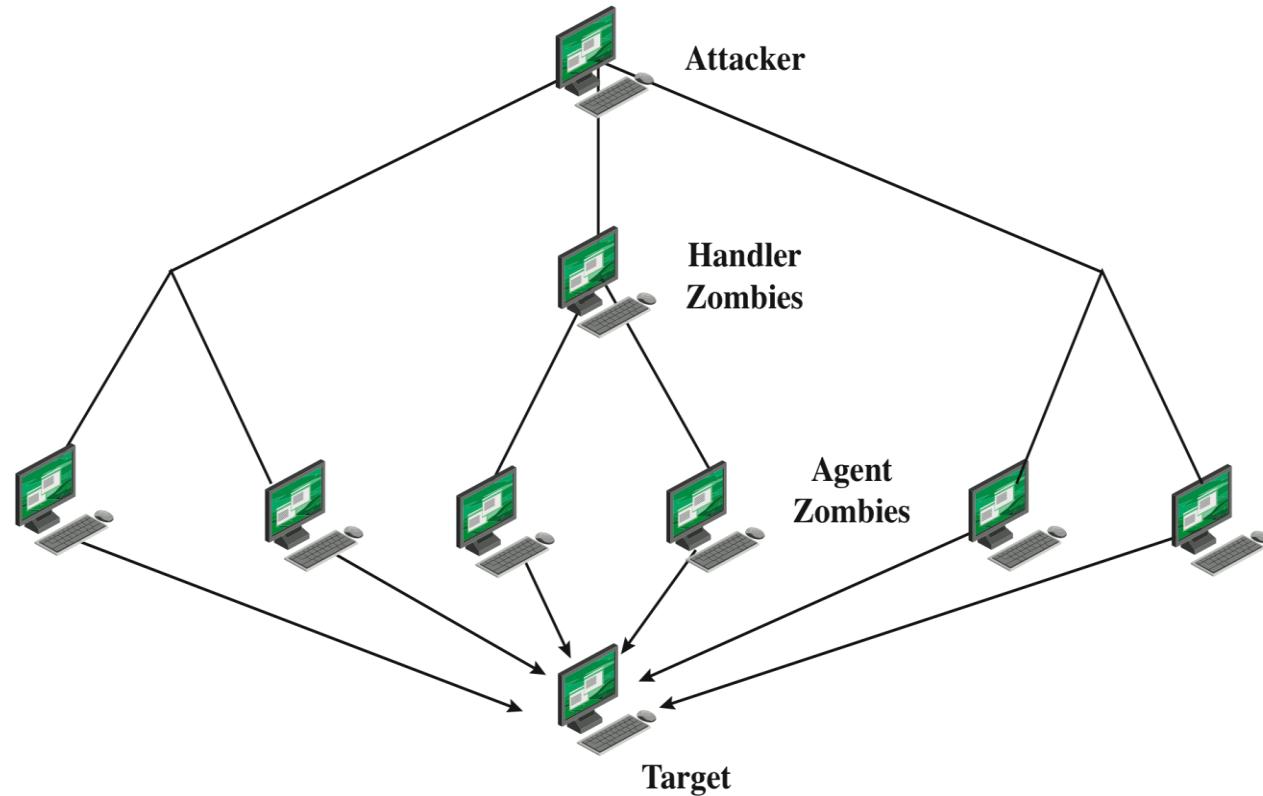


Figure 7.4 DDoS Attack Architecture

# 분산 DoS 공격

- 최초의 가장 잘 알려진 DDoS 툴
  - Tribe Flood Network(TFN)
  - 2단계 계층 구조를 사용
  - Trojan을 이용하여 좀비 시스템을 만들고 운영함
  - ICMP Flood, SYN flood, UDP flood, ICMP 증폭 공격이 가능
  - 시작 주소 조작하지 않는 대신 많은 좀비 시스템 이용
- DDOS 공격 목표 시스템의 대응
  - Flooding 공격과 동일하지만 추적이나 대응은 더 복잡함

## 응용프로그램기반 대역폭 공격 : 세션 개시 프로토콜 (SIP) Flood

- VoIP기술에 대한 표준 프로토콜
- HTTP와 유사한 문법을 지닌 텍스트 기반의 프로토콜
- SIP 메시지의 두 가지 유형: 요청과 응답

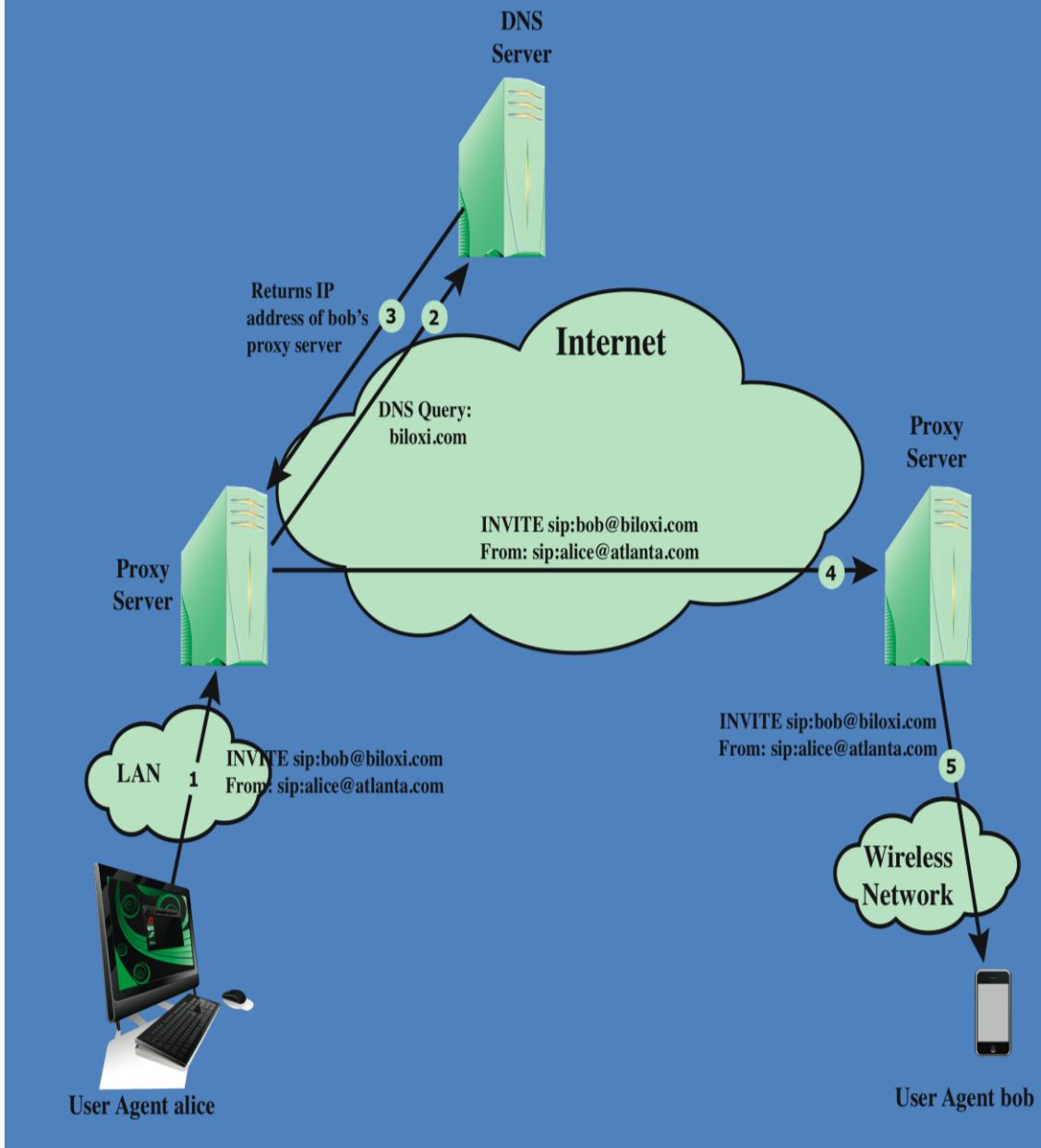


Figure 7.5 SIP INVITE Scenario

# 하이퍼 전송 프로토콜(HTTP) 기반 공격

## HTTP 플러드

- HTTP 요청으로 웹 서버를 포격(bombards)하는 공격
- 상당한 양의 자원 소비
  - 예를들면, 많은 수의 좀비 시스템들이 목표시스템에 용량이 큰 파일을 다운받도록 요청

## 슬로로리스(slowloris)

- 결코 완료되지 않는 HTTP 요청을 전송함으로써 독점하려는 시도
- HTTP 프로토콜은 헤더의 끝과 페이로드의 경계에서 빈줄을 보내게 되어있음
  - 이 줄바꿈을 문자를 보내지 않음으로서 서버는 요청이 실제 들어오기만을 무한정 기다림
- 결국 웹 서버 연결 용량 소비
- 합법적인 HTTP 트래픽 이용
- 기존의 공격 탐지를 위한 시그니처 기반의 침입 탐지 및 예방 솔루션은 대체로 슬로로리스를 인식하지 못함
- 호스트당 요청속도 제한, 타임아웃, delayed biding 등의 방법을 이용하여 방어

# Reflector(반사 공격)

- 공격자는 실제 타겟의 스푸핑 소스 주소를 가진 Reflector를 통해 알려진 서비스로 패킷 전송
- Reflector 가 응답하게 되면, 그 응답은 다시 타겟에게 전송됨
- Reflector 에게 알리지 않고 타겟 시스템의 링크를 범람시키는 많은 양의 패킷을 발생하게 하는 것이 목적
- 서버, 라우터등 네트워크 성능이 좋은 Reflector 를 선정하여 이용
- 이러한 공격에 대한 기본적인 방어책은 스푸핑 소스 패킷을 차단하는 것

# Reflector(반사 공격)

- UDP 서비스를 이용한 공격이 많이 이용됨 – Why?
  - UDP는 연결형 서비스가 아니므로, 요청이 들어오면 데이터를 반사적으로 날림
  - 작은 사이즈의 서비스 요청메시지를 이용하여 큰 용량의 데이터 트래픽을 유발시킬 수 있음
- TCP SYN 패킷 Reflector 공격
  - 3-way handshake를 이용
  - 공격 대상의 주소를 적은 TCP SYC 패킷을 여러 개의 중간 시스템 (Reflector들에게 보냄)
  - 결과는?

# DNS 반사 공격

- 중간 시스템(Reflector)와 공격 시스템 간의 루프 형성
  - 공격자가 공격 시스템의 주소로 질의 메시지 전송
    - 보통 7번 포트를 이용(echo 서비스 포트)
  - 공격 시스템은 다시 응답 -> 더 효과적인 공격 수행

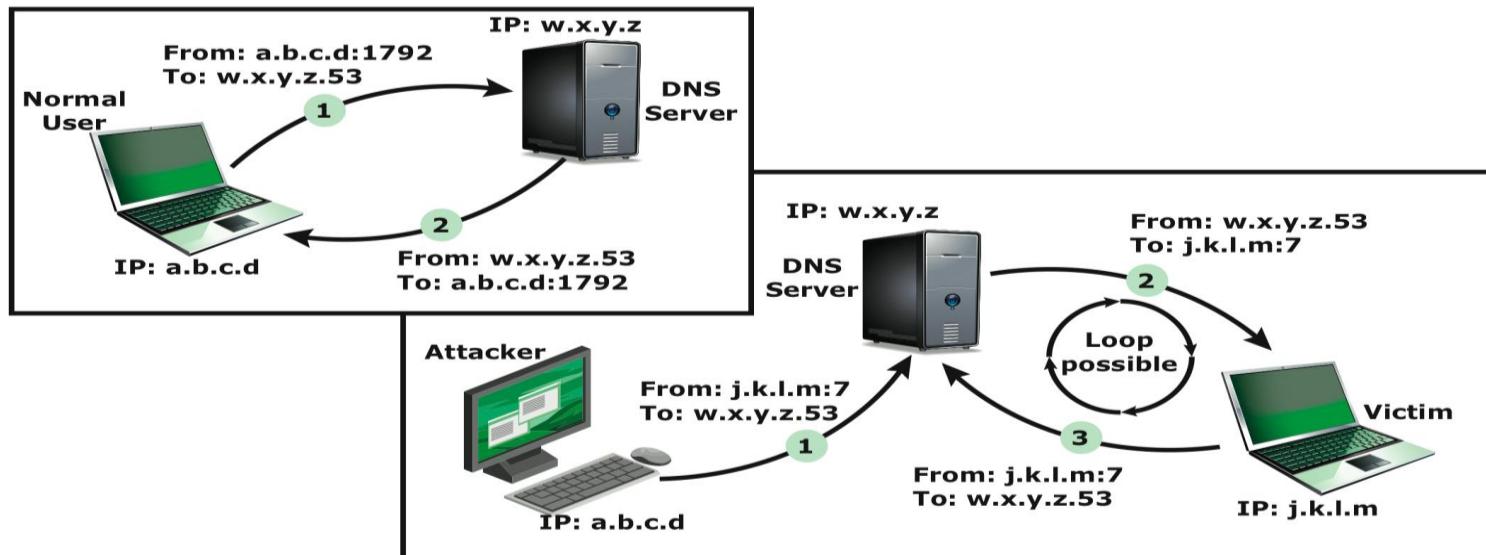


Figure 7.6 DNS Reflection Attack

# Amplifier (증폭 공격)

- 하나의 수신된 패킷에 대해 여러 개의 응답 패킷 생성
- ICMP echo request 이용한 Amplifier 공격 가능 (Ping flood)
  - 소스 주소 : 공격 대상의 주소로 조작
  - 데스티네이션 주소 : 브로드 캐스트 주소로 보냄
- UDP 서비스 사용
  - 데이터 요청 메시지를 브로드캐스트로 전송
  - TCP 서비스는 연결 지향성이므로 공격에 사용 불가
    - 근본적으로 비연결형인 브로드캐스트 주소로 전송 불가능

# 증폭 공격

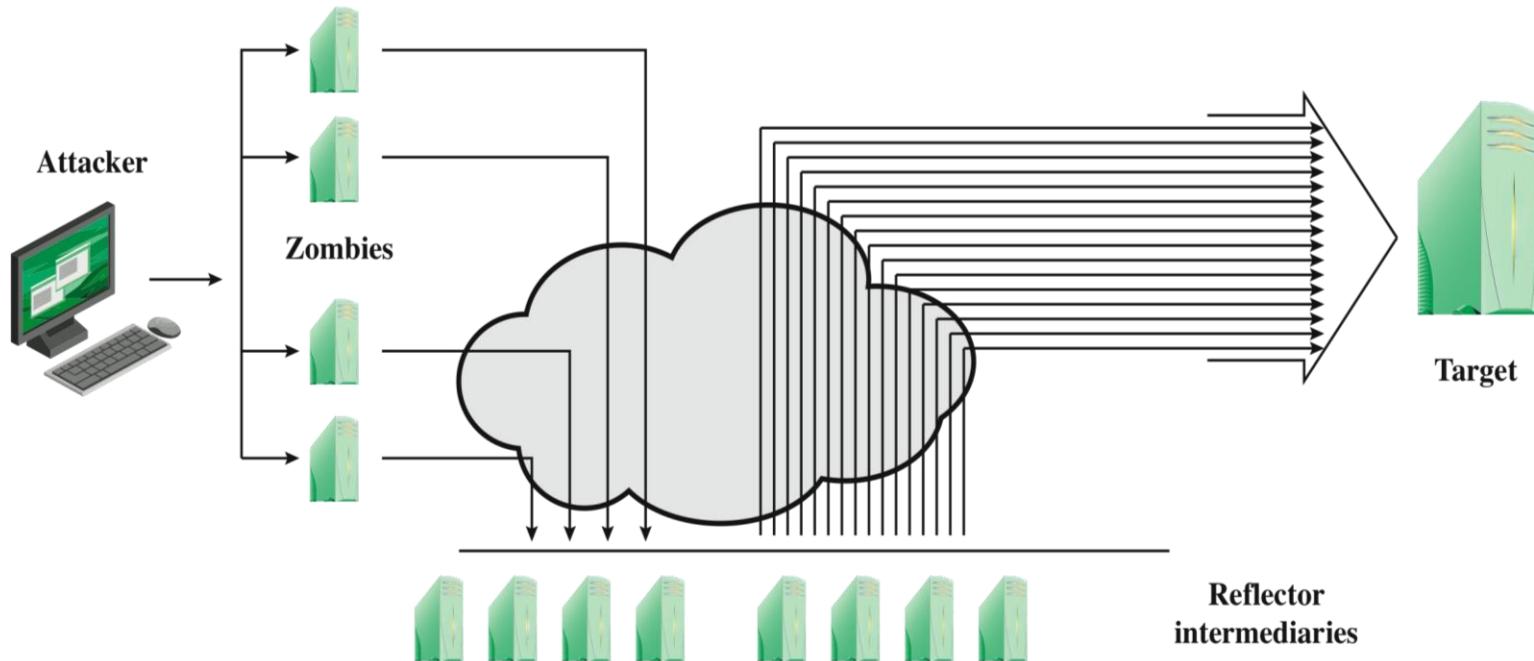


Figure 7.7 Amplification Attack

# DNS 증폭 공격

- Reflector 공격과 같이 합법적인 DNS 서버에 직접적인 패킷 사용
- 공격자는 타겟 시스템의 스푸핑 소스 주소를 담고 있는 DNS 연쇄적 요청 생성
- 작은 요청을 훨씬 더 많은 응답으로 전환 하는 DNS 행위 이용(증폭)
  - 60바이트의 UDP 요청 패킷에 대해 512바이트 응답패킷 생성
- 타겟이 응답으로 인해 범람
- 이러한 공격에 대한 기본적인 방어책은 스푸핑 소스 주소의 사용을 방지 하는 것

# DoS 공격 방어

## DDoS 공격에 대한 네 가지 방어책

- 이러한 공격은 완전히 예방 될 수는 없음
- 합법적으로 트래픽 양이 많을 수도 있는 경우
  - 특정 사이트에 관심이 폭주할 경우
  - 인기 사이트의 활동
  - '*slashdotted*', '*flash crowd*' 또는 '*flash event*'로 묘사됨

### 공격 예방 및 선점(preemption)

- 공격 전

### 공격 탐지 및 필터링

- 공격 기간

### 공격 소스의 역추적 및 식별

- 공격 기간 또는 공격 후

### 공격 대응

- 공격 후

# DoS 공격 예방

- 스퓌핑 소스 주소 차단
  - 공격 진원지와 가까운 곳에서 수행할수록 효과적
  - 소스에 가장 근접한 라우터 상 수행
  - 조직이나 가정에 인터넷 서비스를 제공하는 ISP 회사가 수행해야 함
  - 예를 들면 Cisco 라우터 “ip verify unicast reverse-path” 명령어 사용
    - 패킷이 전송되어온 경로 확인 가능
- Antispoofing 필터링
  - 트래픽이 ISP 네트워크를 떠나기 이전이나 그들 네트워크의 진입점을 통과해 들어가기 전에 필터링이 이루어져야 함
  - 람우터 성능저하가 인터넷의 속도를 낮춘다는 위험성때문에 잘 하지 않음
- TCP 연결을 다루는 코드를 수정하여 사용
  - 서버의 초기 시퀀스 넘버로 전송될 쿠키에 있는 중요 정보들을 암호화
    - 할법적 클라이언트가 증가된 시퀀스 넘버 쿠키를 포함하고 있는 ACK 패킷으로 응답함
  - 올버플로우 발생시 TCP 연결 테이블로 부터 불완전한 연결의 진입을 드롭 시킴

# DoS 공격에 대한 대응

## 적합한 사고 대응 계획

- 기술자와 접촉 방법의 상세화
- 트래픽 필터링 업스트림이 (upstream)이 시행되어야 함
- 공격 대응법의 상세화

- 안티스푸핑, 다이렉트 브로드캐스팅(directed broadcast), Rate limiting 필터가 구현되어야 함
- 네트워크 모니터와 이상 트래픽 패턴들을 탐지하고 알려주는 IDS를 장비

# DoS 공격에 대한 대응

- 공격 유형 확인
  - 패킷의 캡쳐 및 분석
  - 공격 트래픽 업스트림을 차단하는 필터 설계
  - 시스템이나 어플리케이션 버그의 식별 및 수정  
(correct)
- ISP가 패킷의 흐름을 스스로의 역 추적하게 함
  - 어렵고 많은 시간이 소비됨
  - 법적 행위 지침에 대한 계획이 필요한 경우도 있음
- 비상 사태 계획 구현
  - 대안 백업 서버로 전환
  - 새로운 주소를 가진 새로운 사이트의 새로운 서버의
- 사고 대응 계획 업데이트
  - 공격을 분석하여 차후에 대응