6장 네트워크보안
Network Security

박종혁
서울과학기술대학교 컴퓨터공학과
jhpark1@seoultech ac kr

목 차

본 교재

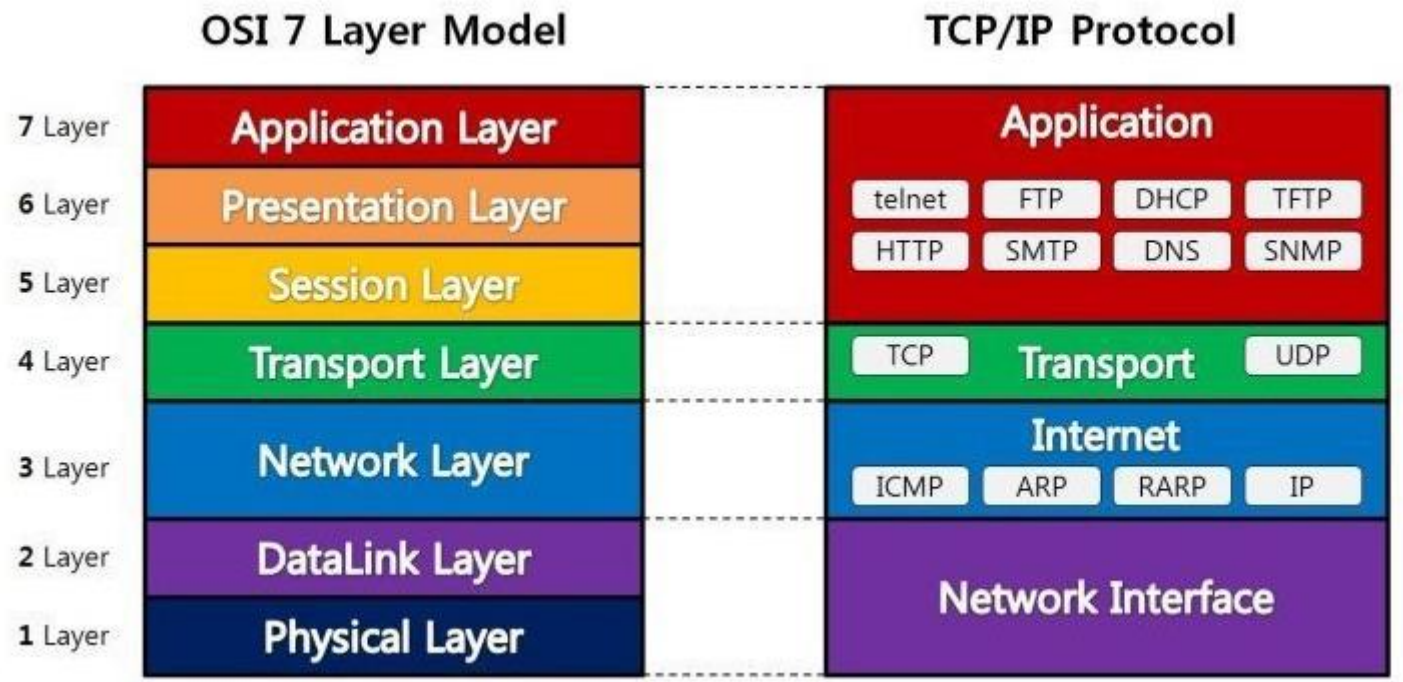
양대일, 정보보안개론(개정3판), 한빛아카데미, 2018

6-1 네트워크의 이해

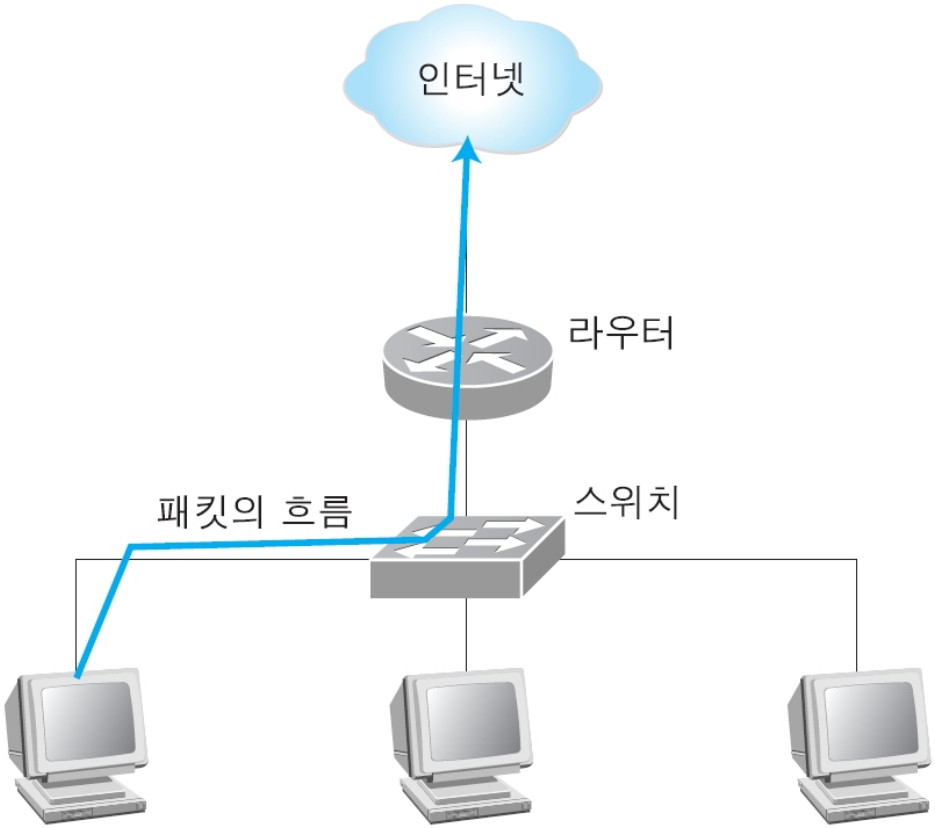
네트워크의 이해

- **OSI 7계층**
  - 국제표준화기구(ISO, International Organization for Standardization)는 다양한 네트워크 간의 호환을 위해 OSI 7계층이라는 표준 네트워크 모델을 만듦

OSI 7계층


OSI 7 Layer Model
TCP/IP Protocol
7 Layer
6 Layer
5 Layer
4 Layer
3 Layer
2 Layer
1 Layer
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
DataLink Layer
Physical Layer
Application
telnet
FTP
DHCP
TFTP
HTTP
SMTP
DNS
SNMP
TCP
Transport
UDP
Internet
ICMP
ARP
RARP
IP
Network Interface

- 2, 3계층에서의 패킷의 흐름



2, 3계층에서의 패킷의 흐름

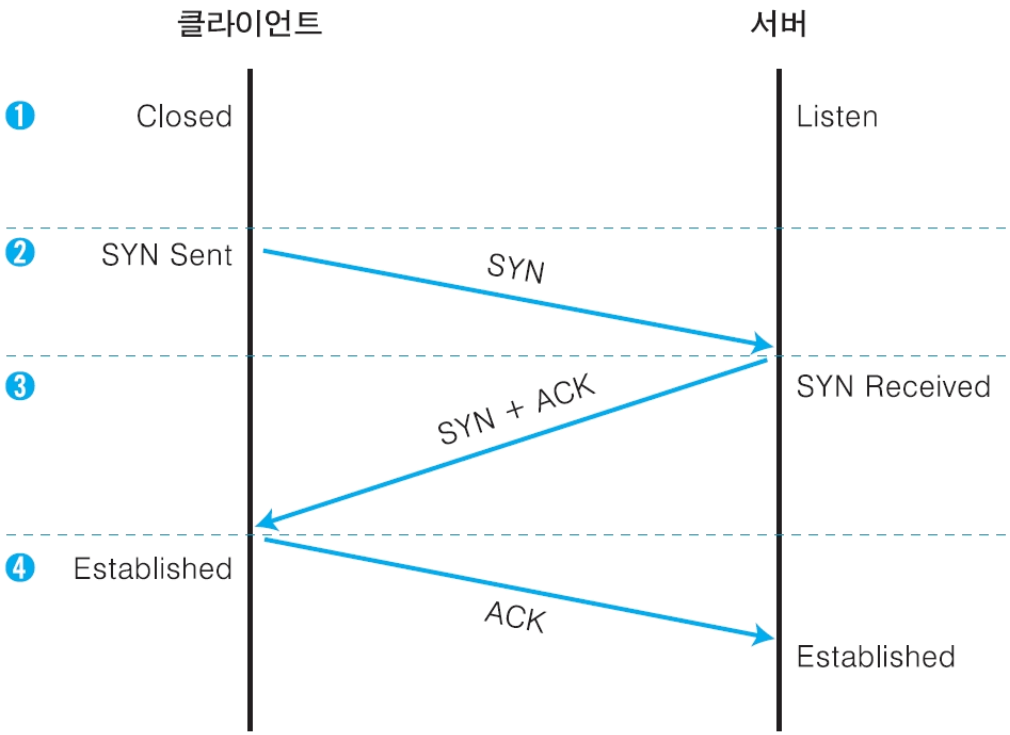
• 3-웨이 핸드쉐이킹 (3-Way Handshaking)

❶ **1**단계**:** 두 시스템이 통신을 하기 전에, 클라이언트는 포트가 닫힌 **Closed** 상태며 서버는 해당 포트로 항상 서비스를 제공할 수 있도록 **Listen** 상태

❷ **2**단계**:** 처음 클라이언트가 통신을 하고자 하면, 임의의 포트 번호가 클라이언트 프로그램에 할당되고 클라이언트는 서버에 연결하고 싶다는 의사 표시로 **Syn Sent** 상태가 됨

❸ **3**단계**:** 클라이언트의 연결 요청을 받은 서버는 **SYN Received** 상태가 됨. 클라이언트에게 연결을 해도 좋다는 의미로 **SYN+ACK** 패킷을 보냄

❹ **4**단계 **:** 마지막으로 클라이언트는 연결을 요청한 것에 대한 서버의 응답을 확인했다는 표시로**ACK** 패킷을 서버에 보냄



TCP에서 연결 설정 과정

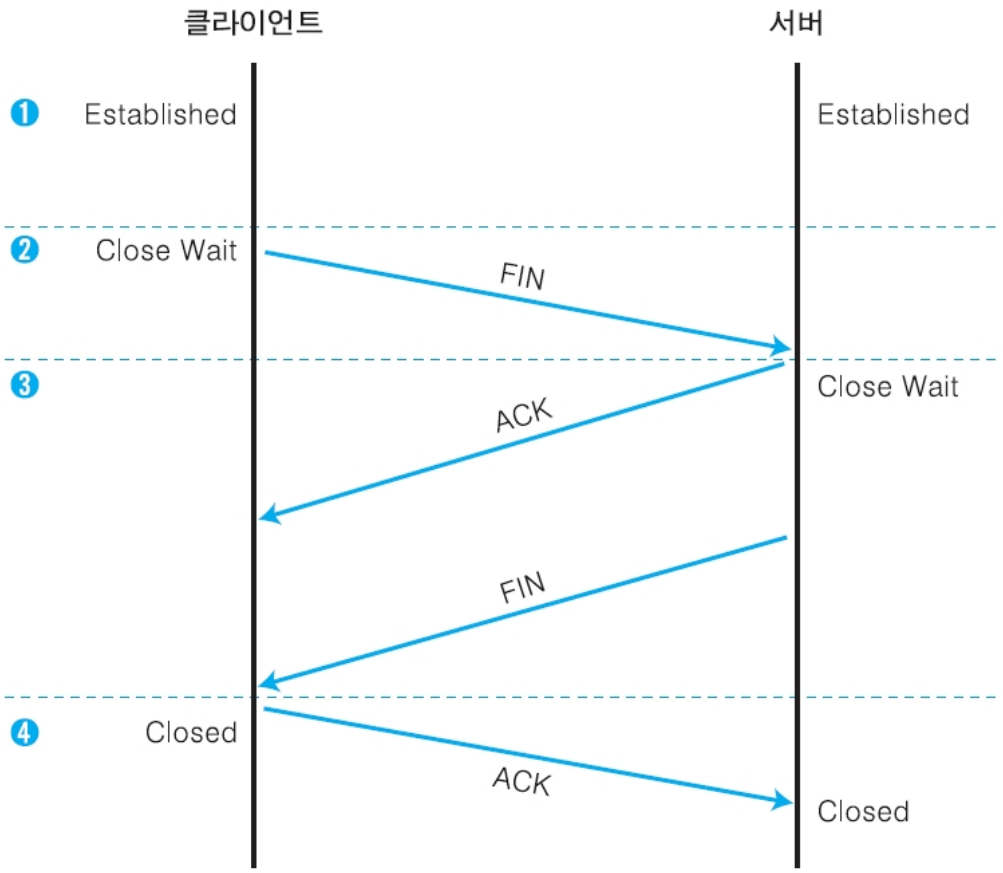
• TCP 세션의 종료

❶ 통신을 하는 중에는 클라이언트와 서버 모두 **Established** 상태

❷ 통신을 끊고자 하는 클라이언트가 서버에 **FIN** 패킷을 보냄 이때, 클라이언트는 **Close Wait** 상태가 됨

❸ 서버는 클라이언트의 연결 종료 요청을 확인하고 클라이언트에게 응답으로 **ACK** 패킷을 보냄. 서버도 클라이언트의 연결을 종료하겠다는 의미로 **FIN** 패킷을 보내고**Close Wait** 상태가 됨

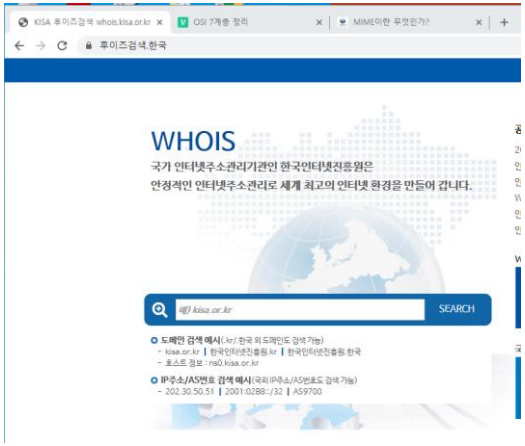
❹ 마지막으로 클라이언트는 연결 종료를 요청한 것에 대한 서버의 응답을 확인했다는 의미로**ACK** 패킷을 서버에 보냄



TCP에서 연결 해제 과정

- **Whois**

  국가 인터넷주소(도메인, IP주소/AS번호) 관리기관인 한국인터넷진흥원이 제공하는 인터넷주소의 등록・할당 정보 검색 서비스



- **Whois 서버**
  - 등록, 관리 기관
  - 도메인 이름
  - 목표 사이트 네트워크 주소와 IP 주소
  - 관리자, 기술 관련 정보
  - 등록자, 관리자, 기술 관리자
  - 레코드 생성 시기와 업데이트 시기
  - 주 DNS 서버와 보조 DNS 서버
  - IP 주소의 할당 지역 위치
  - 관리자 이메일 계정

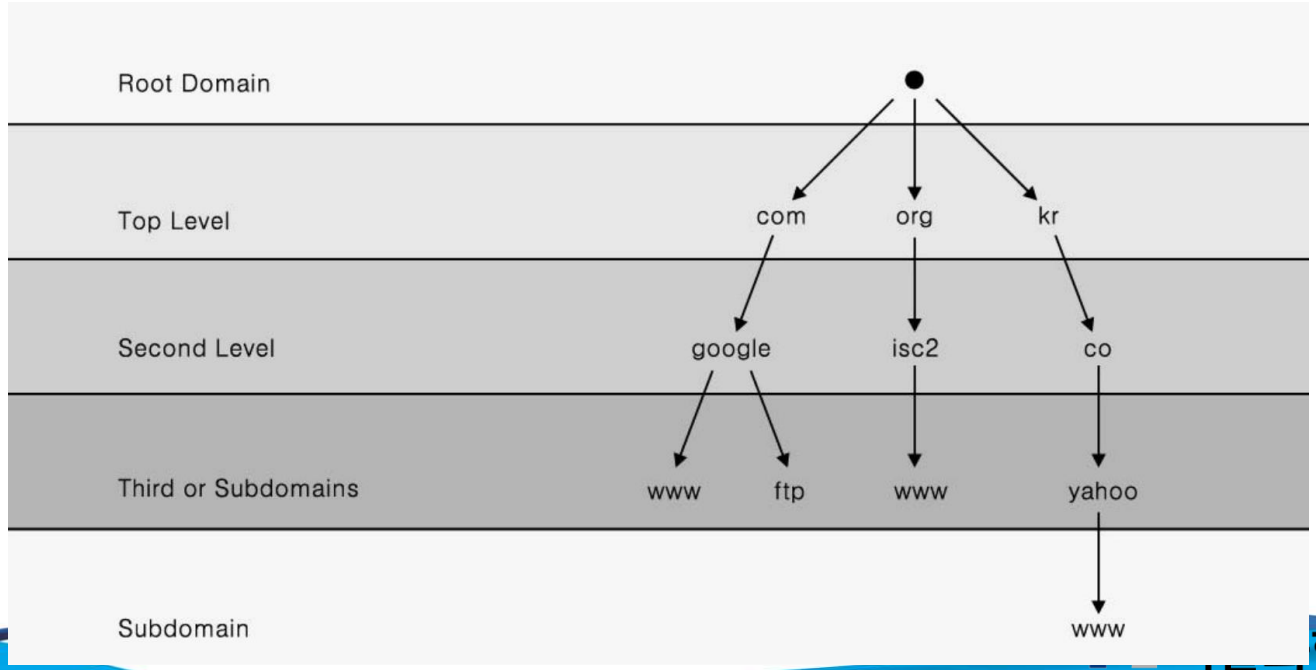
담당 지역	Whois 서버	담당 지역	Whois 서버
유럽	www ripe net	호주	Whois aunic net
아시아	www arin net	프랑스	www nic fr

- **DNS의 계층 구조**

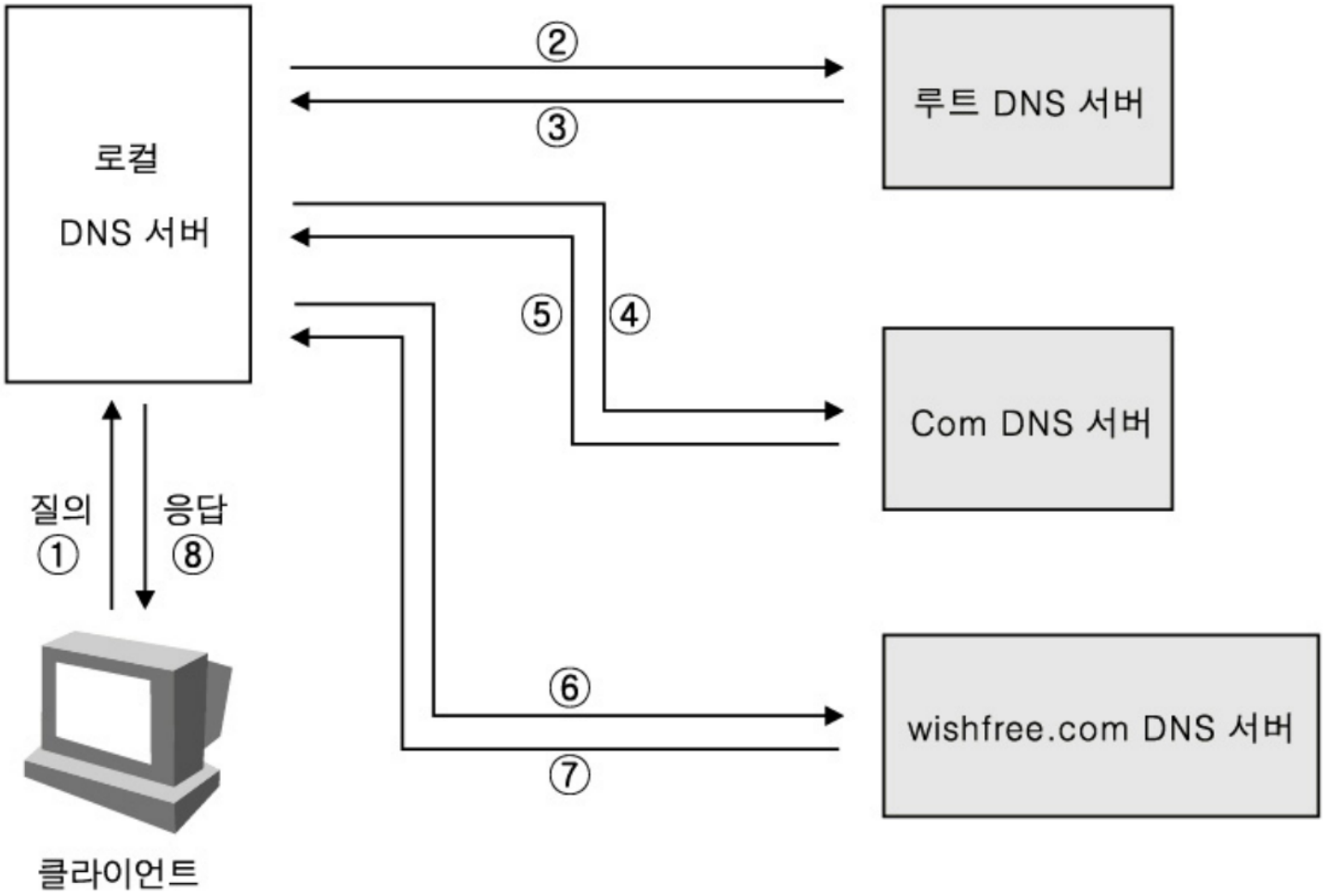
DNS(Domain Name System): 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행할 수 있도록 하기 위해 개발 ('전화번호부'에 비유)

예) **www.google.com.**

Subdomain Second level Top level Root



- **DNS의 서버 이름 해석 과정**

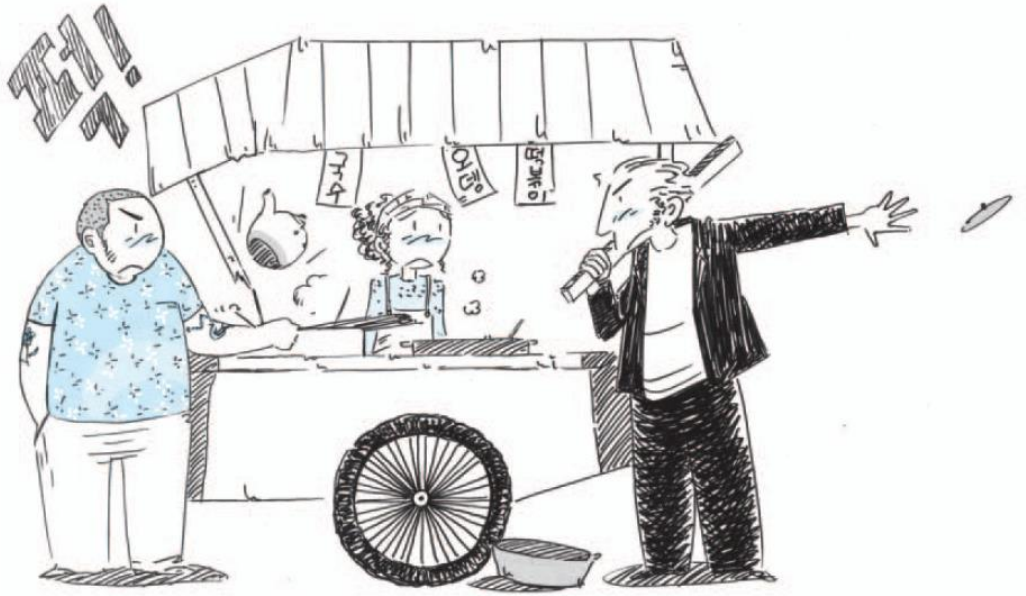


- **DNS 동작 원리 영상**
  https://youtu.be/2ZUxoi7YNgs

6-2 네트워크 공격과 보안

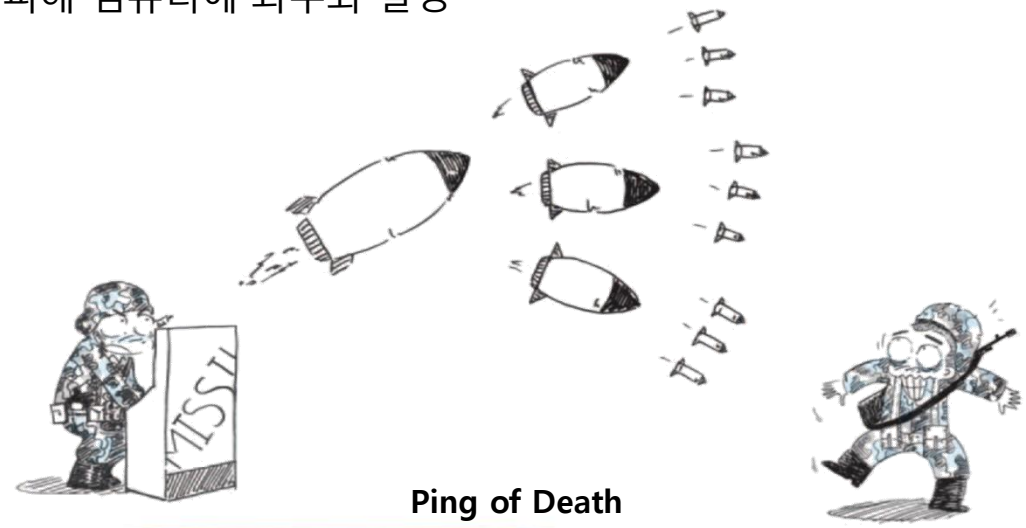
1. 서비스 거부 공격

- **서비스 거부 공격(Denial Of Service : DOS)**
  - 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 초과시켜 동작하지 못하게 하는 공격
  - 자원 고갈 공격형, 취약점 공격형으로 분류



포장마차에서 행해지는 서비스 거부 공격

- **자원 고갈 공격형**
  - 죽음의 핑 공격(Ping of Death)
    - 시스템을 파괴하는 데 가장 흔히 쓰인 초기의 DoS 공격
    - 네트워크에서 패킷을 전송하기 적당한 크기로 잘라서 보내는 특성을 이용한 공격
    - 네트워크의 연결 상태를 잘게 쪼개져 보내짐. 공격 대상 시스템은 대량의 작은 패킷을 수신하면서 네트워크가 마비됨
    - 점검하는 ping 명령을 보낼 때 패킷을 최대한 길게(최대 65,500바이트) 보내면 수백 수천 개의 패킷으로 나누어져 피해 컴퓨터에 과부화 발생



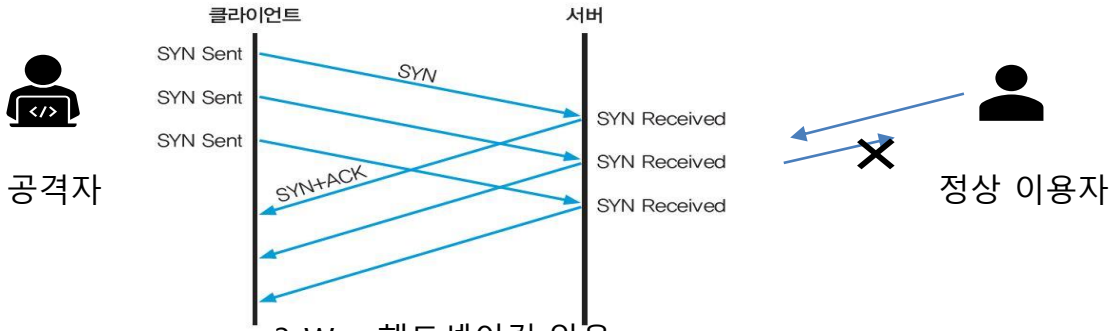
Ping of Death

- **자원 고갈 공격형**
  - SYN 플러딩 공격
    - 네트워크에서 서비스를 제공하는 시스템에 걸려있는 사용자 수 제한을 이용한 공격
    - 존재하지 않는 클라이언트가 서버별로 한정된 접속 가능 공간에 접속한 것처럼 속여 다른 사용자가 서비스를 제공받지 못하게 함

SYN Flooding 공격

- **자원 고갈 공격형**
  - SYN 플러딩 공격
    - TCP의 연결 과정인 3웨이 핸드셰이킹의 문제점을 악용한 공격
      - 마지막에 클라이언트가 서버에 다시 ACK 패킷을 보내야 하는데 보내지 않는다면 ?
      - 서버는 SYN Received 상태로 일정시간 기다려야 함
      - 공격자: 가상의 클라이언트로 위조된 수많은 SYN 패킷을 만들어 서버에 전송

        ➔ 서버의 가용 접속자 수를 모두 SYN Received 상태로 만듦



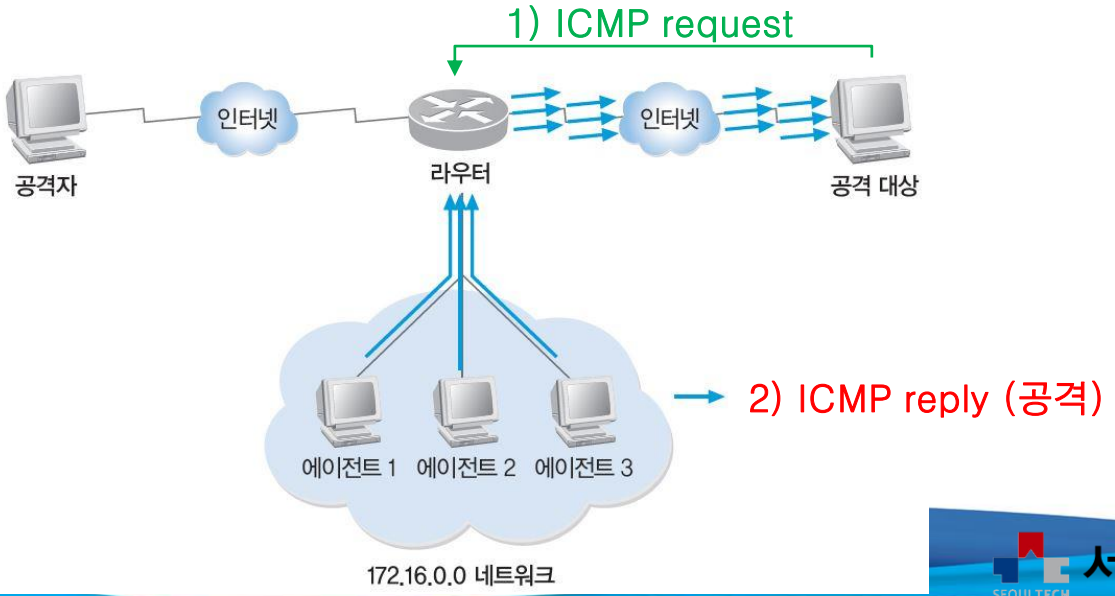
3-Way 핸드셰이킹 악용

- 공격 대응책은 SYN Received의 대기 시간을 줄이는 것
- 침입 방지 시스템과 같은 보안 시스템으로도 공격을 쉽게 차단할 수 있음

- **자원 고갈 공격형**
  - 스머프 공격

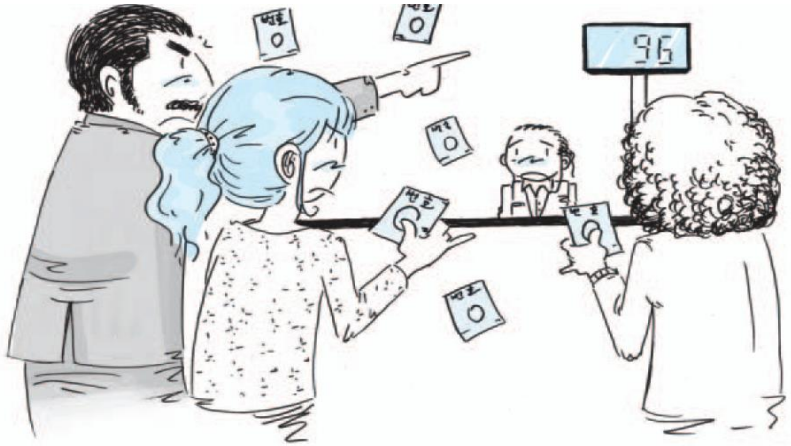
ICMP(Internet Control Message Protocol, 인터넷 제어 메시지 프로토콜)
네트워크 컴퓨터 위에서 돌아가는 운영체제에서 오류 메시지를 전송받는 데 주로 사용됨

    - ICMP 패킷과 네트워크에 존재하는 임의의 시스템으로 패킷을 확장해 서비스 거부 공격을 수행하는 것으로, 네트워크 공격에 많이 사용함
    - 다이렉트 브로드캐스트를 악용하는 것으로 공격 방법은 간단함
      - 기본적인 브로드캐스트: 목적지 IP 주소인 255 255 255 255를 가지고 네트워크의 임의의 시스템에 패킷을 보냄
      - 다이렉트 브로드캐스트(direct broadcast): 172.16.0.0 네트워크에 공격자가 브로드캐스트 하기 위해 목적지 IP 주소를 172.16.0.255 와 같이 설정하여 패킷을 보냄



- **취약점 공격형**
  - Boink, Bonk, TearDrop 공격
    - 프로토콜의 오류 제어 로직을 악용해 시스템 자원을 고갈시키는 방식
    - TCP 패킷에는 각 패킷이 데이터의 어느 부분을 포함하는지 표시를 위한 시퀀스 넘버가 기록
    - 시스템 패킷 재전송, 재조합에 과부하가 걸리도록 시퀀스 넘버를 속이는 공격
    - 이러한 공격에 의한 취약점은 패치를 통해 제거하는데 과부하가 걸리거나 계속 반복되는 패킷은 무시하고 버리도록 처리함

1) Boink와 Bonk 공격

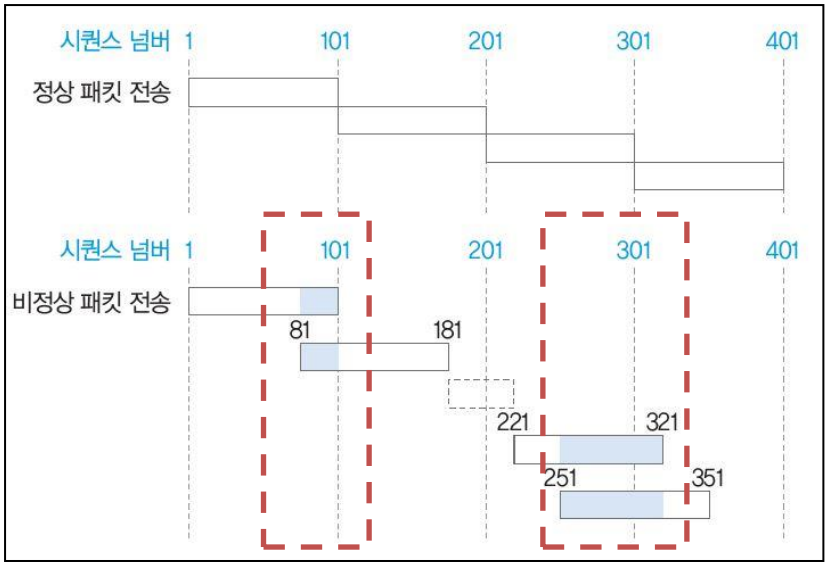


- **취약점 공격형**

2) TearDrop 공격

패킷 번호	정상 패킷의 시퀀스 넘버	공격을 위한 패킷의 시퀀스 넘버
1	1~101	1~101
2	101~201	81~181
3	201~301	221~321
4	301~401	251~351

TearDrop 공격시 패킷의 시퀀스 넘버



TearDrop 공격시 패킷의 배치

겹치는 부분이 있으면 패킷의 재조합 불가!

- **취약점 공격형**
  - Land 공격
    - 패킷을 전송할 때 출발지 IP주소와 목적지 IP주소값을 똑같이 만들어서 공격 대상에게 보내는 공격 (조작된 IP주소값은 공격 대상의 IP여야 함)
    - Land 공격에 대한 보안 대책도 운영체제의 패치를 통해서 가능
    - 방화벽 등과 같은 보안 솔루션에서 패킷의 출발지 주소와 목적지 주소의 적절성을 검증하는 기능을 이용하여 필터링

Land 공격

2. 분산 서비스 거부 공격

- **분산 서비스 거부 공격(DDOS: Distributed Denial Of Service)**
  - 공격 대상에 여러 대의 공격자를 분산적으로 배치하여 동시에 DoS를 발생시켜 공격하는 방법
  - DoS 공격의 상위 단계
  - 최근 발생하는 분산 서비스 거부 공격은 악성 코드와 결합된 형태가 다수

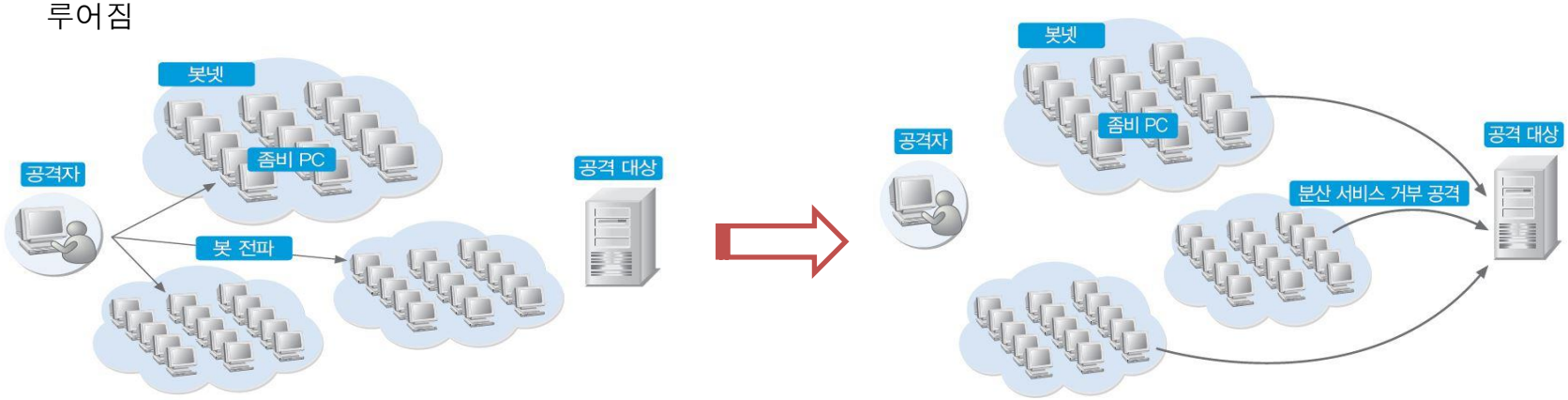
① PC에서 전파가 가능한 형태의 악성 코드 작성

② 사전에 공격 대상과 스케줄을 정한 뒤 미리 작성한 악성 코드에 코딩

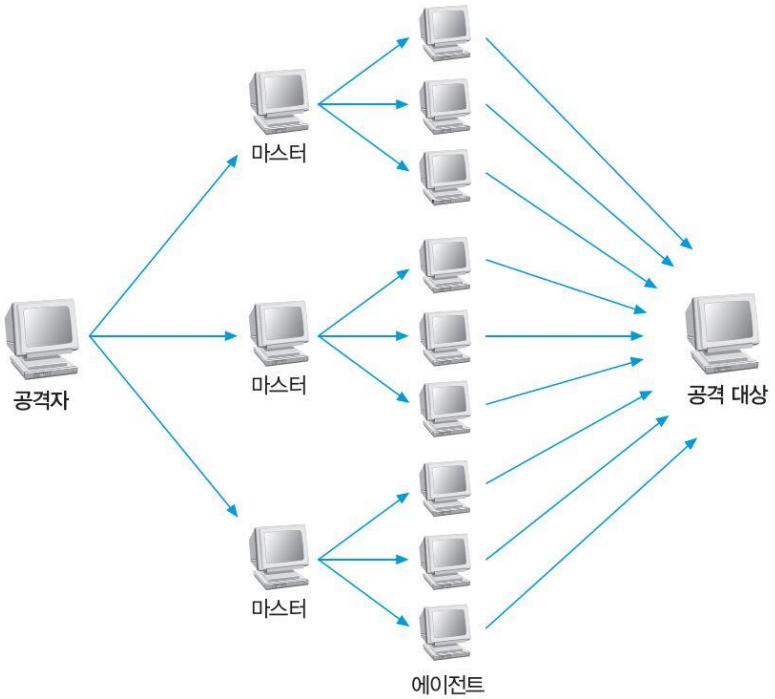
③ 인터넷으로 악성 코드 전파하는데 전파 과정에서는 공격이 이루어지지 않도록 잠복

– 봇넷(botnet): 좀비 PC끼리 형성된 네트워크

④ 공격자가 명령을 내리거나 정해진 스케줄에 따라 일제히 공격을 수행하면 대규모의 분산 서비스 거부 공격이 이루어짐



- **분산 서비스 거부 공격(DDOS)**
  - 분산 서비스 거부 공격의 기본 구성



- ✓ **공격자(attacker):** 공격을 주도하는 해커 컴퓨터
- ✓ **마스터(master):** 공격자에게 직접 명령을 받는 시스템으로 여러 대의 에이전트를 관리
- ✓ **핸들러(handler) 프로그램**: 마스터 시스템의 역할을 수행하는 프로그램
- ✓ **에이전트(agent):** 직접 공격을 가하는 시스템
- ✓ **데몬(daemon) 프로그램:** 에이전트 시스템의 역할을 수행하는 프로그램

- **DOS/DDOS 탐지 및 보안 방법**
  - 사이버 대피소 이용 : DDoS 트래픽을 대피소로 우회하여 분석, 차단
  - DDoS보안 솔루션 이용 : 서버 접속 사용자를 정상 사용자와 좀비PC 구분 검증
    - ✓ 안랩, 시큐아이, 윈스 등 네트워크 보안 기업

KISA 사이버대피소

DDoS 보안 솔루션

3. 스니핑 공격

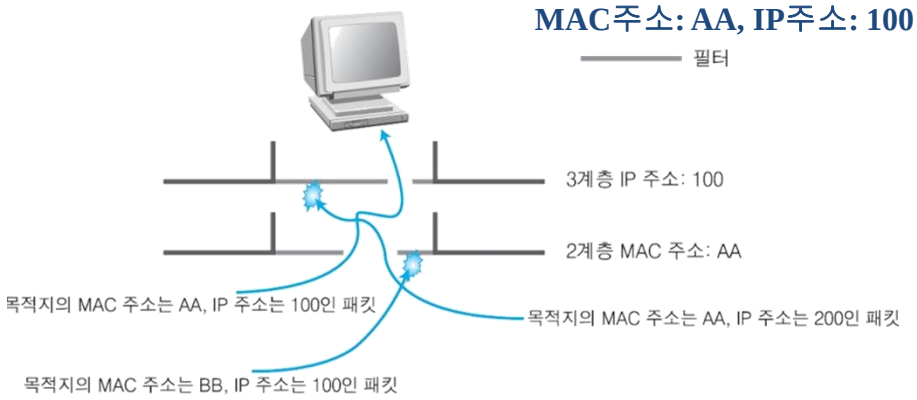
- **스니핑 공격**
  - Sniff : '코를 킁킁거리다'
  - 데이터 속에서 정보를 찾는 것으로 공격 시 아무것도 하지 않고 조용히 있음 (수동적 공격)
  - 스니핑 공격자는 가지지 말아야 할 정보까지 모두 볼 수 있어야 하므로

랜 카드의 프러미스큐어스(promiscuous) 모드를 이용해 데이터 링크 계층과 네트워크 계층의 정보를 이용한 필터링을 해제함

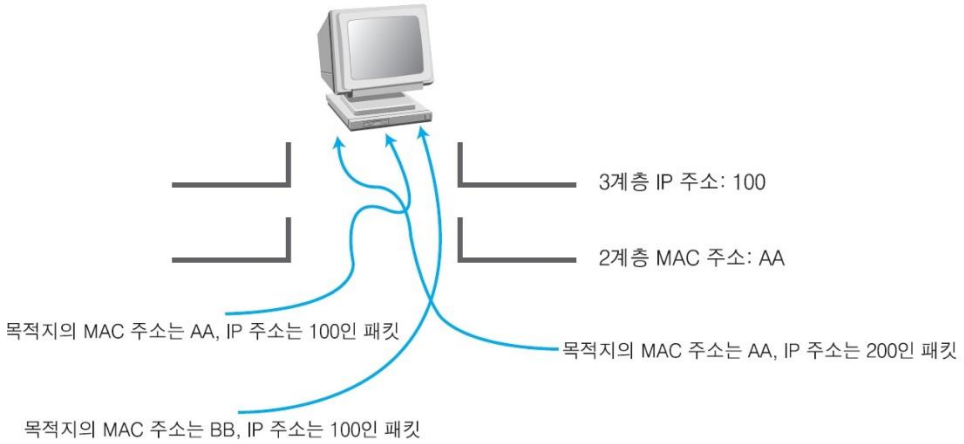
스니퍼 공격

❖ 스니핑 공격자의 프러미큐어스 모드

- 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 볼 수 있어야 하기 때문에 2계층과 3계층 정보를 이용한 필터링은 방해물임
- 이럴 때 2, 3계층에서의 필터링을 해제 ➔ 랜 카드의 모드를 프러미큐어스 (Promicuous) 모드



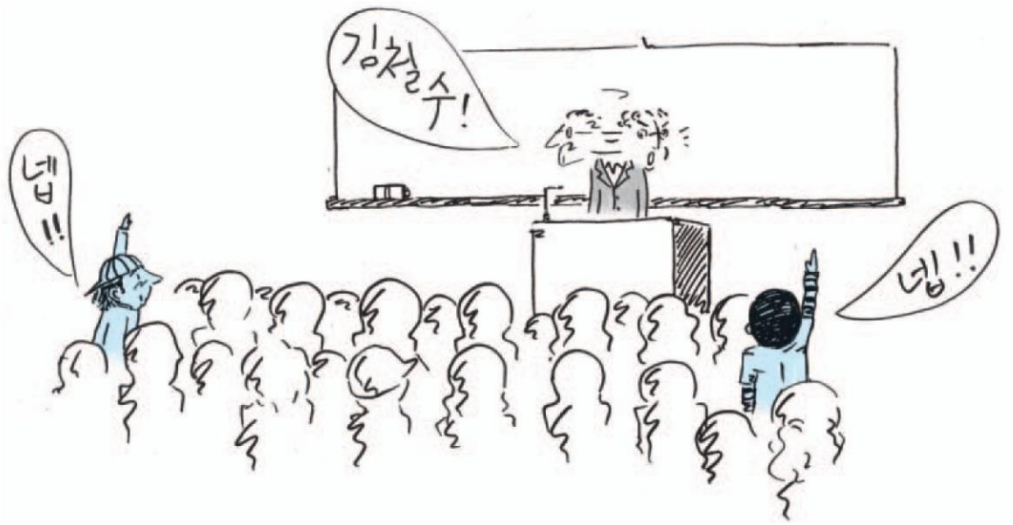
정상적인 네트워크 필터링



네트워크 필터링 해제 상태

- **스니핑 공격의 종류**
  - 스위치 재밍 공격
    - 스위치가 MAC 주소 테이블을 기반으로 포트에 패킷을 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격
    - MACOF 공격 이라고도 함
    - 고가의 스위치는 MAC 테이블의 캐시와 연산자가 쓰는 캐시가 독립적으로 나뉘어 있어 스위치 재밍 공격이 통하지 않음
  - SPAN 포트 태핑 공격
    - 스위치의 포트 미러링(port mirroring) 기능을 이용한 공격
    - 포트 미러링: 각 포트에 전송되는 데이터를 미러링하는 포트에도 똑같이 보내는 것으로 침입 탐지 시스템이나 네트워크 모니터링 또는 로그 시스템을 설치할 때 많이 사용

- **스니핑 공격의 탐지**
  - 자신의 이름이 아닌데도 아무 이름에나 받아들여 대답하다가 교수님께 걸리는 프리미스큐어스 모드의 학생



대출이 들키는 상황

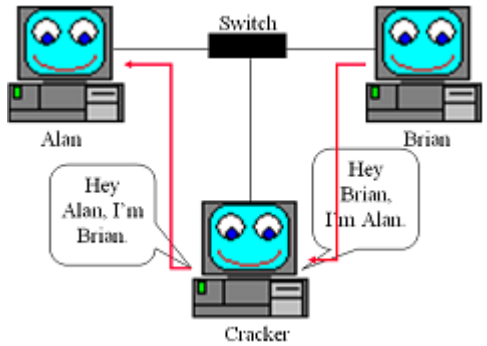
- **스니핑 공격의 탐지**
  - ping을 이용한 스니퍼 탐지
    - 의심이 가는 호스트에 네트워크에 존재하지 않는 MAC 주소를 위장해서 ping을 보내면 스니퍼 탐지 가능
    - 존재하지 않는 MAC 주소를 사용했으므로 스니핑을 하지 않는 호스트라면 ping request를 볼 수 없는 것이 정상이기 때문
  - ARP를 이용한 스니퍼 탐지
    - 위조된 ARP request를 보냈을 때 ARP response가 오면 프러미스큐어스 모드로 설정된 것이므로 탐지 가능
  - DNS를 이용한 스니퍼 탐지
    - 일반적인 스니핑 프로그램은 스니핑한 시스템의 IP 주소에 DNS의 이름 해석 과정인 Reverse-DNS lookup을 수행함
    - 대상 네트워크로 ping sweep를 보내고 들어오는 Reverse-DNS lookup을 감시하면 스니퍼 탐지 가능

- 유인을 이용한 스니퍼 탐지
  - 가짜 아이디와 패스워드를 네트워크에 계속 뿌려서 공격자가 이를 이용해 접속을 시도하면 스니퍼 탐지 가능

- ARP watch를 이용한 스니퍼 탐지
  - ARP watch는 MAC 주소와 IP 주소의 매칭 값을 초기에 저장하고 ARP 트래픽을 모니터링하여 이를 변하게 하는 패킷이 탐지되면 알려주는 툴
  - 대부분의 공격 기법은 위조된 ARP를 사용하기 때문에 쉽게 탐지 가능

4. 스푸핑 공격

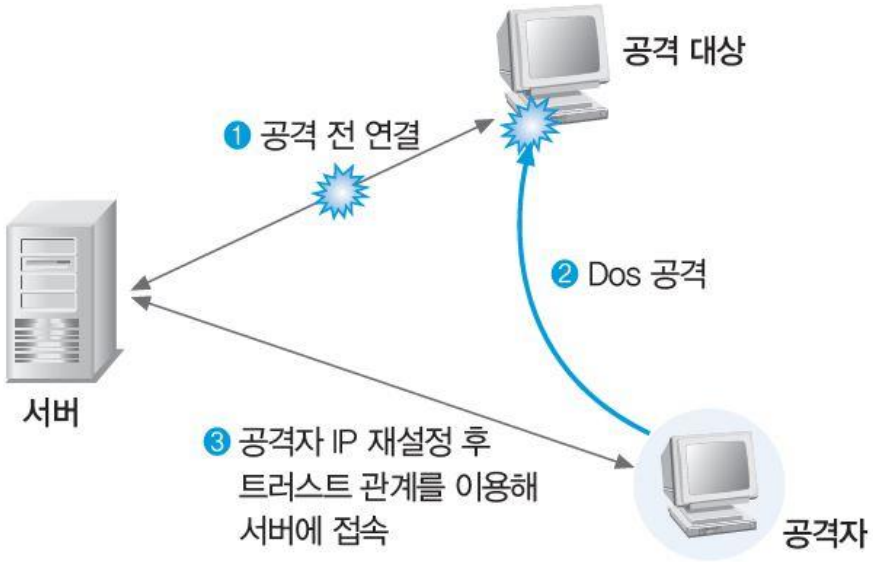
- **스푸핑 공격**
  - Spoof : '속이기'
  - 외부의 악의적 공격자가 웹사이트를 구성하여 사용자 방문을 유도, TCP/IP 구조적 결함을 이용하여 사용자 시스템 권한을 획득한 뒤, 정보를 빼가는 공격



- **ARP 스푸핑 공격**
  - ARP 스푸핑은 MAC 주소를 속이는 것
  - 로컬에서 통신하는 서버와 클라이언트의 IP 주소에 대한 데이터 링크 계층의 MAC 주소를 공격자의 MAC 주소로 속여
  - ➢ 클라이언트에서 서버로 가는 패킷이나 서버에서 클라이언트로 가는 패킷이 공격자에게 향하게 하여 랜의 통신 흐름을 왜곡하는 공격
  - 현재 인지하는 IP와 해당 IP를 가진 시스템의 MAC 주소 목록 확인 가능

➔ ARP 테이블

- **IP 스푸핑 공격**
  - 트러스트 관계(신뢰 관계)를 맺고 있는 서버와 클라이언트를 확인한 후
  - 클라이언트에 서비스 거부 공격을 하여 연결을 끊은 뒤
  - 클라이언트의 IP 주소를 확보한 공격자는 실제 클라이언트처럼 패스워드 없이 서버에 접근



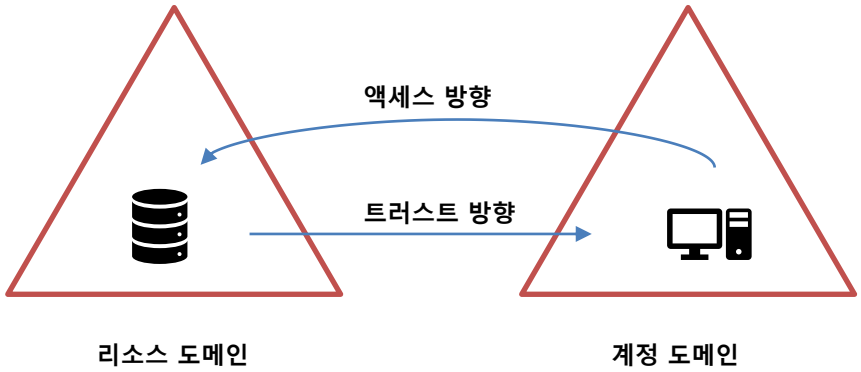
[IP 스푸핑을 이용한 서버 접근]

❖ 트러스트에 대한 이해

- 트러스트는 도메인 사이에 설정되는 신뢰 관계
- 서버에 미리 정보가 기록된 클라이언트가 접근하면 아이디와 패스워드 입력 없이 로그인을 허락하는 인증법
- 사용자가 다른 도메인 자원을 사용할 수 있도록 함

• 트러스트의 방향성

- 단방향 : 트러스트 방향이 일방적으로 설정된 경우
- 양방향 : 두 개의 도메인이 서로 상대방 도메인에 대해 트러스트를 준 경우



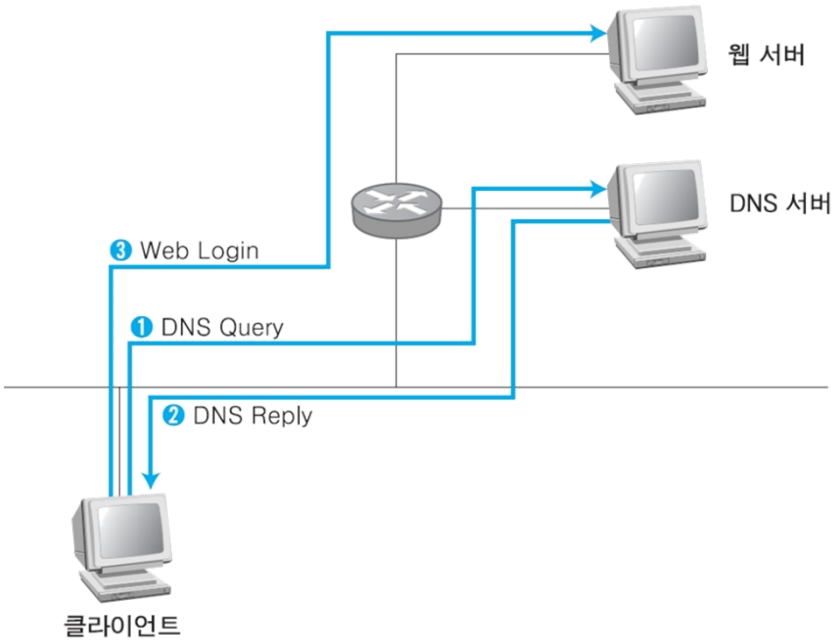
- **DNS 스푸핑 공격**
  - 실제 DNS 서버보다 빨리 DNS response 패킷을 보내어 공격 대상이 잘못된 IP 주소로 웹 접속을 하도록 유도하는 공격
  - DNS 스푸핑 공격을 막으려면 중요 서버에 대해 DNS query를 보내지 않으면 되는 데 이를 위해서는 중요 접속 서버의 URL에 대한 IP를 hosts 파일에 등록해야 함
  - 모든 서버의 IP를 등록하는 것은 무리이므로 모든 서버의 DNS 스푸핑을 막기는 어려움
  - DNS Cache Poisoning 공격, DNS 서버 변조 공격, 도메인 서버 변조 공격 등

- **정상적인 DNS**

① 클라이언트가 DNS 서버에게 접속하고자 하는 IP 주소(www wishfree com과 같은 도메인 이름)를 물어봄 (패킷은 DNS Query)

② DNS 서버가 해당 도메인 이름에 대 한 IP 주소를 클라이언트에게 보내줌

③ 클라이언트가 받은 IP 주소를 바탕으로 웹 서버를 찾아감

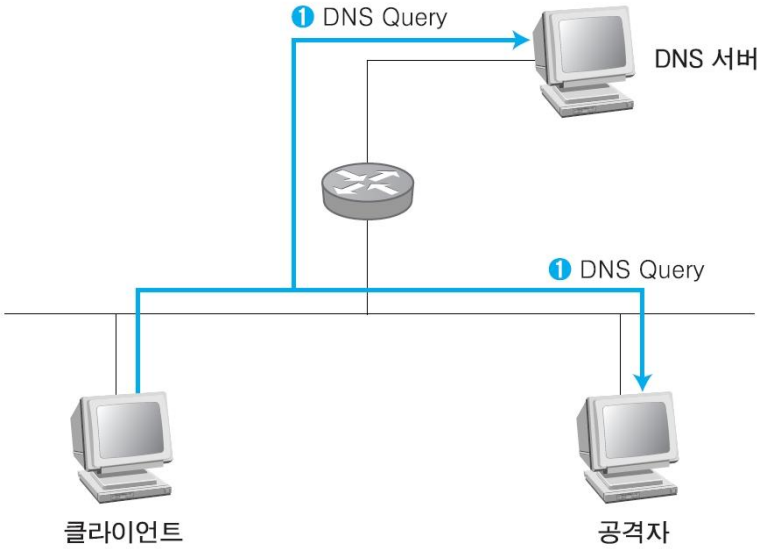


정상적인 DNS 서비스

- **DNS 공격**

① 클라이언트가 DNS 서버로 DNS Query 패킷을 보내는 것을 확인

- 스위칭 환경일 경우에는 클라이언트 DNS Query 패킷을 보내면 이를 받아야 하므로 ARP 스푸핑과 같은 선행 작업이 필요함
- 만약 허브를 쓰고 있다면 모든 패킷이 자신에게도 전달되므로 클라이언트가 DNS Query 패킷을 보내는 것을 자연스럽게 확인할 수 있음



DNS Query

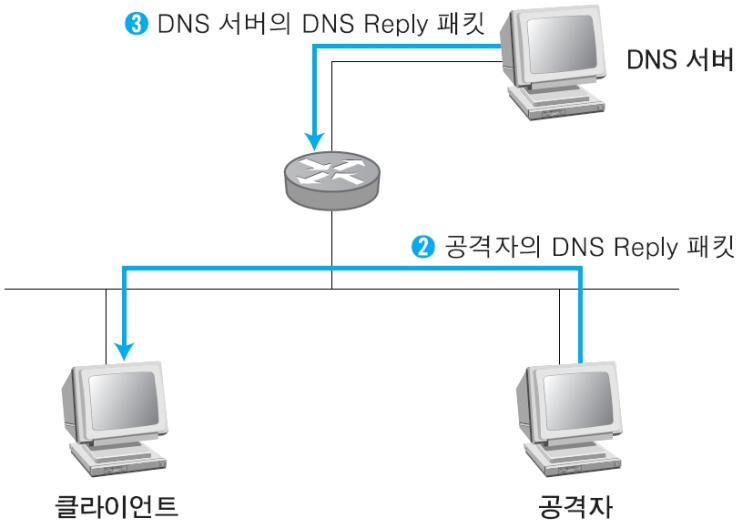
- **DNS 공격**

② 공격자는 로컬에 존재하므로 DNS 서버보다 지리적으로 가까움

따라서 DNS 서버가 올바른 DNS Response 패킷을 보내주기 전에 클라이언트에 게 위조된 DNS Response 패킷을 보낼 수 있음

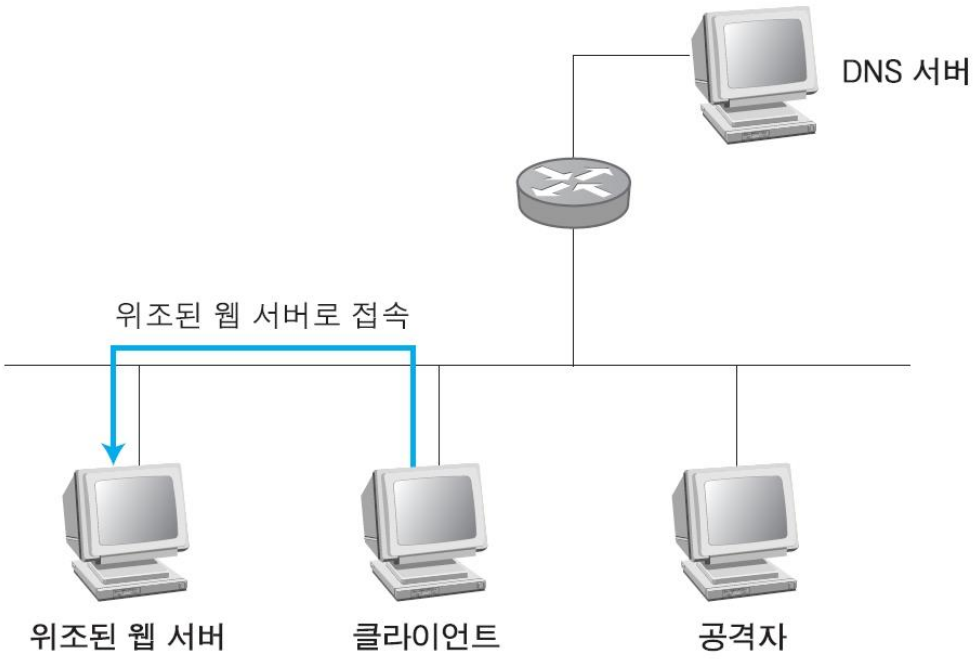
② 클라이언트는 공격자가 보낸 DNS Response 패킷을 올바른 패킷으로 인식하고, 웹에 접속

- 지리적으로 멀리 떨어져 있는 DNS 서버가 보낸 DNS Response 패킷은 버림



공격자와 DNS 서버의 DNS Response

- **DNS 공격 결과**



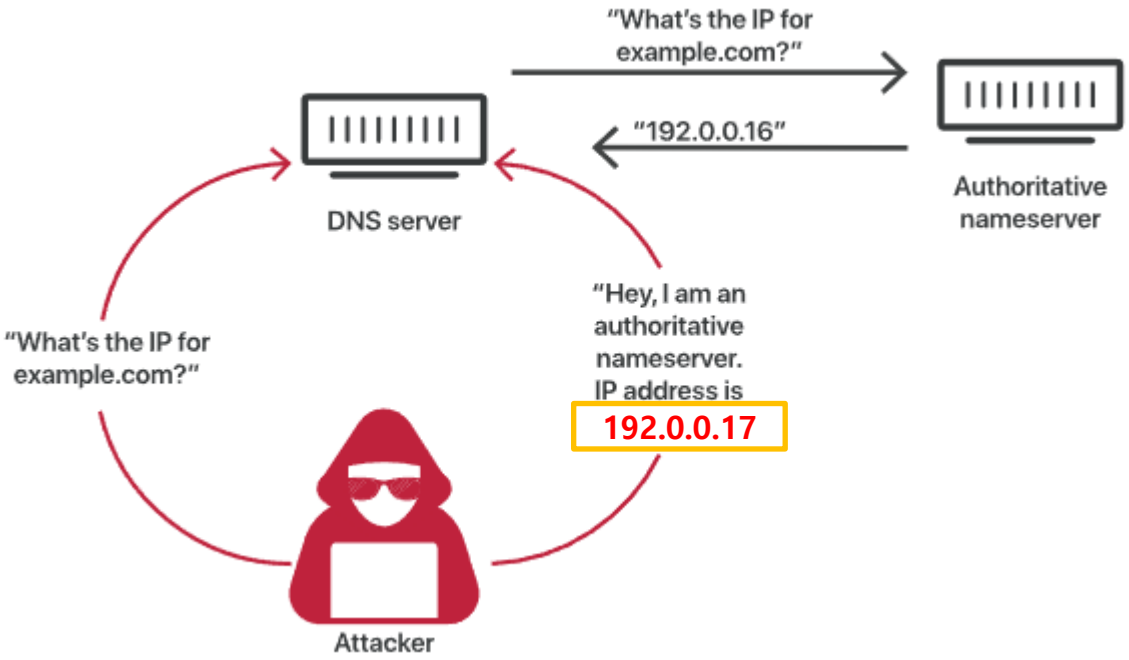
공격 성공 후 도착한 DNS 서버의 DNS Response

- **DNS 스푸핑 공격에 대한 대응책**
  - hosts 파일에는 주요 URL과 IP 정보가 등록

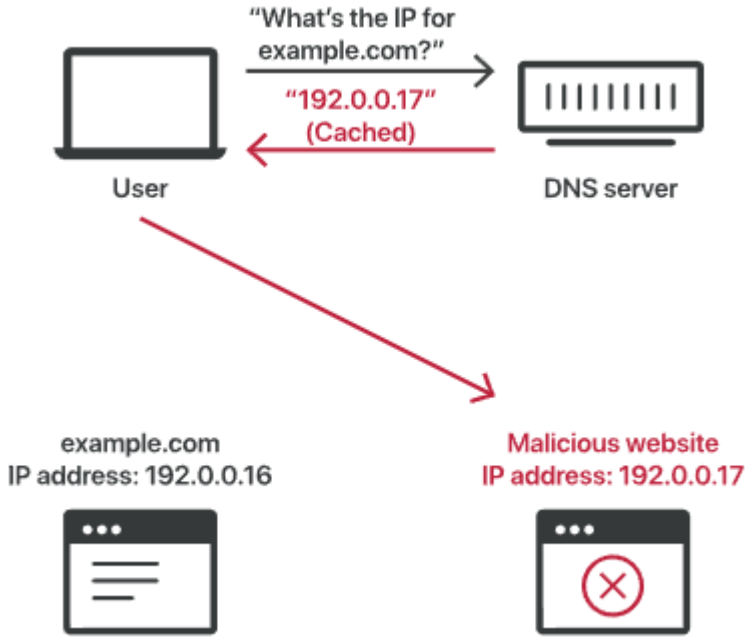
```
127 0 0 1              localhost
200 200 200 123    www wishfree com
201 202 203 204    www sysweaver com
```

- **DNS Cache Poisoning (캐시 오염)**
  - DNS의 Resolver 캐시에 변조된 주소를 주입해 사용자가 웹페이지 접속 시 공격자가 의도한 페이지로 접속을 유도하는 주소 변조 공격

- **DNS 캐시 악성 침입 프로세스**
  - 공격자는 DNS 이름 서버를 가장하여 DNS 확인자에 요청을 보낸 후,
  - DNS 확인자가 이름 서버를 쿼리할 때 응답을 위조하여 DNS 캐시를 감염시킴



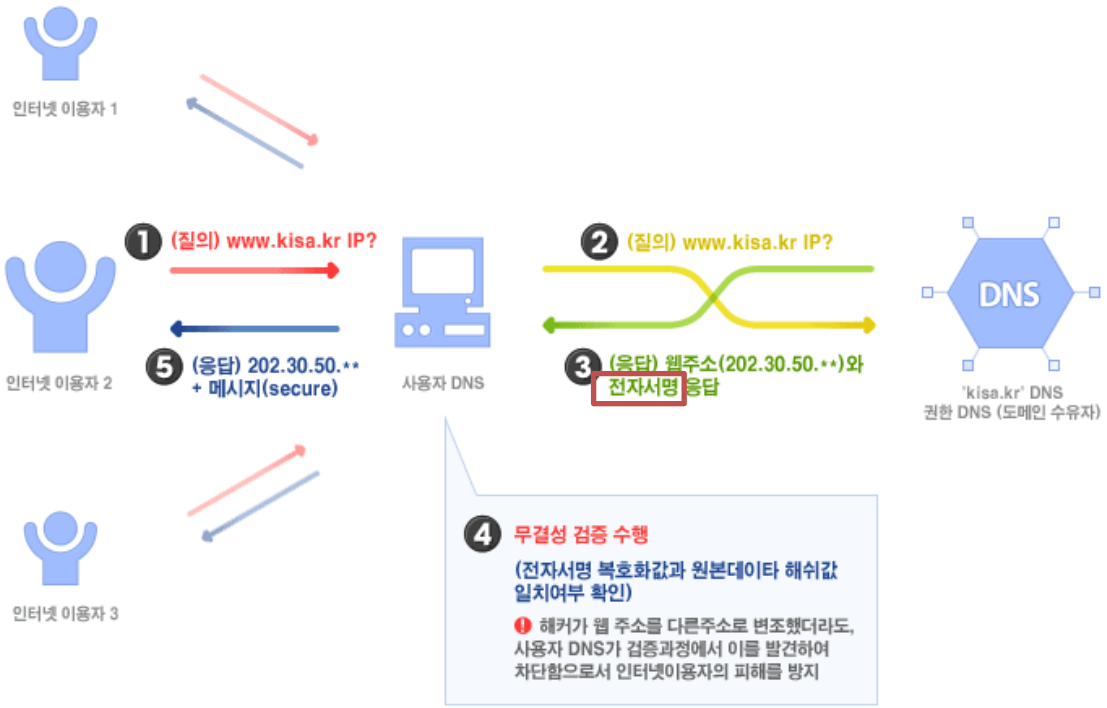
- 악성 침입된 DNS 캐시



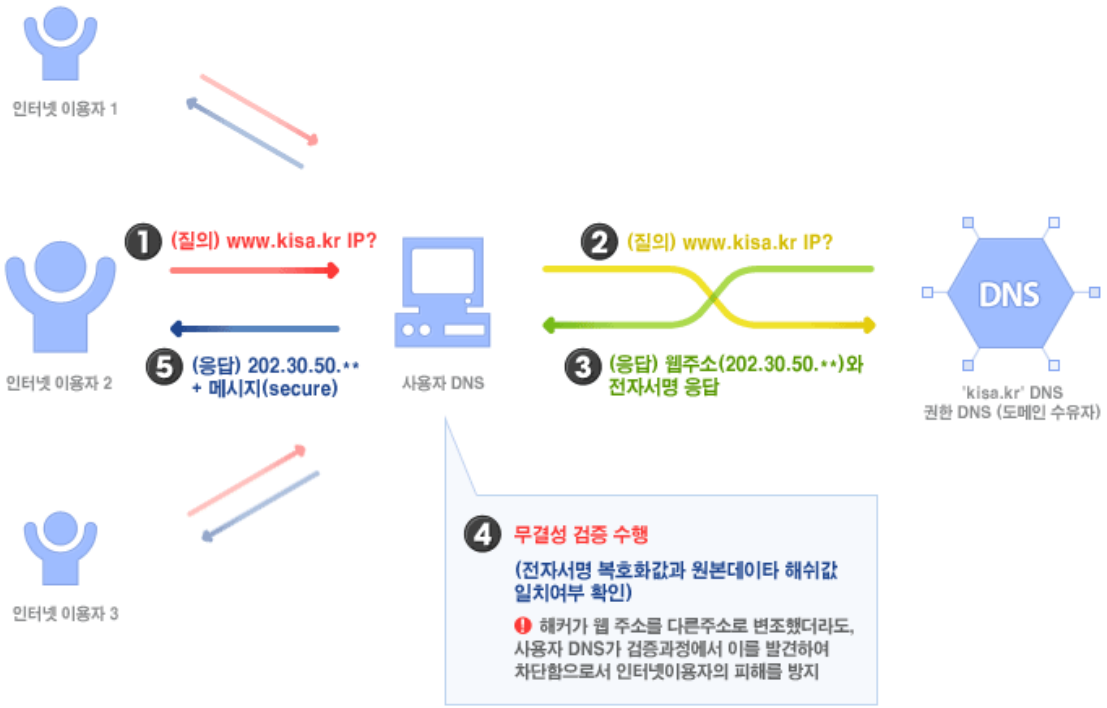
- **DNS Cache Poisoning 공격의 대응**

  ==> DNSSEC(DNS Security Extension)

- **DNSSEC(DNS Security Extensions)**
  - DNS 데이터 대상의 데이터 위조-변조 공격을 방지하기 위한 인터넷 표준기술
  - 공개키 암호화방식(Public Key Cryptography)의 전자서명 기술을 DNS 체계에 도입 적용



- **DNSSEC(DNS Security Extensions)**
  - DNS 데이터 대상의 데이터 위조-변조 공격을 방지하기 위한 인터넷 표준기술
  - 공개키 암호화방식(Public Key Cryptography)의 전자서명 기술을 DNS 체계에 도입 적용



- **보안침해 공격에 대한 DNSSEC이 제공하는 보안성 범위**

공격유형	방어여부	비고
파밍 (캐시 포이즈닝)	방어/방지	- DNS 데이터 위-변조 방식 이용 공격에 효과적 대응
피싱	해당없음	- 피싱은 유사 도메인네임 사용하지만, 데이터 위-변조에 해당하지 않음
DDoS 공격	해당없음	- DDoS 공격방어 메커니즘이 아님
웜바이러스에 의한 호스트 정보변조	해당없음	- DNSSEC은 DNS 질의응답 절차관련 "데이터 위-변조" 방지기술

- **세션 하이재킹**
  - 세션 가로채기라는 뜻으로 세션은 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태
  - 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로채는 것
  - 가장 쉬운 세션 가로채기
    - ✓ 누군가 작업을 하다가 잠시 자리를 비운 PC를 몰래 사용해 원하는 작업을 하는 것

- **TCP 세션 하이재킹**
  - TCP의 고유한 취약점을 이용하여 정상적인 접속을 빼앗는 방법
  - 서버와 클라이언트에 각각 잘못된 시퀀스 넘버를 사용해서 연결된 세션에 잠시 혼란을 준 뒤 자신이 끼어 들어가는 방식

    ① 클라이언트와 서버 사이의 패킷을 통제하고 ARP 스푸핑 등으로 통신 패킷 모두가 공격자를 지나가게 함

    ② 서버에 클라이언트 주소로 연결을 재설정하기 위한 RST reset 패킷을 보냄

    서버는 패킷을 받아 클라이언트의 시퀀스 넘버가 재설정된 것으로 판단하고 다시 TCP 3-웨이 핸드셰이킹을 수행

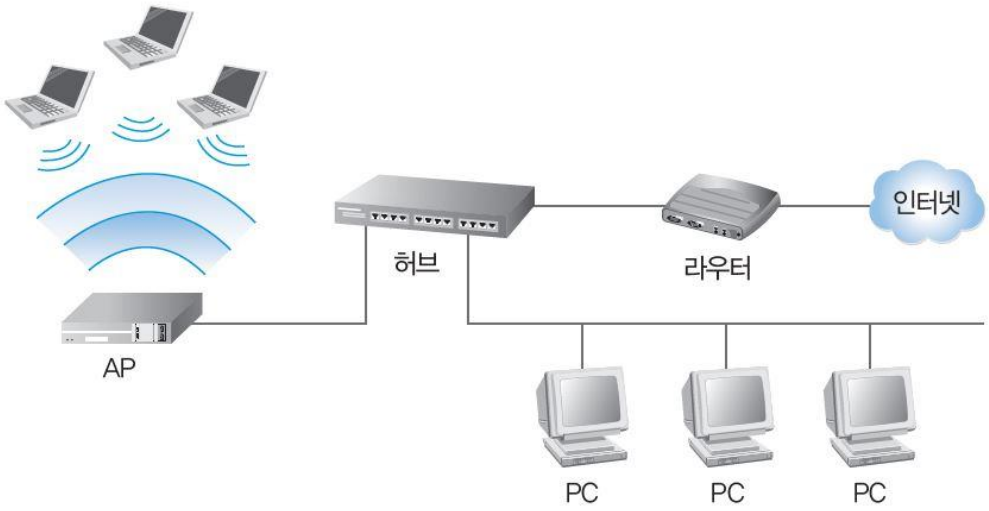
    ③ 공격자는 클라이언트 대신 연결되어 있던 TCP 연결을 그대로 물려받음

- **세션 하이재킹 대응책**
  - 텔넷과 같은 취약한 프로토콜을 이용하지 않고 SSH와 같이 세션 인증 수준이 높은 프로토콜로 서버에 접속해야 함
  - 또는 클라이언트와 서버 사이에 MAC 주소를 고정해야 함

6-3 무선 네트워크 공격과 보안

무선 네트워크 공격과 보안

- **무선 랜**
  - 유선 랜의 네트워크를 확장하려는 목적으로 사용되며 이를 위해서는 내부의 유선 네트워크에 AP (Access Point) 장비를 설치해야 함
  - 확장된 무선 네트워크는 AP를 설치한 위치에 따라 통신 영역이 결정되며 보안이 설정되어 있지 않으면 공격자가 통신 영역 안에서 내부 사용자와 같은 권한으로 공격 가능

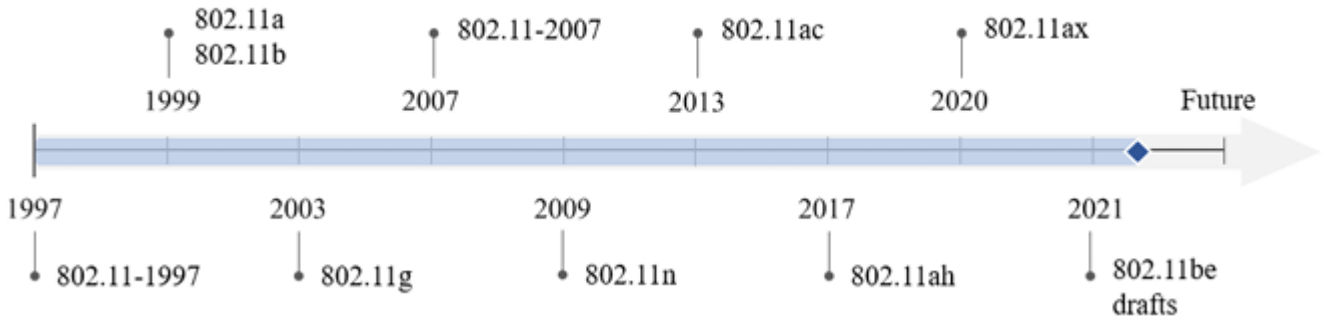


무선 네트워크 공격과 보안

- **무선 랜**
  - 주요 무선 랜 프로토콜

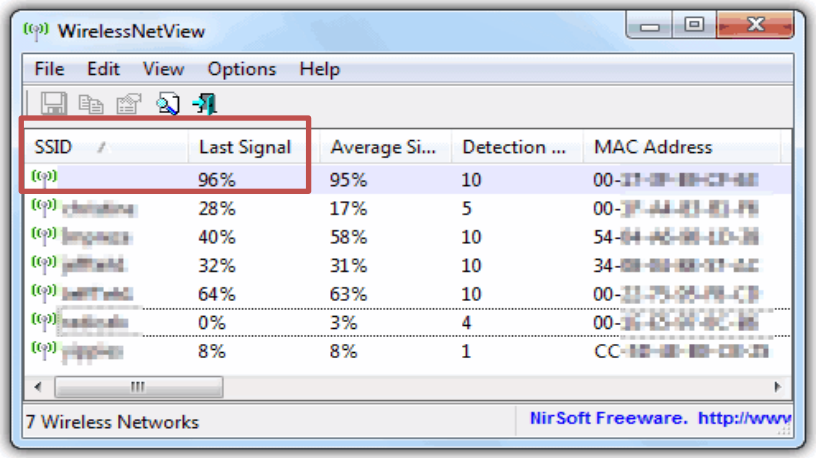
시기	프로토콜	주요 사항	설명
1997년 7월	802.11	2.4GHz/2Mbps	최초의 무선 랜 프로토콜이다.
1999년 9월	802.11b	2.4GHz/11Mbps	와이파이(Wi-Fi)라고 하며 WEP 방식의 보안을 구현한다.
	802.11a	5GHz/54Mbps	와이파이5(Wi-Fi5)라고 하며, 전파 투과성과 회절성이 떨어져 통신 단절 현상이 심하고 802.11b와 호환되지 않는다.
2003년 6월	802.11g	2.4GHz/54Mbps	802.11b에 802.11a의 속도 성능을 추가한 프로토콜로, 802.11b와 호환되지만 네트워크 공유 시 데이터 처리 효율이 현격히 떨어지는 문제가 발생한다.
2004년 6월	802.11i	2.4GHz/11Mbps (802.11b와 동일)	802.11b 표준에 보안성을 강화한 프로토콜이다.
2007년	802.11n	5GHz, 2.4GHz	여러 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술로, 대역폭 손실을 최소화하고 최대 속도는 600Mbps이다.
2012년	802.11ac	5GHz, 2.4GHz	5GHz 주파수에서 높은 대역폭(80~160MHz)을 지원하고, 2.4GHz에서는 802.11n과의 호환성을 위해 40MHz까지 대역폭을 지원한다.
2014년	802.11ad	60GHz	최대 속도가 7Gb/s이다. 기존 2.5GHz/5GHz 대신 60GHz 대역을 사용하여 데이터를 전송하는 방식으로, 대용량 데이터나 무압축 HD 비디오 등 높은 비트레이트 동영상 스트리밍에 적합하다. 60GHz는 장애물 통과가 어려워서 10m 이내 같은 공간 내에서만 사용 가능하여 근거리 기기에만 사용할 수 있다.

- **IEEE 802.11 WLAN 표준 타임라인**



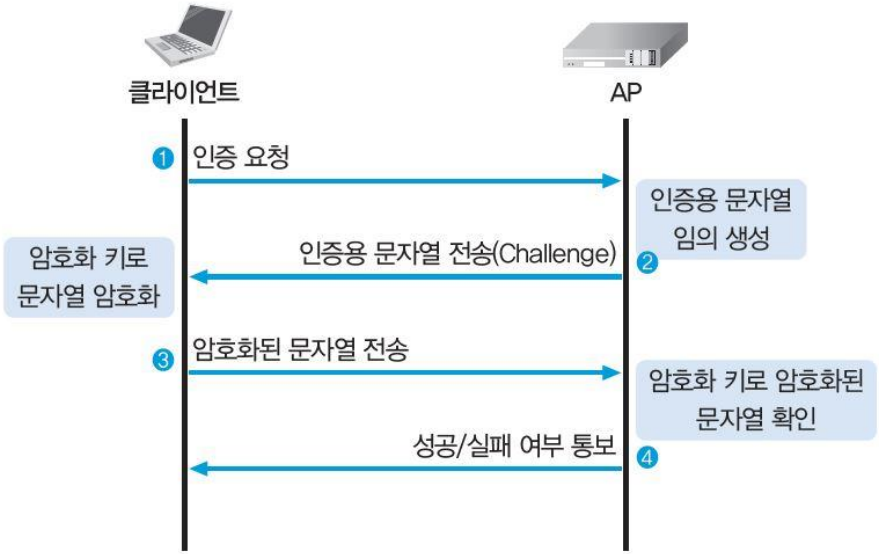
무선 네트워크 공격과 보안

- **무선 네트워크 보안**
  - **물리적인 보안 및 관리자 패스워드 변경**
    - AP 보호를 위한 첫 번째 사항은 물리적인 보안
    - AP 신호 세기가 건물 내에 한정되도록 출력을 조정하고, 눈에 쉽게 띄지 않는 곳에 설치
    - 설치 후 기본 계정 패스워드는 반드시 재설정
  - **SSID 브로드캐스팅 금지**
    - 무선랜을 검색을 위한 AP 탐색 이후, 나타나는 SSID(Service Set Identifier)는 쉽게 노출 되지 않도록 Hidden AP로 변경한다



무선 네트워크 공격과 보안

- **무선 랜 통신의 암호화**
  - **WEP (Wired Equivalent Privacy)**
    - ✓ 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용되기 시작
    - ✓ 1987년에 만들어진 RC 4 암호화와 알고리즘을 기본으로 사용
    - ✓ 문제점
    - 전사공격 (Brute force Attack)에 취약
    - 짧은 길이(24bit)의 초기벡터(IV) 사용 위험
    - RC4암호 안전성 깨짐

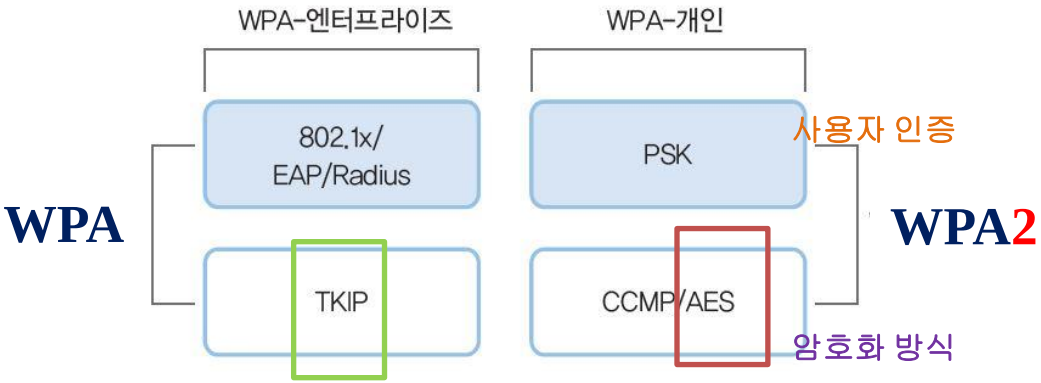


[WEP 암호화 세션의 생성]

무선 네트워크 공격과 보안

- **무선 랜 통신의 암호화**
  - **WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)**
    - WEP 방식 보안의 문제점을 해결하기 위해 만들어짐
    - WPA 규격은 WPA-개인과 WPA-엔터프라이즈로 각각 규정

[WPA 규격의 구조]

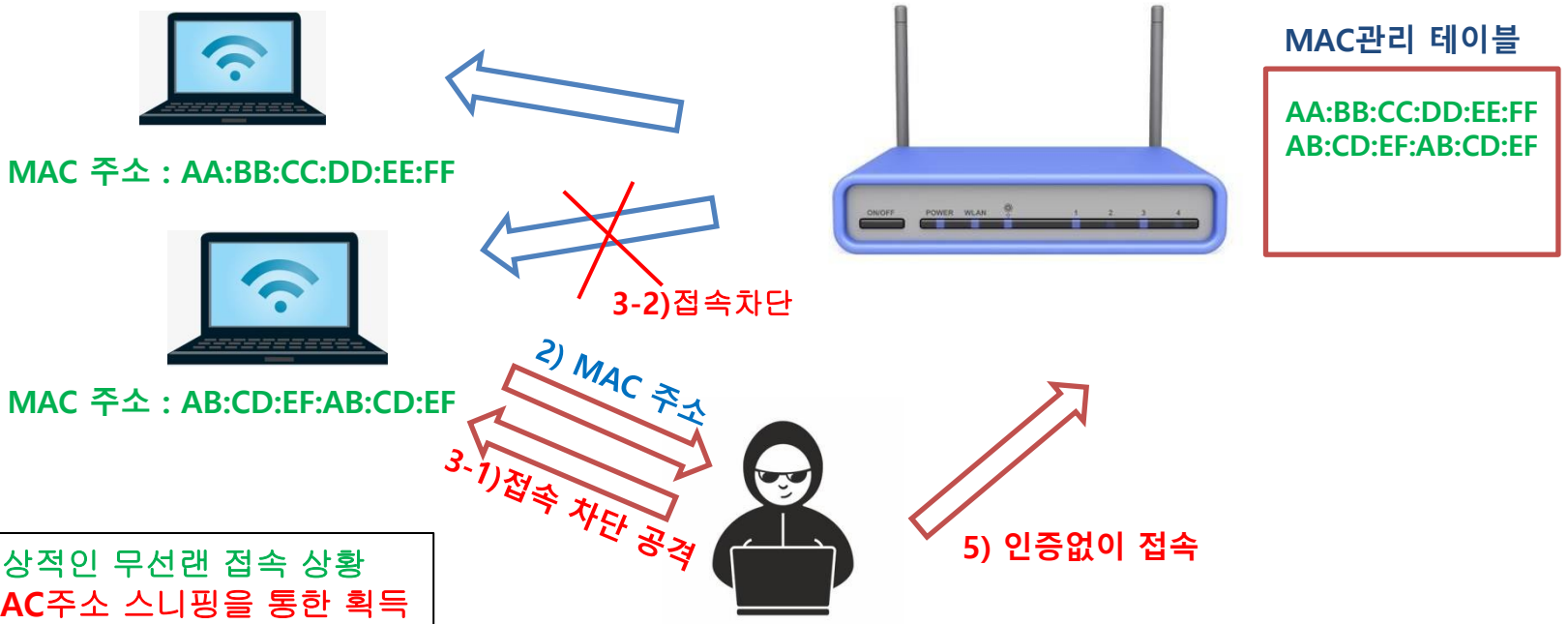


- EAP: Extensible Authentication Protocol
- TKIP: Temporal Key Integrity Protocol
- PSK: Pre-Shared Key
- CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

WEP - **RC4** 안전성 문제로 한시적으로 대체하기 위한 개선 확장판

무선 네트워크 공격과 보안

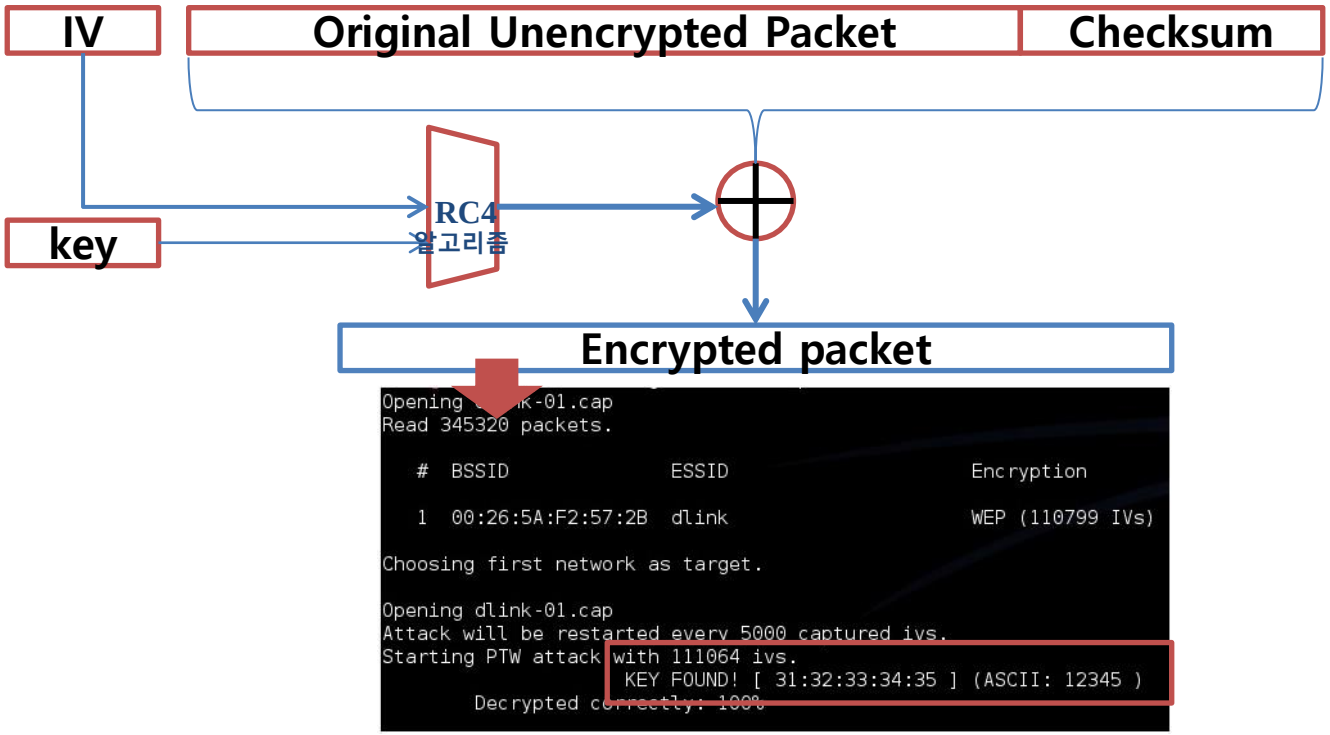
- **무선 네트워크 공격**
  - 무선 랜 인증 우회



1) 정상적인 무선랜 접속 상황
2) MAC주소 스니핑을 통한 획득
3) 공격으로 대상PC 접속 차단
4) 공격자의 MAC주소 변경
5) 공격자의 무선랜 접속 성공

무선 네트워크 공격과 보안

- **무선 네트워크 공격**
  - WEP 암호 크랙
    - 키스트림을 재사용하는 취약점이 있음
    - 일정 평문을 얻고 암호문을 만드는 IV에 대한 키스트림 테이블을 생성할 수 있음
    - 2004년 발표된 802 11i 표준에서 IEEE는 WEP를 사용중단(deprecated) 선언



[WEP키 생성 과정과 누적 패킷으로 WEP 암호 크랙]

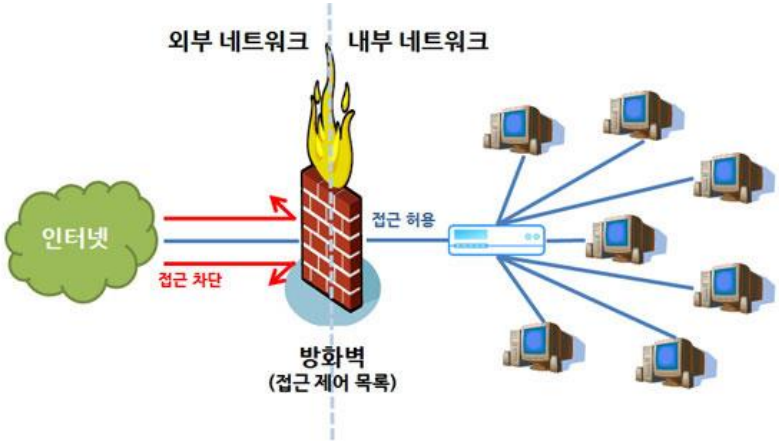
무선 네트워크 공격과 보안

- **무선 네트워크 공격**
  - 기존 유선 네트워크에 적용되었던 DoS, Man in the Middle Attack, Spoofing, Sniffing 등의 공격 방법도 무선 네트워크에서도 이루어질 수 있음

6-4 방화벽

방화벽

- **방화벽**
  - 네트워크 트래픽을 모니터링하고 정해진 보안 규칙을 기반으로 특정 트래픽의 허용 또는 차단을 결정하는 네트워크 보안 디바이스
  - 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 미리 정한 규칙에 따라 차단하거나 보내주는 기능을 하는 하드웨어나 소프트웨어
  - 내부 네트워크의 보안을 제공하기 위한 가장 기본적인 솔루션



- **방화벽의 기능**
  - 접근 제어
    - ✓ 관리자가 통과시킬 접근과 거부할 접근을 명시하면 방화벽이 그에 따라 수행
    - ✓ 구현 방법에 따라 패킷 필터링(packet filtering) 방식, 프록시(proxy) 방식으로 나뉨
    - ✓ 접근 제어를 수행하는 룰셋(rule set)
      - 방화벽을 기준으로 보호하려는 네트워크의 외부
      - 내부에 존재하는 시스템의 IP 주소와 포트로 구성

방화벽 룰셋의 예

번호	외부(From)		내부(To)		동작
	IP 주소	포트	IP 주소	포트	
1	External	Any	192.168.100.100	80	Allow
2	Any	Any	Any	Any	deny

방화벽

- 로깅과 감사 추적
  - ✓ 방화벽은 룰셋 설정과 변경, 관리자 접근, 네트워크 트래픽의 허용 또는 차단과 관련한 사항을 로그로 남김
  - ✓ 사고 발생시 출입자를 확인하여 추적을 하기 위함

- 인증
  - ✓ 방화벽에서는 메시지 인증, 사용자 인증, 클라이언트 인증 방법 사용
  - ✓ 메시지 인증

    .VPN과 같은 신뢰할 수 있는 통신선으로 전송되는 메시지의 신뢰성을 보장
  - ✓ 사용자 인증

    .패스워드를 이용한 단순한 인증부터 OTP, 토큰 기반 인증 등 높은 수준의 인증 등
  - ✓ 클라이언트 인증

    .모바일 사용자처럼 특수한 경우에 접속을 요구하는 호스트 자체가 정당한지 확인하는 방법
- 데이터 암호화
  - ✓ 한 방화벽에서 다른 방화벽으로 데이터를 암호화해서 보내는 것
  - ✓ 일반적으로 VPN의 기능을 이용

방화벽의 한계

- 바이러스 감염 등은 근본적으로 방화벽이 영향을 미치기 어려움

.일부 웜은 막을수 있지만, 정상적인 서비스포트의 웜 공격은 불가

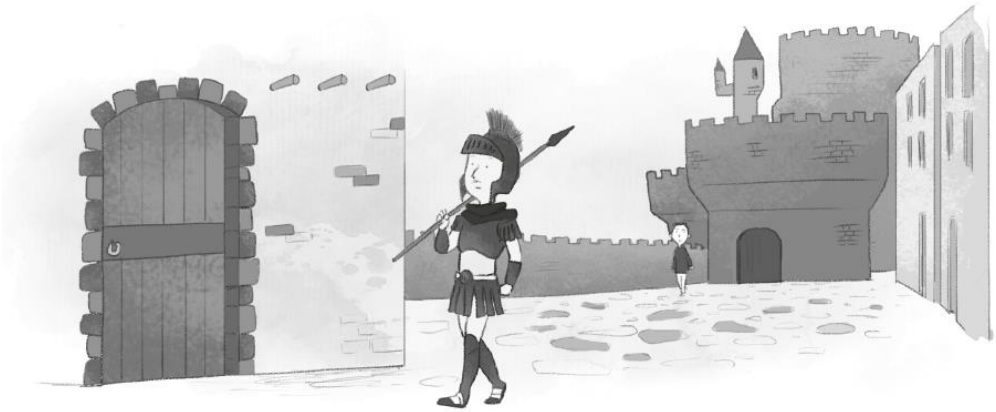
6-5 침입 탐지 시스템

침입 탐지 시스템

- **정의**
  - 침입 탐지 시스템은 네트워크를 통한 공격을 탐지하기 위한 장비로 내부의 해킹이나 악성 코드 활동 탐지와 같이 방화벽이 하지 못하는 일을 수행

  - 설치 위치와 목적에 따른 구분
    - ✓ 호스트 기반 침입 탐지 시스템
      (Host-based Intrusion Detection System, HIDS)

    - ✓ 네트워크 기반 침입 탐지 시스템
      (Network-based Intrusion Detection System, NIDS)



침입 탐지 시스템

- **주요 기능**
  - 데이터 수집
    - 호스트 기반의 침입 탐지 시스템(HIDS)
      - 윈도우나 유닉스 등의 운영체제에 부가적으로 설치, 운용되거나 일반 클라이언트에 설치
      - 운영체제에 설정된 사용자 계정에 따라 어떤 사용자가 어떤 접근을 시도하고 어떤 작업을 했는지 기록을 남기고 추적
      - 네트워크 환경과의 연계성이 낮으므로 전체 네트워크에 대한 침입 탐지가 불가능하고 자신이 공격 대상이 될 때만 침입 탐지 가능
      - 운영체제의 취약점이 HIDS를 손상할 수 있으며 다른 침입 탐지 시스템보다 **비용이 많이** 드는 것이 단점

침입 탐지 시스템

- 네트워크 기반의 침입 탐지 시스템(NIDS)
  - 네트워크에서 하나의 독립된 시스템으로 운용
  - 감사와 로깅을 할 때 네트워크 자원이 손실되거나 데이터가 변조되지 않고 HIDS로는 할 수 없는 네트워크 전반에 대한 감시를 할 수 있으며 감시 영역이 상대적으로 큼
  - IP 주소를 소유하지 않아 해커의 직접적인 공격을 거의 완벽하게 방어할 수 있고 존재 사실도 숨길 수 있음
  - 공격에 대한 결과를 알 수 없으며 암호화된 내용을 검사할 수 없음
  - 스위칭 환경에서 NIDS를 설치하려면 다른 부가 장비 필요
  - 10Gbps 이상의 고속 네트워크에서는 네트워크 카드 등의 하드웨어 적인 한계로 네트워크의 모든 패킷을 검사하기 어렵다는 것이 단점
- HIDS와 NIDS는 각각 장단점이 있어 상호 보완적으로 사용함

침입 탐지 시스템

- 데이터 필터링과 축약
  - HIDS와 NIDS로 수집한 침입 관련 데이터를 상호 연관시켜 좀 더 효과적으로 분석하면 공격에 빠르게 대응 가능
  - 보안이 강화된 시스템에 데이터를 보관하면 침입으로 인한 손실을 막을 수 있음
  - 보안 감사에서는 세밀하고 자세한 데이터보다 빠르고 정확하게 파악할 수 있는 데이터가 더 유용하므로 데이터의 효과적인 필터링과 축약이 필수
  - 효과적인 필터링에는 데이터 수집 규칙을 설정하는 작업 필요
  - 클리핑 레벨(clipping level)을 설정

    - 잘못된 패스워드로 일정 횟수 이상 접속하면 로그를 남기도록 하여 조정 가능

침입 탐지 시스템

- 침입 탐지
  - 오용 탐지 기법 (Misuse Detection)
    - 이미 발견되고 정립된 공격 패턴을 미리 입력해 두었다가 해당하는 패턴이 탐지되면 알려주는 것
    - 비교적 오탐률이 낮고 효율적이지만, 알려진 공격 외에는 탐지할 수 없고 대량 데이터를 분석하는 데는 부적합
    - 어떤 순서로 공격을 실시했는지에 대한 정보를 얻기 어려움
    - 오용 탐지 기법의 또 다른 형태인 **상태 전이(state transition) 방법**
      - » 공격 상황에 대한 시나리오를 작성해두고 각각의 상태에 따른 공격을 분석하는 것
      - » 결과가 매우 직관적이지만 세밀한 시나리오를 만들기가 어렵고 추론 엔진이 포함되어 시스템 부하 가능
    - **오탐률이 낮음**

침입 탐지 시스템

- 지식 기반 침입탐지 (Knowledge-based Detection)

비정상 행위에 대한 패턴을 입력하여 일치하는 패턴을 탐지

✓ 전문가 시스템(Expert System)

✓ 상태전이 모델

✓ 패턴 매칭(Signature-based Detection)

침입 탐지 시스템

- 이상 탐지 기법 (Anomaly Detection)
  - 정상적이고 평균적인 상태를 기준으로 급격한 변화를 일으키거나 확률이 낮은 일이 발생하면 알려주는 것
  - 면역 시스템은 새로운 공격을 당하면 ***스스로 학습****하여 다시 그 공격이 발생하면 대응*, 재설치를 하면 처음 상태로 되돌아가는 것이 단점
  - 인공지능을 활용하여 침입 탐지 시스템에 활용하는 사례가 급속하게 늘어남
  - **행위 기반 침입탐지** (Behavior Detection)

    정상 행위와 비정상 행위를 프로파일링하여 통계 및 AI를 이용하여 정상/비정상을 구분
    - ✓ 통계적 분석
    - ✓ 예측 가능한 패턴 생성
    - ✓ 신경망 모델
  - 오탐률이 높음

➢ 오탐과 미탐
- 오탐(false positive): 공격이 아닌 것을 공격으로 탐지
- 미탐(false negative) : 실제 공격을 정상으로 인식하여 탐지하지 못함

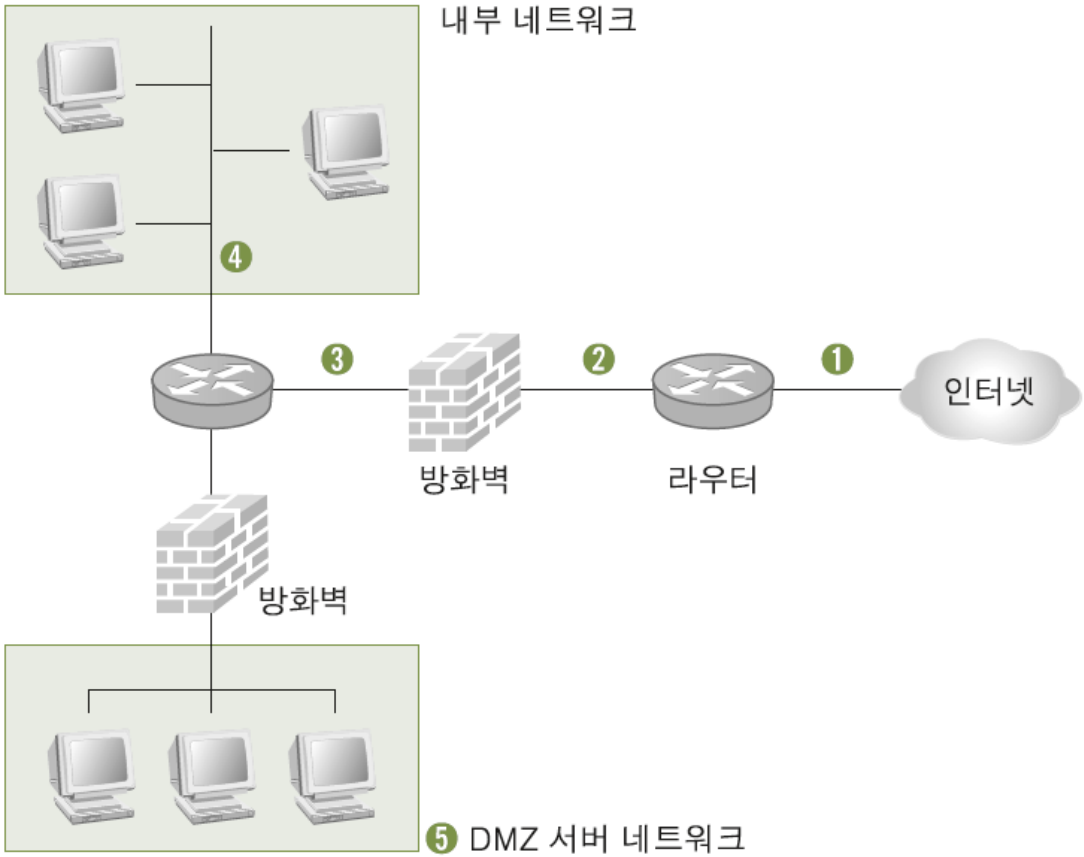
침입 탐지 시스템

- 책임 추적 및 대응
  - 침입 탐지 시스템은 기본적으로 침입을 알려주는 시스템
  - 최근에는 공격을 역추적하여 침입자의 시스템이나 네트워크를 사용하지 못하게 하는 **능동적인 기능이** 많이 추가됨

    ➔ 침입 방지 시스템(Intrusion Prevention System, IPS)

침입 탐지 시스템

- 설치 위치



침입 탐지 시스템의 위치

침입 탐지 시스템

- **설치 위치**
  - ❶ 패킷이 라우터로 들어오기 전
    - 네트워크에 실행되는 모든 공격 탐지 가능
    - 공격 의도를 가진 패킷을 미리 파악할 수 있지만 공격이 아닌 패킷을 너무 많이 수집하고 내부 네트워크로 침입한 공격과 그렇지 않은 것이 구분되지 않아 효율적인 대응이 어려움
  - ❷ 라우터 뒤
    - 라우터의 패킷 필터링을 거친 패킷 검사
    - 패킷 필터링 과정에서 단순한 공격 패킷이 걸러지므로 더 강력한 의지를 가진 공격자 탐지 가능
  - ❸ 방화벽 뒤
    - 방화벽 뒤에서 탐지되는 공격은 네트워크에 직접 영향을 주므로 공격에 대한 정책과 방화벽 연동성이 가장 중요
    - 내부에서 외부로 향하는 공격도 탐지할 수 있어 내부 공격자도 어느 정도 탐지 가능
    - 침입 탐지 시스템을 한 대만 설치할 수 있다면 이곳에 설치하는 것이 좋음

침입 탐지 시스템

❹ 내부 네트워크

- 내부의 클라이언트를 신뢰할 수 없어 내부 네트워크 해킹을 감시하려 할 때 설치

❺ DMZ

- DMZ에 침입 탐지 시스템을 설치하는 이유
  - » 능력이 매우 뛰어난 외부 및 내부 공격자에 의한 중요 데이터의 손실이나 서비스 중단을 막기 위함
- 중요 데이터와 자원을 보호하기 위해 침입 탐지 시스템을 별도로 운영하기도 함

- 침입 탐지 시스템의 설치 우선순위는 ❸ → ❺ → ❹ → ❷ → ❶
- 네트워크의 목적에 따라 중간에 NIDS를 선택적으로 설치 가능
- HIDS는 유지, 관리 비용이 너무 많이 들어서 웹 서버와 같이 사업을 유지하는 매우 중요한 시스템에만 설치

6-6 침입 방지 시스템

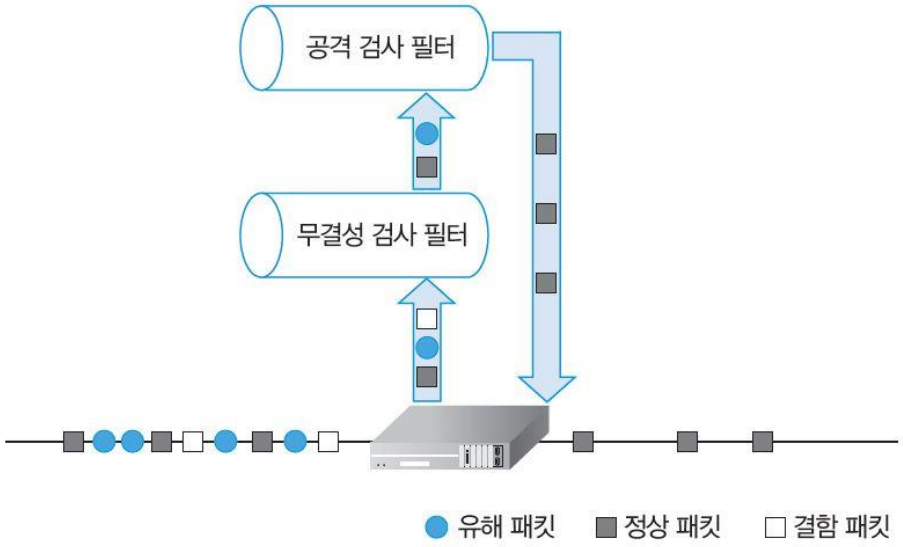
침입 방지 시스템

- **개발 이유**
  - 방화벽이 공격을 차단하는 비율은 30%
  - 공격에 대한 능동적인 분석과 차단을 수행하기 위해 침입 방지 시스템 (Intrusion Prevention System, IPS) 개발

- **필요성**
  - 방화벽은 IP 주소나 포트에 의한 네트워크 공격을 차단할 수 있지만
  - 응용 프로그램 수준의 공격과 새로운 패턴의 공격에 대한 적응력이 낮고 실시간 대응이 어려움
  - 침입 탐지 시스템은 실시간 탐지는 가능하지만 대응책을 제시하지 못하기 때문에 대안 필요
  - 취약점 발표 후 실제 공격까지 하루가 채 걸리지 않는 제로데이 공격(zero day attack)이 많음
  - **방화벽과 침입탐지 시스템의 단점을 보완할 시스템이 필요**

침입 방지 시스템

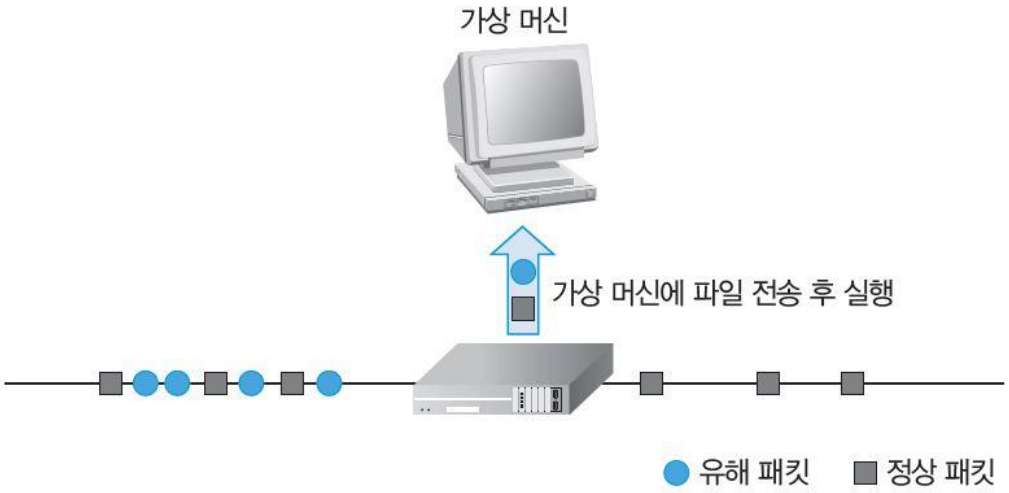
- **동작 원리**
  - 침입 방지 시스템은 침입 탐지 시스템과 방화벽의 조합
  - 침입 탐지 기능을 수행하는 모듈이 패킷 하나하나를 검사, 분석하여 정상적이지 않으면 방화벽 기능의 모듈로 패킷 차단



[침입 방지 시스템의 동작 원리]

침입 방지 시스템

- 공격의 종류와 기술이 다양해지면서 모든 유형의 패턴을 등록하여 차단할 수는 없음
- 침입 방지 시스템에 가상 머신(virtual machine)을 이용한 악성 코드 탐지 개념 도입



[가상 머신을 이용한 침입 방지 시스템의 동작 원리]

- 가상 머신을 이용한 탐지
  - ✓ 네트워크에서 확인되는 실행 파일, 악성 코드와 같은 형태, 공격으로 보이는 패킷 등을 분석하지 않고 침입 방지 시스템에 내장된 가상 머신에 보내 그대로 실행시키는 것
  - ✓ 가상 머신에서 실행된 코드나 패킷이 키보드 해킹이나 무차별 네트워크 트래픽 생성 등 악성 코드와 유사한 동작을 보이면 해당 패킷을 차단

침입 방지 시스템

- **설치**
  - 침입 방지 시스템은 일반적으로 방화벽 다음에 설치
  - 방화벽이 네트워크 앞부분에서 불필요한 외부 패킷을 한 번 걸러주어 더 효율적으로 패킷 검사 가능

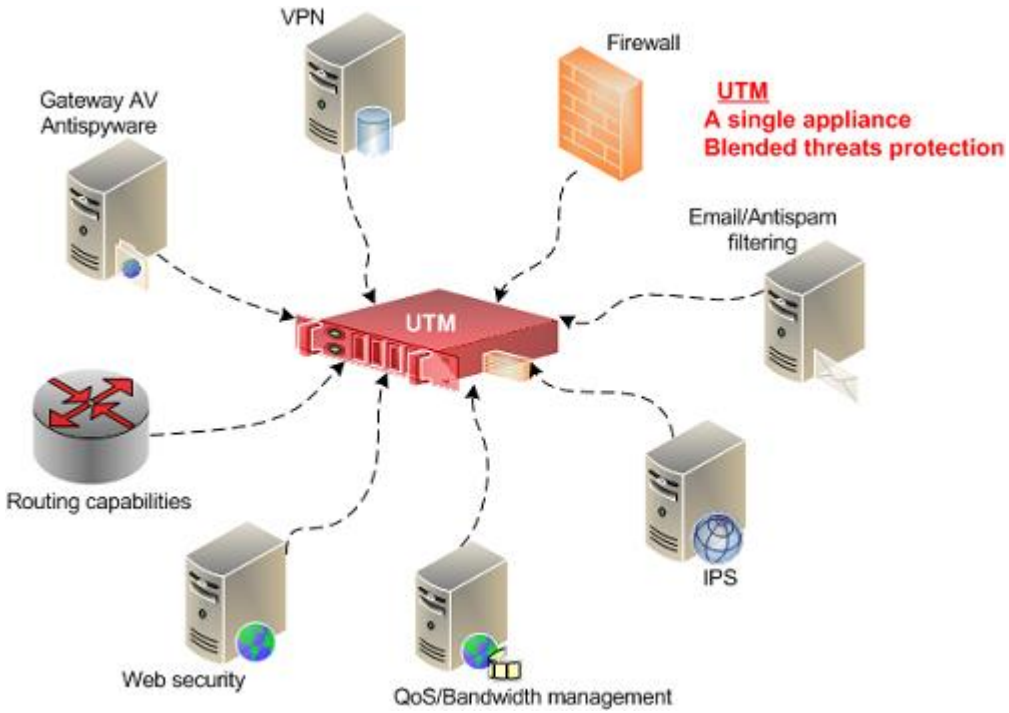
침입 방지 시스템과 방화벽의 구성

  - 방화벽 없이 침입 방지 시스템만 설치하기도 함
  - 하드웨어 칩으로 만든 ASIC(Application Specific Integrated Circuit)를 소프트웨어로 많이 이용

6-7 기타 보안 시스템

통합보안시스템(UTM)

- UTM (Unified Threat Management): 방화벽 기반의 VPN, IPS, 웹 필터링, 안티바이러스, 트래픽 관리 등 다양한 기능을 통합해 지원



- 초기의 UTM은 성능 저하, 이후 진화 → HW 사양 업그레이드 됨
- 근래 보안 성능이 더 추가된 미래의 보안위협에 대응할 수 있는 차세대 UTM, '확장형 위협 관리(eXtensible Threat Management, 이하 XTM)' 솔루션 등장
- UTM의 대안: 차세대 방화벽(Next Generation Firewall: NGFW)에 대한 요구 증가

차세대 방화벽 (NGFW: Next Generation Firewall)

- **차세대 방화벽 기능**
  - 애플리케이션 인식
    - ✓ 포트만이 아닌 애플리케이션을 기반으로 트래픽을 필터링하고 복잡한 규칙을 적용
      - ➔ NGFW의 핵심 기능: 이 기능을 통해 특정 애플리케이션의 트래픽을 차단할 뿐 아니라 개별 애플리케이션을 더 잘 제어
  - 심층 패킷 검사
    - ✓ 패킷에 포함된 데이터를 검사
    - ✓ 패킷의 IP 헤더만을 검사하여 소스와 대상을 확인하는 기존의 방화벽 기술보다 개선
  - 침입 방지 시스템(IPS)
    - ✓ 네트워크의 악성 활동을 모니터링하여 이러한 활동이 발생하는 위치에서 차단
    - ✓ 시그니쳐 기반, 정책 기반, 또는 이상 기반 운영
  - 고성능
    - ✓ 속도 저하 없이 막대한 양의 네트워크 트래픽을 모니터링
  - 외부 위협 인텔리전스
    - ✓ 네트워크와 통신하여 위협에 대한 정보를 최신 상태로 유지하고 악성 행위자를 파악

UTM과 NGFW의 차이

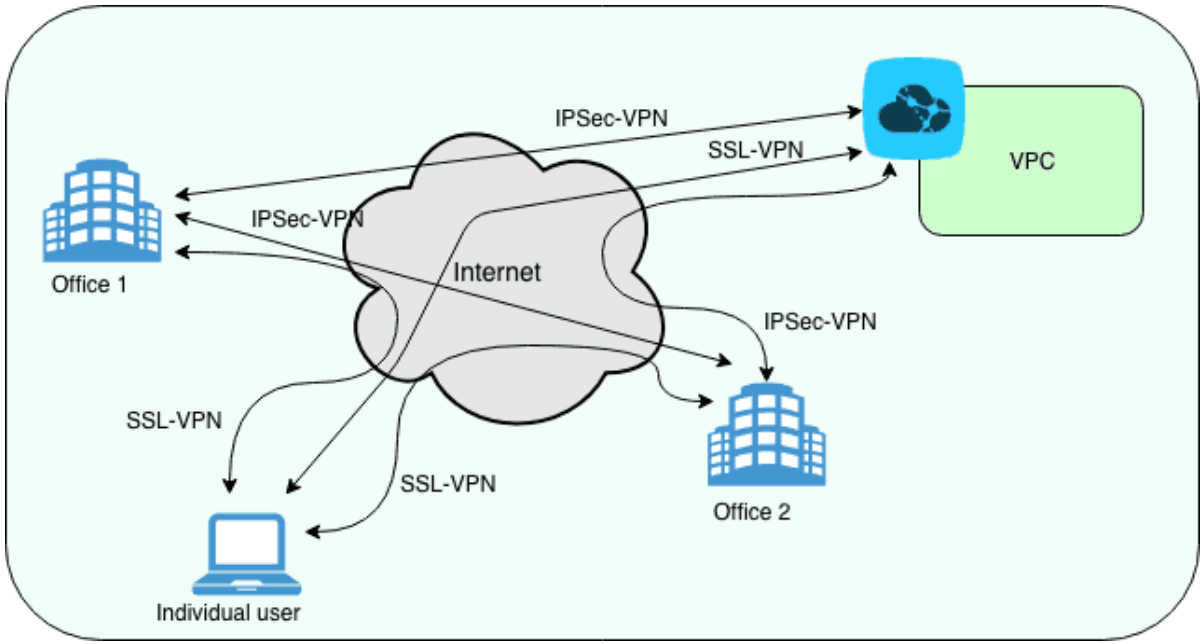
	UTM (Unified Threat Management)	NGFW (Next Generation Firewall)
구성요소	• FW + IPS/Anti-DDoS+AV/AS+IPSecVPN +WebFilter	• UTM +애플리케이션제어+사용자 기반제어+DLP + SSL Inspection + SSL VPN + Anti-APT+Etc.
트래픽 제어	• 정적 정보인 IP, Port 기반의 제어 • Layer-4까지 제어	• 동적 정보인 애플리케이션, 사용자 기반의 제어 • Layer-7 까지 제어
주요 특징	• 암호화 트래픽 제어 불가 • 고도화된 위험에 대한 탐지/제어 불가	• 암호화 트래픽 제어 가능(w/SSL Inspection) • 고도화된 위협에 대한 탐지/ 제어 가능 - 외부 기능과의 연동을 통해 제공
정보 가시성 (Visibility)	• 단순/나열식 형태의 모니터링 정보 • 정보의 판단/분석은 100% 관리자의 몫	• 상관 분석, Drill-Down 형태 등의 모니터링 정보 • 정보의 판단/분석을 일정 부분 장비 자체적으로 수행하여 관리자 판단이 용이한 형태로 제공
관리 편의성 (Manageability)	• 설정 추가/수정 등의 기본적인 편의성	• 정책/객체에 대한 고도화된 편의성 제공 • 다양한 부가 기능 제공 - 미사용/미참조 정책 검색, 중복 정책 검색 등

(출처: 안랩)

- **VPN**
  - VPN(Virtual Private Network): 가상사설망
  - 방화벽, 침입 탐지 시스템과 함께 사용되는 가장 일반적인 보안 솔루션
  - 기존의 인터넷 서비스를 통해 하나의 사설 네트웍처럼 사용하는 가상 사설망
  - 터널링 프로토콜과 보안 과정을 거쳐 내부 기밀을 유지
  - 기업 내부의 네트워크에서 주고받는 데이터는 외부로 유출되면 안 되는 경우가 많아 기업 내의 데이터 통신에는 인터넷과 구분된 별도의 임대 회선(leased line)을 사용

- **VPN 터널을 위한 프로토콜**
  - 2계층: PPTP(Point-toPoint Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), L2F(Layer 2 Fowarding Protocol)
  - 3계층: SSL(Secure Sockets Layer)

- **VPN의 용도**
  - ✓집에서도 회사 내의 서버에 보안 상태로 접근하는 경우
  - ✓원격의 두 지점을 내부 네트워크처럼 이용하는 경우
  - ✓해외여행 중 국내 온라인 게임에 접속하는 경우



- **VLAN (Virtual Local Area Network)**
  - VLAN을 이용할 때 네트워크 관리자는 네트워크를 작은 네트워크로 나눔
  - VLAN은 ACL(Access Control List)을 통해 접근 통제 가능, 악성 코드 발생시 범위 제한 가능
  - VLAN은 스위치에서 설정하며 포트별로 구분
  - 통신을 위한 절차

① 패킷 전송

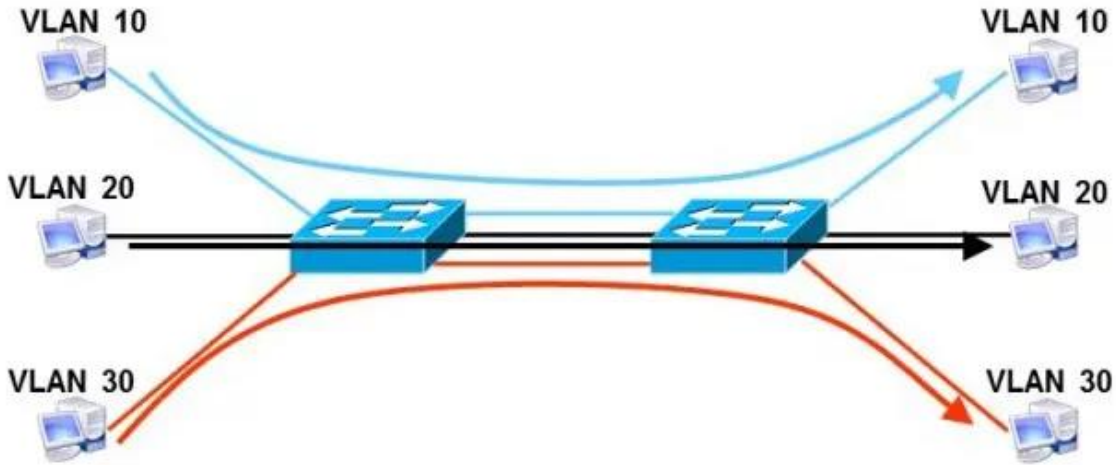
– 클라이언트가 스위치에 프레임을 전달하면 스위치는 클라이언트가 속한 VLAN을 표시하기 위해 전송받은 프레임에 VLAN 정보 붙임

② 패킷 수신

– 프레임을 스위치 밖으로 보내기 전에 프레임의 VLAN 정보와 스위치 포트의 VLAN 정보 비교
– 두 정보가 같으면 프레임에 붙어 있는 VLAN 정보를 떼어내고 프레임만 전송
– 다른 VLAN으로 프레임을 보낼 때는 해당 포트의 VLAN과 프레임에 추가된 VLAN이 다르므로 프레임 차단

③ 스위치 간의 VLAN 통신

– 2개 이상의 스위치에서 VLAN 간 통신을 하려면 여러 개의 VLAN 프레임을 전송할 수 있는 트렁크(trunk) 포트 이용


VLAN 10
VLAN 20
VLAN 30
VLAN 10
VLAN 20
VLAN 30

- **VLAN의 스위치 구현 방법 6가지 예**
  - Port 기반
  - MAC address 기반
  - Network layer protocol 기반
  - IP multicast 기반
  - Policy
  - 사용자 정의 기반

- **NAC**
  - NAC(Network Access Control) : 네트워크에 접근하는 접속단말의 보안성을 강제화 할 수 있는 보안 인프라 (하드웨어 및 소프트웨어)
  - IP 관리 시스템에서 발전한 솔루션

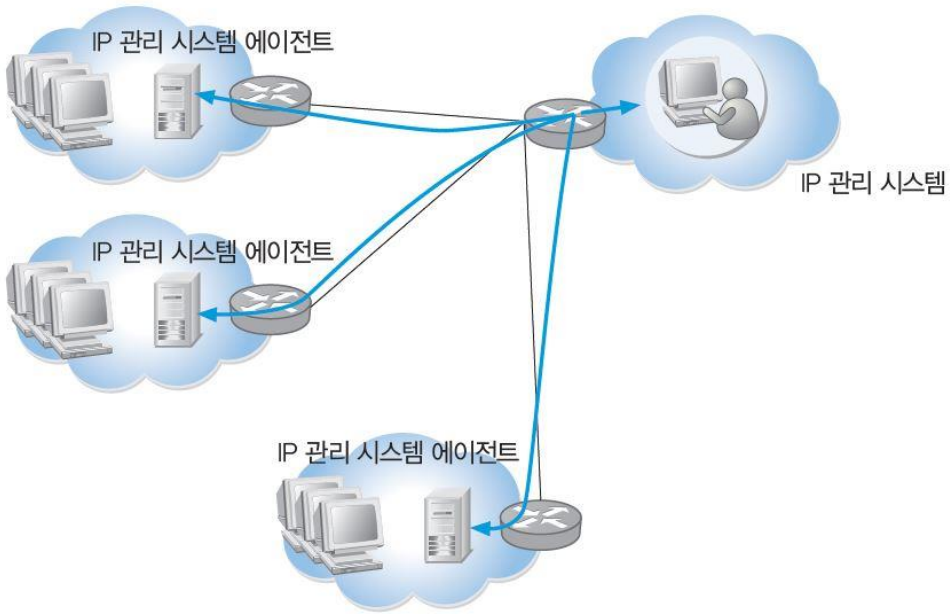
- **도입 배경**
  - 모바일 환경의 일반화
  - 접속단말의 다양화
  - 내부 보안관리의 필요성 증가

- NAC 주요 기능

구분	기능
접근 제어 및 인증	• 내부 직원 역할 기반의 접근 제어 • 네트워크의 모든 IP 기반 장치 접근 제어
PC 및 네트워크 장치 통제(무결성 확인)	• 백신 관리 • 패치 관리 • 자산 관리(비인가 시스템 자동 검출)
해킹, 웜, 유해 트래픽 탐지 및 차단	• 유해 트래픽 탐지 및 차단 • 해킹 행위 차단 • 완벽한 증거 수집

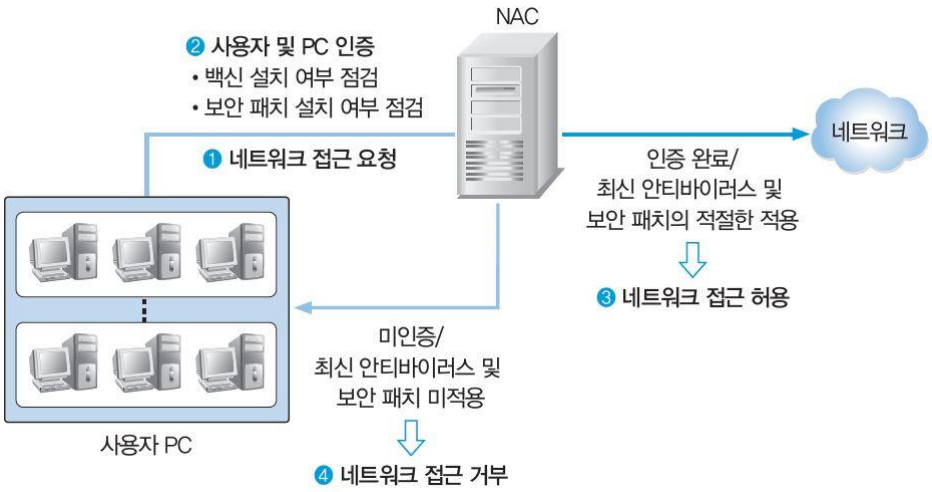
[NAC의 주요 기능]

- 접근 제어 및 인증 기능은 MAC 주소를 기반으로 수행
- NAC는 등록된 MAC 주소만 네트워크에 접속할 수 있게 허용
- 라우터로 구분된 서브 네트워크마다 에이전트 시스템이 설치되어야 함



[NAC의 구성]

- **NAC 사용자 인증 절차**



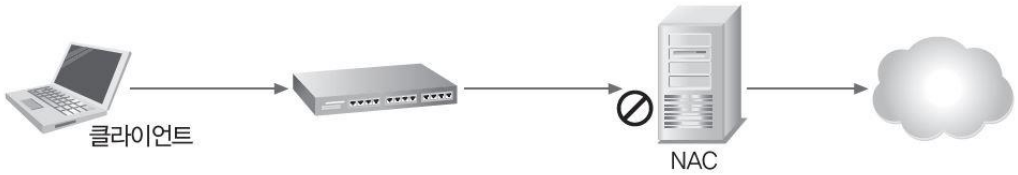
① 네트워크 접근 요청: 접속하려는 PC 사용자가 네트워크에 대한 접근을 처음 시도

② 사용자 및 PC 인증
- NAC에 등록되어 있는 MAC 주소로 사용자 PC 인증
- SSO와 연계하여 네트워크에 접근하는 사용자의 아이디와 패스워드를 추가로 요청하여 인증 수행
  . 인증 과정 중 백신, 보안 패치의 적절성 여부 검토

③ 네트워크 접근 허용: 인증이 완료되면 네트워크 접근 허용

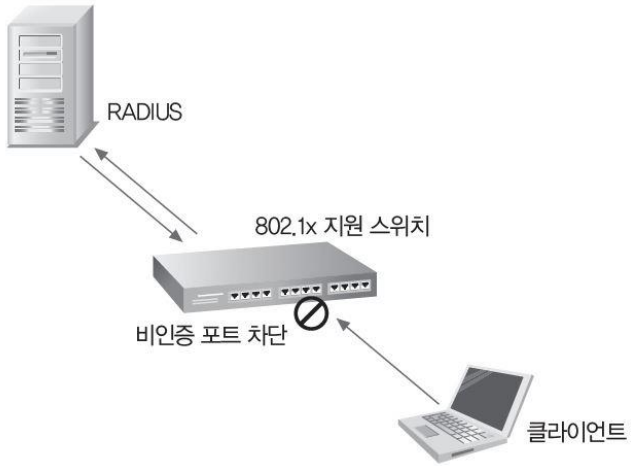
④ 네트워크 접근 거부
- 보안 정책을 제대로 준수하지 않거나 바이러스에 감염되었을 때는 네트워크 접근이 거부되고 네트워크에서 격리됨
- 격리된 PC는 필요한 정책 적용이나 치료 과정을 거친 후 다시 점검

- **NAC 구현 방식**
  - 인라인 방식
    - ✓NAC를 이용하여 방화벽과 같은 방식으로 접근 차단
    - ✓게이트웨이 형태로 일부 물리적 네트워크에 NAC를 추가하는 것으로, 기존 네트워크 변경을 최소화하여 적용 가능



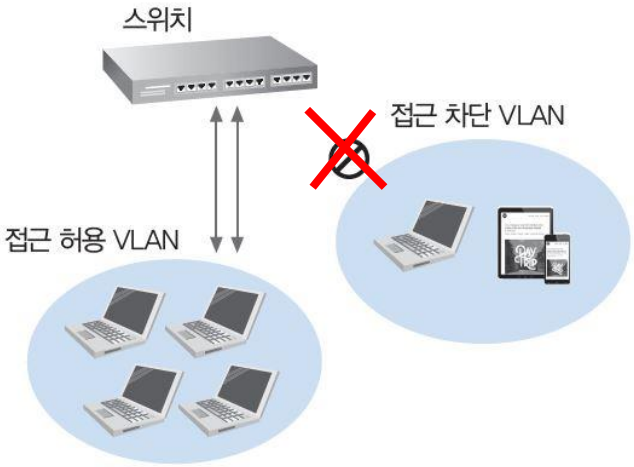
[인라인 방식을 이용한 NAC 구현]

- **NAC 구현 방식**
  - 802.1x 방식 (스위치 이용)
    - ✓802.1x 프로토콜과 RADIUS 서버를 이용하는 것
    - ✓실질적인 접근 허용이나 차단은 스위치에서 수행
    - ✓신규 클라이언트에 대한 인증 요청은 실제로 인증을 수행하는 RADIUS 서버로 전달
    - ✓RADIUS 서버에서 스위치로 반환되는 결과에 따라 스위치는 네트워크에 대한 클라이언트 접근을 허용하거나 거부



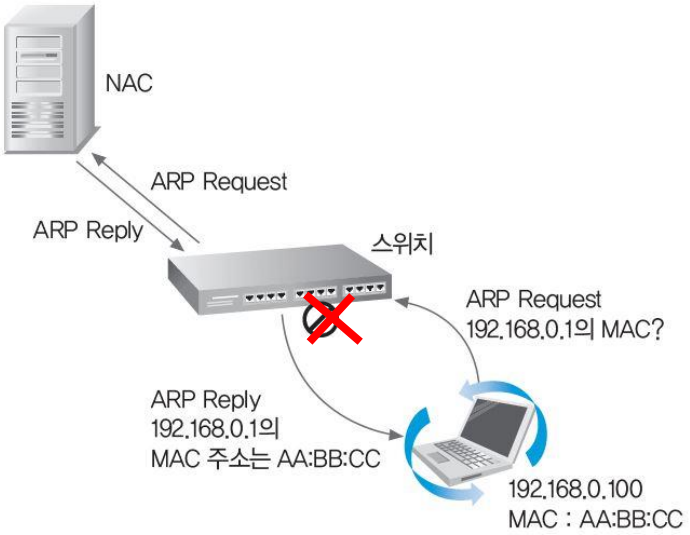
[802.1x 방식을 이용한 NAC 구현]

- **NAC 구현 방식**
  - VLAN 방식
    - ✓인가받지 않은 사용자는 VLAN으로 미리 분리된 망 중에서 통신이 되지 않는 VLAN 망에 신규 클라이언트 할당
    - ✓인가받은 사용자라면 통신이 가능한 VLAN 망에 할당



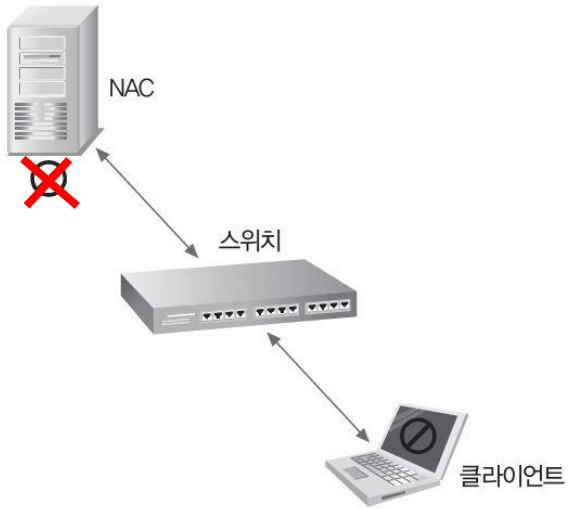
[VLAN 방식을 이용한 NAC 구현]

- **NAC 구현 방식**
  - ARP 방식
    - ✓신규 클라이언트가 적법한 사용자라면 NAC가 게이트웨이의 정상적인 MAC 주소를 알려줌
    - ✓적법하지 않은 사용자라면 비정상적인 MAC 주소를 전송하여 네트워크에 대한 접근을 막음



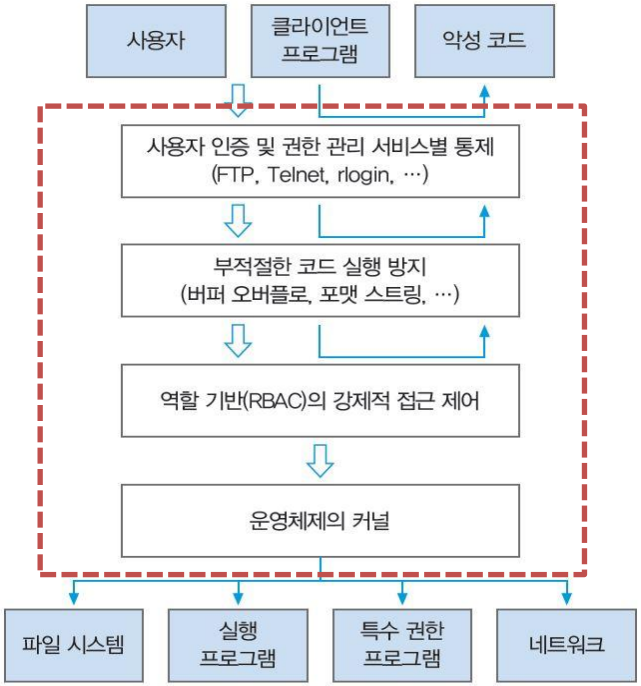
[ARP 방식을 이용한 NAC 구현]

- **NAC 구현 방식**
  - 소프트웨어 에이전트 설치 방식
    - ✓네트워크에 접속하려는 모든 클라이언트에 에이전트를 설치하는 것
    - ✓서버에서 차단 정책을 설정하여 설치된 에이전트로 네트워크를 차단



[소프트웨어 에이전트 설치 방식을 이용한 NAC 구현]

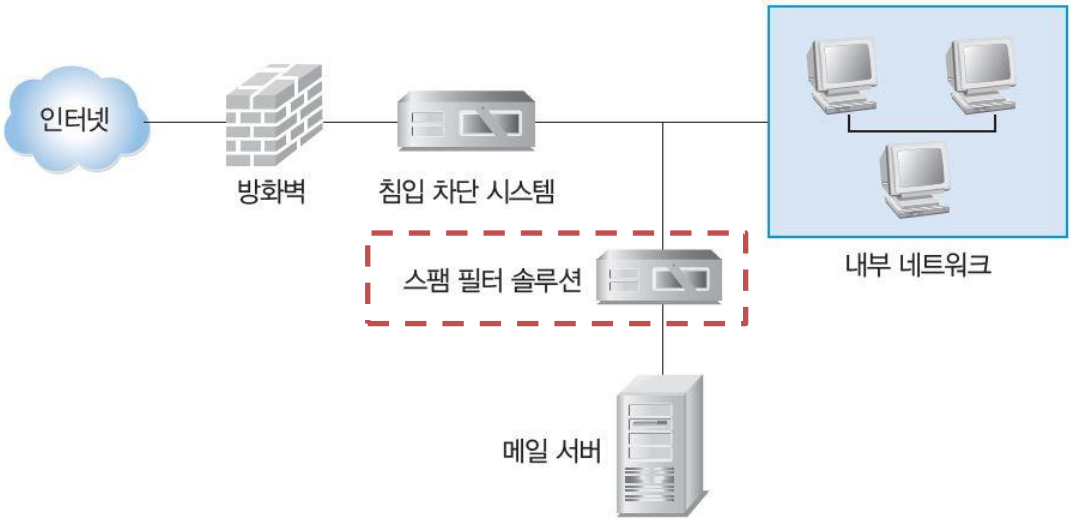
- **보안 운영체제**
  - 운영체제에 내재된 결함으로 발생할 수 있는 각종 해킹으로부터 시스템을 보호하기 위해 보안 기능이 통합된 보안 커널을 추가로 이식한 운영체제
  - 일반적인 서버용 시스템은 보안성보다 가용성이 우선이지만
  - 보안 운영체제는 기본으로 열려 있는 취약 서비스를 모두 차단하여 더 나은 보안 체계로 운영되도록 함



[보안 운영체제의 구성]

- ✓ 보안 운영체제는 일정 수준의 CPU를 점유하므로 성능이 중요할 때는 신중하게 도입해야 함
- ✓ 보안상의 이유로 구매했다가 성능 때문에 다시 제거하는 경우가 많음

- **스팸 필터 솔루션**
  - 메일 헤더 필터링
    - ✓메일 헤더의 내용 중에서 ID/보내는 사람 이름/도메인에 특정 내용이 포함되어 있는지 검사 후
    - ✓보낸 서버에서 IP/도메인/반송 주소(Reply-to)의 유효성과 이상 유무 검사
    - ✓메일 헤더의 받는 사람, 참조자, 숨은 참조자 필드에 너무 많은 수신자가 포함되어 있는지, 존재하지 않은 수신자가 포함되어 있는지 검사



[스팸 필터 솔루션의 구성]

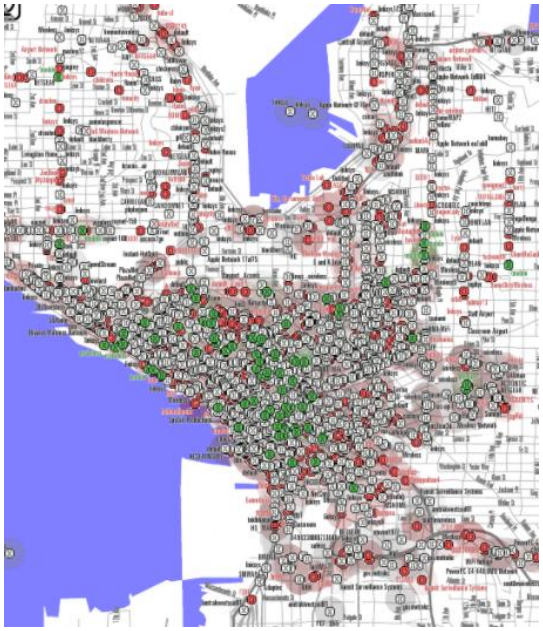
- 제목 필터링
  - ✓메일을 이용한 웜 공격은 제목에 특정 문자열이 있거나 일정 수 이상의 공백 문자열이 있는 것이 특징
  - ✓메일 제목에 '광고' 등의 특정 문자열이 포함되어 있는지 검사하여 웜 차단 가능

- 본문 필터링
  - ✓메일 본문에 특정 단어나 문자가 포함되어 있는지 검사
  - ✓메일 본문과 메일 전체의 크기를 비교하여 유효성 확인

- 첨부 파일 필터링
  - ✓첨부된 파일의 이름, 크기, 개수 및 첨부 파일 이름의 길이를 기준으로 필터링 수행
  - ✓특정 확장자를 가진 첨부 파일만 전송되도록 설정
    - exe, com, dll, bat처럼 실행이 가능한 확장자를 가진 첨부 파일을 필터링

- **모바일 보안 – 이동성 문제**
  - 모바일 기기는 이동성이 뛰어나므로 공격을 받을 때보다 공격에 사용될 때 더 위험
  - 워드라이빙 (wardriving) : 노트북에 수신율 좋은 안테나 연결하고 차에 탄 채 보안이 취약한 무선 랜을 탐색하며 해킹 시도하는 것
    - ✓ 워워킹 (War walking): 걸어 다니면서 하는 행위

[워드라이빙]



[어느 학생이 제작한 시애틀의 무선랜 노드 맵, Wikipedia]

- **블루투스**
  - 선을 사용하지 않고 휴대전화, 휴대용 단말기, 주변 장치 등을 연결하는 기술
  - 여러 가지 장치가 작은 규격과 적은 전력으로 접근하기 때문에 높은 수준의 암호화와 인증을 구현하기가 어려워 다양한 위험에 노출될 수 있음
  - 블루투스와 관련된 다양한 해킹 기술은 네트워크 해킹과 개념이 유사

  - 블루프린팅
    - 블루프린팅(blueprinting)은 블루투스 공격 장치의 검색 활동을 의미
    - 블루투스 장치의 종류(전화 통화, 키보드 입력, 마우스 입력 등)를 식별하기 위해 사용하는 서비스 발견 프로토콜(Service Discovery Protocol, SDP)을 이용해 공격이 가능한 블루투스 장치 검색 및 모델 확인 가능

  - 블루스나프
    - 블루스나프(bluesnarf)는 블루투스 취약점을 이용하여 장비의 임의 파일에 접근하는 공격
    - 블루투스 장치끼리 인증 없이 정보를 교환하도록 개발된 OPP(Obex Push Profile) 기능을 사용
    - 특정 내용을 요청 및 열람하거나 취약한 장치의 파일에 접근함

  - 블루버그
    - 블루버그(bluebug)는 블루투스 장비 간의 취약한 연결 관리를 악용한 공격
    - 한 번 연결되면 다시 연결하지 않아도 서로 연결되는 인증 취약점을 이용

참고문헌

- 양대일, 정보보안개론(개정4판), 한빛아카데미, 2021
- 양대일, 네트워크 보안과 해킹, 한빛아카데미, 2016
- 박영호, 문상재 (1995) OSI 참조모델의 네트워크 계층 보호 프로토콜 정보보호학회지, 5(2), 64-73
- 장성렬, 이영경, and 이경현 "보안성을 개선한 WEP 프로토콜 제안 " 한국멀티미디어학회 학술발표논문집 (2002): 271-274
- 강유성, et al "무선 LAN 보안 취약점과 단계적 해결 방안 " 한국통신학회지 (정보와통신) 20 7 (2003): 117-128
- Kavitha, T , and D Sridharan "Security vulnerabilities in wireless sensor networks: A survey " Journal of information Assurance and Security 5 1 (2010): 31-44
- 진화하는 국내 UTM 시장, 2017. 11, http://www.comworld.co.kr/news/articleView.html?idxno=49330
- How the DNS works, http://www.centr.org
- DNS 캐시 중독이란 무엇입니까? | DNS 스푸핑, Cloudflare, https://www.cloudflare.com/ko-kr
- DNSSEC소개, 한국인터넷정보센터, 한국인터넷정보센터/jsp/resources/dns/dnssecInfo/dnssecInfo.jsp
- 차세대 무선통신 네트워크 기술 동향 및 보안 이슈 분석, 주소영 외 2인, 한국정보보호학회지, 제31권 제3호, 2021
- 차세대 방화벽, wmware, 2021, https://www.vmware.com/kr.html
- VPN이란 무엇인가요?, Alibaba Cloud, 2021, https://www.alibabacloud.com/ko/knowledge/what-is-vpn
- Switch VLAN configuration basis and examples, OPTCORE, 2021, https://www.optcore.net/switch-vlan-configuration-basis-and-examples/

Q & A