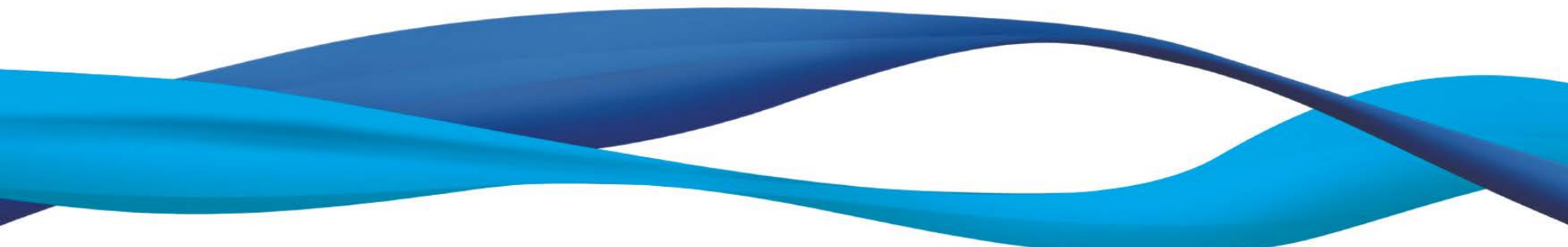


# 6장. 네트워크보안

**박종혁**

서울과학기술대학교 컴퓨터공학과

[jhpark1@seoultech.ac.kr](mailto:jhpark1@seoultech.ac.kr)



- 학습목표

- OSI 7계층의 세부 동작을 이해한다.
- 네트워크와 관련된 해킹 기술의 종류와 방법을 알아본다.
- 네트워크 해킹을 막기 위한 대응책을 알아본다.

# 목 차

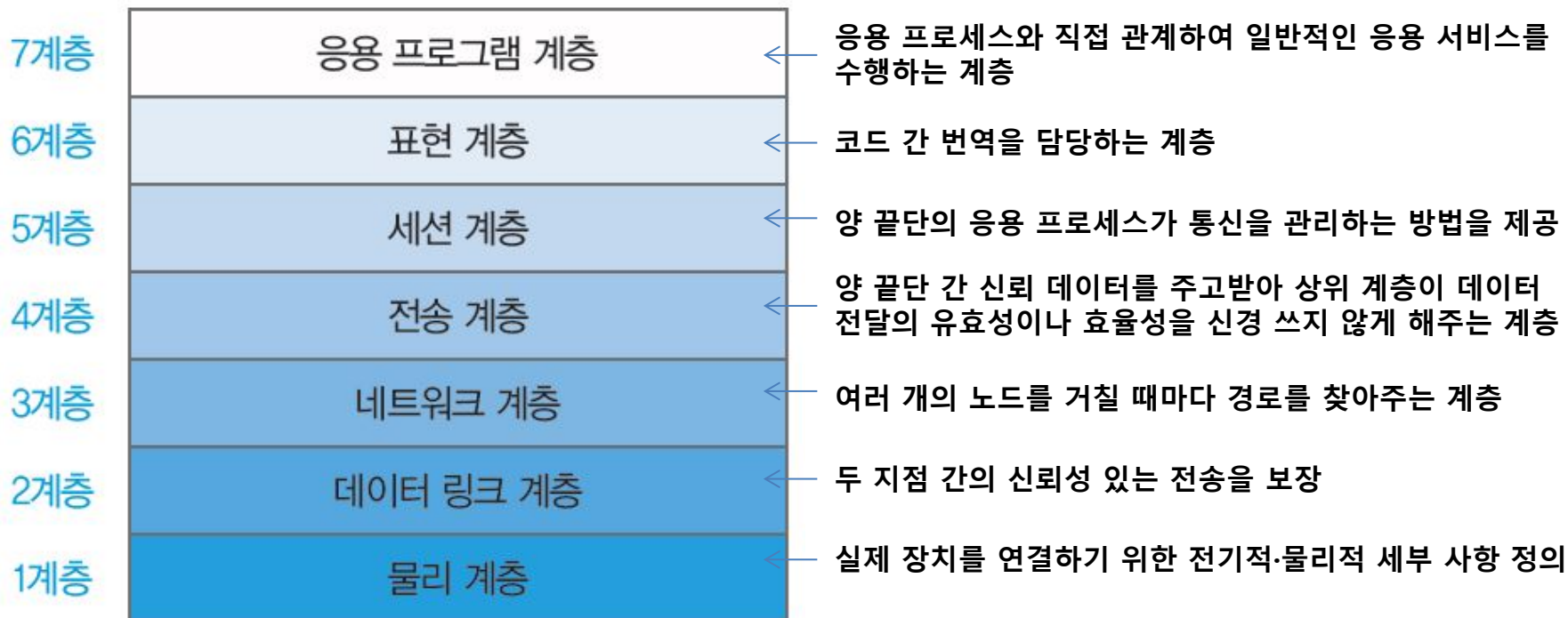
1. 네트워크의 이해
2. 네트워크 공격과 보안
  - Dos와 Ddos
  - 스니핑 공격
  - 스푸핑 공격
  - 세션 하이재킹 공격
3. 무선 네트워크 공격과 보안

# 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 만들



OSI 7계층

## 6-2. 네트워크 공격과 보안

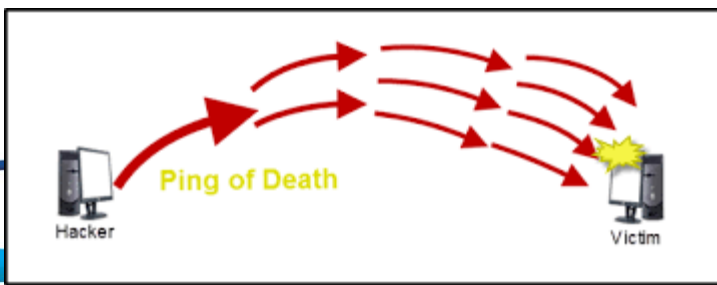
# 네트워크 공격과 보안

## • 서비스 거부 공격(DOS)

- 공격 대상이 수용할 수 있는 능력 이상의 정보를 제공하거나 초과시켜 동작하지 못하게 하는 공격
- 자원 고갈 공격형, 취약점 공격형으로 분류

## • 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 과부하 발생

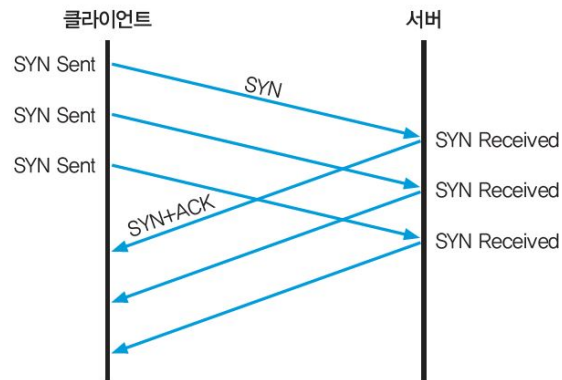


# 네트워크 공격과 보안

## • 자원 고갈 공격형

### - SYN 플래딩 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.
- TCP의 연결 과정인 3-웨이 핸드셰이킹의 문제점을 악용한 공격



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

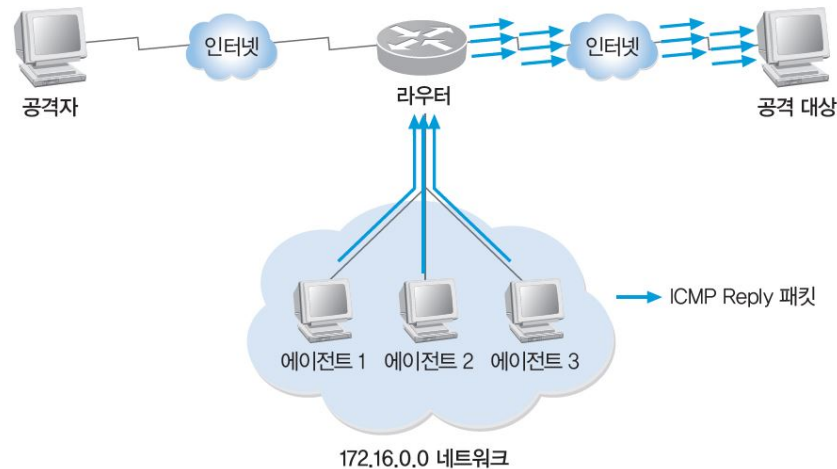


# 네트워크 공격과 보안

## • 자원 고갈 공격형

### - 스머프 공격

- ICMP 패킷과 네트워크에 존재하는 임의의 시스템으로 패킷을 확장해 서비스 거부 공격을 수행하는 것으로, 네트워크 공격에 많이 사용함.
- 다irect 브로드캐스트를 악용하는 것으로 공격 방법은 간단함.
  - 다irect 브로드캐스트(direct broadcast): 기본적인 브로드캐스트는 목적지 IP 주소인 255.255.255.255를 가지고 네트워크의 임의의 시스템에 패킷을 보내는 것

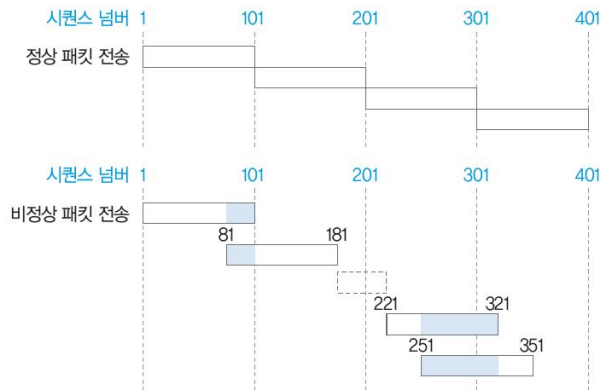


# 네트워크 공격과 보안

## • 취약점 공격형

### – Boink, Bonk, TearDrop 공격

- 프로토콜의 오류 제어 로직을 악용해 시스템 자원을 고갈시키는 방식
- TCP 패킷 안에는 각 패킷이 데이터의 어느 부분을 포함하는지 표시하기 위하여 시퀀스 번호가 기록되어 있는데, 시스템의 패킷 재전송과 재조합에 과부하가 걸리도록 시퀀스 번호를 속이는 공격임.
- 이러한 공격에 의한 취약점은 패치를 통해 제거하는데 과부하가 걸리거나 계속 반복되는 패킷은 무시하고 버리도록 처리함.



티어드롭 공격 시 패킷의 배치

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

티어드롭 공격 시 패킷의 시퀀스 번호

# 네트워크 공격과 보안

## • 분산 서비스 거부 공격(DDOS)

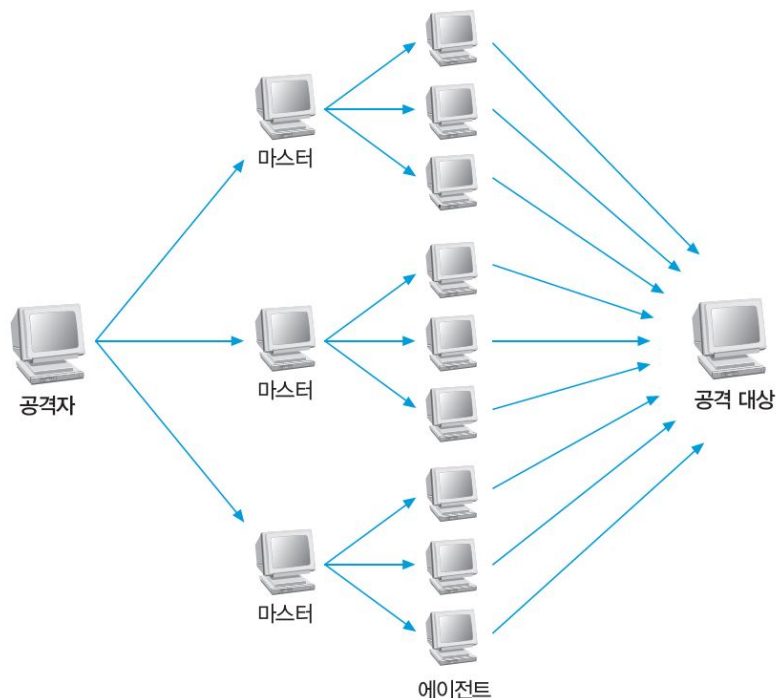
- 공격 대상에 여러 대의 공격자를 분산적으로 배치하여 동시에 DoS를 발생시켜 공격하는 방법
- DoS 공격의 상위 단계
- 최근 발생하는 분산 서비스 거부 공격은 악성 코드와 결합된 형태가 다수
  - ① PC에서 전파가 가능한 형태의 악성 코드 작성
  - ② 사전에 공격 대상과 스케줄을 정한 뒤 미리 작성한 악성 코드에 코딩.
  - ③ 인터넷으로 악성 코드 전파하는데 전파 과정에서는 공격이 이루어지지 않도록 잠복. 이렇게 악성 코드에 감염된 PC를 좀비 PC, 좀비 PC끼리 형성된 네트워크를 봇넷(botnet)이라고 부름.
  - ④ 공격자가 명령을 내리거나 정해진 스케줄에 따라 일제히 공격을 수행하면 대규모의 분산 서비스 거부 공격이 이루어짐.



# 네트워크 공격과 보안

- 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

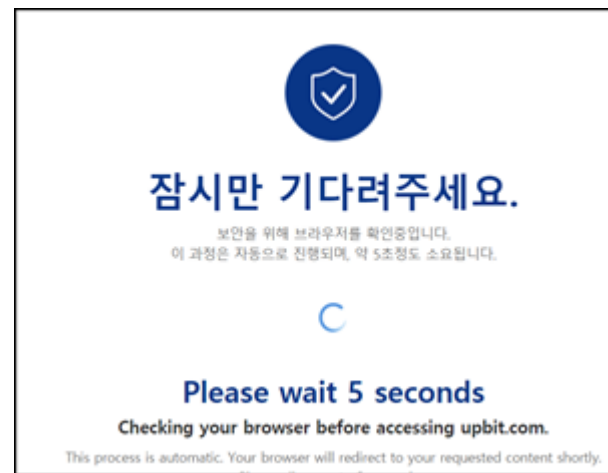
# 네트워크 공격과 보안

## • 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(AWS, CloudFlare)



KISA 사이버대피소

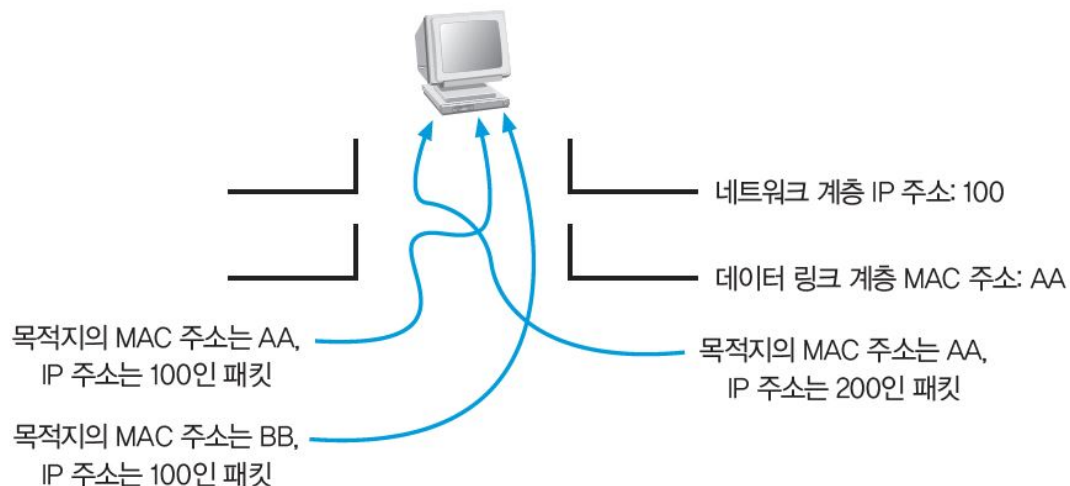


DDoS 보안 솔루션

# 네트워크 공격과 보안

## • 스니핑 공격

- Sniff : '코를 킁킁거리다'
- 데이터 속에서 정보를 찾는 것으로 공격 시 아무것도 하지 않고 조용히 있는 것만으로도 충분하여 수동적 공격이라 함
- 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



네트워크 필터링 해제 상태(프러미스큐어스 모드)

# 네트워크 공격과 보안

## • 스니핑 공격의 종류

### - 스위치 재밍 공격

- 스위치가 MAC 주소 테이블을 기반으로 포트에 패킷을 스위칭할 때 정상적인 스위칭 기능을 마비시키는 공격. MACOF 공격이라고도 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.

# 네트워크 공격과 보안

## • 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.



# 네트워크 공격과 보안

- 스니핑 공격의 탐지

- 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.

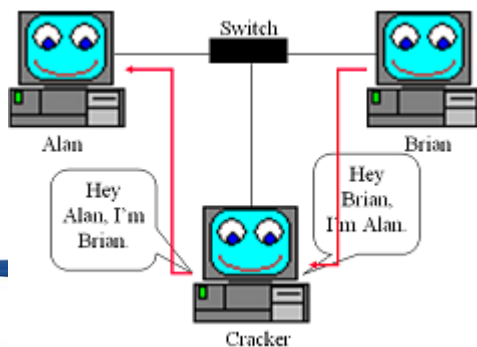
# 네트워크 공격과 보안

- 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. 이 목록을 ARP 테이블이라고 함.

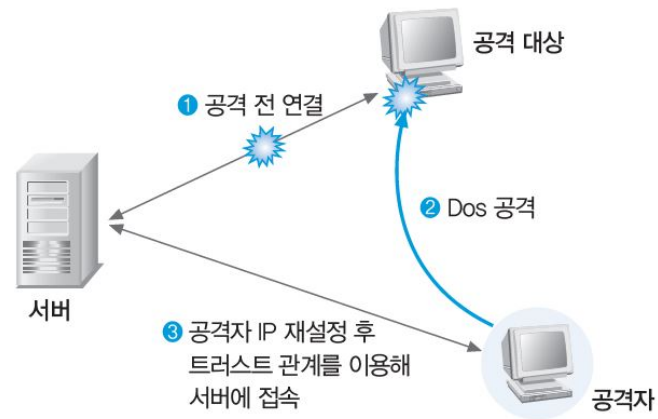


# 네트워크 공격과 보안

## • 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 접근하는 기법.

트러스트: 서버에 미리 정보가 기록된 클라이언트가 접근하면 아이디와 패스워드 입력 없이 로그인을 허락하는 인증법.

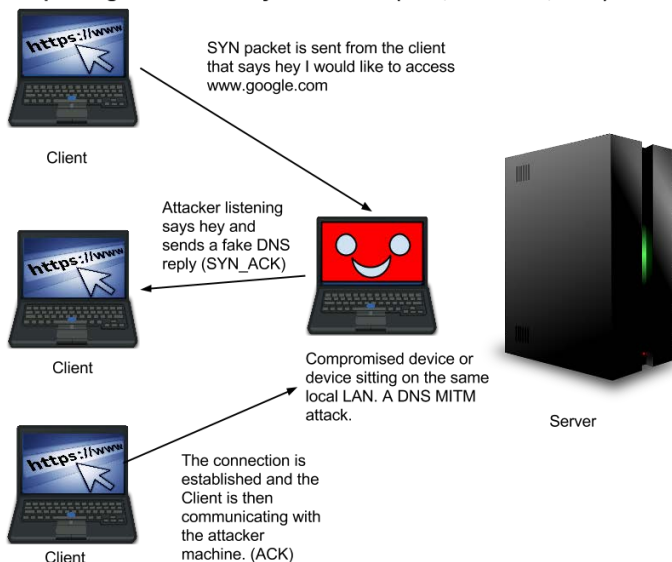


# 네트워크 공격과 보안

## • 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.

음. DNS spoofing TCP Three Way Handshake (SYN, SYN-ACK, ACK)



# 네트워크 공격과 보안

## • 세션 하이재킹

- 세션 가로채기라는 뜻으로 세션은 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 상태이므로 세션 하이재킹은 두 시스템 간의 연결이 활성화된 상태, 즉 로그인된 상태를 가로채는 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

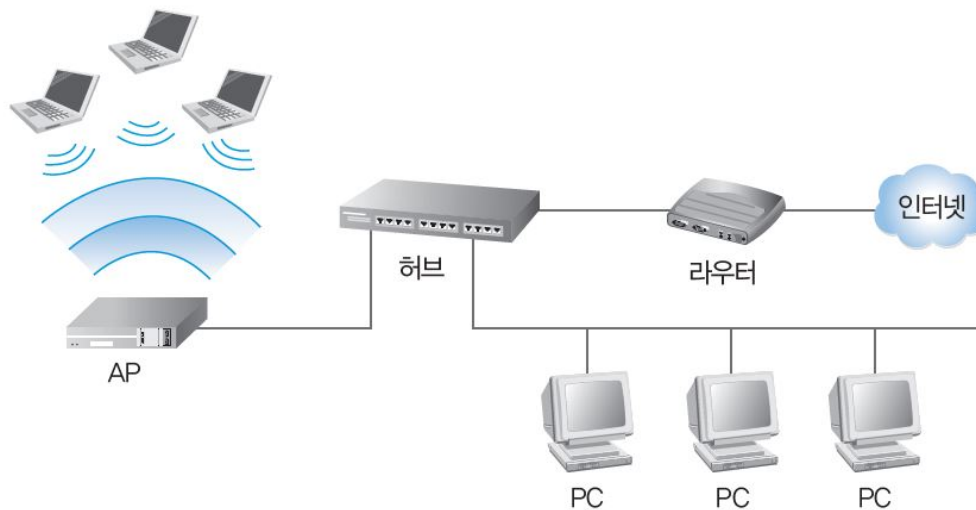
- 텔넷과 같은 취약한 프로토콜을 이용하지 않고 SSH와 같이 세션 인증 수준이 높은 프로토콜로 서버에 접속해야 함.
- 또는 클라이언트와 서버 사이에 MAC 주소를 고정해야 함.

## 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.



# 무선 네트워크 공격과 보안

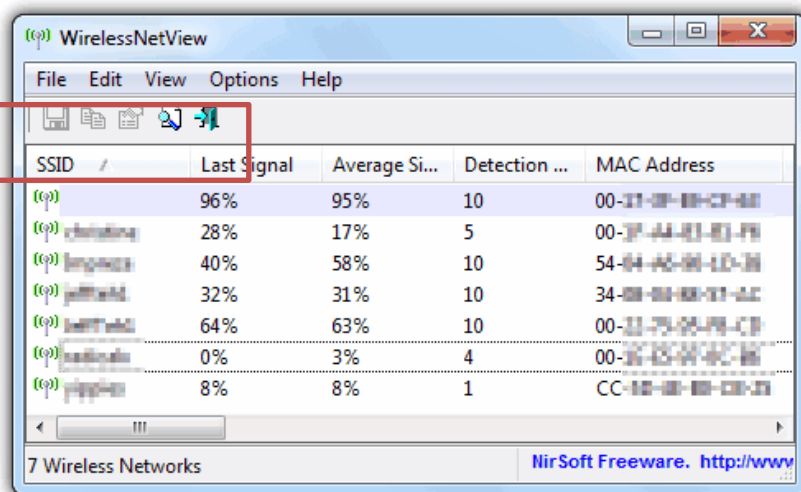
## • 무선 네트워크 보안

### – 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.



WirelessNetView

File Edit View Options Help

SSID	Last Signal	Average Si...	Detection ...	MAC Address
(e) 96%	95%	10	00-11-38-88-07-88	
(e) christina	28%	17%	5	00-17-44-83-83-F8
(e) impassa	40%	58%	10	54-04-4C-88-1D-78
(e) jettfield	32%	31%	10	34-08-04-88-07-8C
(e) jettfield	64%	63%	10	00-11-38-88-07-88
(e) jettfield	0%	3%	4	00-11-38-88-07-88
(e) jettfield	8%	8%	1	CC-18-08-88-07-88

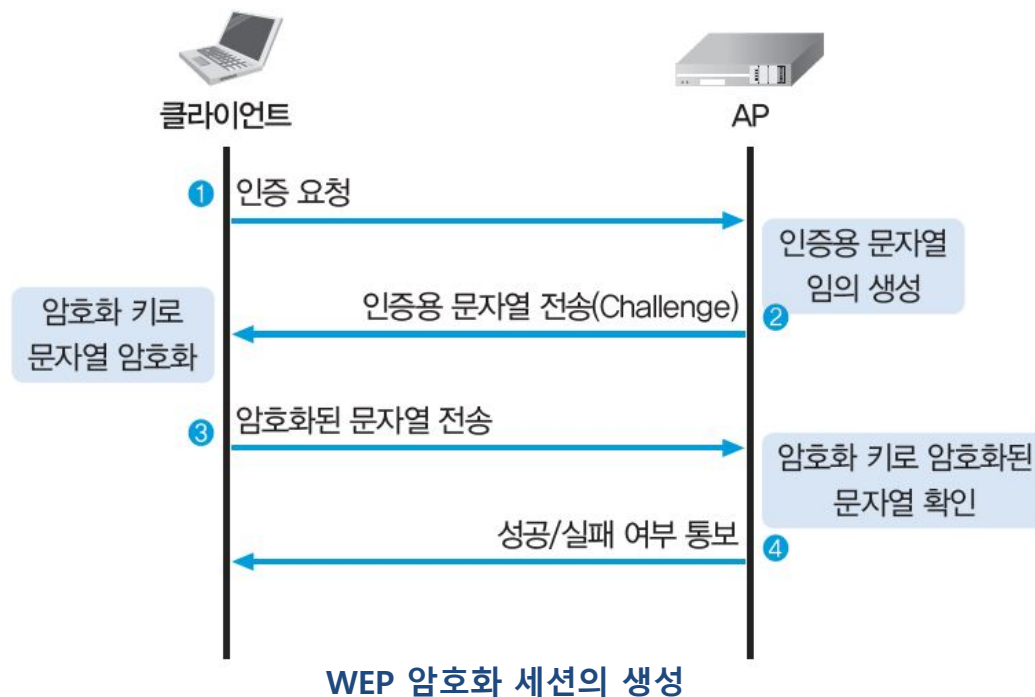
7 Wireless Networks NirSoft Freeware. <http://www...>

# 무선 네트워크 공격과 보안

- 무선 랜 통신의 암호화

  - WEP

    - WEP(Wired Equivalent Privacy)는 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용되기 시작, 1987년에 만들어진 RC 4Ron's Code 4 암호화 알고리즘을 기본으로 사용.

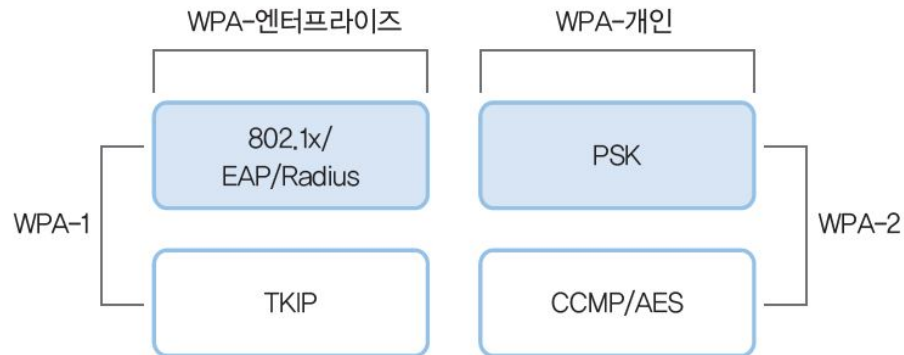


# 무선 네트워크 공격과 보안

- 무선 랜 통신의 암호화

- WPA-PSK

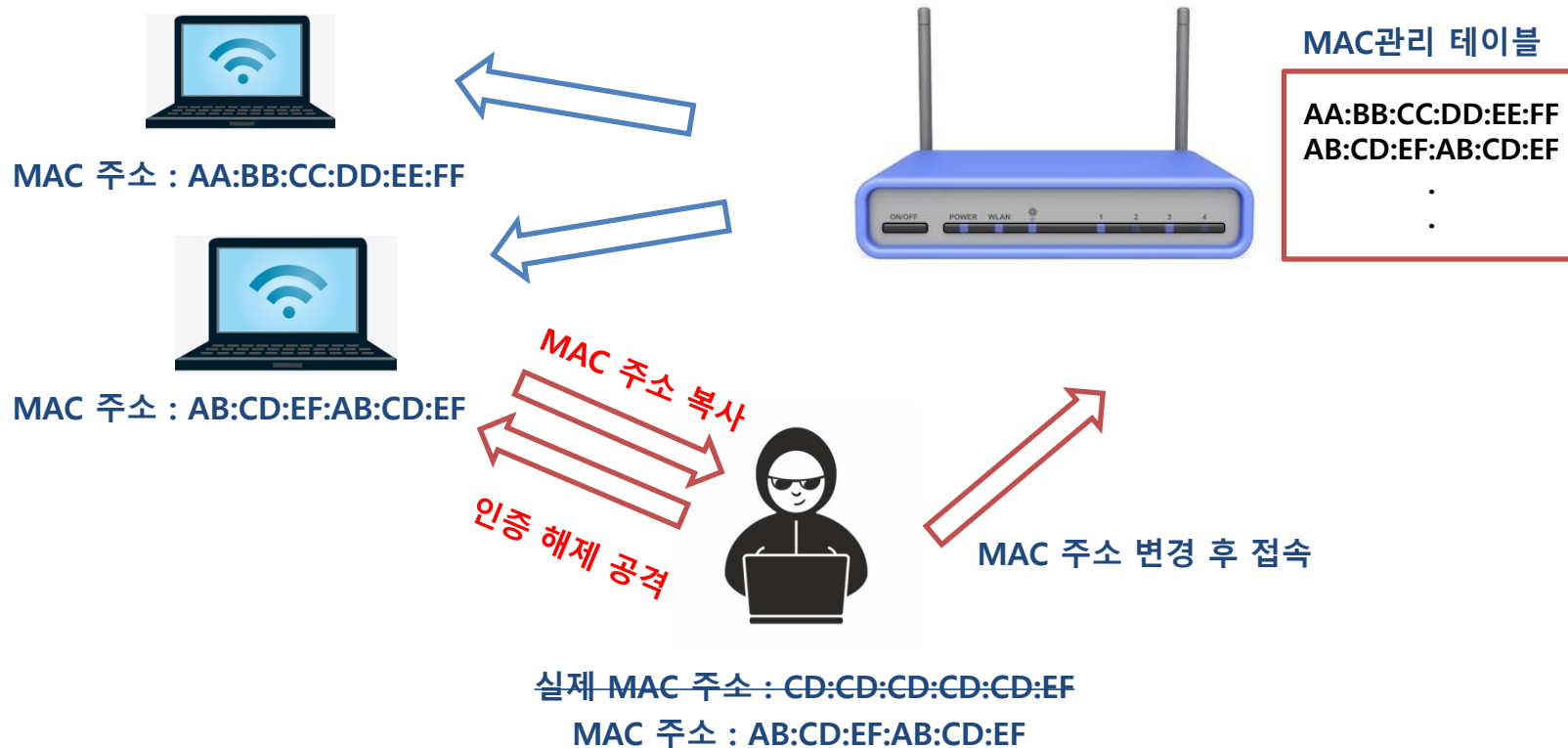
- WPA-PSK(Wi-Fi Protected Access Pre-Shared Key) WEP 방식 보안의 문제점을 해결하기 위해 만들어짐.
    - WPA 규격은 WPA-개인과 WPA-엔터프라이즈로 각각 규정.



WPA 규격의 구조

# 무선 네트워크 공격과 보안

- 무선 네트워크 공격
  - 무선 랜 인증 우회

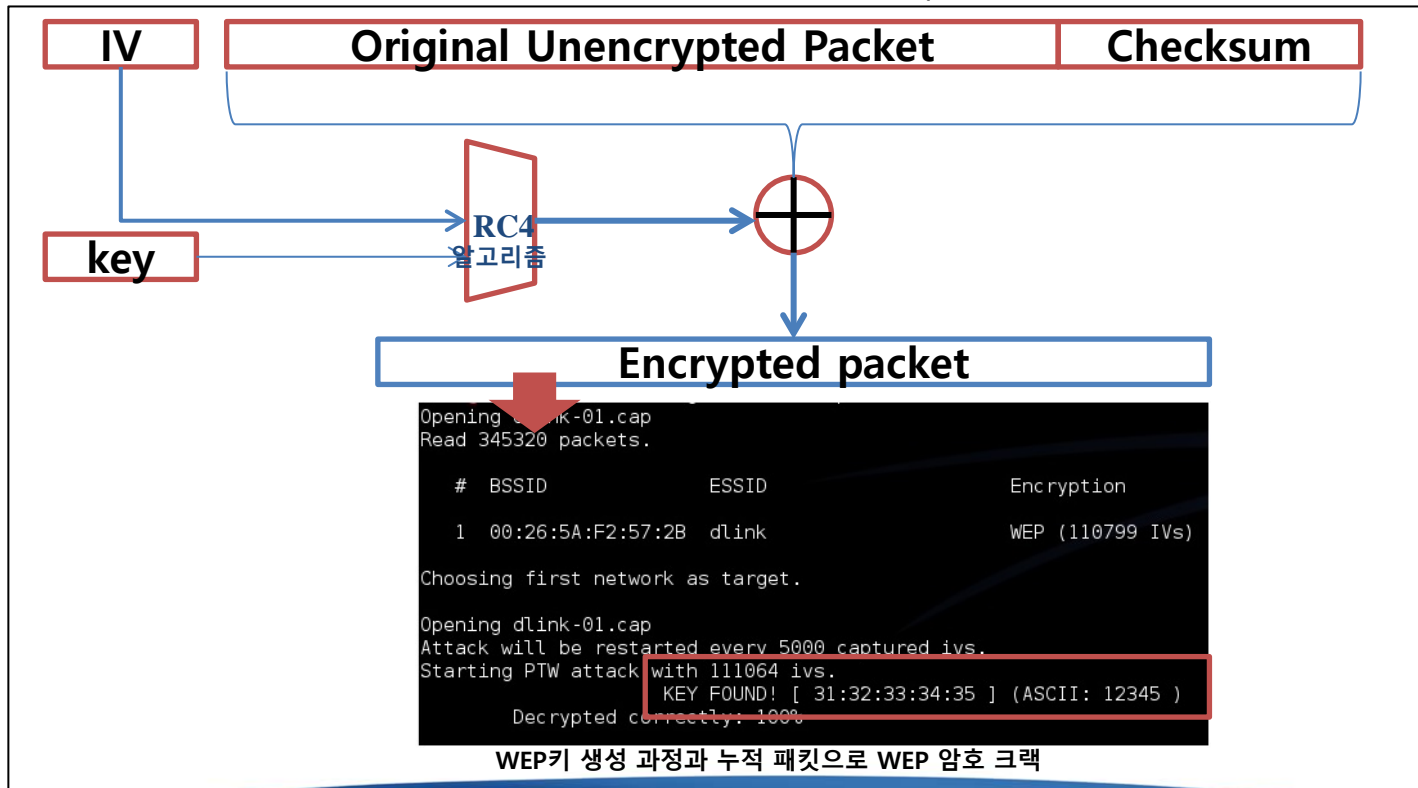


# 무선 네트워크 공격과 보안

## • 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.



# 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.

# 참고문헌

- 양대일, 정보보안개론(개정3판), 한빛아카데미, 2018
- 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.

Q

&

A