5주차 3차시 무선 네트워크 공격

【학습목표】

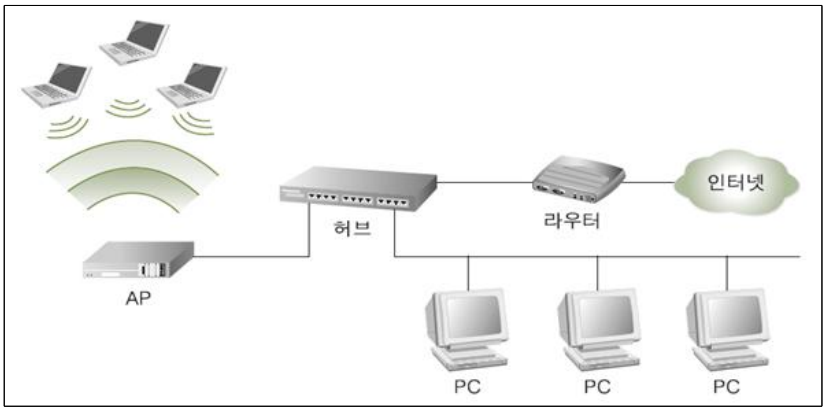
1. 무선네트워크보안의 개념을 설명할 수 있다.
2. 무선 네트워크 보안의 유형을 그 특징에 따라 구분할 수 있다.

학습내용1 : 무선 네트워크 보안의 개념

1. 무선 랜

<기본적으로 Ethernet Like 개념>
- 보통 내부 네트워크의 확장으로서 이용됨
- 무선 랜을 사용하기 위해서는 내부의 유선 네트워크에 AP(Access Point) 장비를 설치해야 함

1) [그림] 유선 네트워크에 연결된 AP로 무선 랜까지 확장된 네트워크



2) [표] 안테나의 종류와 수신 가능 거리

안테나의 종류	수신 가능 거리
무지향성 안테나	200~300m
지향성 안테나	1Km
무지향성 증폭 안테나	(200mW)2~3Km
접시형 안테나	수Km
접시형 안테나 + 지향성 증폭 안테나	50~60Km

3) 안테나의 종류

① 무지향성 안테나
- 주로 봉의 형태
- 전파 수신에 일정한 방향성이 없어 AP의 위치에 상관없이 동작
- 대부분의 무방향성 안테나는 수평면에 대한 무지향성을 지원

② 지향성 안테나
- 수직과 수평인 것으로 나누어짐
- 지향성 안테나는 목표 방향을 지정해 그 방향으로만 전파를 탐지
- 지향성 안테나는 보통 쟁반이나 접시 모양

4) [표] 무선 랜 주요 프로토콜

시기	프로토콜	주요 사항	특징
1997.7	802.11	2.4GHz /2Mbps	최초의 무선 랜 프로토콜
1999.9	802.11b	2.4GHz /11Mbps	위피(WiFi)라고도 하며, WEP 방식의 보안을 구현할 수 있음
	802.11a	5GHz /54Mbps	위피5(WiFi 5)라고도 하며, 전파 투과성과 회절성이 떨어져 통신 단절 현상이 심하며, 802.11b와 호환이 되지 않음

시기	프로토콜	주요 사항	특징
2003.6	802.11g	2.4GHz /54Mbps	• 802.11b에 802.11a의 속도 성능을 추가한 프로토콜 • 802.11b와 호환이 되나 네트워크 공유 시 데이터 처리 효율이 현격히 줄어드는 문제점이 있음
2004.6	802.11i	802.11b 동일	802.11b 표준에 보안성을 강화한 프로토콜

시기	프로토콜	주요 사항	특징
2007	802.11n	5GHz, 2.4GHz	• 최대 600Mbps의 속도 • 여러 개의 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술과 대역폭 손실의 최소화

학습내용2 : 무선 네트워크 보안의 유형

1. AP 보안

1) 물리적인 보안 및 관리자 패스워드 변경
- AP 보호를 위한 첫 번째 사항은 물리적인 보안
- AP는 전파가 건물 내에 한정되도록 전파 출력을 조정하고, 건물 안쪽의 중심부의 눈에 쉽게 띄지 않는 곳에 설치
- 설치한 후에 AP의 기본 계정 패스워드는 반드시 재설정해야 함

2) SSID 브로드캐스팅 금지
- AP를 탐색하면 나타나는 각 AP의 이름이 바로 SSID(Service Set Identifier)임
- 무선 랜에서 가장 설정하기 쉬운 보안 사항은 이 SSID가 AP 탐색에 쉽게 노출되지 않도록 SSID의 브로드캐스팅을 막는 것

3) SSID 브로드캐스팅 금지

* [그림] [제어판]-[네트워크 및 인터넷]-[무선 네트워크 관리]에서 추가

2. 무선 랜 통신 암호화

1) WEP의 암호화

<무선 랜을 암호화하는 가장 기본적인 방법>

[그림] WEP 암호화 세션의 생성 과정

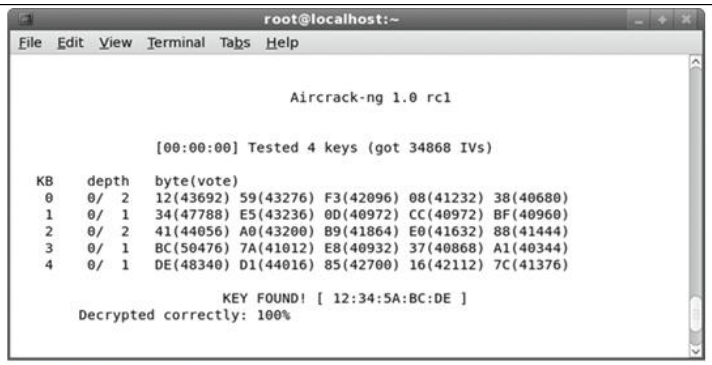
① 클라이언트에서 AP에 인증을 요청함

② AP는 무작위로 IV(Initial Vector)를 생성하여 클라이언트에 전달함

③ 클라이언트는 전달받은 IV를 본인이 알고 있는 WEP 키(RC4 키)로 암호화하여 AP에 전송함

④ AP는 전달받은 암호문을 WEP 키로 복호화하여 본인이 최초 전송한 IV와 일치하면 연결을 허락함

<WEP 키를 이용한 무선 랜 암호화 통신의 보안성은 그다지 높지 않음>
- 통신 과정에서 IV는 무작위로 생성되어 암호화 키에 대한 복호화를 어렵게 하지만, 24비트의 IV는 24비트의 짧은 길이로 인해 반복되어 사용되기 때문



[그림] 복호화된 WEP 키

2) WPA, WPA-PSK의 암호화
<WPA(WiFi Protected Access)는 키값이 쉽게 깨지는 WEP의 취약점을 보완하기 위해 개발됨>
- 데이터 암호화를 강화하기 위해 TKIP(Temporal Key Integrity Protocol)라는 알고리즘을 사용
- WEP와 달리 WPA는 단순한 패킷 수집을 통해서 크랙이 이루어지지 않지만, 최초 인증 과정에서 인증 패킷이 노출될 경우 간단한 패스워드는 몇 시간~몇 일만에 크래킹됨

3. EAP와 802.1x의 암호화

* WPA-EAP로 불리는 WPA Enterprise 방식
- 인증 및 암호화를 강화하기 위해 다양한 보안 표준 및 알고리즘을 채택
- 그 중 가장 중요하고 핵심적인 사항은 유선 랜 환경에서 포트 기반 인증 표준으로 사용되는 IEEE 802.1x 표준과 함께, 다양한 인증 메카니즘을 수용할 수 있도록 IETF의 EAP 인증 프로토콜을 채택한 것

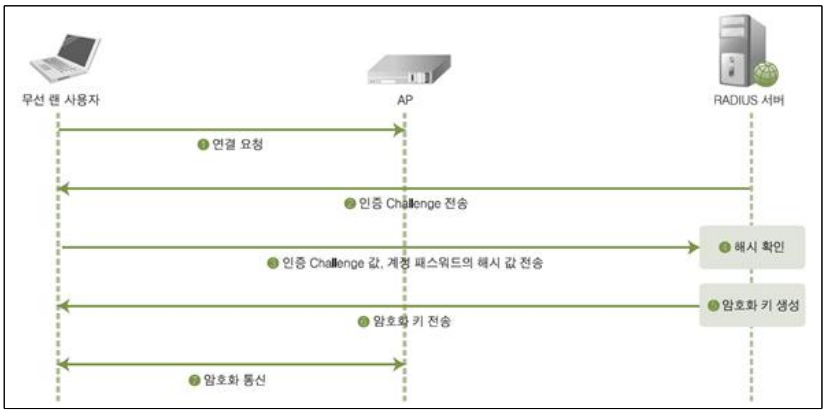
1) 802.1x/EAP(Extensible Authentication Protocol)이 개인 무선 네트워크의 인증 방식과 비교해 추가된 사항
① 사용자에 대한 인증을 수행

② 사용 권한을 중앙 관리

③ 인증서, 스마트카드 등의 다양한 인증을 제공

④ 세션별 암호화 키를 제공

2) [그림] RADIUS와 802.1x를 이용한 무선 랜 인증



3) RADIUS와 802.1x를 이용한 무선 랜 인증

① 클라이언트는 AP에 접속을 요청함
- 이때 클라이언트와 AP는 암호화되지 않은 통신을 수행함
- 그러나 클라이언트가 AP와 연결된 내부 네트워크로 접속하는 것은 AP에 의해 차단됨

② RADIUS 서버는 클라이언트에 인증 Challenge를 전송함

③ 클라이언트는 Challenge에 대한 응답으로서 최초로 전송 받은 Challenge 값, 계정, 패스워드에 대한 해시 값을 구하여 RADIUS 서버에게 전송함

④ RADIUS 서버는 사용자 관리 DB 정보에서 해당 계정의 패스워드를 확인함
- 연결 생성을 위해 최초로 전송한 Challenge의 해시 값을 구하여 클라이언트에서 전송받은 해시 값과 비교함

⑤ 해시 값이 일치하면 암호화 키를 생성함

⑥ 생성한 암호화 키를 클라이언트에게 전달함

⑦ 전달받은 암호화 키를 이용하여 암호화 통신을 수행함

【학습정리】

1. AP 보호를 위한 첫 번째 사항은 물리적인 보안이며 두 번째는 기본 계정 패스워드의 재설정이다.

2. 무선 랜에서 가장 설정하기 쉬운 보안 사항은 이 SSID가 AP 탐색에 쉽게 노출되지 않도록 SSID의 브로드캐스팅을 막는 것이다.

3. 무선 랜 통신 암호화에는 WEP의 암호화, WPA, WPA-PSK의 암호화, WPA-EAP의 암호화 등이 있다.