WiFi 무선 LAN 보안

박승철교수

강의 내용

- **보안 요구사항**
  - 인증, 암호화, 무결성
- **WEP(Wired Equivalent Privacy)**
  - AP에 의한 그룹 키 인증 & 스트림 암호화(Group Key/RC4)
- **IEEE 802.11i**
  - IEEE802.1x/EAPOL 인증 & 키 교환
  - 암호화
    - TKIP : WPA(WiFi Protected Access)
    - AES : WPA2

보안 요구사항

- 인증(authentication)
  - 허가된 사용자만 WiFi 네트워크에 연결
- 암호화(encryption)
  - 키를 알고 있는 사용자만 정보 해석
- 무결성(integrity)
  - 정보의 진위 여부 확인

WiFi 보안 기술 발전

- **WEP(Wired Equivalent Privacy)**
  - 1999년 IEEE 802.11 초기 표준의 보안 사양
- **WPA(WiFi Protected Access)**
  - 2003년 WEP에 대한 잠정적인 대체 표준
- **WPA2**
  - 2004년 IEEE 802.11i 표준
  - WPA 대체

WEP(Wired Equivalent Privacy)

암호화(encryption)

- RC4 스트림 암호
- 40비트 사전 공유 키(Pre-Shared Key)
- 24비트 IV(Initialization Vector)를 사용하여 프레임 마다 서로 다른 64비트 스트림 키 생성
- 전사 공격(Brute Force Attack)에 노출

참고

- Youtube, 박승철 대칭키 암호화

WEP(Wired Equivalent Privacy)

❖ 인증(authentication)

- AP에서 인증 수행
- 개방 인증(Open Authentication)
- 공유 키 인증(Shared Key Authentication)

WEP(Wired Equivalent Privacy)

❖공유 키 인증(Shared Key Authentication)

① 무선 스테이션은 AP에게 인증을 요청한다.

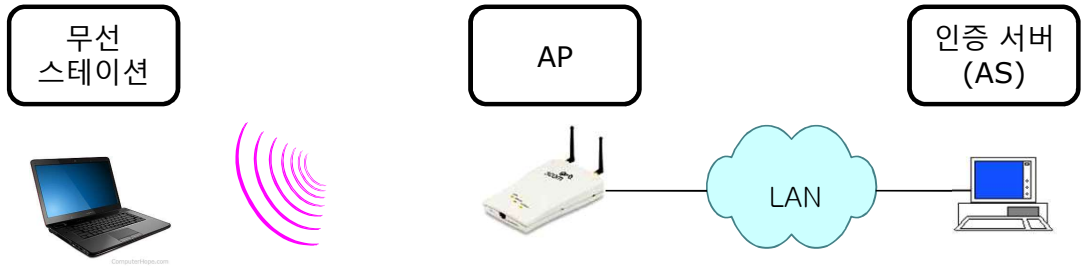
② AP는 넌스(Nonce)라 불리는 128 바이트 1회용 임시 정보를 평문 형태로 무선 스테이션에게 응답한다.

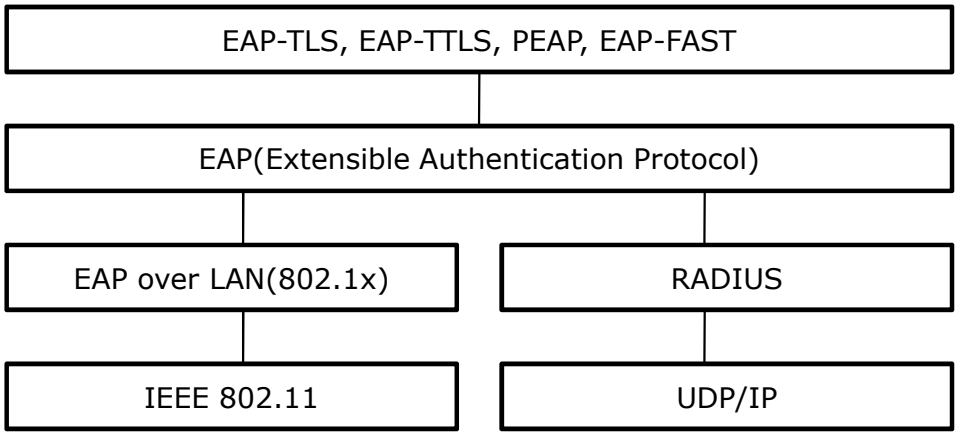
③ 무선 스테이션은 AP와 공유하고 있는 대칭 키를 사용하여 할당된 넌스를 RC4로 암호화하여 AP에게 전송한다.

④ AP는 자신이 보유하고 있는 대칭 키를 사용하여 암호화된 넌스를 복호화한 후 자신이 할당한 넌스와 비교함으로써 해당 무선 스테이션을 인증한다.

IEEE 802.11i

❖ 프레임워크(framework)





IEEE 802.11i 동작 절차

① **발견(Discovery) :**
- AP는 자신이 제공할 수 있는 인증 기법과 암호화 기법을 무선 스테이션들에게 광고한다.

② **상호 인증(Mutual Authentication) :**
- AP를 발견한 무선 스테이션은 AS와 인증 작업을 수행한다.

③ **키 생성 및 분배(Key Generation and Distribution) :**
- 인증이 완료되면 AS는 마스터 키(Master key)를 생성하고, AS는 마스터 키를 안전하게 AP에게 전달한다.

④ **안전한 데이터 전송(Protected Data Transfer) :**
- 무선 스테이션과 AP는 마스터 키로부터 세션키를 생성하고, 세션키를 사용하여 안전하게 데이터를 전송한다.

IEEE 802.11i 인증

- **사전-공유 키(Pre-shared Key)**
  - AP에서 그룹 인증
  - 개인 모드(Personal Mode)
- **IEEE 802.1x 기반 상호 인증**
  - 인증 서버에서 개별 인증
  - 엔터프라이즈 모드(Enterprise Mode)

IEEE 802.11i 인증

IEEE 802.1x 기반 상호 인증

- 인증 과정에서 AP는 EAP 메시지만 전달
- 인증이 완료된 사용자의 데이터 프레임 통과 허용 - 불필요한 트래픽에 대한 접근 제어
- 포트 기반 접근 제어(Port-based Access Control)
- 구체적인 인증 방법은 EAP 종류에 따라 다름

IEEE 802.11i 인증

- **EAP-TLS : EAP-TLS 인증 기법**
  - 무선 스테이션과 AS가 공인 인증서를 사용하여 상호 인증
  - AS와 무선 스테이션이 공인 인증서 유지
- **EAP-TTLS(Tunneled TLS)**
  - AS만 공인 인증서로 인증
  - 무선 스테이션은 TLS에 의해 설정되는 안전한 채널을 통해 패스워드로 인증
- **참고**
  - Youtube, 박승철 공개키암호화, 디지털서명, SSL/TLS 참조

IEEE 802.11i 인증

- **EAP-FAST(Flexible Authentication via Secure Tunneling)**
  - 공인 인증서 대신 사전-공유 키(Pre-shared Key) 기반의 보안 채널 사용
  - 공인 인증서 처리에 부담이 되는 소형 장비 인증에 적합

IEEE 802.11i 암호화

TKIP(Temporal Key Integrity Protocol)

- WEP 취약점을 임시적으로 보완 : WPA
- MIC(Message Integrity Code) 지원
- 각 프레임에 대한 128비트 WEP 키
- 48비트 IV 적용
- IEEE 802.11-2012부터 표준에서 빠짐

IEEE 802.11i 암호화

- **WPA2(WiFi Protected Access 2)**
  - AES(Advanced Encryption Standard) 적용
  - 현재 WiFi 암호 표준
- **참고**
  - Youtube, 박승철 대칭키암호2-AES 참조

IEEE 802.11i 암호화

❖키 생성 및 분배

- 인증 과정에서 생성된 안전한 채널을 통해 무선 스테이션과 AS는 마스터 키(Master key) 생성
- AS는 마스터 키를 안전하게 AP에게 전달
- 무선 스테이션과 AP는 마스터 키를 기반으로 데이터 암호화와 메시지 인증에 사용될 다수의 세션 키 생성