정보보호 개론

17. 무선랜과 보안

무선랜 탄생 배경

- 1970년 하와이 대학교에서 라디오 주파수를 사용한 알로하넷을 개발
- 1979년 적외선 통신을 사용한 실험적 랜에 대한 IEEE 보고서 출판
- 1980년대 초 아마추어 무선 기사가 1세대 무선 데이터 모뎀 개발
- 1987년 IEEE 802.4 토큰 버스 WG 내에서 무선화 검토 개시
- 1987년의 미국 연방통신위원회(FCC : Federal Communications Commission)에서 ISM 대역(Industrial, Scientific, Medical band) 제정
- 1990년 무선 LAN 표준안 작성을 위하여 IEEE 802.11 WG 승인

무선랜의 역사 (1)

- 1987년의 미국 연방통신위원회(FCC : Federal Communications Commission)에서 면허가 필요 없는 무선 주파수 대역(ISM 대역: Industrial, Scientific, Medical band) 규정 제정
- 대표적인 초기 무선 LAN 제품
  - AT&T의 WaveLAN
    - 2.4GHz ISM 대역
    - 직접 대역 확산(DSSS : Direct Sequence Spread Spectrum)과 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance) 방식을 사용
    - 2Mbps 전송속도
  - 모토롤라의 Altair
    - 1990년 FCC가 인가한 19GHz의 주파수 대역 사용
    - 15Mbps까지 고속 전송이 가능
- 군수용 무선기기를 제조하던 프록심, 심볼의 참여
  - FHSS(Frequency Hopping Spread Spectrum)방식에 1.6Mbps 전송속도를 지원
  - 백화점, 창고, 호텔 등에 제한적으로 사용

무선랜의 역사 (2)

- 1997년 6월 IEEE 802.11 표준화
  - FHSS, DSSS, IR(Infrared) 등의 3가지 물리 계층을 규정 (각 물리 계층 간에는 호환성이 보장되지 않음)
  - 시장에서는 프록심을 중심으로 하는 FHSS 지지 업체들과 DSSS 기술을 지지하는 업체간의 극심한 대립
- 1999년 9월 IEEE 802.11b 고속 무선 LAN 규격 표준화
  - 루슨트 테크놀로지와 해리스반도체(현재 인터실)가 공동으로 제안한 DSSS/CCK(Complementary Code Keying) 방식 기반
  - 시장이 FHSS 중심에서 DSSS 중심으로 이동
- 1999년 OFDM 변조 방식 도입하여 5GHz UNII(unlicensed Information Infrastructure) band에서 최고 54Mbps 지원하는 802.11a 표준 승인

무선랜의 역사 (3)

- 1999년 WECA(Wireless Ethernet Capability Alliance) 창립
  - 비영리 조직
  - 무선 LAN 제품간 상호운용성에 대한 인증을 제공
  - 2003년 Wi-Fi Alliance(WFA)로 명칭 변경
- 2003년 2.4GHz 대역에서 802.11b 호환 유지하며 802.11a와 동일한 전송 속도 지원하는 802.11g 승인
- 2009년 2.4GHz – 5GHz 대역에서 최대 600 Mbps 전송 속도를 지원하는 802.11n 승인
- 2013년 Gbps 이상의 전송속도지원을 위해 802.11ac와 802,11ad 표준 승인

무선랜 보안 역사 (1)

- IEEE 802.11b에 인증과 데이터 암호 포함
  - 인증
    - Open system
    - Shared Key 인증
  - 데이터 암호
    - WEP(Wired Equivalent Privacy)
- WEP(Wired Equivalent Privacy) 알고리즘의 취약점이 밝혀지면서 무선 LAN MAC(Medium Access Control) 계층 보안기능 향상을 위하여 2001년 5월부터 IEEE 802.11i TG(Task Group)가 결성
- 2004년 IEEE 802.11i 규격 제정
  - 무선 LAN 사용자 보호를 위해서 사용자 인증방식, 키 교환 및 키 관리 방식, 향상된 무선 구간 암호 알고리즘을 정의

무선랜 보안 역사 (2)

- IEEE 802.11i TG의 표준화 논의가 길어지면서, 점점 높아만 가는 시장에서의 보안 규격 요구에 따라 WFA에서 2003년 2월에 IEEE 802.11i Draft 3.0을 기반으로 WPA(Wi-Fi Protected Access)라는 표준 제정
  - 사용자 인증
    - Personal mode(PSK)
    - Enterprise mode(IEEE 802.1x 인증서버 이용)를 규정
  - 암호화 방식
    - WEP의 고정 키 방식을 개선한 Rekeying 방식인 Dynamic WEP
    - WEP의 문제점을 소프트웨어적으로 개선한 TKIP(Temporal Key Integrity Protocol)
- 2004년 7월 정식 IEEE 802.11i에 기반한 WPA2 발표
  - 암호 방식으로 CCMP-AES가 추가
    - Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol)
      - 가변 키 크기를 가지는 수학적 알고리즘을 사용하여 암호키를 특정 시간이나 일정 크기의 패킷 전송 후 자동 변경시키는 방식

802.1x와 802.11i

- IEEE 802.1x
  - IEEE 802.1 WG에서 표준화한 LAN 접근 제어 프로토콜
  - IEEE 802에서 개발하는 모든 표준과 호환되는 프로토콜이므로 무선랜에서도 활용 가능
- IEEE 802.11i TG RSN(Robust Security Network) 보안 구조를 드래프트 표준에 반영
  - RSN
    - IEEEE 802.1x를 이용하여 가입자 인증 및 키 관리 메커니즘, 무선구간 암호 알고리즘 그리고, 빠르고 안전한 핸드오프 보안 프레임워크를 제시한 새로운 형태의 보안 구조
  - 이때부터 무선랜 보안과 IEEE 802.1x는 불가분의 관계를 갖기 시작
  - Enterprise mode에서는 반드시 IEEE 802.1x를 지원하는 인증 시스템 도입이 전제됨

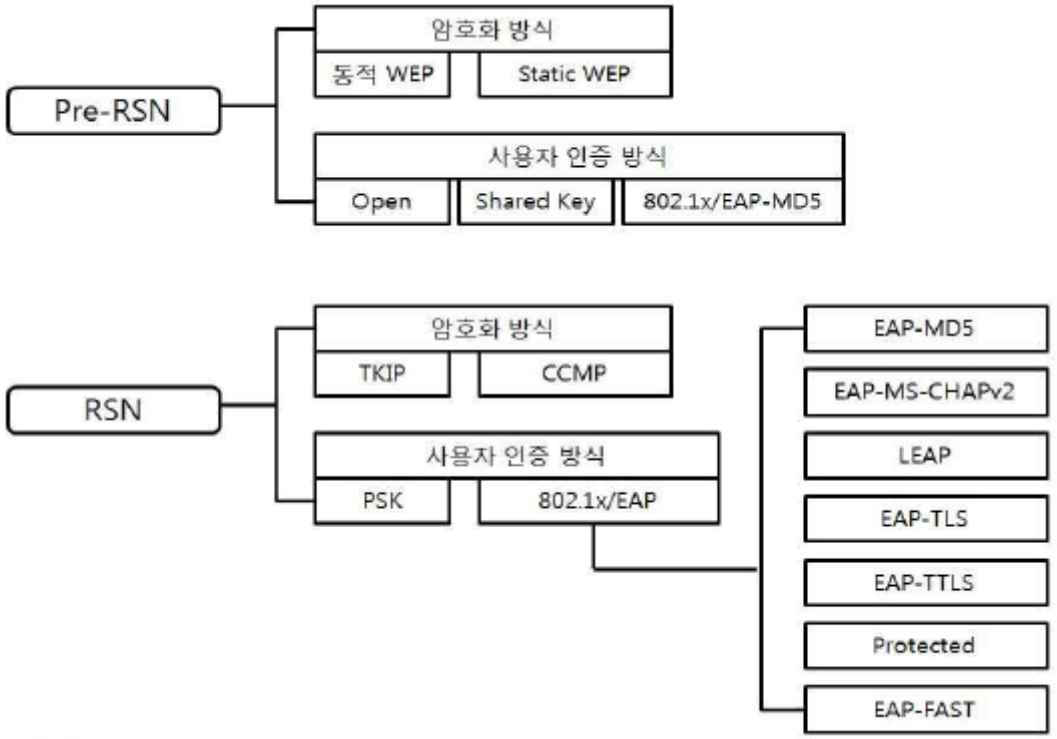
WEP의 문제점 (1)

- 2001년 스콧 플러러, 이식 맨틴, 아디 사미르
  - "RC4 키 스케쥴링 알고리즘의 취약성(Weakness in the Key Scheduling Algorithm of RC4)" 논문을 통하여 WEP에 대한 이론적인 공격 방법을 제시
- 2001년 제레미 브러슬과 블레이크 헤게를
  - AirSnort라는 오픈 소스 WEP 키 복구 프로그램 발표
- 주요 취약점
  - 짧은 길이의 초기벡터(IV) 사용으로 초기벡터 값이 재사용될 확률이 높음
    - 특히 IV는 패킷 암호키의 일부분으로 사용되므로 WEP 키 유추가 보다 용이
  - 불안전한 RC4 암호 알고리즘의 사용으로 암호키 노출의 가능성이 높음
  - 짧은 길이의 암호키 사용으로 크래킹의 위험
  - 암호키 노출 위험이 높아, 전송 데이터의 도감청의 위협
  - 단방향 인증 메커니즘으로, Man-in-the-middle 공격이나 Session hijacking이 가능
  - 전송 패킷의 무결성 보장을 위해서 단순한 CRC-32(Cyclic Redundancy Check) 알고리즘을 사용하여 무선 패킷 전송 시 패킷의 위/변조 공격에 취약

WEP의 문제점 (2)

- 단방향 인증 메커니즘의 취약성
  - 단방향 인증 : SK(Shared Key, 공유키) 방식
    - AP 입장에서 단말이 자신과 동일한 key를 소유하고 있는지를 확인하는 메커니즘
  - 단말 입장에서 AP가 자신과 동일한 key를 소유하고 있는지를 확인하는 절차가 없기 때문에 문제가 발생
  - 동일한 key를 소유하지 않은 불법 AP라 할지라도 단말에서 제공하는 인증 정보에 대해 OK 메시지를 전달하면, 단말 입장에서는 믿을 수 밖에 없음
  - 이를 개선한 것이 PSK(Pre Shared Key)이며, 상호 인증 형태로 이러한 문제를 해결
- PSK 인증 메커니즘의 취약성
  - Off line dictionary attack이 가능한 메커니즘
    - 사전에 등록된 단어를 이용한 key는 크랙이 가능
  - key 배포 문제
    - AP와 단말에 수동으로 동일한 key를 설정하는 방식으로 모든 단말은 동일한 key를 설정
    - 상황에서 해당 key가 유출되거나, 임직원이 퇴사하게 되는 경우 심각한 문제가 발생
  - IEEE 802.11i와 WAP2에서는 PSK를 개인 또는 SOHO에서 사용하도록 권고(Personal mode)
  - 기업/기관 등 복수의 사용자가 이용하는 무선랜 환경에서는 IEEE 802.1x 인증 시스템을 사용할 것을 권고(Enterprise mode)

Pre-RSN과 RSN


Pre-RSN
암호화 방식
동적 WEP
Static WEP
사용자 인증 방식
Open
Shared Key
802.1x/EAP-MD5
RSN
암호화 방식
TKIP
CCMP
사용자 인증 방식
PSK
802.1x/EAP
EAP-MD5
EAP-MS-CHAPv2
LEAP
EAP-TLS
EAP-TTLS
Protected
EAP-FAST

무선랜 인증과 암호화 비교

표준	키분배 방식	장비 인증	사용자 인증	암호화
OPEN	없음	없음	없음	없음
WEP	정적(공유키)	가능(약함)	공유키	RC4
WPA	정적(공유키) 동적(TKIP)	가능	802.1x	RC4
802.11i(WPA2)	정적(공유키) 동적(CCMP)	가능	802.1x	AES