11장 무선 네트워크와 IOT 보안

5.무선랜 암호화/인증기술

6.모바일 보안

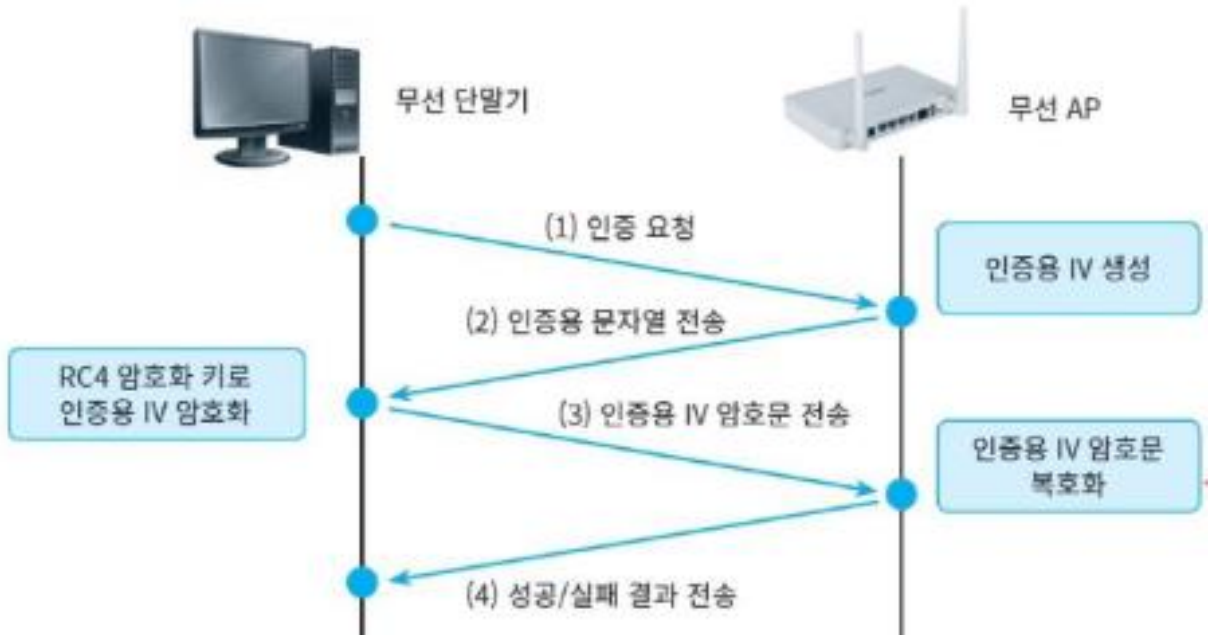
7.IOT 보안

무선랜 암호화/인증 기술

- WEP 특징
- 암호화 방식 : WEP는 RC4 스트림 암호를 사용하여 데이터 패킷을 암호화 한다.
- 키 길이 : WEP는 주로 64, 128 비트 두가지 키 길이를 사용한다. 64비트는 40 비트의 실제 키, 24비트의 IV로 구성된다. 128 비트의 경우 실제키 104비트 24 비트의 IV로 구성된다.
- 초기 벡터(IV) : 암호화 과정에서 동일한 암호문을 생성하지 않게해주는 역할을한다.

무선랜 암호화/인증 기술

- WEP 인증 과정



WEP 인증 과정

- 인증 요청
- 무선 단말기(노트북, 스마트폰)가 무선 네트워크에 연결하려 할 때 “이 네트워크에 접속하고 싶다”라는 신호를 무선 AP에 전송한다.
- IV 생성 및 전송
- 무선 AP는 인증 요청을 받고 IV를 랜덤하게 생성하고 이는 이후에 암호화 과정에서 중요한 역할을 수행하고 보안성 강화를 위해 인증 과정마다 새롭게 생성된다.
- IV 암호화
- 사전에 무선 AP와 공유된 암호화 키를 사용해 AP로부터 받은 IV를 암호화 한다.
- 이때 암호화 키는 와이파이에 접속할 때 비밀번호와도 같은 것이다.
- 암호화된 IV 전송 및 검증
- 암호화된 IV를 다시 무선 AP로 전송하고 무선 AP는 암호화 키를 사용해 암호화된 IV를 복호화 한다. 이 과정 이후에 성공/실패 결과 전송

WEP의 문제점

- 보안 취약점
- 가장 큰 문제는 IV가 너무 짧고 길이가 고정되어있어 동일한 IV가 반복될 가능성이 높다. 이로 인해 공격자가 패킷을 쉽게 분석하고 키를 추측할 수 있다.
- 키 관리 문제
- WEP에서는 키가 수동으로 관리되며 자주 변경되지 않는 경우가 많아서 공격에 취약하다.

WEP의 대체

- WPA
- WPA는 초기 벡터(IV)가 48비트로 확장되어 사용되어 IV의 재사용 가능성을 줄였다.
- IV의 순차적 증가 규칙 적용을 통해 WEP와는 다르게 IV의 중복이 사실상 없는 수준으로 설계 되었다.
- 하지만 WPA 역시 WEP와 같은 RC4 암호화 알고리즘을 사용하므로 키 크랙 공격 가능성이 있어 본질적인 개선은 이루어지지 않았다.
- WPA2
- WPA를 보완하고자 WPA2에서는 RC4 대신 안정성이 입증된 AES 블록 암호화 알고리즘을 채택해 128비트 암호화 키 및 48비트 IV를 사용한다.
- 현재까지 매우 강한 암호화 방식으로 인정받고 있지만 키 값이 외부로 노출될 경우에 많은 보안 문제를 일으킬 수 있다는 점, 간단한 패스워드로 설정된 경우는 무차별 공격에 당할 수 있다는 취약점이 존재한다.

모바일 보안

- IOS
- 애플의 IOS는 다윈 커널을 기반으로 만들어 졌으며 이는 2000년에 만든 오픈소스 기반의 유닉스 운영체제의 이름이다.
- IOS 자체는 소스코드가 공개되어있지 않은 폐쇄형 구조이며 안드로이드에 비해 앱 업데이트가 느리지만 악성코드의 위협에서 안전하다.
- 안드로이드
- 리눅스 커널을 기반으로 만들어져 소스코드가 공개되어있는 개방형 운영체제이다.
- IOS에 비해 앱 배포가 편리하지만 반대로 악성코드의 위협에 많이 노출되어있다.

모바일 보안 위협 요소

- 악성코드
- PC와 마찬가지로 악성코드가 설치 될 수 있는데 모바일 기기는 24시간 가동되며 사용자의 사생활이 더 노출되어있어 치명적이다.
- 플랫폼 해킹
- 제조사에서 배포하는 단말기 운영체제의 최고 권한을 가지는 행위이다. 루트 계정을 가진다는 의미로 루팅이라고도 부르고 IOS에서는 탈옥이라고 한다.
- 일반 유저의 권한으로 접근할 수 없던 시스템에 접근하고 기본 앱 제거나 주요 설정 변경이 가능하다
- 플랫폼 해킹을 위한 도구가 존재하는데 누군가 이 도구에 악성코드를 삽입하여 배포하면 보안을 위협하는 요소가 된다.
- 앱 위변조
- 보통은 안드로이드 계열 단말기 대상으로 발생한다.

IOT 보안

- IOT
- 각종 사물에 센서와 무선 네트워크 기능을 내장해 인터넷에 연결하는 기술이다.
- 가전제품, 모바일 장비 등 다양한 사물이 해당된다.
- 다양한 가전제품이 해당되는만큼 그 대상들이 모두 보안 공격의 대상이 될 수 있다는 점에서 보안 위협이 증가하고 있다.

IOT 보안 위협 대응 방안

- 물리적 보안 취약점

- 인증 메커니즘 부재
- 초기 설치 단계에서 인증 정보(아이디, 비밀번호)를 필수적으로 변경해서 비인가 사용자의 접근을 방지한다.
- 잘못된 인증 시도에 횟수 제한을 부여하여 무차별 공격을 막을 수 있다.
- 접근 통제 부재
- 일반 사용자에게는 최소한의 권한만 허용하고 관리자 권한은 다른 패스워드로 설정하여 인가된 사용자만 접근 할 수 있도록 한다.