CLAY

무선 네트워크와 IoT 보안

목차

무선 네트워크 개요

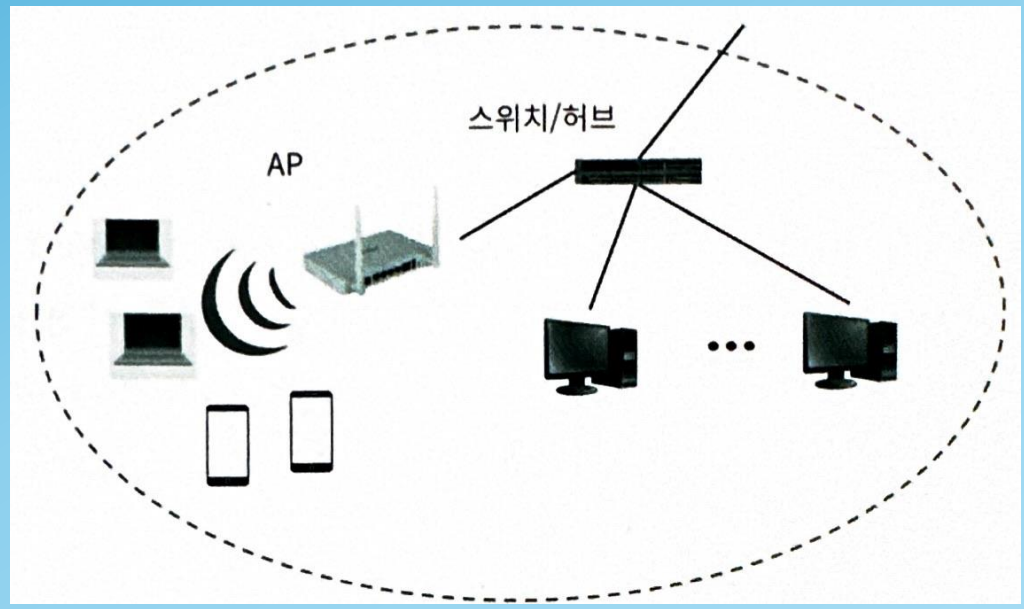
- 1. 무선 네트워크 유형
  - WPAN : 무선 헤드셋
  - WLAN : 와이파이
  - WMAN : 와이맥스 -> 예) 국군 무전기
  - WWAN : 무선 광대역 통신망(휴대폰)

구분	설명	전송 거리	예
WPAN	10m 이내의 근거리(단거리)	10m	블루투스, 지그비(ZigBee)
WLAN	유선랜의 확장, 무선랜	100m	와이파이(Wi-Fi)
WMAN	대도시와 같은 넓은 지역을 대상으로 높은 전송 속도 제공	10km	와이브로(WiBro), 와이맥스(WiMax)
WWAN	무선 광대역 통신망	100km	이동 통신 (셀룰러 네트워크)

무선 네트워크 개요

2. 무선 네트워크의 특징

- 감쇠 현상
  - 신호가 모든 방향으로 퍼진다.
  - 거리에 따라서 신호의 강도가 정해진다.
  - 강도가 낮아질수록 통신 품질은 떨어진다.
- 간섭 현상
  - 신호가 중첩되어 전파 교란이 발생한다.
  - 다중 경로 전달 현상이 있다.
  - 유선에 대비하여 오류 현상이 매우 심각하게 발생한다.
  - 실내 혹은 실외의 다양한 환경적 요소에 의해서 비정상적인 데이터가 전달될 가능성이 매우 높다.



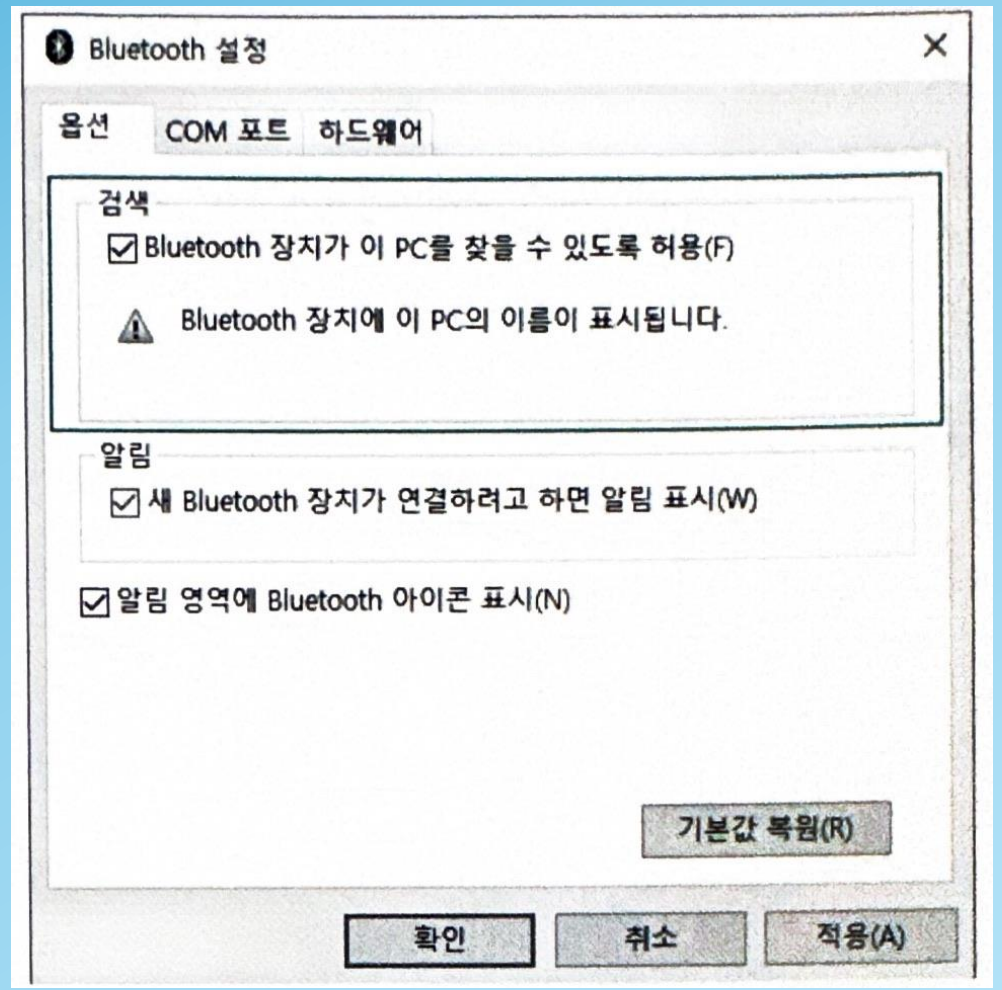
블루투스 보안

- 블루투스 : 1994년 스웨덴의 통신장비 제조사인 에릭슨이 최초로 개발한 근거리 무선 네트워크다.
  - 예) 마우스, 키보드 스마트폰, 태블릿, 스피커 등 문자 정보 음성 정보를 주고 받는 목적으로 사용됨
- 높은 수준의 암호화 알고리즘 적용 혹은 인증과 같이 보안성과 관련된 기능을 구현하기 쉽지 않다. 즉, 다소 보안성이 낮다는 특징이 있으며 특징들로 인하여 많은 보안 위협을 받는다.

블루투스 보안

1. 블루프린팅

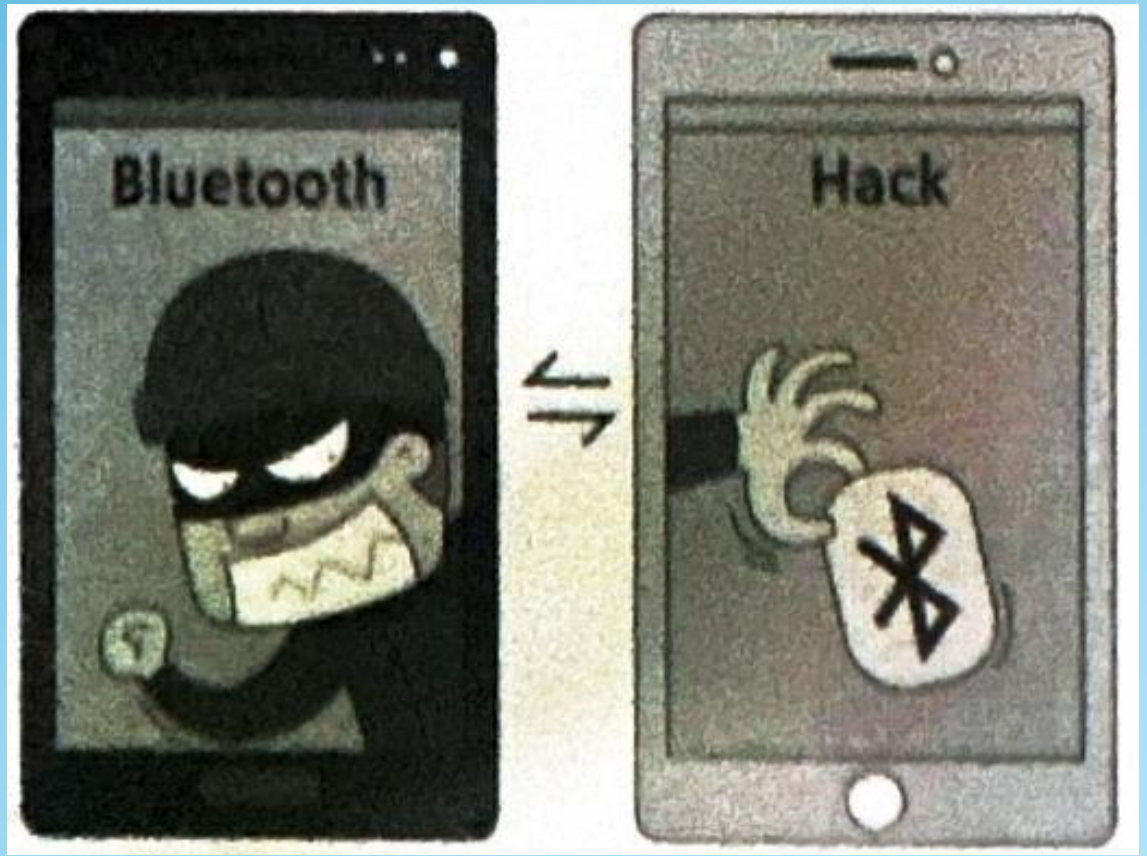
- 블루투스 공격 장치의 검색 활동을 뜻한다.
- 블루투스 장치는 유선 네트워크의 하드웨어 주소에 해당하는 고유 번호가 있다.
- 인근한 모든 블루투스 장치를 스캔 할 수는 없지만, 검색이 허용된 장치만 대상으로 스캔이 가능하다.
- 보안 공격자는 블루프린팅을 시작으로 하여 능동적 공격을 준비할 수 있기 때문에 평상시에는 블루투스 검색 허용 옵션을 꺼두는 것이 보안적으로 권장된다.



블루투스 보안

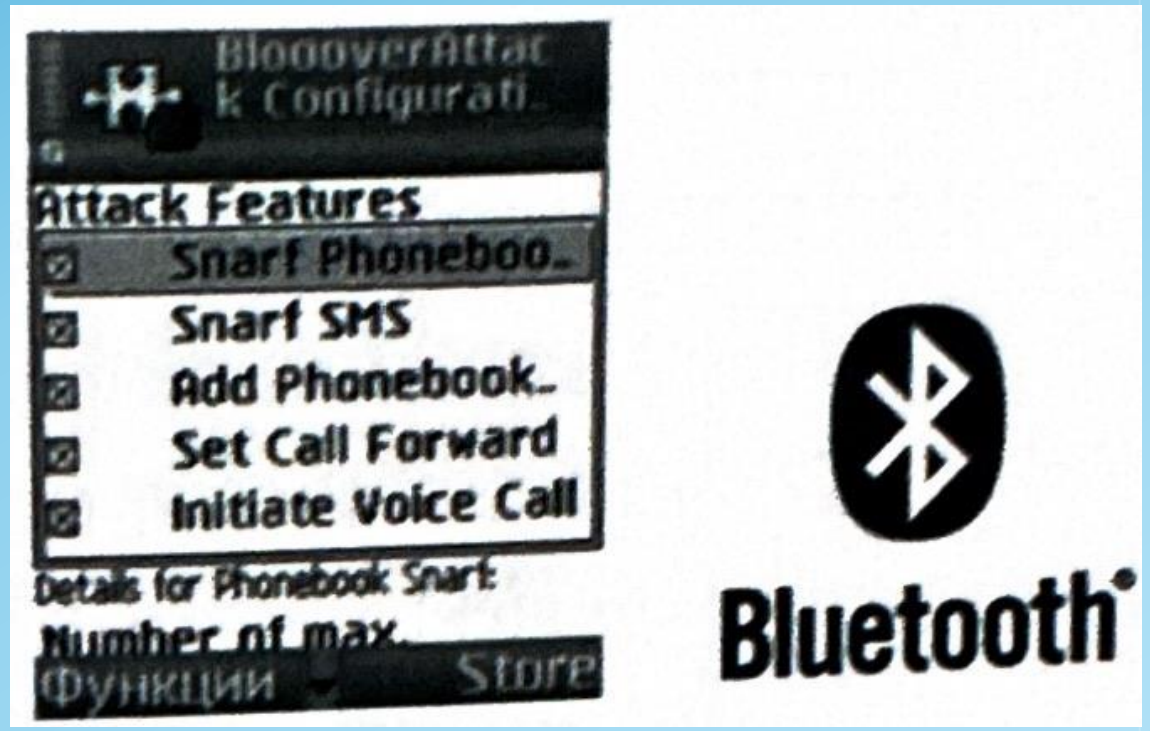
2. 블루스나핑

- 블루투스의 취약점을 이용하여 블루투스 기기의 정보에 접근하는 공격
- 공격자는 블루투스 장치까지 인증 없이 정보를 간편하게 주고받을 수 있는 OPP기능을 악용하여, 블루투스 장치로부터 주소록 또는 달력 등의 내용을 요청하고 이를 열람하거나 보안적으로 취약한 임의의 파일에 접근할 수 있다.
- 기기가 펌웨어에 버그가 있는 기기라면 공격자는 경우에 따라 피해 디바이스의 모든 파일에 접근이 가능하다.



블루투스 보안

- 블루버깅
  - 공격 대상이 되는 블루투스 장치를 원격에서 연결하여 임의의 동작을 실행시키는 공격
    - 장치가 서로 한 번 연결되면 그 이후에는 별다른 인증 절차 없이도 자동으로 서로 연결되는 인증 취약점을 악용한 공격
  - 공격 대상과 10M이내에서 가능하고 이러한 공격으로 전화 걸기, 불특정 번호로 문자 메시지 보내기 기존의 문자 메시지 읽기 주소록 읽기 및 쓰기 인터넷 서핑 등을 수행할 수 있으며 심지어 전화 내용을 감청도 가능하다.



블루투스 보안

- 블루재킹
  - 블루투스를 이용해 스팸 메시지를 익명으로 퍼트리는 것을 말한다.
  - 기기의 가용성을 떨어트리는 것으로 보안과 관련하여서는 상대적으로 위협이 적다.

무선랜 보안

- 구성요소 및 유형
  - 무선 단말기와 유선랜의 가장 마지막에 위치하여 무선 단말기에게 무선랜 접속을 가능하게 하는 무선 AP로 구성된다.
  - 2개 이상의 무선랜을 연결하는 무선 브리지가 사용되기도 하는데, 무선랜의 특성상 2개의 브리지 사이에는 전파의 전송을 방해하는 물체가 존재해서는 안 된다.

무선랜 보안

구분	설명	주요 스펙	제정 시기
802.11	최초의 무선랜 프로토콜	2.4GHz/2Mbps	1997.07
802.11b	WEB 방식의 보안 기능 추가	2.4GHz/11Mbps	1999.09
802.11a	전파 투과성과 회절성이 떨어져 통신 단절 현상이 심하며 802.11b와 호환되지 않음	5GHz/54Mbps	
802.11g	802.11b와 호환되며, 최대 54Mbps까지 고속 통신에 대한 스펙을 지원. 단, 네트워크 공유 시 데이터 처리 효율이 급격히 줄어드는 문제점이 있음	2.4GHz/54Mbps	2003.01
802.11i	802.11b 표준에 WPA 규격을 포함하여 보안성을 강화한 프로토콜	2.4GHz/11Mbps	2004.06
802.11n	최대 600Mbps 속도, 여러 안테나를 사용하는 다중 입력/다중 출력(MIMO) 기술 사용, 대여폭 손실 최소화	5GHz,2.4GHz	2009.09

무선랜 보안

- 무선랜의 보안 취약점
  - 물리적 취약점 : 외부 노출로 인해 비인가자에 의한 장비의 파손 및 장비 리셋을 통한 설정값 초기화 등의 문제가 발생할 수 있다.
  - 기술적 취약점 1 : 도청
    - 무선 데이터의 수신을 통해 도청이 가능하다.
  - 기술적 취약점 2: 서비스 거부(DoS)
    - AP장비에 대량의 무선 패킷을 전송하는 서비스 거부 공격을 통해 해당 무선랜을 무력화할 수 있는것을 말한다.
  - 기술적 취약점 3: 불법AP
    - 불법적으로 무선 AP를 설치하여 무선랜 사용자들이 해당 불법 AP에 접속하게끔 유도할 수 있다.
  - 기술적 취약점 4: 비인가 접근-SSID 노출
    - 개방형 인증 방식을 별도의 인증 절차 없이도 무선 AP에 연결이 가능하다.

무선랜의 보안성 강화

- 물리적 보안 및 기본 관리자 패스워드 변경
  - 전파가 건물 내에 한정되도록 전파 출력을 조절하거나 혹은 위치를 이동시킨다.
  - 건물의 외부 벽 쪽이 아니라 건물 안 쪽의 중심부에 눈에 쉽게 띄지 않는 곳에 설치한다
  - 설치 후 반드시 기본 관리자 패스워드를 재설정한다.
  - 사용하지 않을 시 전원을 꺼둔다.
- SSID 브로드캐스팅 금지
  - SSID값을 숨김으로 설정하면 SSID를 모르는 사용자의 접속 시도를 줄일 수 있다.
  - 높은 수준의 보안 권한이 필요한 무선랜 환경이라면 이처럼 SSID의 브로드캐스팅을 금지하여 폐쇄 시스템으로 운영함으로써 보안성을 높인다.
- 통신 암호화 및 인증
  - 통신 과정 뿐 아니라 인증 시에도 암호화를 수행한다.