사물인터넷 (IoT) 보안

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

1. 사물인터넷 개요

2. 사물인터넷 보안위협과 고려사항

3. 사물인터넷 보안

1.사물인터넷 개요

사물인터넷 개요

사물인터넷 (IoT: Internet of Thing)

- 정보통신기술 기반으로 모든 사물을 연결해 사람과 사물, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 인프라 및 서비스 기술

- 인간과 사물, 그리고 서비스를 상호 연결해주는 기술로써 인간, 사물, 서비스가 주요 구성요소로 서로 상호작용

- 사물
  - 웨어러블 디바이스, 모바일 장치, 가전제품 등 다양한 임베디드 시스템
  - 상호 간 통신을 위해 IP주소 OID(Object IDentifier) 등 고유의 식별자 가짐
  - 유무선 네트워크에서의 단말 장치(end-device) 뿐만이 아닌
  - 인간, 차량, 교량, 각종 전자장비, 문화재, 자연환경을 구성하는 물리적 사물 등도 포함

- **이동통신망을 통해 사람과 사물, 사물과 사물 간 지능 통신이 가능한 Machine to Machine(M2M)의 개념을 인터넷으로 확장**
  - 사물은 물론, 현실과 가상세계의 모든 정보가 상호작용하는 개념으로 진화

- **사물인터넷 플랫폼은 디지털화한 생태계를 이끌 기술로 선정**
  - 가트너(Gartner)에서 발표하는 유망 기술 하이프 사이클 (Hype Cycle for Emerging Technologies)

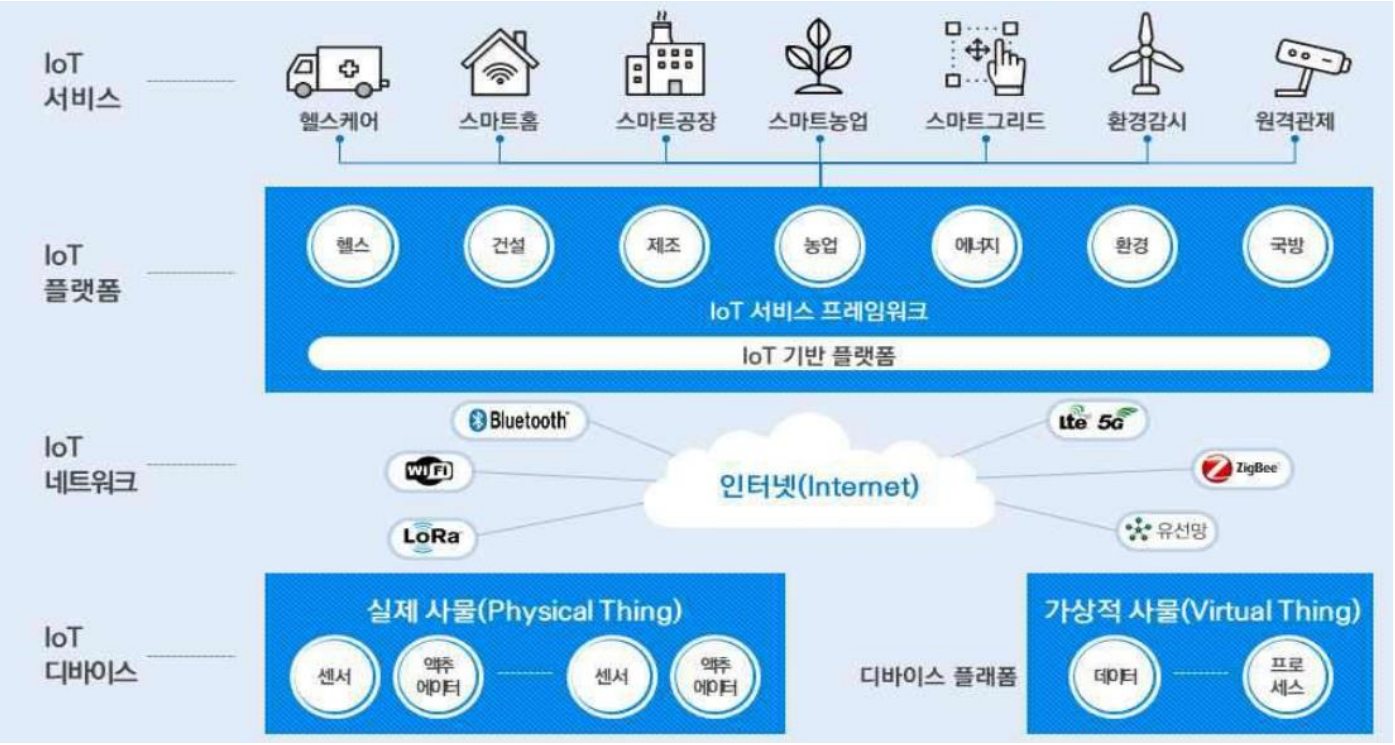
- **관련 연구**
  - 의료분야, 스마트 시티, 스마트 팩토리, 자율 자동차 등 여러 산업 분야

- **모든 사물을 인터넷으로 연결하여 사물 간 센싱, 네트워킹, 정보처리 등으로 사람의 개입 없이 지능적 / 자율화 서비스를 제공하는 방향으로 발전**

- **사물인터넷은 4차 산업혁명의 핵심 기술으로써 정보통신기술의 핵심 산업으로 급부상**
  - 글로벌 사물인터넷 시장 규모는 연평균 12.8% 성장세가 관측되며 1,225 조원까지 확대될 전망

- **시간과 장소의 제약 없이 연결되는 통신환경은 IoT 환경을 획기적으로 변화시키고 있음**
  - 무선 통신 환경의 실생활 적용으로 다양한 경제적 가치, 효용성 및 편의성 증대

- 사물인터넷의 구성
  - 디바이스 : 데이터 수집용 센서, 제어용 액추에이터, 통신모듈 등
  - 네트워크 : 근거리·장거리(저전력) 무선통신, 유선통신 기술
  - 플랫폼 : 빅데이터·인공지능 등 지능정보기술로 구현된 서비스 프레임워크
  - IoT 서비스: 헬스케어, 스마트홈, 환경감시, 원격관리 등



사물인터넷 개념도

사물인터넷의 특성

- 자원 제약성, 이동성, 정보보안, 이종성

- 사물인터넷은 CPU, 배터리, 메모리 등 자원 제약성을 극복하기 위해 최소자원으로 필요성을 만족해야 함
  - 사물인터넷의 경량화 필수

- 높은 이동성으로 네트워크 토폴리지가 동적
  - 사물인터넷의 낮은 성능과 대역폭의 영향으로 연결성은 좋지 않음

- 사물인터넷 기술의 발달로 CCTV 영상, 사용자 건강 정보 등 다양한 영역에서 민감정보가 생성 → 정보보안 중요

- 다양한 종류의 디바이스 (센서, 엑추에이터 등)들이 상이한 플랫폼에서 동작하면서 디바이스 간의 상이한 프로토콜을 이용한 통신이 가능

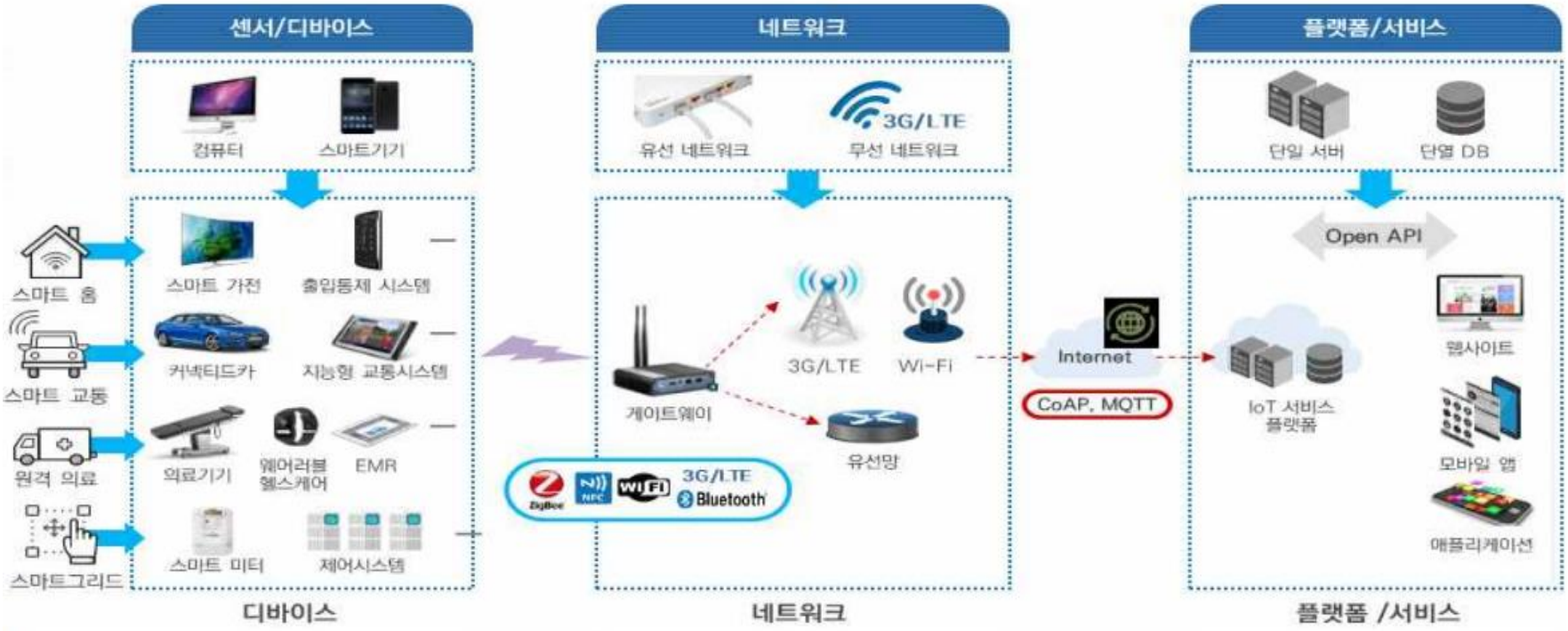
사물인터넷의 기술요소

사물인터넷의 3대 주요기술

- 센서 기술, 네트워크 기술, 플랫폼 및 서비스 인터페이스 기술

- 센서 기술
  - 전통적인 센서 기술인 온도, 습도, 열, 가스, 조도, 초음파 센서 등
  - 원격감지, 위치 및 모션, 영상 센서 등 주위 환경으로부터 정보를 획득하는 물리적 센서를 포함
  - 사물인터넷의 핵심기능: 스마트센서
    .임베디드 소프트웨어와 반도체 칩 기술의 발전으로 지능화

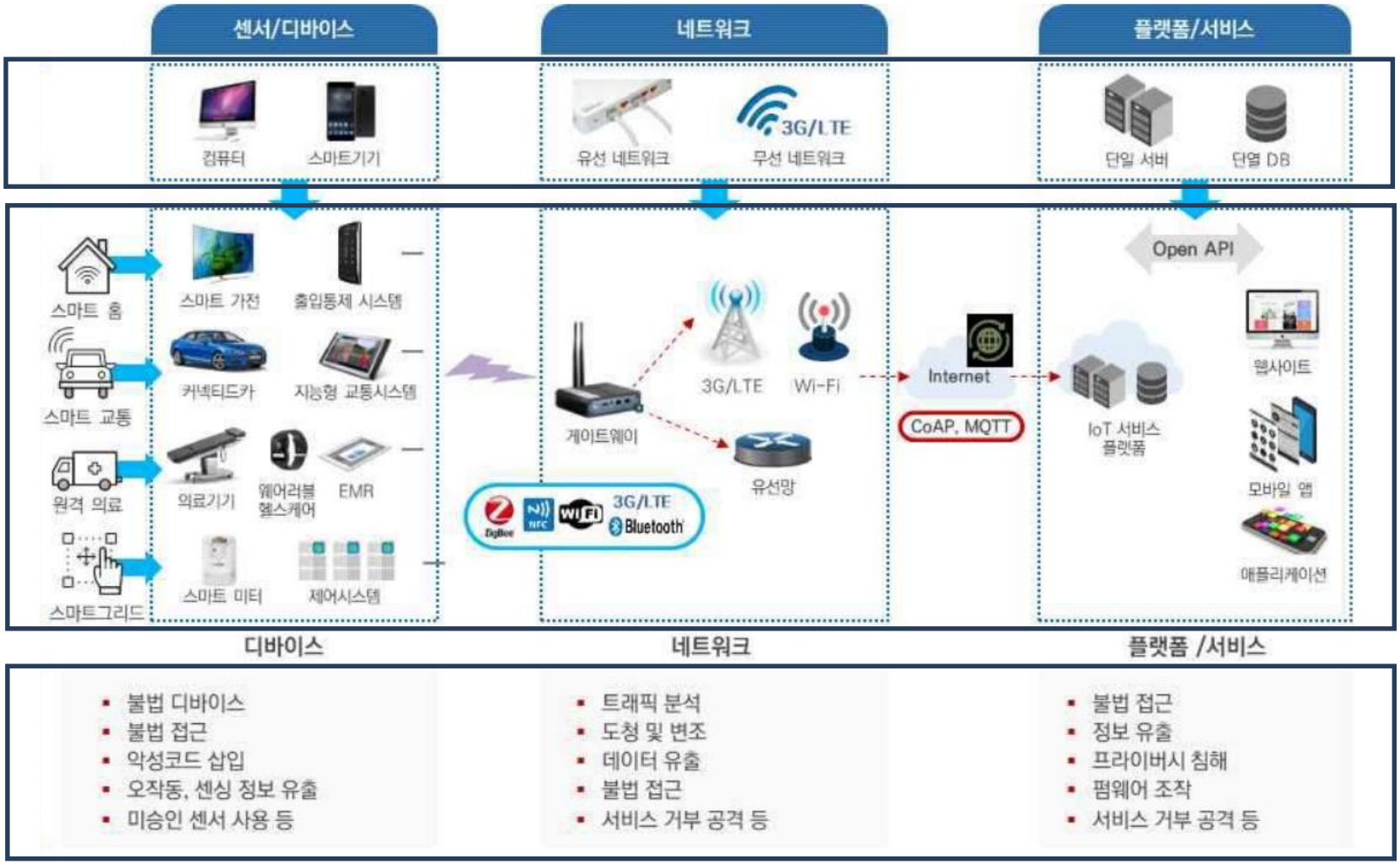
사물인터넷의 기술요소


센서/디바이스
네트워크
플랫폼/서비스
컴퓨터
스마트기기
유선 네트워크
3G/LTE
무선 네트워크
단일 서버
단열 DB
Open API
스마트 홈
스마트 가전
출입통제 시스템
스마트 교통
커넥티드카
지능형 교통시스템
원격 의료
의료기기
웨어러블 헬스케어
EMR
스마트그리드
스마트 미터
제어시스템
게이트웨이
3G/LTE
Wi-Fi
유선망
Internet
CoAP, MQTT
IoT 서비스 플랫폼
웹사이트
모바일 앱
애플리케이션
ZigBee
NFC
Wi Fi
3G/LTE
Bluetooth
디바이스
네트워크
플랫폼 /서비스

2. 사물인터넷 보안위협과고려사항

- IoT 보안 영상 개념

사물인터넷 환경에서의 보안 위협



사물인터넷 보안사고 사례

- **서울 강서구 마곡에 위치한 한 아파트가 해외 해커들의 공격을 받아 아파트 공용 서버가 파괴되는 사건 발생**
  - 많은 가구들이 가구내 윌패드(홈서버) 기능이 마비되어 조명, 현광 출입 등 각종 스마트홈 서비스가 중단

Mirai Botnet

- 사물인터넷을 통한 DDoS 공격을 일으킨 대표적인 사례
- 수십만대의 사물인터넷 디바이스를 감염시켜 대규모 DDoS 공격을 일으킨 트로이 목마 프로그램
- 관리자 페이지에서 기본 아이디/패스워드를 사용하는 기기를 이용

- 공격 시나리오
  - 관리자 페이지에서 약 60여 개의 공장 출하 아이디/패스워드를 통해 전사 공격을 진행하여 접속
  - 접속 후 악성 코드를 감염시켜 주변을 스캐닝한 후 감염되지 않은 취약한 사물인터넷 디바이스를 찾아 전파
  - 초당 400~500GB의 패킷을 전송하는 대규모 DDoS 공격 시행

IP 카메라 해킹

- 네트워크에 연결되어 있는 디바이스를 해킹한 사례
- 노출된 IP를 통해 기본 아이디/패스워드를 사용하고 있는 IP 카메라를 해킹하여 실시간으로 카메라의 영상 노출
  - Sohdan, Insecam 사이트에서 전 세계 7만3000여대의 IP카메라가 해킹되어 생중계됨
  - 국내에서는 약 6000여개 카메라가 해킹 피해

IoT 보안 추세

- 한국인터넷진흥원(KISA) 조사 결과 국내 IoT 해킹과 관련한 신고 건수가 빠르게 증가하는 추세
  - 2013년, 0 건 → 2018년, 387건.

- KISA 정보보호 실태 설문조사 결과 대부분이 IoT 보안 위협 우려
  - 개인정보 침해 위협 증가를 우려(54.9%), 사이버 공격과 가능성 증대(44.8%), 대규모 피해 확산 위협(10.7%) 등

- 사물인터넷 보안사고는 단순히 개인정보 유출이나 전자금융 사기, 대규모 DDoS 공격으로 일부 기업이나 기관이 마비로 멈추지 않음

- 재난안전망에 쓰인 센서를 비롯하여 자동차 제어시스템 등이 해킹당할 경우 사회나 국가가 마비되거나 국민 생명을 위협하는 재앙을 초래할 가능성이 있음

사물인터넷 보안 고려사항

- **사물인터넷 사용량 및 실생활에 밀접한 관련이 있는 서비스 (차량, 홈·가전, 헬스케어 등)의 사물인터넷 적용이 증가하는 추세**
  - 디바이스 및 관련 시스템의 오작동, 불법 조작 발생시 이용자의 신체나 생명, 재산 등에까지 피해가 확대될 수 있음

- **사물인터넷을 구성하는 수많은 기기와 시스템들이 서로 네트워크로 연결되어 작동하는 특성**
  - 사물인터넷의 광범위한 연결로 사물인터넷 외의 다른 기기 및 서비스에도 영향을 미치는 예상하지 못했던 문제 발생 우려

- **사물인터넷망은 다양한 디바이스들이 연결되고 무선망 기반으로 되어 각종 보안위협 노출됨**
  - 모든 단계별 요구사항을 점검하여 보안 내재화 필요
    - 설계단계부터 개발, 운영, 폐기까지 단계별 보안위협과 취약성을 점검해야 함

사물인터넷 보안 고려사항

- IoT 보안얼라이언스에서는 IoT 공통 보안 7대 원칙 제시

- IoT 디바이스 및 서비스 제공자와 사용자가 IoT 디바이스의 세부 단계에서 고려해야 하는 공통 보안 요구 사항

사물인터넷 보안 고려사항

단계	보안 원칙
설계	**(보안원칙 1) 정보보호와 프라이버시 강화를 고려한 IoT 제품 서비스 설계** ① IoT 장치의 특성을 고려하여 보안 서비스의 경량화 구현 ② IoT 서비스 운영 환경에 적합한 접근권한관리 및 인증, 데이터 암호화 등의 방안 제공 ③ 소프트웨어 보안기술과 하드웨어 보안 기술의 적용 검토 및 안정성이 검증된 보안 기술 활용 ④ 민감 정보보호를 위해 암호화, 비식별화, 접근관리 등의 방안 제공 ⑤ 민감정보 수집목적 및 이용방법 등에 대한 운영정책 가사화를 통한 투명성 보장
개발	**(보안원칙 2) 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증** ⑥ 보안취약점 사전 예방을 위한 시큐어 코딩 적용 ⑦ 다양한 S/W에 대해 보안 취약점 점검 수행 및 보안패치 방안 구현 ⑧ 다양한 하드웨어 보안 기법 적용
배포 설치 구성	**(보안원칙 3) 안전한 초기 보안설정 방안 제공** ⑨ IoT 제품 서비스 설치 Secure by Default 원칙에 따라 파라미터 설정 **(보안원칙 4) 안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라미터 설정** ⑩ 안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라미터 설정
운영	**(보안원칙5) IoT 제품 서비스의 취약점 보안패치 및 업데이트 지속 이행** ⑪ IoT 제품 서비스의 보안취약점 분석 및 보안패치 이행 ⑫ IoT 제품서비스 보안취약점 및 조치사항에 대해 공지
관리	**(보안원칙6) 안전한 운영 관리를 위한 정보보호 및 프라이버시 관리체계 마련** ⑬ 개인정보보호정책 수립 및 기술적 관리적 보호조치 마련
폐기	**(보안원칙7) IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련** ⑭ 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행 ⑮ 침해사고 발생 원인분석 및 책임 추적성 확보를 위해 로그기록 저장 관리

3.사물인터넷 보안

디바이스 보안

- 기밀성 (Confidentiality)
  - 사물인터넷 기기간 전송되는 메시지는 불법적인 스니핑 (Sniffing) 또는 도청 방지를 위해 메시지를 암호화된 형태로 전송되어야 함
  - 사물인터넷 기기기는 정보유출 방지를 위해 개인정보 및 암호키와 같은 중요 데이터를 암호화하여 안전하게 처리 및 저장 관리해야 함

- 무결성 (Integrity)
  - 사물인터넷 기기는 데이터 위변조 방지를 위해 데이터 무결성 검증 기능을 제공해야 함

- 가용성 (Availability)
  - 사물인터넷 기기는 소프트웨어 오류나 악성코드 감염에 의한 오동작 시 소프트웨어 안전성을 보장해야 함
  - 해당 모듈 분리 및 제거, 접근권한 제한 기능 등

- 인증/허가 (Authentication/Authorization)
  - 안전하고 자율적인 통신 환경 구축, 기기 간 상호인증 기능과 정보유출 방지 및 프라이버시 보호를 제공해야 함
  - Ownership 제어와 같은 권한 제어 및 설정 기능

- 별도 유저 인터페이스가 제공되는 사물인터넷 기기
  - 비인가 된 사용자의 접근을 차단하기 위해 사용자 인증 기능을 제공할 수 있어야 함
  - 불법적인 기기의 접근을 차단하기 위한 기기 인증 기능을 제공해야 함

디바이스 관련 보안 위협

보안위협	위협내용
Interference/ Jamming/Collision	• 노이즈 발생, 동시 동일 주파수 접속, 주파수 위변조 등을 통해 실제 신호의 정상적인 송수신을 방해하는 공격
Sybil	• 기존의 Wireless Ad-hoc, 센서 네트워크에서 Multi-Identity가 허용되는 취약점을 이용한 공격으로 각 디바이스나 센서에 Unique ID을 부여하지 않을 경우 발생
Traffic Analysis	• 암호화되지 않은 패킷 (NPDU) 프레임 (DLPDU) 페이로드를 분석하여 정보를 취하는 공격 • (단, 암호화 할 경우 상대적으로 안전하지만, System Performance에 영향이 갈 수 있음)
DoS	• 주변 노드에 지속적인 광고 패킷을 송신, DLPDU 반복수정, CRC 반복체크로 시스템에 무리를 주거나 주파수 재밍 등을 통해 신호 송수신을 방해하는 공격
De-synchronization	• Device Pool에 잘못된 시간 정보를 송신하여 디바이스가 계속적으로 시간을 교정하는데 자원을 소모하도록 하는 공격
Wormhole	• 상호 통신이 허가되지 않은 두 디바이스의 무선 통신 모듈을 공격해 상호간 통신을 가능하게 만들고, 통신 라우팅을 고의로 변경하거나 악성코드 배포 경로로 이용하는 공격
Tampering	• 단말에 저장된 데이터 혹은 송수신 데이터를 임의로 위변조하는 공격
Eavesdropping	• 암호화되지 않은 디바이스 (센서)와 게이트웨이 구간 정보를 도청하는 공격
Selective Forwarding Attack	• 선택적으로 특정 노드에 패킷을 포워딩하지 않게 하여 해당 노드를 블랙홀로 만들어 버리는 공격
Spoofing	• 네트워크에 공유된 네트워크 키를 취득하여 허가되지 않은 Fake 디바이스(센서)를 네트워크에 접속시켜 악의적인 행위를 하도록 하는 공격

게이트웨이 보안 요구사항

- 임의의 메시지를 주입하여 발생할 수 있는 보안 위협에 대응 할 수 있어야 함
  - 예) Buffer Overflow 공격에 대응하기 위한 Secure Coding 준수

- 송·수신 데이터는 불법적인 스니핑(sniffing) 또는 도청 방지를 위해 암호화된 형태로 전송되어야 함

- 프로토콜 변환 과정에서 데이터 기밀성을 유지하고, 악의적인 위·변조를 방지할 수 있어야 함
  - 방화벽, IPS와 같은 수단을 통해 네트워크 침입 탐지 및 네트워크 트래픽 제어 필요

- 사물인터넷 네트워크 및 기기에 대한 모니터링 기능을 지원하고, 오작동·악의적인 조작·트래픽 폭증과 같은 이상징후를 탐지해야함

- 사물인터넷 기기의 최초 등록 시, 게이트웨이와의 보안키(Secure Key) 합의, 보안정책 설정과 같은 초기 보안 설정을 지원할 수 있어야 함

IoT 서비스 관련 보안 위협

보안위협	위협내용
웜, 바이러스	• 시스템을 파괴하거나 작업을 지연 또는 방해할 수 있음
비인가된 접근	• 비인가자가 불법적으로 시스템에 로그인하여 디스크 자료 불법 열람, 삭제 및 변조 등 시스템에 물리적인 피해를 유발할 수 있음
패치되지 않은 시스템 OS 보안취약성	• 운영체제, 데이터베이스, 응용 프로그램, 시스템 프로그램 등 모든 정보 자산에 존재하는 허점(버그)에 의해 주로 발생 • 사용자의 민감정보 유출, 바이러스 또는 악성코드에 의한 시스템의 비정상적인 동작 발생 가능
설정 오류 및 실수	• 패스워드 공유, 데이터 백업의 부재 등 운영자의 부주의와 태만으로 시스템의 불법접근 및 데이터 손실 등의 문제 발생 가능
기밀성/무결성 공격	• 네트워크 도청, 감청을 통해 데이터 위변조, 악성코드 삽입, 암호키 유출 등을 통한 보안위협 발생 가능
개인정보 유출 및 프라이버시 침해	• 다양한 디바이스로부터 수집된 단편적인 정보의 조합으로 새로운 개인식별정보 생성

참고문헌

- ICT융합보안의 이해, 이기혁외 1인 저, 진한출판사
- 정부사물인터넷 도입 가이드라인, 한국정보화진흥원
- IoT보안, LG CNS 홍보영상

Q & A

Thanks!