안전한 스마트 시티를 위한 IoT 보안 이슈와 대응 방안

2018. 03. 16

김 학 용

순천향대학교
SOON CHUN HYANG UNIVERSITY

Speaker : 김학용 교수/공학박사/작가/칼럼니스트

- 現) 순천향대학교 IoT보안연구센터 교수
- 現) IoT전략연구소 대표 컨설턴트
- 前) 부산대학교 사물인터넷연구센터 교수
- 前) LG유플러스 M2M사업담당 부장
- 前) 삼성SDS 신사업추진센터 차장

이메일 : IoTStLabs@gmail.com
honest72@sch.ac.kr
전 화 : 010-4711-1434

4차산업혁명 시대의
비즈니스 전략

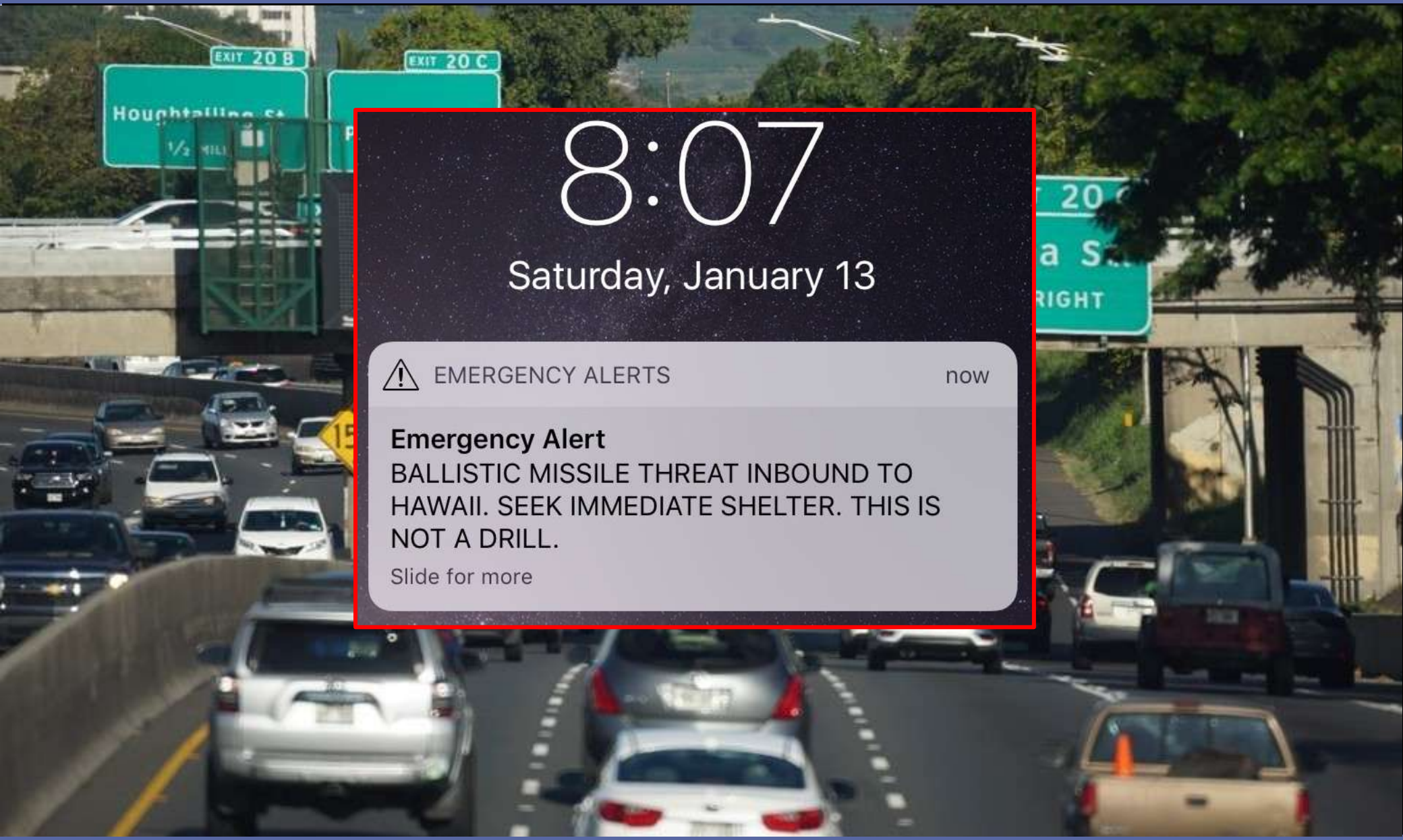
**냉장고를
공짜로 드립니다**

만약 해커가 도시를 해킹한다면?

※ 출처 : 구글 이미지 검색 (다이하드 4.0)

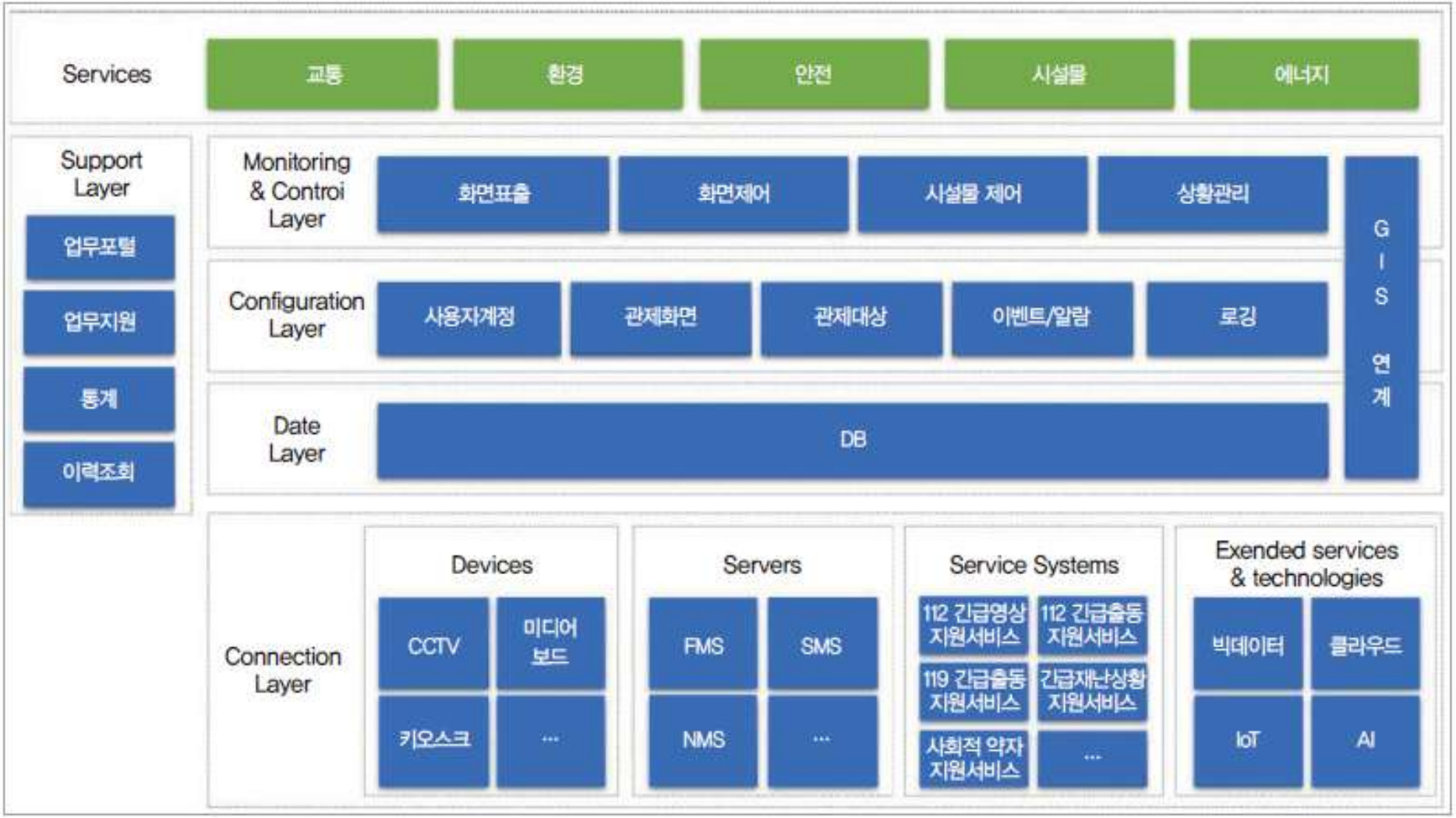
만약 해커가 도시를 해킹한다면?

오동작이나 사람의 실수가 발생한다면??



스마트시티 전략에 보안 이슈는 빠져 있음

◆ **스마트시티 통합 플랫폼 참조 모델 (국토교통부, 2017.10)**



정부의 스마트시티 추진 전략 및 세부 과제 ('18.1.29)

추진전략		세 부 과 제
도시 성장 단계별 차별화된 접근		① 신규개발 ☞ 국가 시범도시 + 지역거점
		② 도시운영 ☞ 기존도시 스마트화 및 확산
		③ 노후도심 ☞ 스마트시티형 도시재생
도시가치를 높이는 맞춤형 기술		① 도시에 접목 가능한 미래 신기술 육성
		② 체감도 높은 스마트 솔루션 적용 확산
주체별 역할	민간 창의성 활용	① 과감한 규제혁파를 통한 기업 혁신활동 촉진
		② 혁신 창업 생태계 조성
		③ 민간 비즈니스 모델 발굴 및 맞춤형 지원
		④ 공공 인프라 선도투자로 기업투자환경 조성
	시민 참여	① 시민참여를 위한 개방형 혁신시스템 도입
		② 공유 플랫폼을 활용한 리빙랩 구현
	정부 지원	① 법 · 제도적 기반 정비
		② 스마트 도시관리 및 추진체계
		③ 해외진출 확대 및 국제협력 강화

어디에도 스마트 시티에 대한 보안 이슈는 없음

※ 출처 : 대통령 직속 4차산업혁명추진위원회 (2018. 1. 29)

발표 내용 요약

- 스마트시티를 추진함에 있어, 보안은 반드시 처음부터 고려되어야 함
- 스마트시티 보안은 시스템의 안전(Security) 관점에서뿐만 아니라 시민의 안전(Safety) 관점에서 추진되어야 함
- 이를 위해서는 기존의 사이버 보안과 사물인터넷(CPS) 보안의 차이에 대해 이해해야 함
- 기존과 다른 보안 이슈를 반영하기 위한 기능 및 구조 설계가 필요
- 기술적인 이슈뿐만 아니라 운영적인 측면까지 고려해야 함

스마트시티 (Smart City)

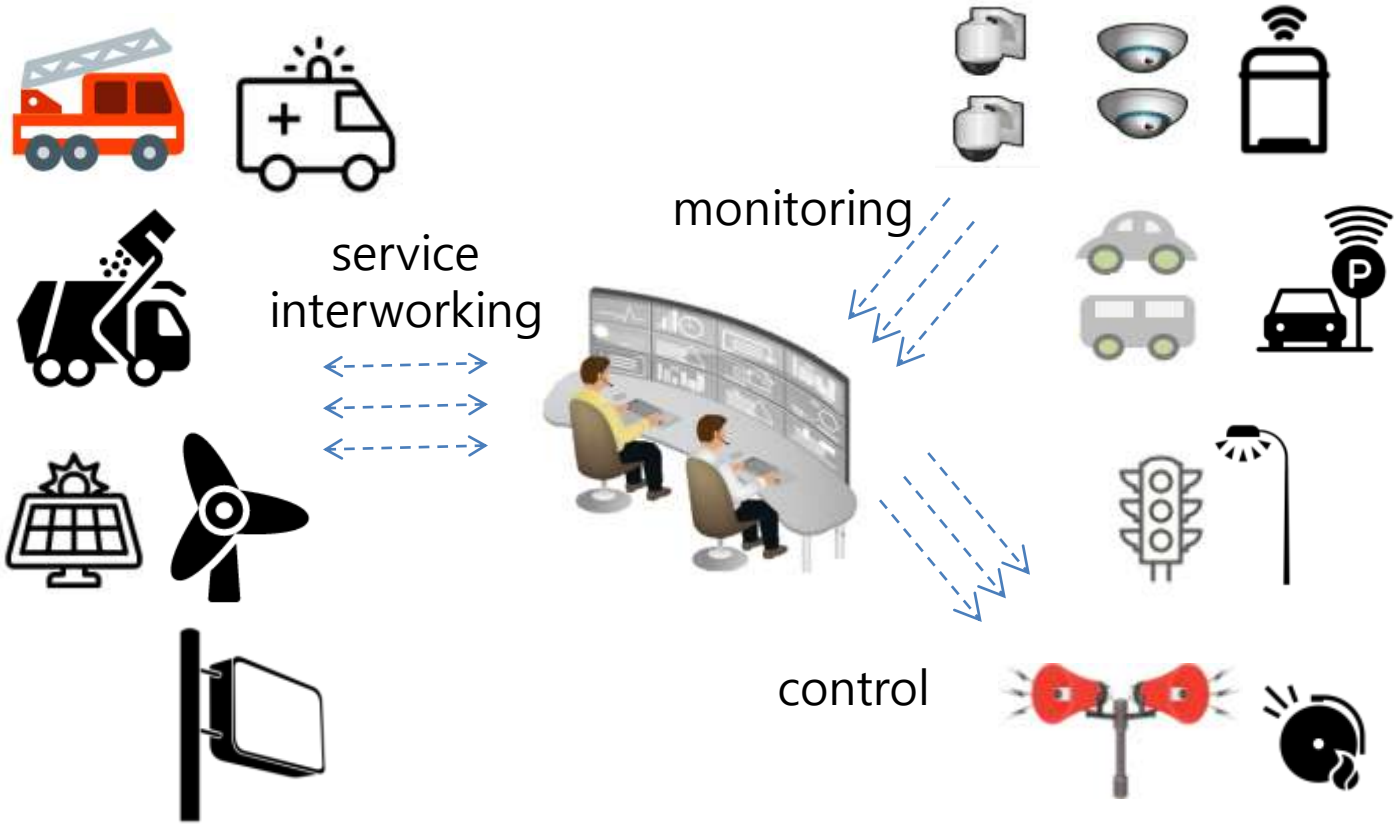
◆ ICT 기술을 이용하여 만들어진 시민들이 더 살기 좋은 도시

- 도시의 문제를 해결하고 효율성과 안정성을 높여 시민들의 삶의 질의 향상
- 단순히 막연한 편리함 뿐만 아니라 시간적, 경제적, 심리적 가치를 제공
- 사물인터넷, 빅데이터, 인공지능과 같은 디지털 기술을 기존 도시 기술과 결합

※ 출처 : Forbes

스마트시티 기술의 활용

- 도시 시설물 상태의 원격 모니터링 (monitoring)
- 도시 시설물의 원격 제어 (control) → 최적화 (optimization)
- 도시 서비스 연계 (service interworking) → 자율화 (autonomy)



스마트시티가 제대로 동작하지 않는다면??

- 도시 시설물 상태의 원격 모니터링 (monitoring)
- 도시 시설물의 원격 제어 (control) → 최적화 (optimization)
- 도시 서비스 연계 (service interworking) → 자율화 (autonomy)

의도적인 해킹
(분명한 목적)

시스템 오류/장애/실수
(시스템 설계, 거버넌스 이슈)

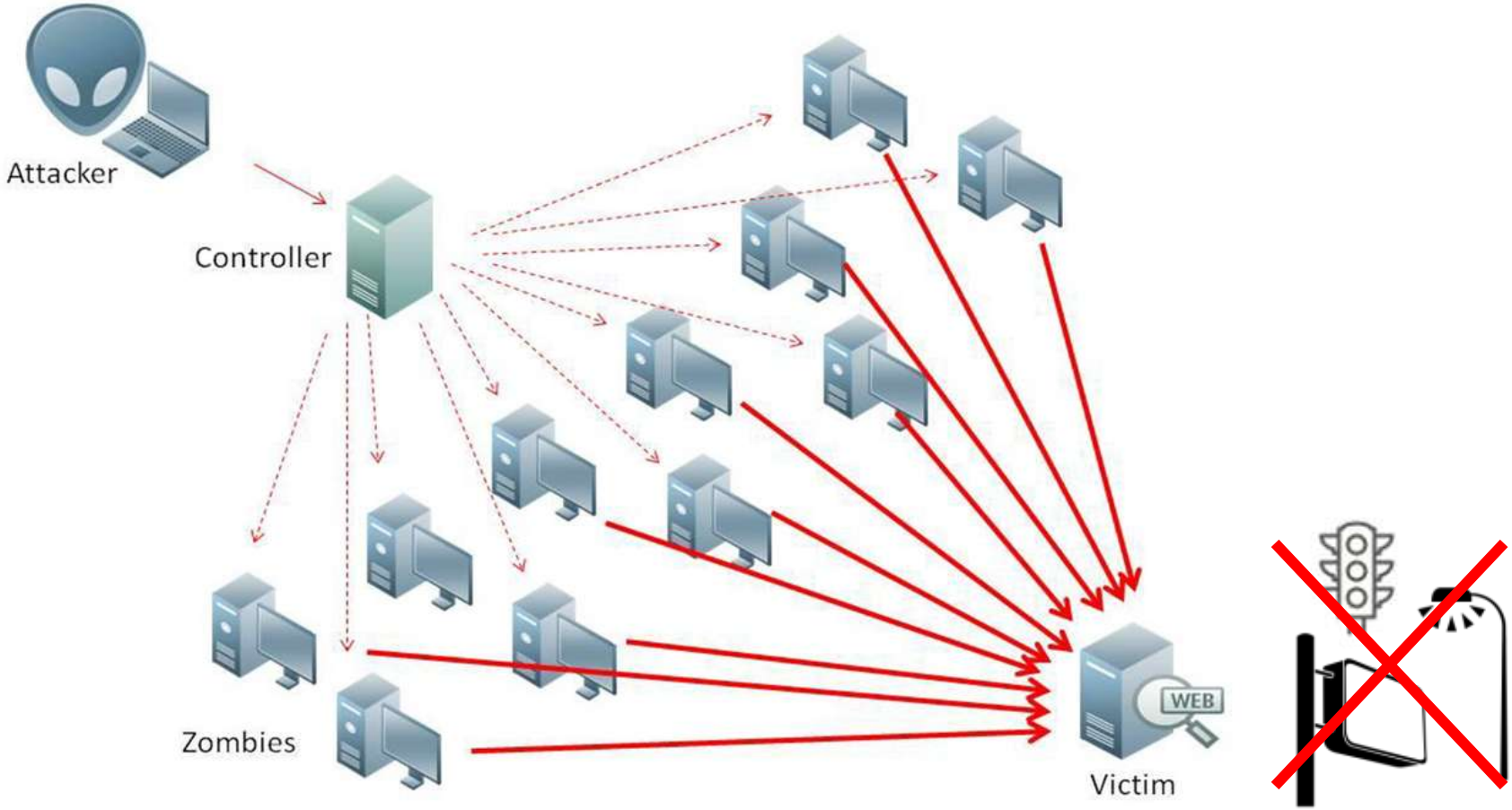
불편, 불결, 혼란, 혼동, 공포, 손실

스마트시티 보안 공격의 유형

- **전통적인 사이버 공격 (Cyber Attack)**
  - **악성코드 유포, 데이터 변조, DDoS, 피싱, 파밍, 스미싱 등**
- **사물인터넷 혹은 CPS 기반의 새로운 보안 이슈**
  - **커넥티드 디바이스 기반의 전통적인 사이버 공격**
    - 보안이 취약한 디바이스를 해킹해서 전통적인 사이버 공격 유발
  - **센서 재밍(Sensor Jamming or Sensor Spoofing)**
    - 시스템 외부에서 센서 신호를 조작
  - **무선 신호 간섭에 의한 오작동 유발**
    - 안정적인 통신 방해
  - **정전 및 방전에 의한 시스템 정지 유발**
  - **관리자의 실수 및 오작동**

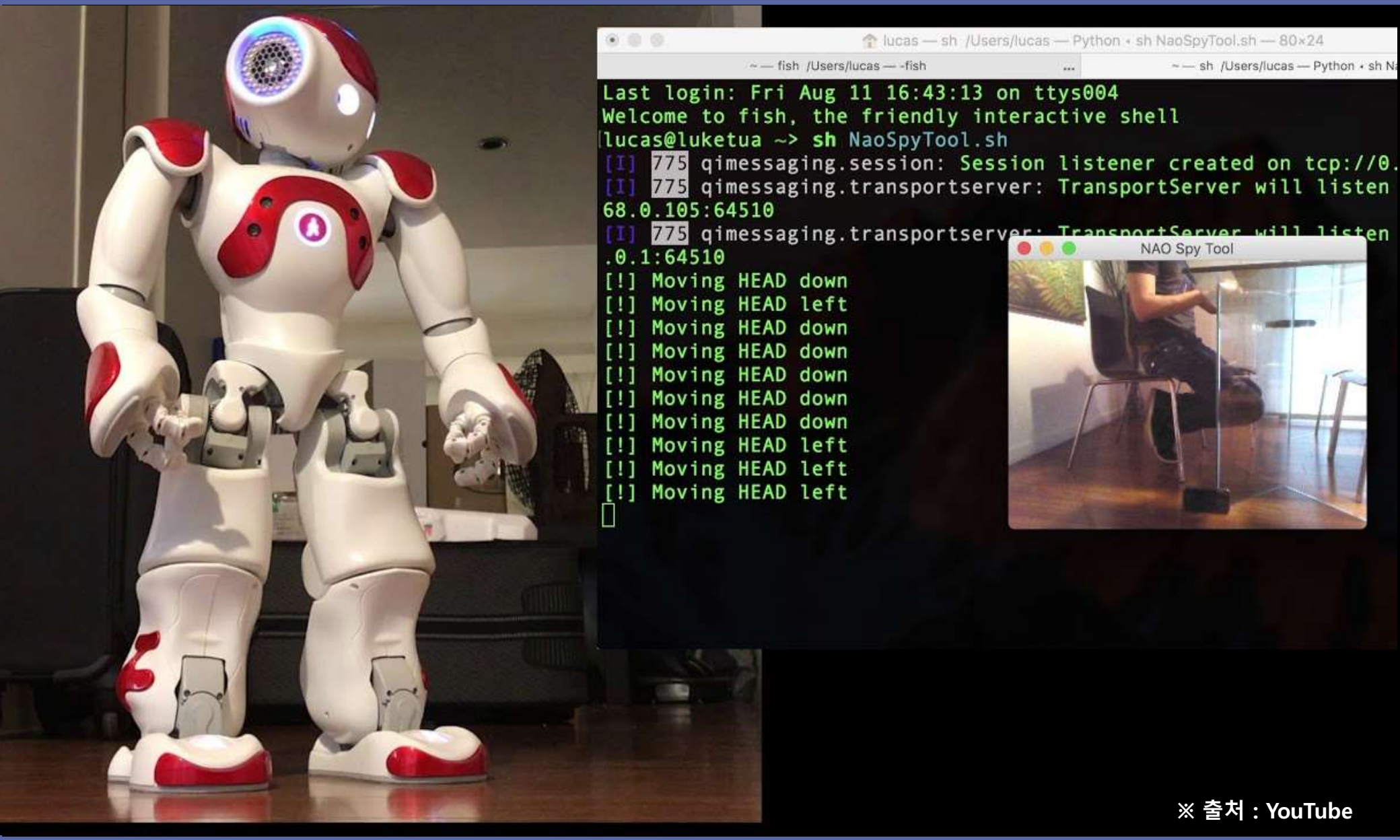
커넥티드 디바이스 기반의 전통적인 사이버 공격

- **보안 수준이 낮은 IoT 기기를 해킹하여 스마트 시티 시스템을 공격**
  - 동일한 유추하기 쉬운 패스워드 사용, 사용자 인증 기능 부재, 낮은 암호화 기술



※ 출처 : How-To Geek

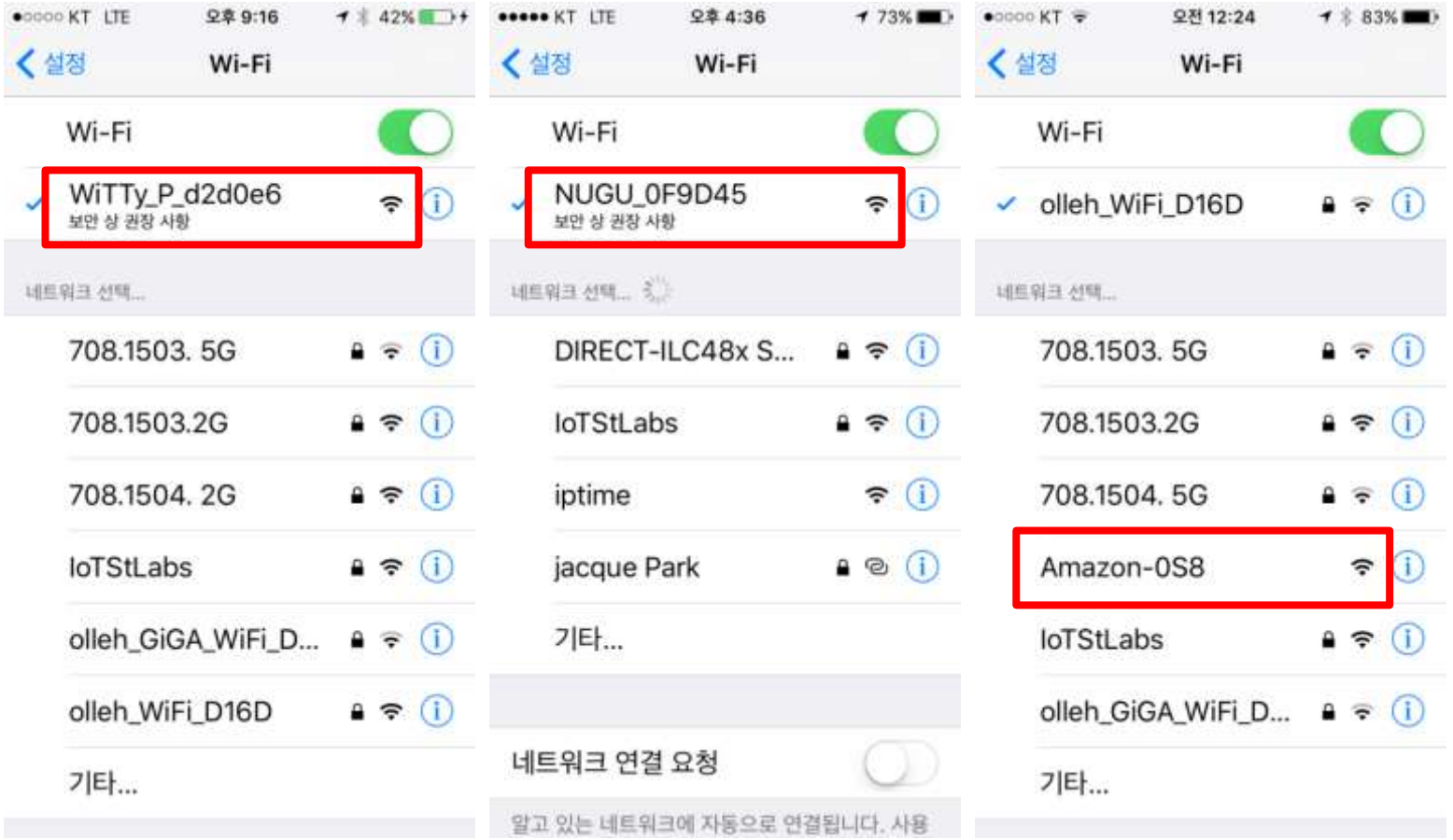
와이파이 통해 로봇 해킹



※ 출처 : YouTube

사물인터넷 보안 인증 의무화

- **대부분 스마트 디바이스의 설정 : 비밀번호조차 사용하지 않음**
  - **사용하더라도 0000, 1234, 123456 등과 같은 것을 바꾸지 않고 사용**



사물인터넷 보안 인증제

◆ 사물인터넷(IoT) 보안 인증제

- IoT 공통보안가이드('16.9), '홈가전 IoT 보안가이드('17.7) 등에서 제시했던 보안 요구사항을 바탕으로 개발
- 인증, 암호, 데이터, 플랫폼, 물리적 보호 등 5개 영역에서 32개/41개 항목 테스트
- 2017년 12월부터 개시 → 2개 등급으로 구분 : Lite & Standard
  - ➔ 제조사가 기기의 특성에 맞춰 등급을 정하고 인증을 거치면 됨
  - ➔ 정부기관 납품 건에 대해서는 발주사가 보안 등급 지정

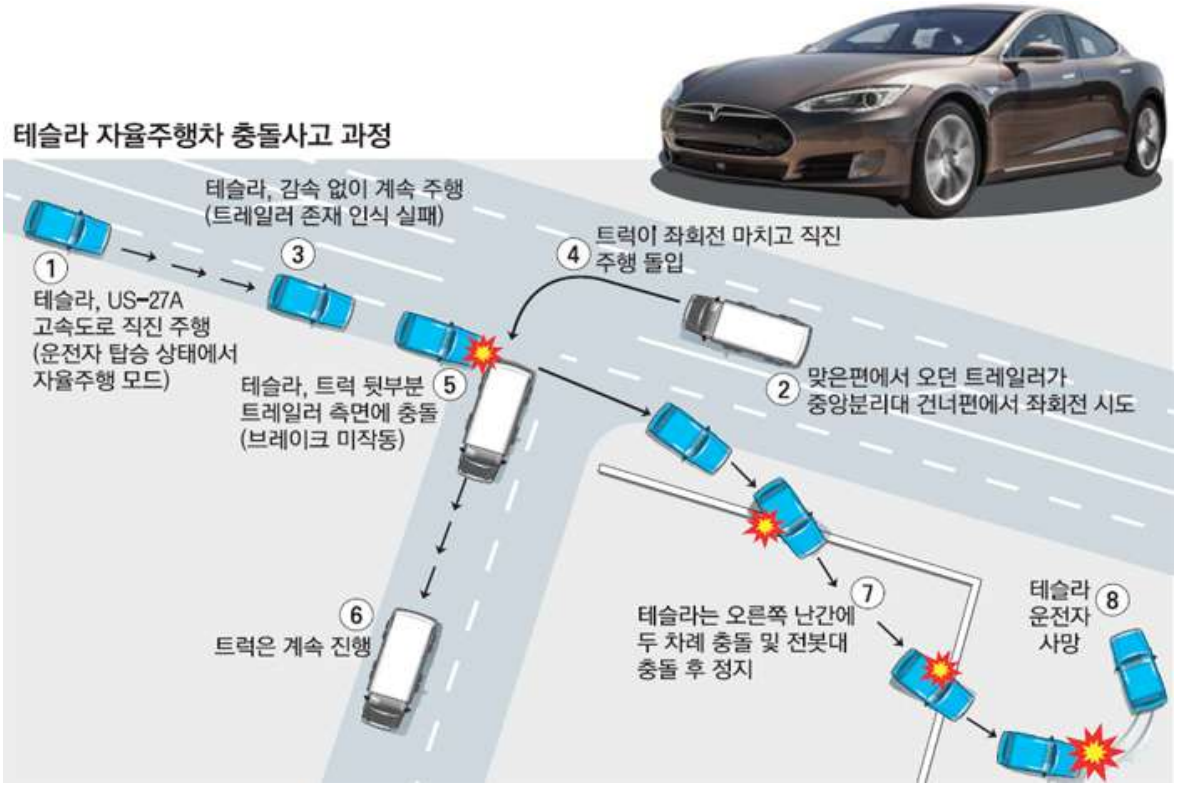
◆ 사물인터넷 기기의 해킹을 막기 위한 최소한의 조치

◆ 스마트시티 서비스 등 다양한 상황에 대한 대응방안이 될 수는 없음

Sensor Jamming에 의한 해킹 가능성

◆ Tesla 자율주행 자동차의 사고

- **빛과 거리를 측정하는 Lidar (Light Detection and Ranging) 센서의 오동작**
  - Lidar 센서가 밝은 하늘과 트럭의 흰색 면을 구분하지 못한 것으로 추정
- **의도적으로 강한 빛을 쏘거나 거리 센싱값에 영향을 주는 방식으로 사고 유발 가능**



※ Source : 매일경제, 자율주행 첫 사망사고 충격…센서만으론 한계 드러낸 무인차, 2016.7.1

Sensor Jamming을 활용한 보안 사고 유발

◆ 음성 인식 비상벨 시스템의 악용

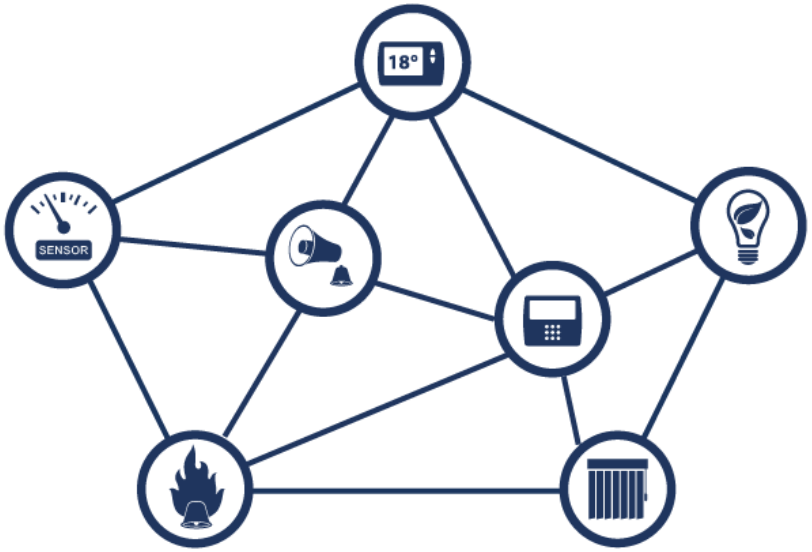
- 비명, 구조 요청 음성, 폭행·구타 소리, 유리 파열음 등의 이상 음원을 실시간으로 감지해 경찰청 112 종합상황실에 발생 위치 전송
- 가짜 소리로 경찰 유인 후, 타 지역에서 범행 → 聲東擊西 방식의 보안/안전 문제

※ Source : 아시아경제, “중견련 회원사 '한전산업개발', 음성인식 비상벨 솔루션 보급 확대 나선다,” 2017.7.6.

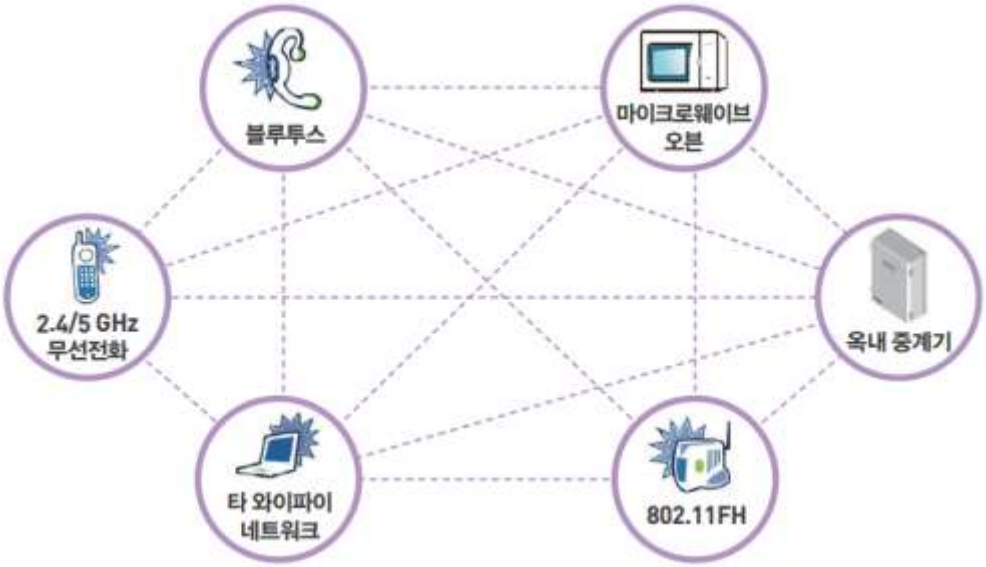
무선신호 간섭에 의한 오작동 유발

◆ ISM 대역을 이용하는 디바이스의 무선 출력을 높게 해서 송신

- IoT 활성화를 위해 900MHz 대역의 최대출력을 기존 10mW에서 200mW로 상향 (2016년 3월 15일 행정 예고)
- 900MHz 대역(917~923.5 MHz)은 LoRa나 SigFox 같은 LPWA 기술뿐만 아니라 RFID와 Z-Wave용으로도 이용 중



<900MHz ISM 대역>



<2.4GHz ISM 대역>

정전 및 방전에 의한 시스템 정지

◆ 스마트 디바이스는 상전 혹은 배터리로 동작

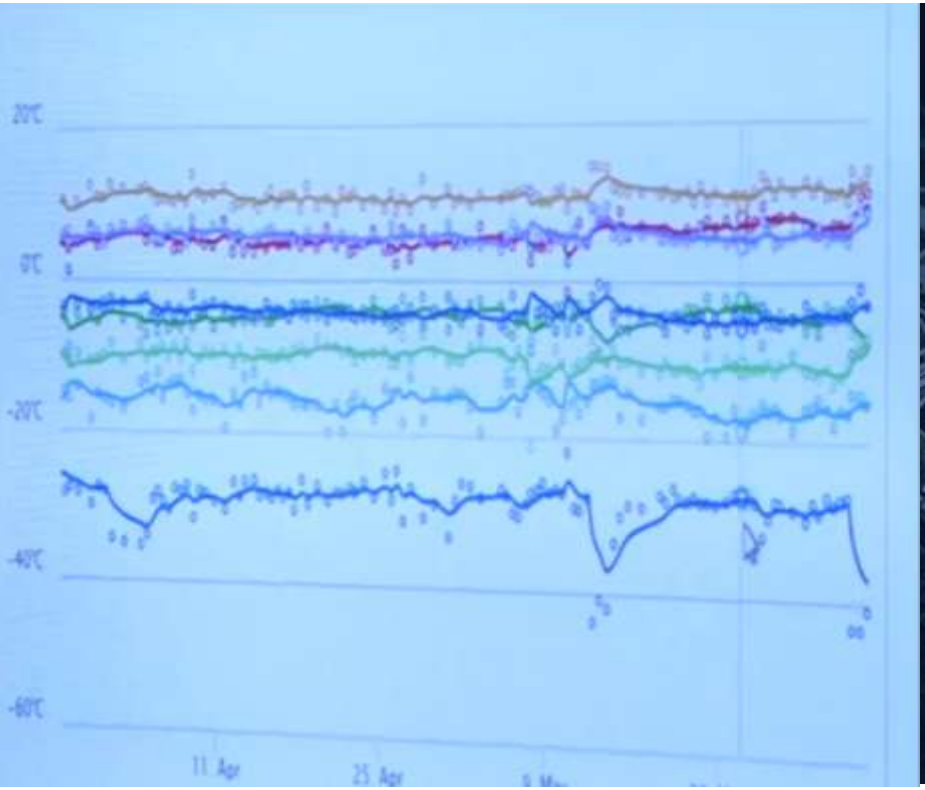
- 안정적인 전력 공급 방안 : 시스템 전원 이중화, 보조 전원 장치, 에너지 하베스팅 등
- 전원 공급이 끊겼을 때의 동작 및 시나리오에 대한 정의 필요
- 수작업에 의한 시스템 운용 방안 마련 필요

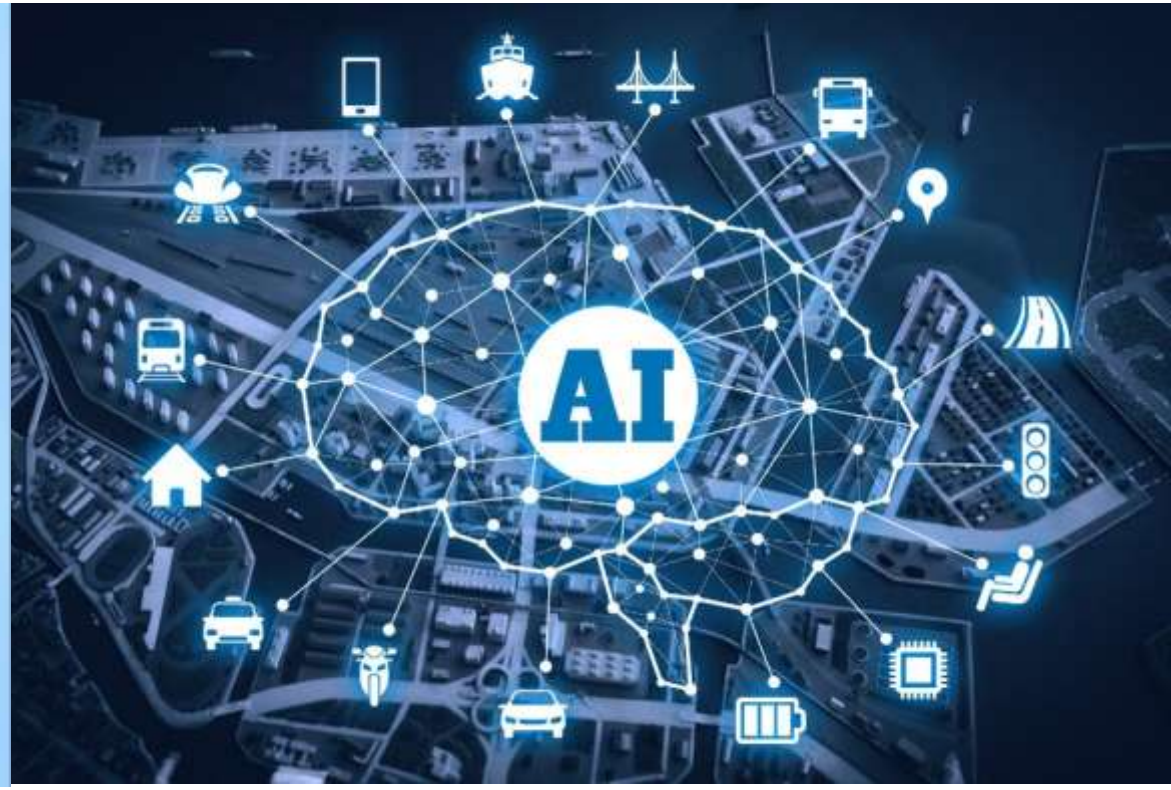
※ 출처 : CNET (CES 2018 Blackout)

※ 출처 : Nest Labs

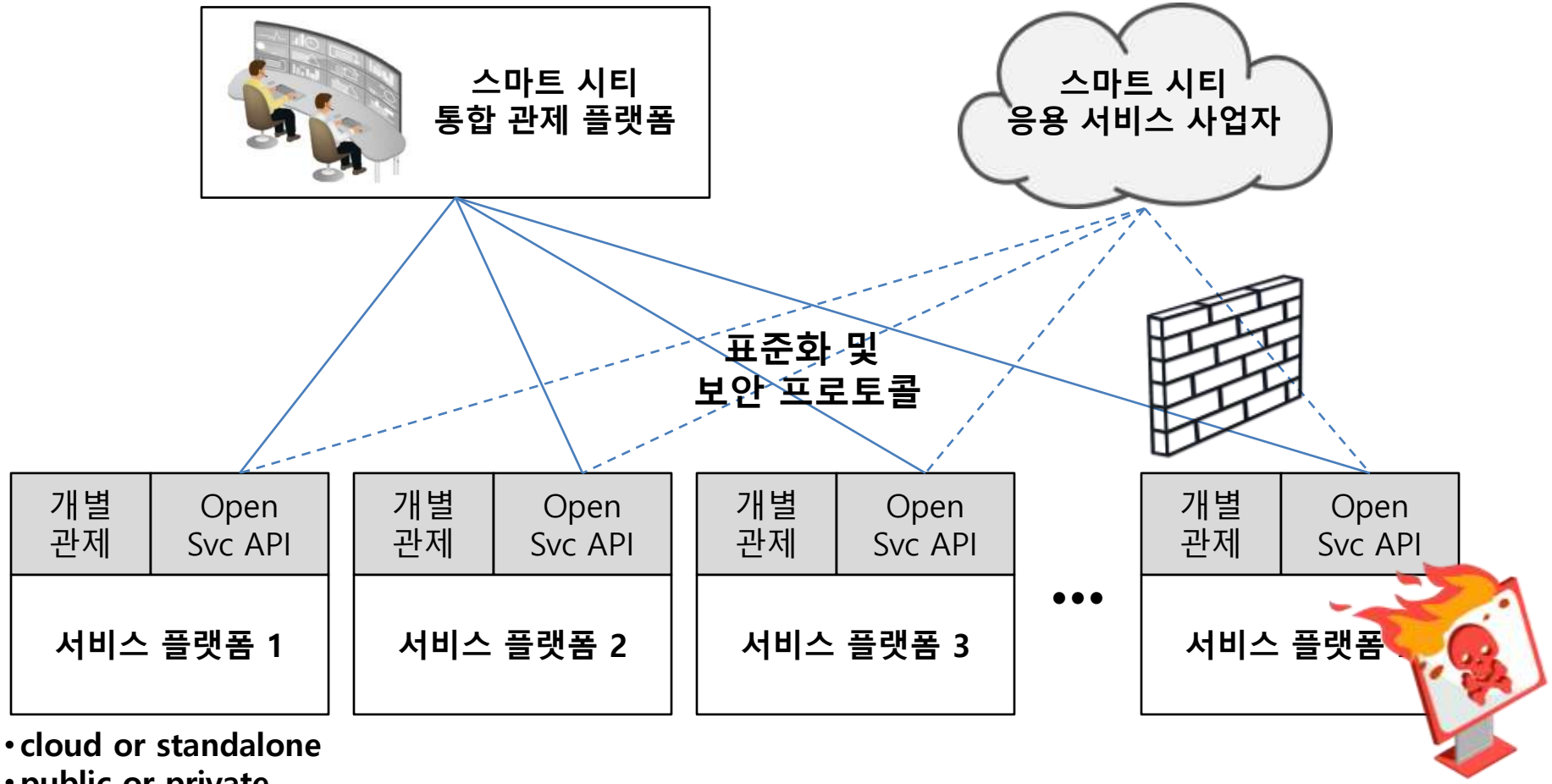
사람의 실수 및 오작동

- 실수에 의한 이벤트 개시를 막기 위한 프로세스의 이중화
- 빅데이터 분석 및 인공지능을 활용한 이상 징후 감지
  - 인공지능에 의한 해킹 시도 탐지 및 차단
  - 상황 데이터 분석 결과를 바탕으로 한 이벤트/서비스 개시





IoT 보안을 고려한 스마트시티 플랫폼 구조



- cloud or standalone
- public or private

IoT 보안을 위한 블록체인 기술의 활용

- 다양한 디바이스가 연결되는 중앙집중형 구조의 사물인터넷 시스템은 확장성이 떨어지고 보안성이 취약함
  ➔ 분권화된 통제를 가능하게 하는 블록체인 기술로 해결 가능
- IOTA, HDAC, Augmate, Orbis, IBM Watson IoT, Slock.it 등
- 사물인터넷과 블록체인 기술 결합의 한계
  - 저성능 소형 디바이스는 정식 노드로서의 참여가 불가능
  - 블록체인 관련 프로세싱을 위한 전력 소모 높음
  - 저속 통신, 단방향 통신을 이용하는 네트워크에 적용 불가
  - 블록체인 내에서 사물인터넷 기기의 인식, 식별자 검증, IoT 플랫폼 연동을 위한 외부 API 호출 기술 등이 개발되어야 함
  - 사물인터넷 디바이스가 생성하는 데이터의 양이 너무 큼
  - 아직 사물인터넷을 위한 블록체인으로 돈을 벌 수 있는 BM이 없어 확산이 불가능
- 블록체인은 사물인터넷 보안을 위한 보완재 수준에서 이해해야 함

Concluding Remarks

- IoT 기술을 적용한다고 U-City가 Smart City가 되지는 않습니다.
- 연결 되면서 달라지는 특성(CPS)에 대해 이해해야 합니다.
  → 다양한 서비스 시나리오 및 보안 공격 유형
  → 이에 대한 새로운 해결 방법
  → 사후적 대응이 아닌 사전적 대응
- CPS 환경 특성 및 보안 이슈를 반영한 서비스 플랫폼 구조의 도입
- 서비스 특성에 따라 블록체인 기술 활용

Thank You!!

For more information, please visit

- IoT Strategy Labs Homepage http://weshare.kr
- 사물인터넷 카페 : http://cafe.naver.com/iotioe
- 김학용 블로그 : http://blog.naver.com/honest72
- https://www.facebook.com/hakyong.kim.12139

or contact me

- phone : 010-4711-1434
- e-mail : iotstlabs@gmail.com