IoT 보안 적용 방안

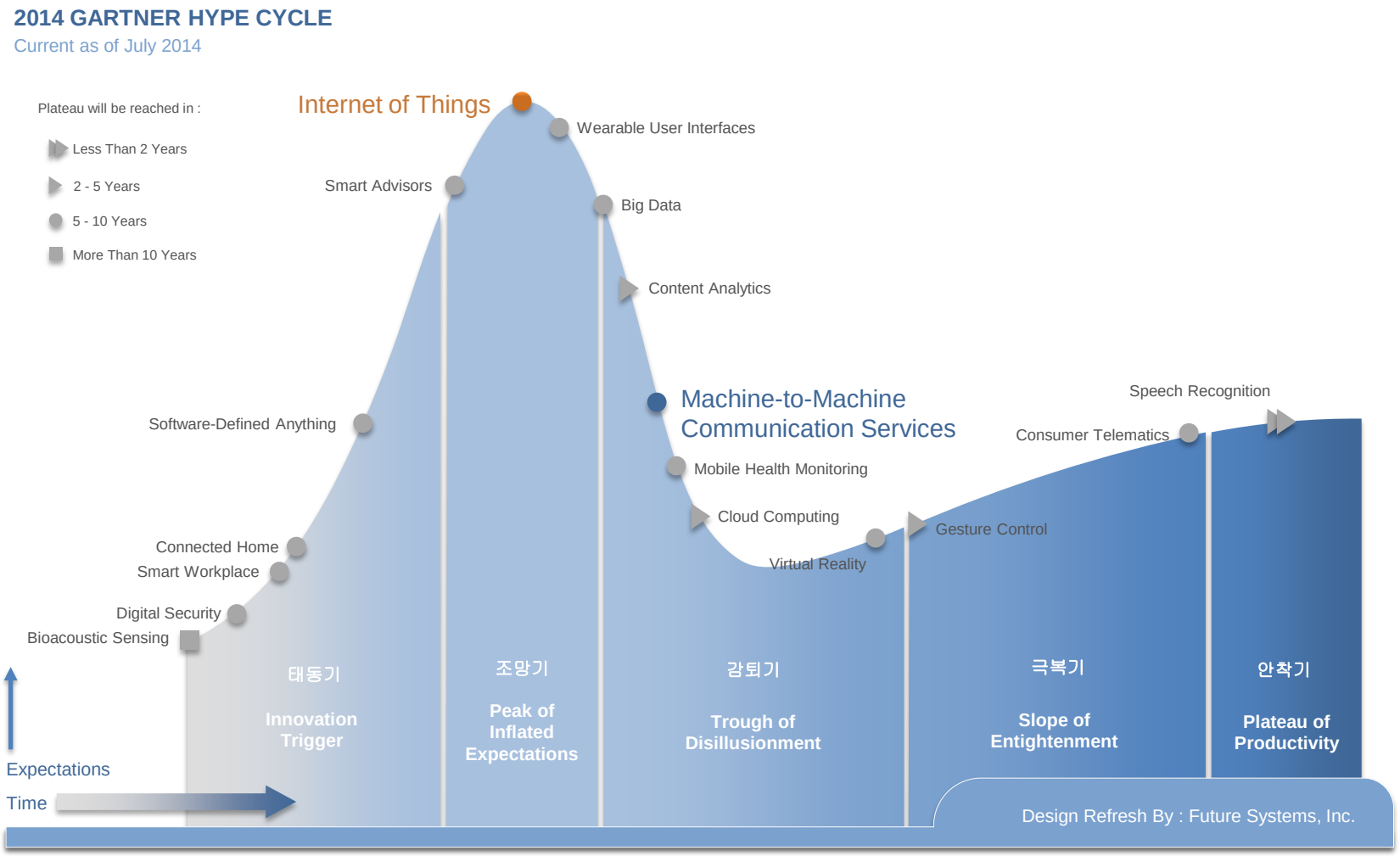
이현규
IoT 사업부 부사장

Future Systems

INDEX

2014년 Gartner Hype Cycle 상의 IoT 관련 기술

Future Systems



IoT 보안 이슈

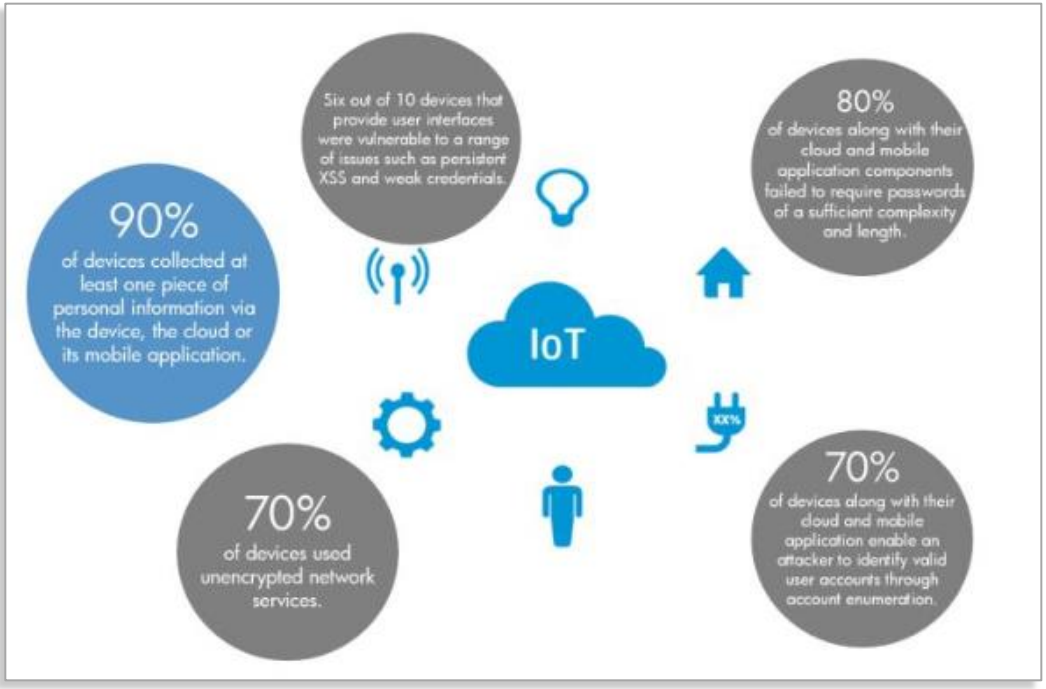
- OWASP(Open Web Application Security Project)
  - Core purpose
    - Be the thriving global community that drives visibility and evolution in the safety and security of the world's software
    - Mobile Top 10, Web Top 10, IoT Top 10 등..
  - Internet of Things Top 10
    - A list of the 10 Most Significant IoT Security Surface Areas
      - 제조사, 개발자, 사용자에게 IoT와 유관된 보안 이슈들 (최소의 권고) 제공
      - 사용자가 IoT를 구축/적용할 때 보안관점의 결정을 내릴 수 있는 방안 제공

I1. Insecure Web Interface
I2. Insufficient Authentication/Authorization
I3. Insecure Network Services
I4. Lack of Transport Encryption
I5. Privacy Concerns
I6. Insecure Cloud Interface
I7. Insecure Mobile Interface
I8. Insufficient Security Configurability
I9. Insecure Software/Firmware
I10. Poor Physical Security

IoT 위협요인 및 취약점 (1)

HP Fortify: Defense for the Internet of Things (IoT)

by HP Next Team on August 1, 2014



http://www8.hp.com/hpnext/posts/hp-fortify-defense-internet-things-iot

For the study, we leveraged HP Fortify on Demand to test 10 of the most commonly used IoT devices—along with their cloud and mobile application components. In the process we uncovered an average of **25 vulnerabilities per device**.

The results were clear: **70 percent of the most commonly used IoT devices contain vulnerabilities**, including password security, encryption and software protection.

IoT 위협요인 및 취약점 (2)

HP Fortify: Defense for the Internet of Things (IoT)

- **Privacy concerns**: 80 percent of the devices tested, along with their corresponding cloud and mobile application components, raised privacy concerns regarding the collection of consumer data such as name, email address, home address, date of birth, credit card credentials and health information.
- **Insufficient authorization**: 80 percent of IoT devices tested, including their cloud and mobile components, failed to require passwords of sufficient complexity and length. Most devices allowed password such as "1234".
- **Lack of transport encryption**: 70 percent of the devices failed to encrypt communications to the internet and local network, while half of the devices' mobile applications performed unencrypted communications to the cloud, internet or local network—leaving sensitive data vulnerable during its transmission across channels.
- **Insecure web interface**: 60 percent of devices evaluated raised security concerns with their user interfaces such as persistent XSS, poor session management, weak default credentials and credentials transmitted in clear text. 70 percent of devices with cloud and mobile components would enable a potential attacker to determine valid user accounts through account enumeration or the password reset feature.
- **Inadequate software protection**: 60 percent of devices did not use encryption when downloading software updates. Some downloads could even be intercepted, extracted and mounted as a file system in Linux where the software could be viewed or modified.

Same to bad history

http://www8.hp.com/hpnext/posts/hp-fortify-defense-internet-things-iot

IoT 위협요인 및 취약점 (3)

- Smart thermostats
- Smart locks
- Smart light bulbs
- Smart smoke detectors
- Smart energy management devices
- Smart hubs
- Security alarms
- Surveillance IP cameras
- Entertainment systems (smart TV, TV set-top boxes, etc.)
- Broadband routers
- Network attached storage (NAS) devices

Key findings

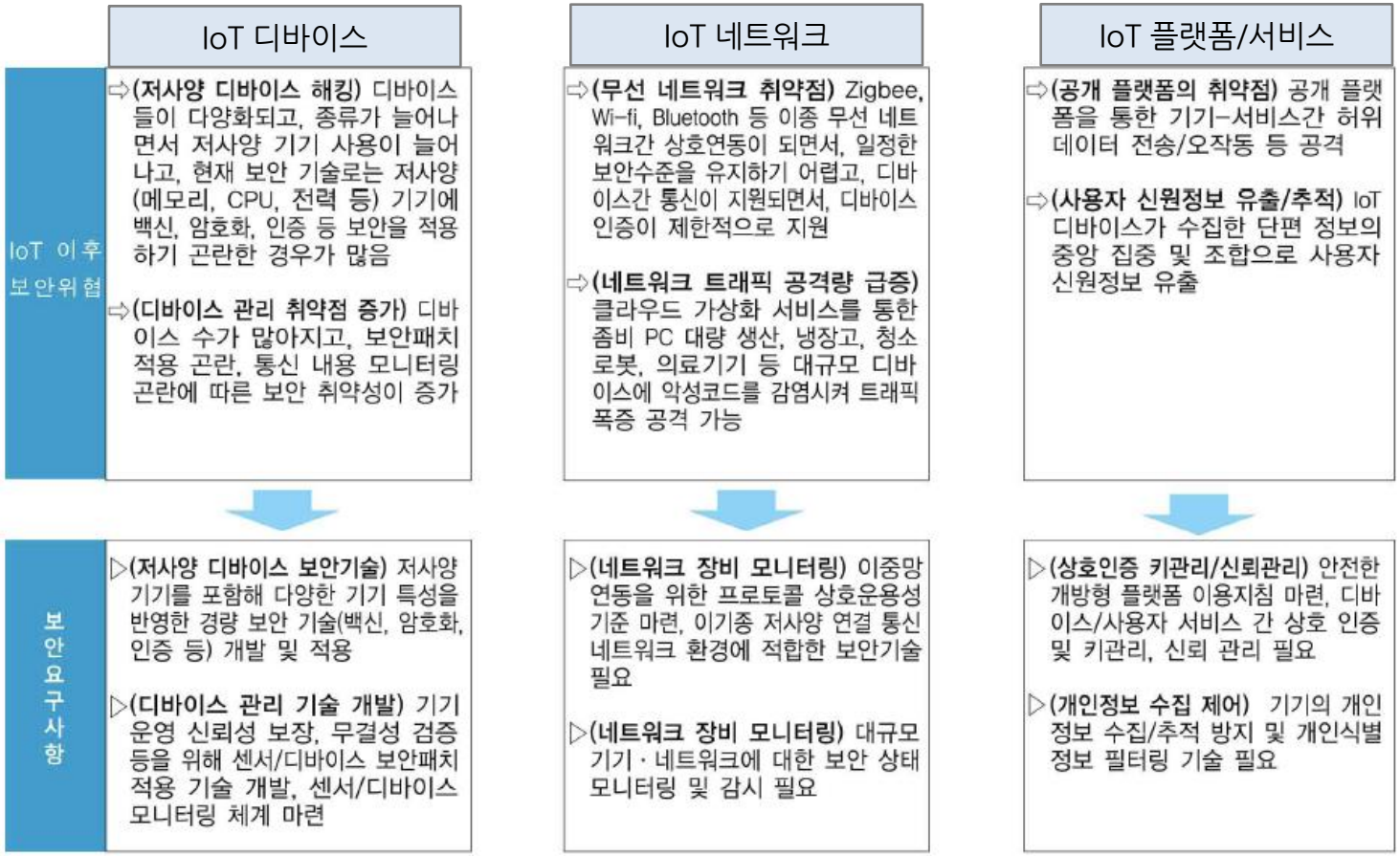
During our research, we found issues such as the following:.

- Around 19 percent of all tested mobile apps that are used to control IoT devices did not use Secure Socket Layer (SSL) connections to the cloud
- None of the analyzed devices provided mutual authentication between the client and the server
- Some devices offered no enforcement and often no possibility of strong passwords
- Some IoT cloud interfaces did not support two-factor authentication (2FA)
- Many IoT services did not have lock-out or delaying measures to protect users' accounts against brute-force attacks
- Some devices did not implement protections against account harvesting
- Many of the IoT cloud platforms included common web application vulnerabilities
- We found ten security issues in fifteen web portals used to control IoT devices without performing any deep tests. Six of them were serious issues, allowing unauthorized access to the backend systems.
- Most of the IoT services did not provide signed or encrypted firmware updates, if updates were provided at all

INDEX

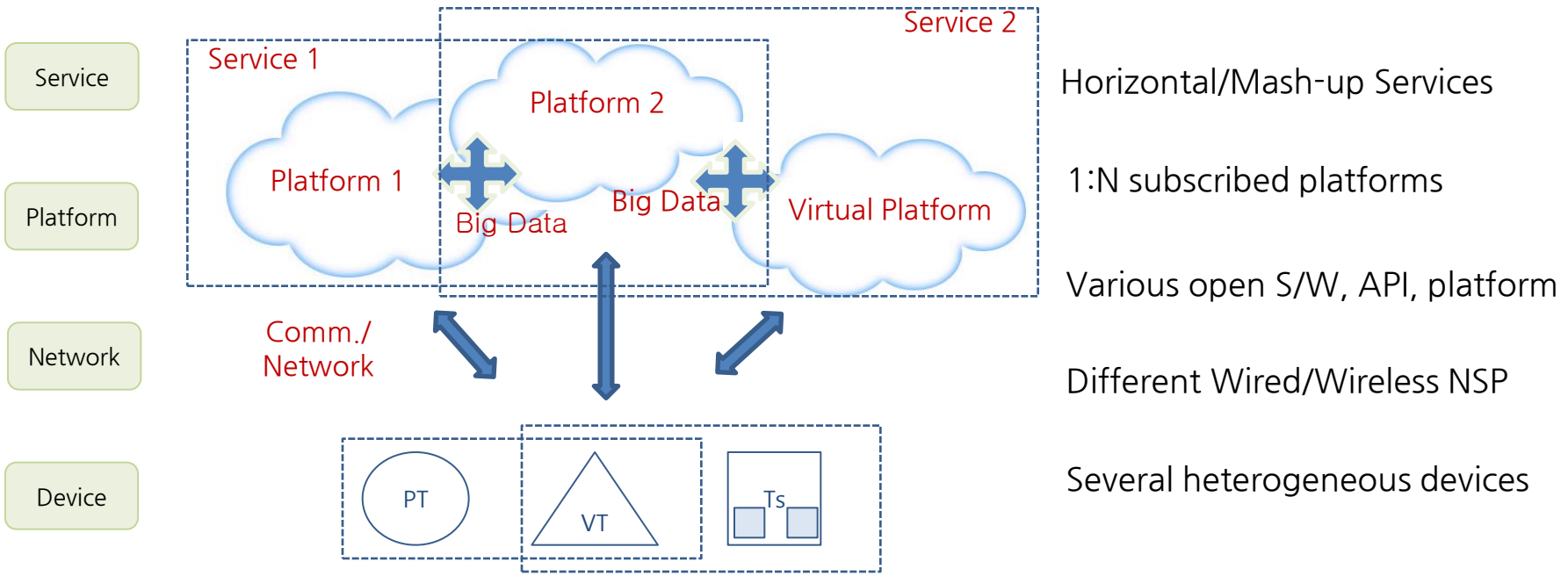
IoT 보안의 고려사항 - 환경적 요인

- 경량 디바이스, 다양한 네트워크, 공개 플랫폼



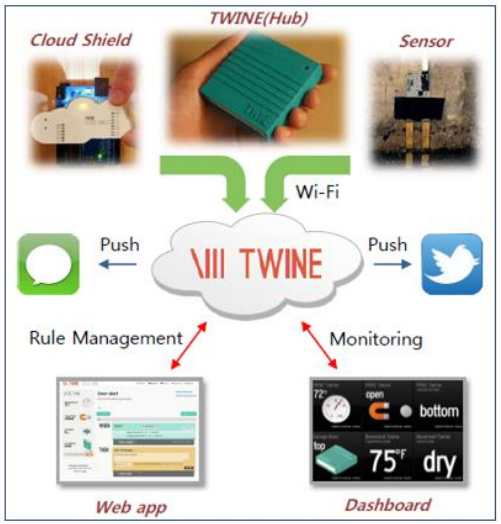
IoT 보안의 고려사항 - Security & Privacy 주체

- 보안기술 제공/관리의 책임과 권한 주체 및 법규의 범위(정의)가 어려움
  - 기존 Internet 기반 서비스나 M2M 응용의 vertical 개념처럼 접근하기는 어려움



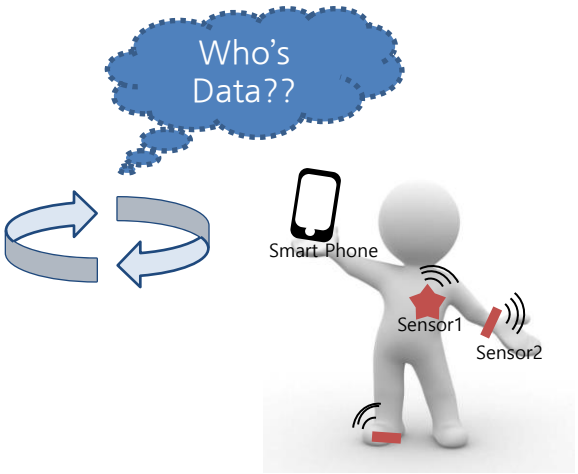
IoT 보안의 고려사항 - IoT 구성요소의 지능화

- 사용자에게 주어졌던 정보 통제권 및 의사결정권 약화
  - 지능화된 IoT의 단말, 플랫폼의 지능화 (사용자의 개입이 최소화)
  - 지능화된 상호 협력 서비스를 통해 사용자의 정보가 다양한 방식으로 가공, 분리, 정보 교환 및 처리 (자율/지능 처리)



TWINE(www.supermechanical.com)

ThingSpeak(www.thingspeak.com)/출처: 엔텔스보고서

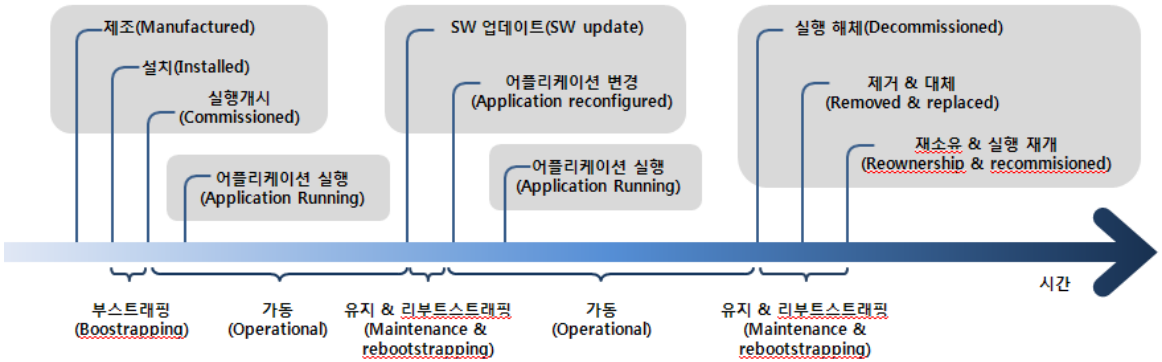


IoT 보안의 고려사항 - 영역별 요소

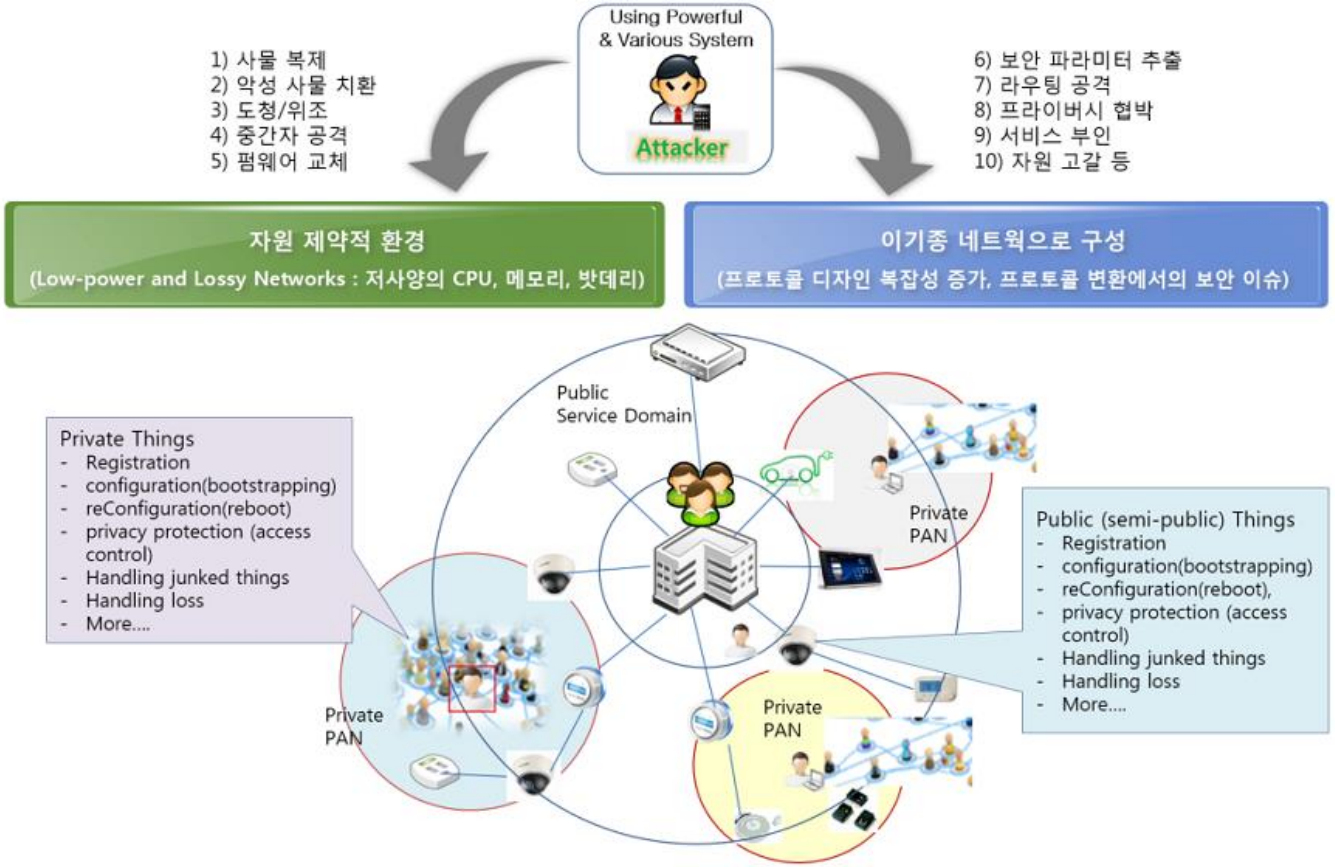
- 임베디드 OS, 포터블 장치 보안 기술
  - TPM, …
- 경량화 디바이스를 위한 경량화 보안 기술 (알고리즘, 프로토콜 관점)
  - 국내외 다양한 경량화 보안 알고리즘 (Present, Clefia, mCryton, Lea…)
- Thing 확인 및 접근 제어 기술
  - 식별, 등록, 인증, 인가, 접근 제어 등 (IETF ACE WG, OneM2M, …)
- Thing 들 사이의 암호화된 전송기술
  - MQTT/TLS, CoAP/DTLS, LWM2M (DTLS, TLS), …
- 보안 플랫폼 기술
  - 표준 기술, 자체 기술, SecaaS, SDSec, etc.
- 프라이버시 제공 기술
  - 정책, 법규(어디까지가 private info인가?), etc…

IoT 보안의 고려사항 - 기타

- Internet 자체의 공격/위협요소 상속
- IoT 환경/도메인/서비스의 특성 공격
- IoT 장치를 이용한 공격
- 어쩔 수 없는 (Internet이기에.. 혹은 환경의 특수성으로..) 취약점
  - 최소한의 detection까지는 해봐야지..
- 신규 기술 개발 Vs. 기존 기술 사용
- 전주기 보안도 고려해야
  - S/W lifecycle 고민
  - Thing lifecycle 고민



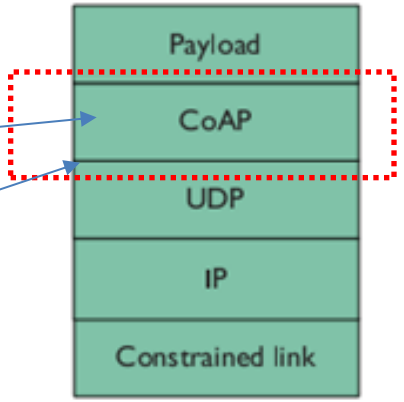
IoT 보안의 어려움


Using Powerful
& Various System
Attacker
1) 사물 복제
2) 악성 사물 치환
3) 도청/위조
4) 중간자 공격
5) 펌웨어 교체
6) 보안 파라미터 추출
7) 라우팅 공격
8) 프라이버시 협박
9) 서비스 부인
10) 자원 고갈 등
자원 제약적 환경
(Low-power and Lossy Networks : 저사양의 CPU, 메모리, 밧데리)
이기종 네트워크로 구성
(프로토콜 디자인 복잡성 증가, 프로토콜 변환에서의 보안 이슈)
Public
Service Domain
Private Things
- Registration
- configuration(bootstrapping)
- reConfiguration(reboot)
- privacy protection (access control)
- Handling junked things
- Handling loss
- More....
Private
PAN
Private
PAN
Private
PAN
Public (semi-public) Things
- Registration
- configuration(bootstrapping)
- reConfiguration(reboot),
- privacy protection (access control)
- Handling junked things
- Handling loss
- More....

INDEX

IoT를 위한 새로운 표준 (1)

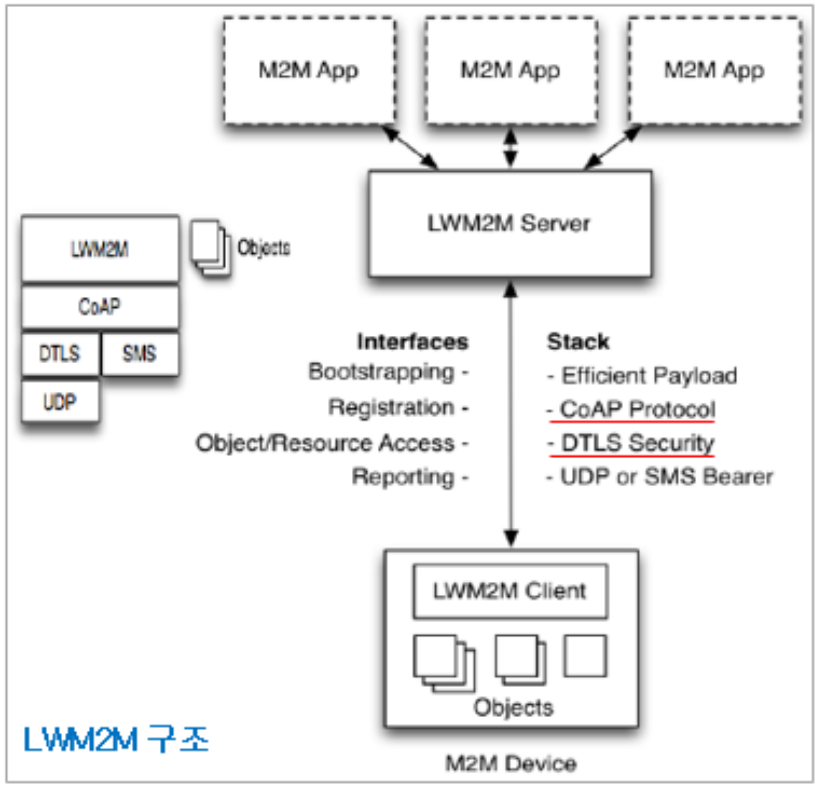
- Common protocol 필요
  - Internet of Things
    - Internet protocol 쓰자!!
      - L2, L3: various specs for supporting M2M/USN
        - » IETF WG: 6lowpan, 6lo, 6tish, lwig, roll
  - IP protocol 기반의 응용은?
    - L4, L5 ??
      - IETF CoRE WG - CoAP
        - » L4는 UDP, L5는 CoAP
      - IETF DICE WG - CoAP/UDP/DTLS
        - » Similar way to HTTP/TCP/TLS
      - IETF ACE WG - Access control for CONST. ENV.



IoT를 위한 새로운 표준 (2)

CoAP를 전송 프로토콜로 고려하고 있는 표준 기관들

- OMA LWM2M
  - CoAP/DTLS bound to UDP ro SMS
- ETSI M2M TC
  - HTTP, CoAP binding 포함
- IPSO Aliance
  - CoAP Plugtest 진행
- ZigBee Alliance
  - ZigBee IP Smart Energy 2.0 Spec에 포함
- OneM2M
  - ETSI, TTA, ATIS, 등 7개 표준개발기관 주도, 12년 1월 설립

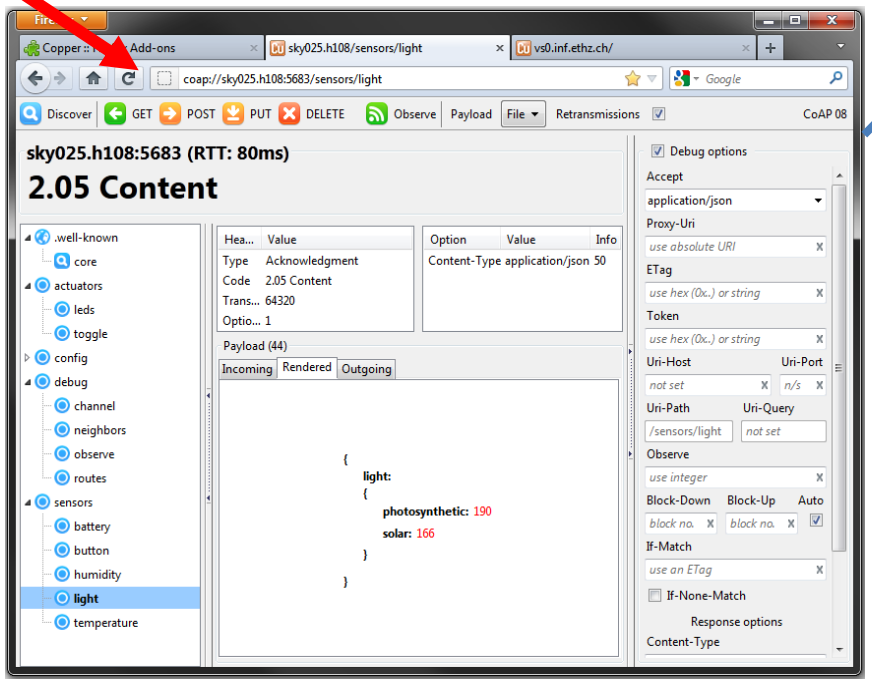


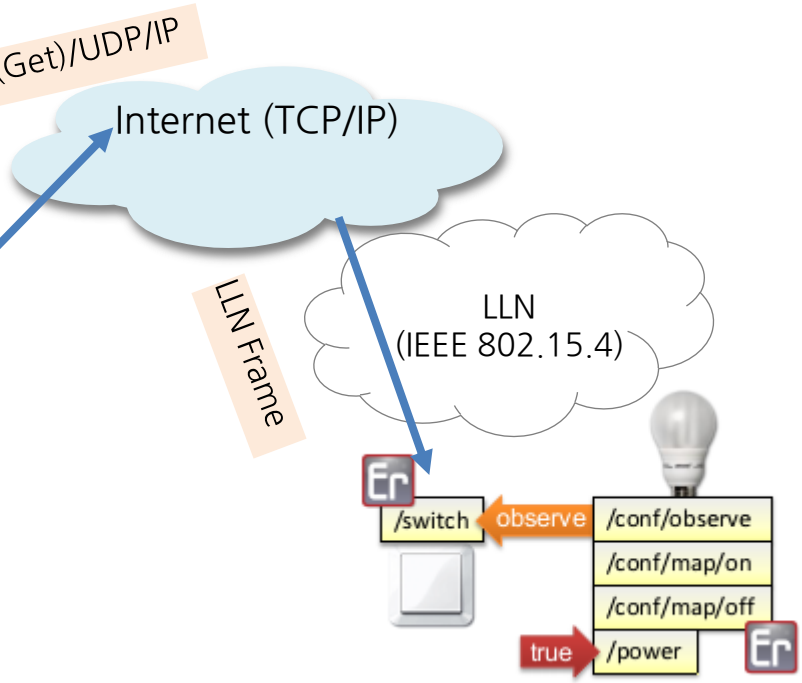
LWM2M 구조

IoT를 위한 새로운 표준 (3)

- CoAP enabled network model

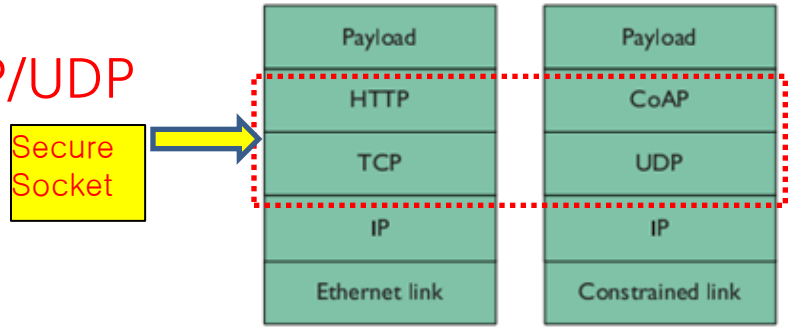
coap://우리집.com/2층/작은방/전등





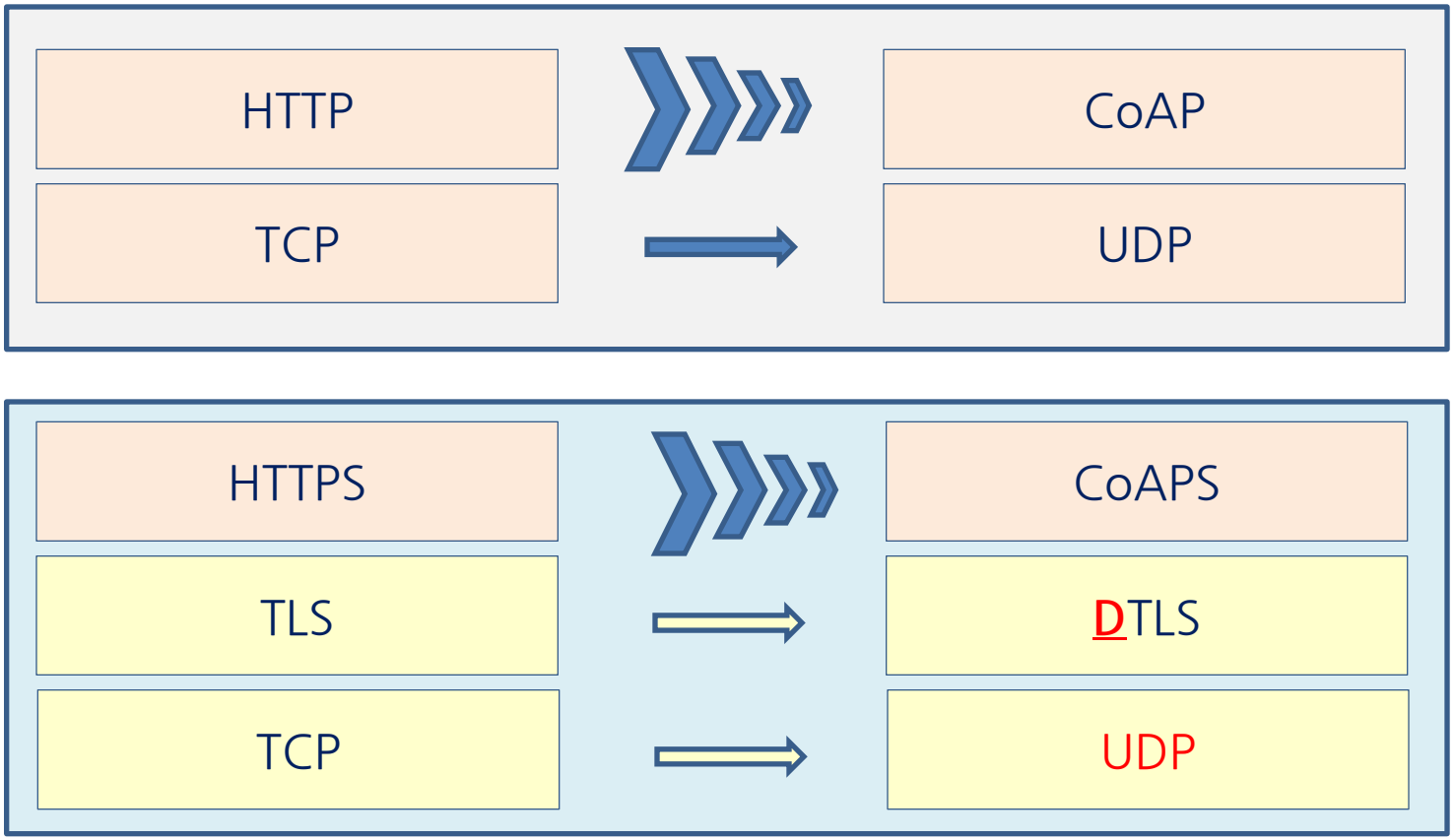
IoT를 위한 새로운 표준 (4)

- IETF protocols for IoT?
  - Layer 4, 5: IETF CoRE WG - CoAP/UDP
  - Security for CoAP: DICE WG
    - CoAP/DTLS/UDP
      - Similar way to HTTP/TLS(SSL)/TCP



IoT를 위한 새로운 표준 (5)

- Secure CoAP(CoAPS)

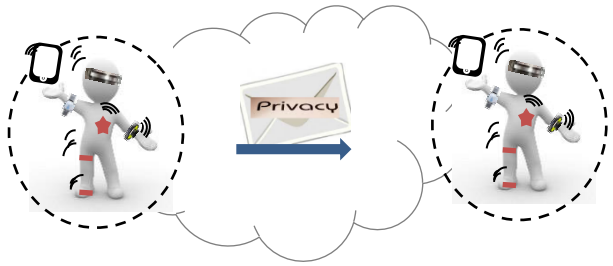


INDEX

CoAP over DTLS

Home, Building 등
사전 등록된 single domain은 O.K

Trust 관계 (PSK 설정이 가능한)



AuthN,
Key Agree.

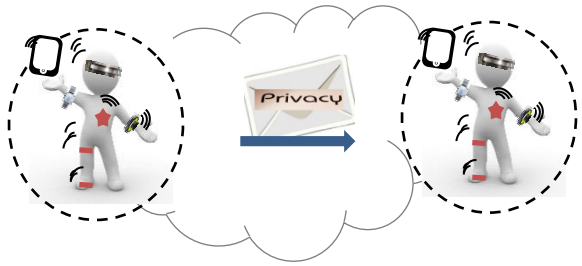
나야! 키 있지?

당근!

C, I, A 제공 통신 채널
Using PSK(사전 설정키 기반)

Emergency Healthcare
Cross domain의 타 장소의 장치 등..

Trust 설정이 없는 장치 간 통신



인증,
키설정,
키동의,
…

나야!

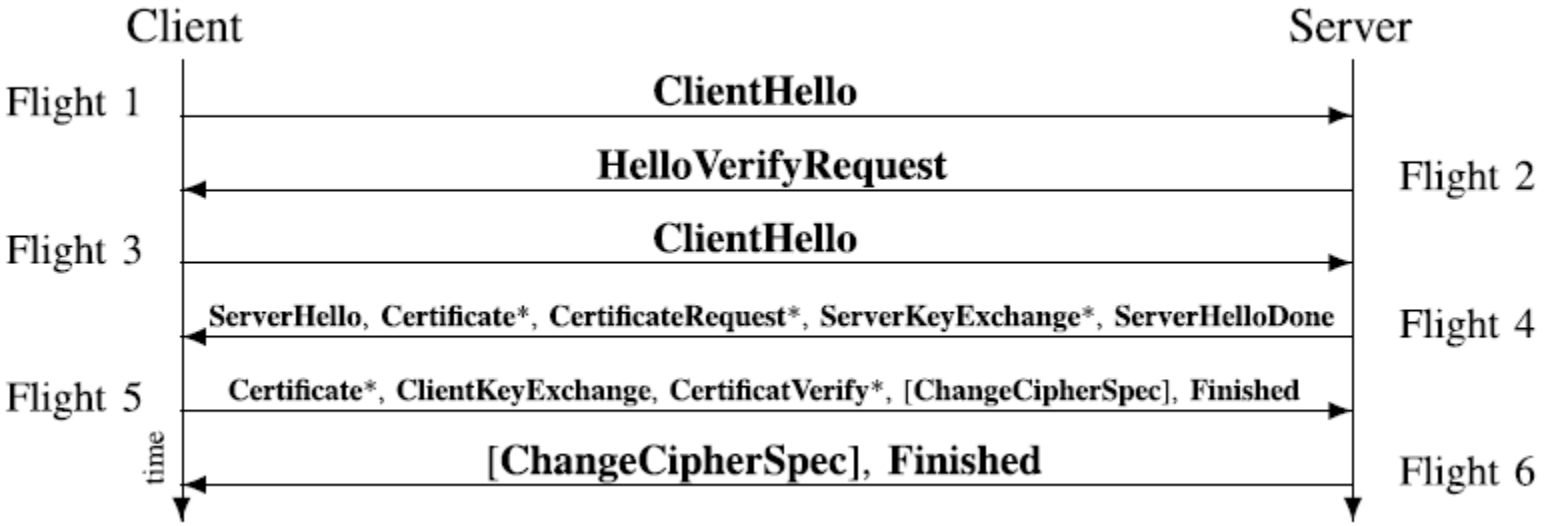
누구??

?

이런 경우 일반적인 방법은?
Public Key로 Key 교환하고,
그 session key를 사용
PKI?

DTLS 적용의 이슈 (1)

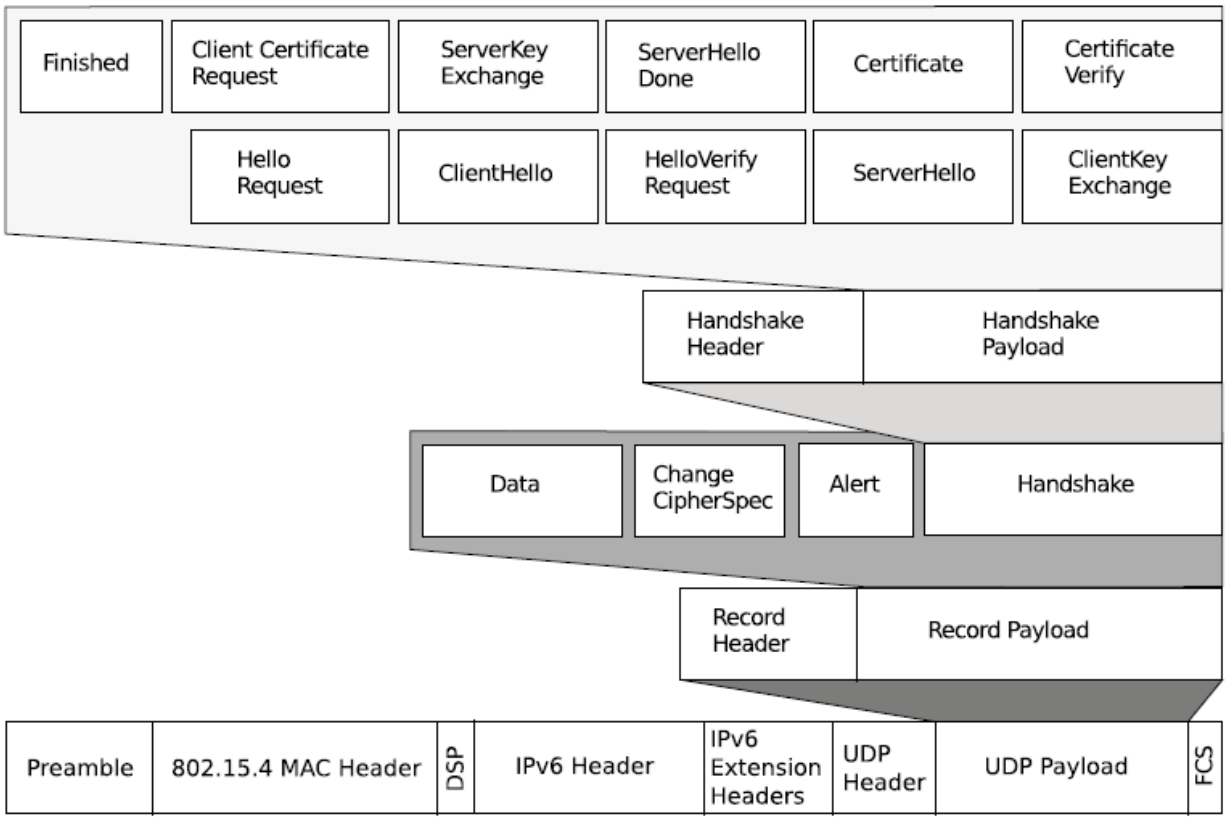
- 사물간 DTLS ==> 동작 및 환경 이슈
  - Limitation in LLN & Const. Nodes
    - **Loss**를 동반한 hand shaking
    - Public key primitive for key sharing
      - 특히 **public key** 기반 방식은 많은 연산이 요구됨



Source: Lightweight Secure CoAP for the Internet of Things, S. Raza, et. al., IEEE Sensors Journal, Oct. 2013.

DTLS 적용의 이슈 (2)

- DTLS ==> 수많은 overhead



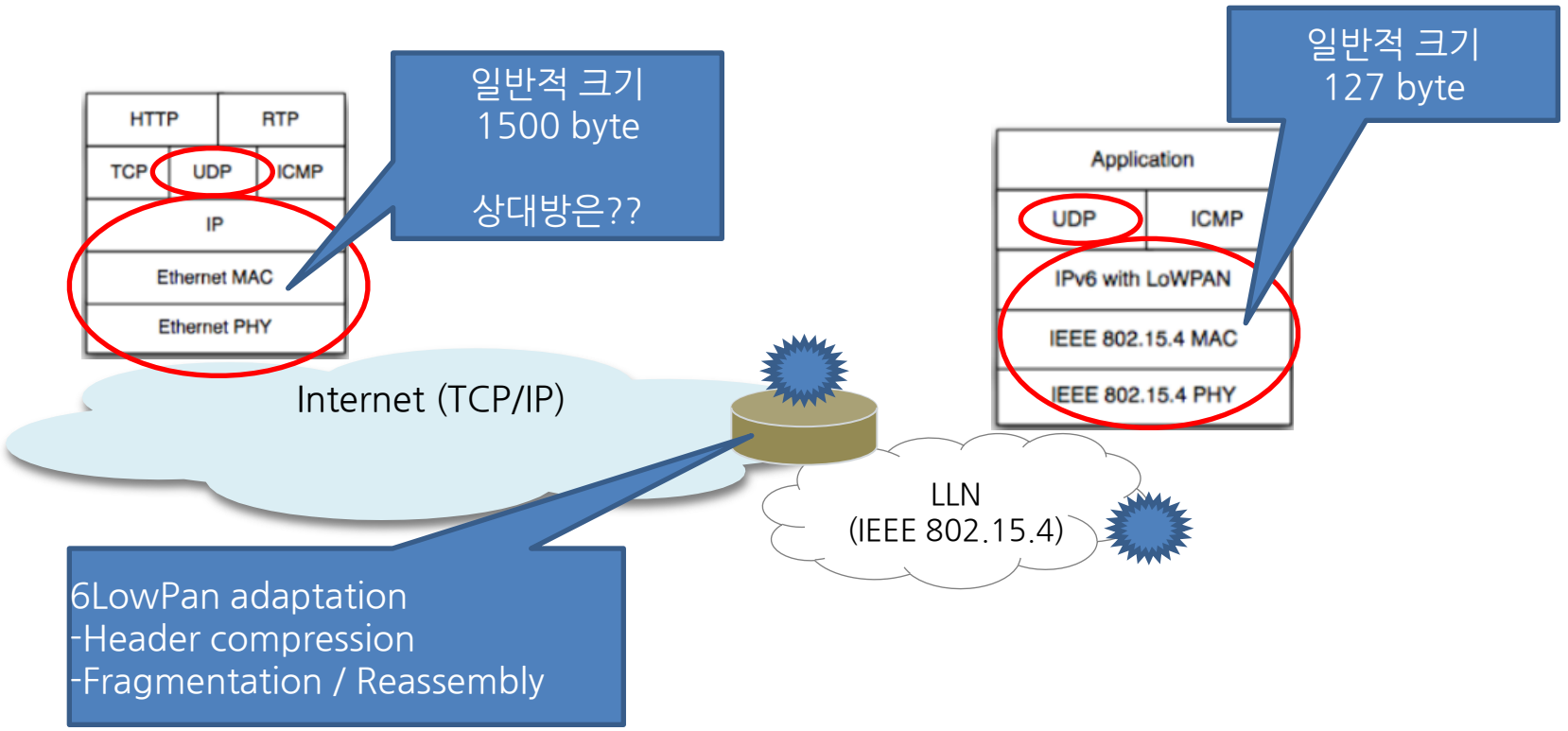
- Code sizie
- Fragmentation
- Computing

고려사항:
MTU size of
the IEEE 802.15.4
is **127 bytes**.

Source: Lightweight Secure CoAP for the Internet of Things, S. Raza, et. al., IEEE Sensors Journal, Oct. 2013.

DTLS 적용의 이슈 (3)

- Packet Fragmentation
  - MTU의 차이 등에 기인



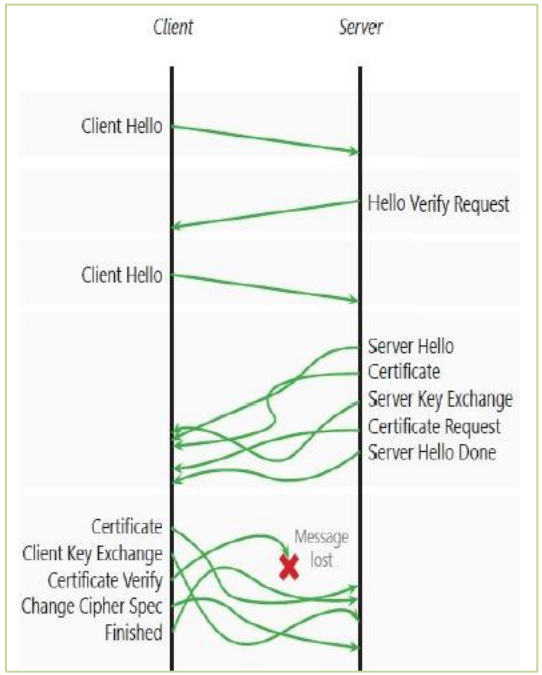
DTLS 적용의 이슈 (4)

- Potential problems in applying DTLS in CoAP domain
  - Handshake Message Fragmentation
    - DTLS records can be large in size for a single 6LoWPAN payload
      - a physical layer MTU of only 127 bytes (60~80bytes of payload)

UDP data size limit (bytes)	Number of datagrams transferred	Total number of bytes transferred	Proportion of header data
50	27	1,182	55 %
55	21	1,037	49 %
60	20	1,081	51 %
65	18	1,003	47 %
70	15	912	42 %
75	14	875	39 %
80	13	874	39 %
85	12	849	37 %
90	12	849	37 %
1,152	6	802	34 %

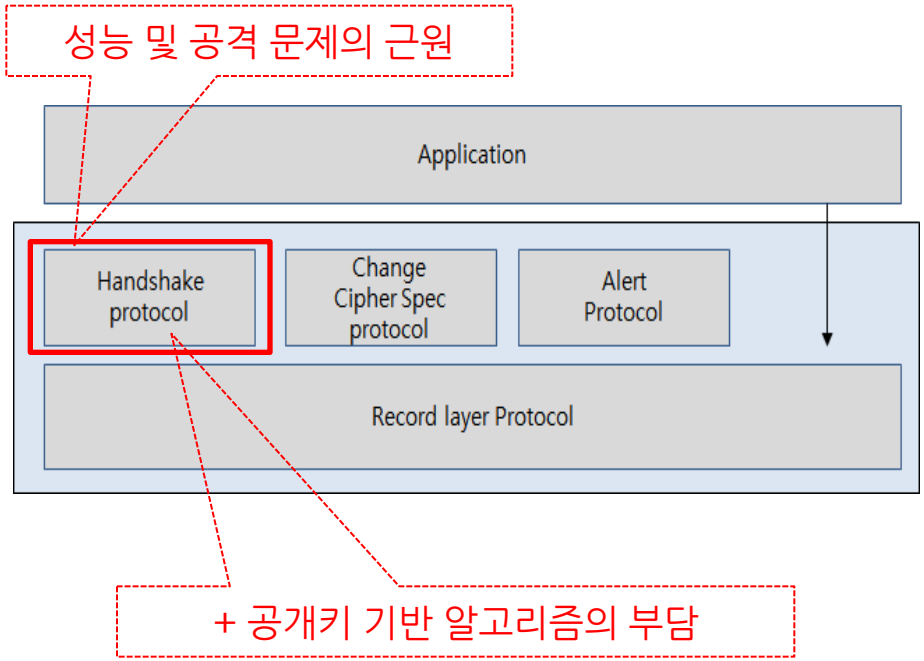
Table 1: Number of datagrams and bytes transferred using different limits for DTLS fragmentation in an example DTLS handshake (TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 with raw public key certificate)

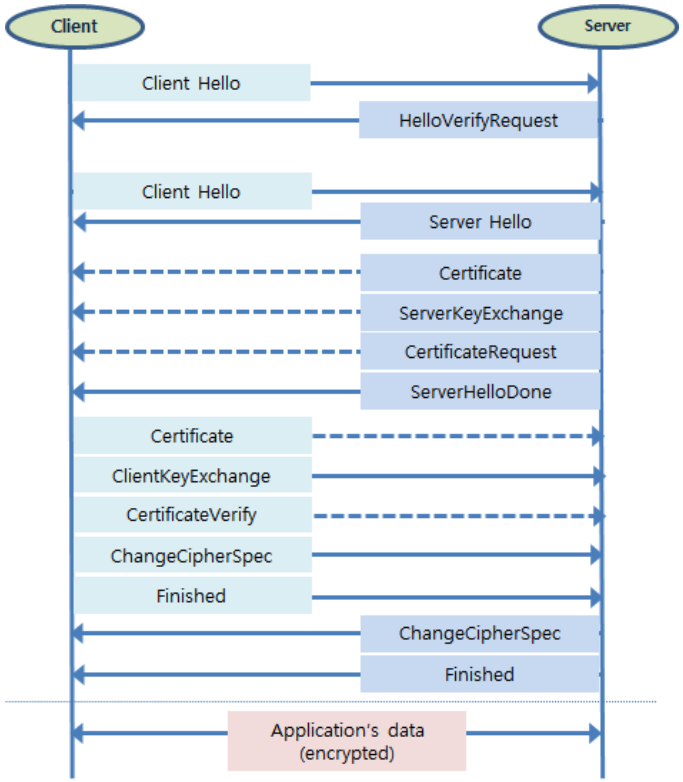
IETF draft, Constrained DTLS



DTLS 적용 방안 (1)

- TLS/DTLS 사용 문제
  - CoAP/DTLS & MQTT/TLS 적용
    - ✦ Delegation but secure semi-e2e

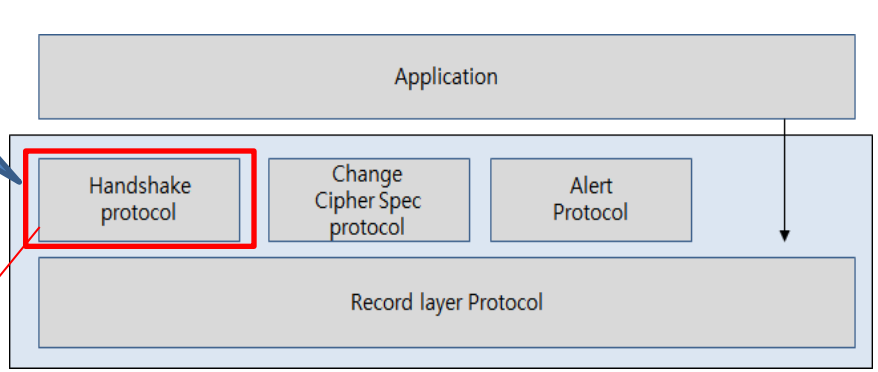


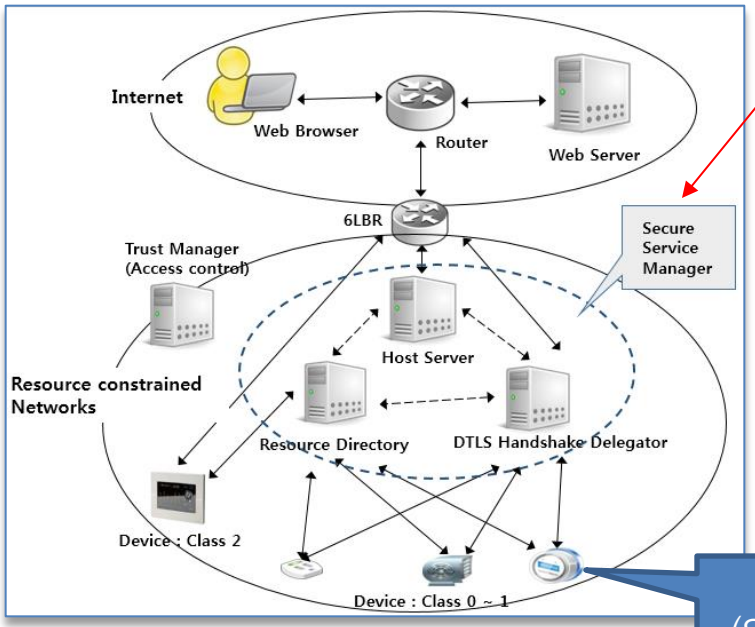


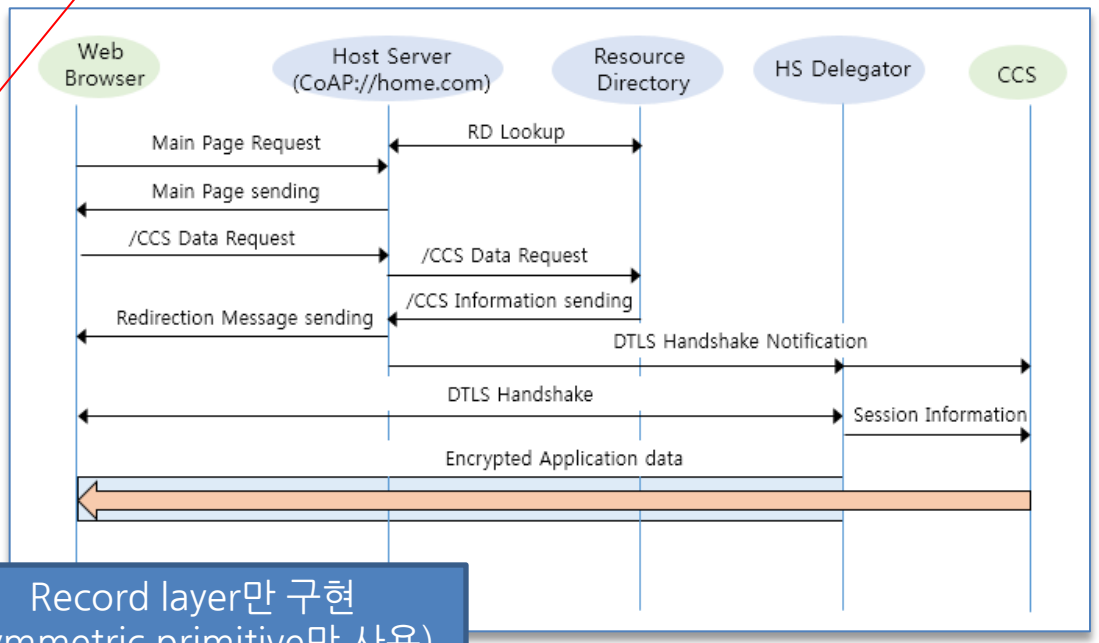
DTLS 적용 방안 (2)

- DTLS delegation
  - No fragmentation
  - Performance enhancement

분리해보자



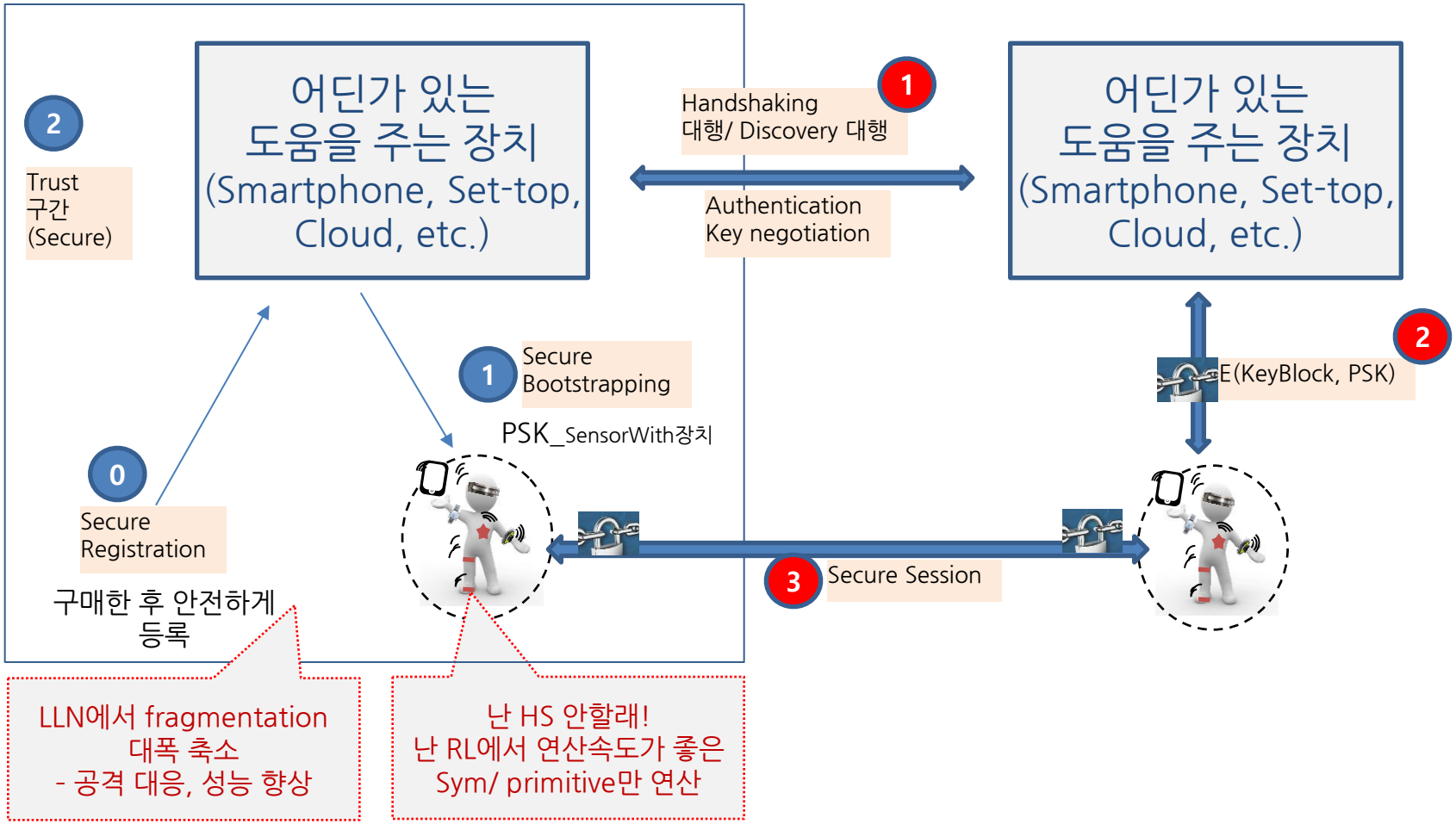




Record layer만 구현
(Symmetric primitive만 사용)

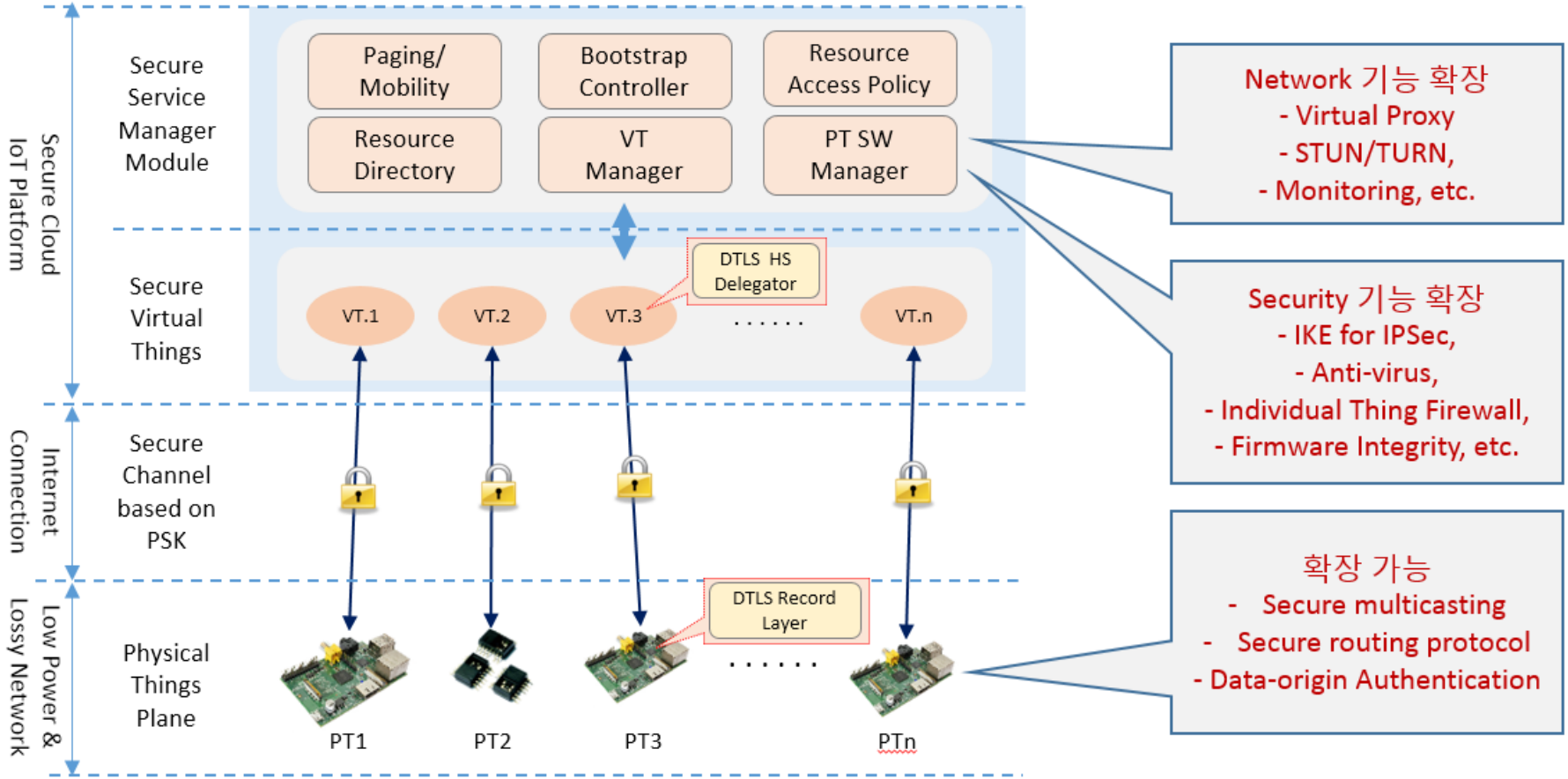
DTLS 적용 방안 (3)

DTLS Deligation 동작 과정



Secure Module의 서비스화?

- Many secure module as a service



결언

Confidentiality

Integrity

Authentication

국제표준과 같은 방향으로 보안 이슈를 해결하되,

- 제한된 응용영역에 따른 Constraint를 최대한 이용한 Light-Weight 구현
- Layer를 통한 역할 분할로부터 시작
- Interoperability 창구를 제한하여 보안이 필요한 요소를 최소화

Thank You!