체계적인 위협분석 : 스마트홈

이
을

Guardians
of
IoT@Home

www.CodeEngn.com
2015 CodeEngn Conference 12

CodeEngn

Index

이 올

I. Introduce

1. 5W1H
2. How do we Secure?
3. What did I do?
4. What is SmartHome?

이 올

1. 5W1H

예전에....., 지금.....,앞으로도....., 쭉.....

동아리 방에서,, 방 구석에서,, 회사에서,, 카페에서,,등등

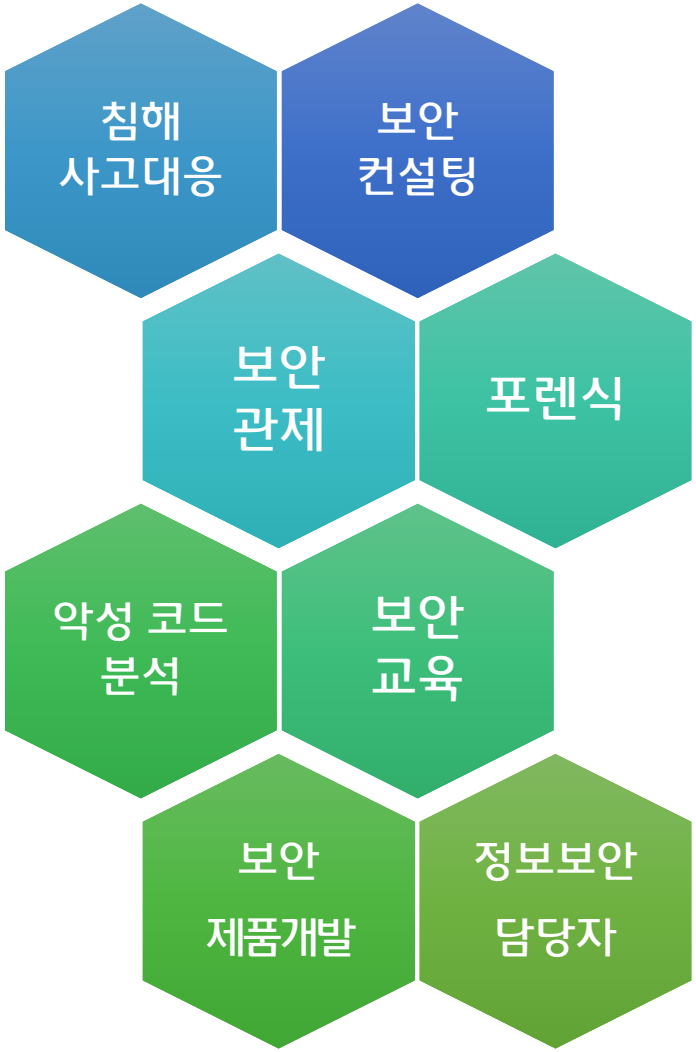
나, 너, 그리고 우리..!!!!!

해킹을! 보안을!

딱히 할게 없어서, 재미있어서, 먹고 살려고,,,

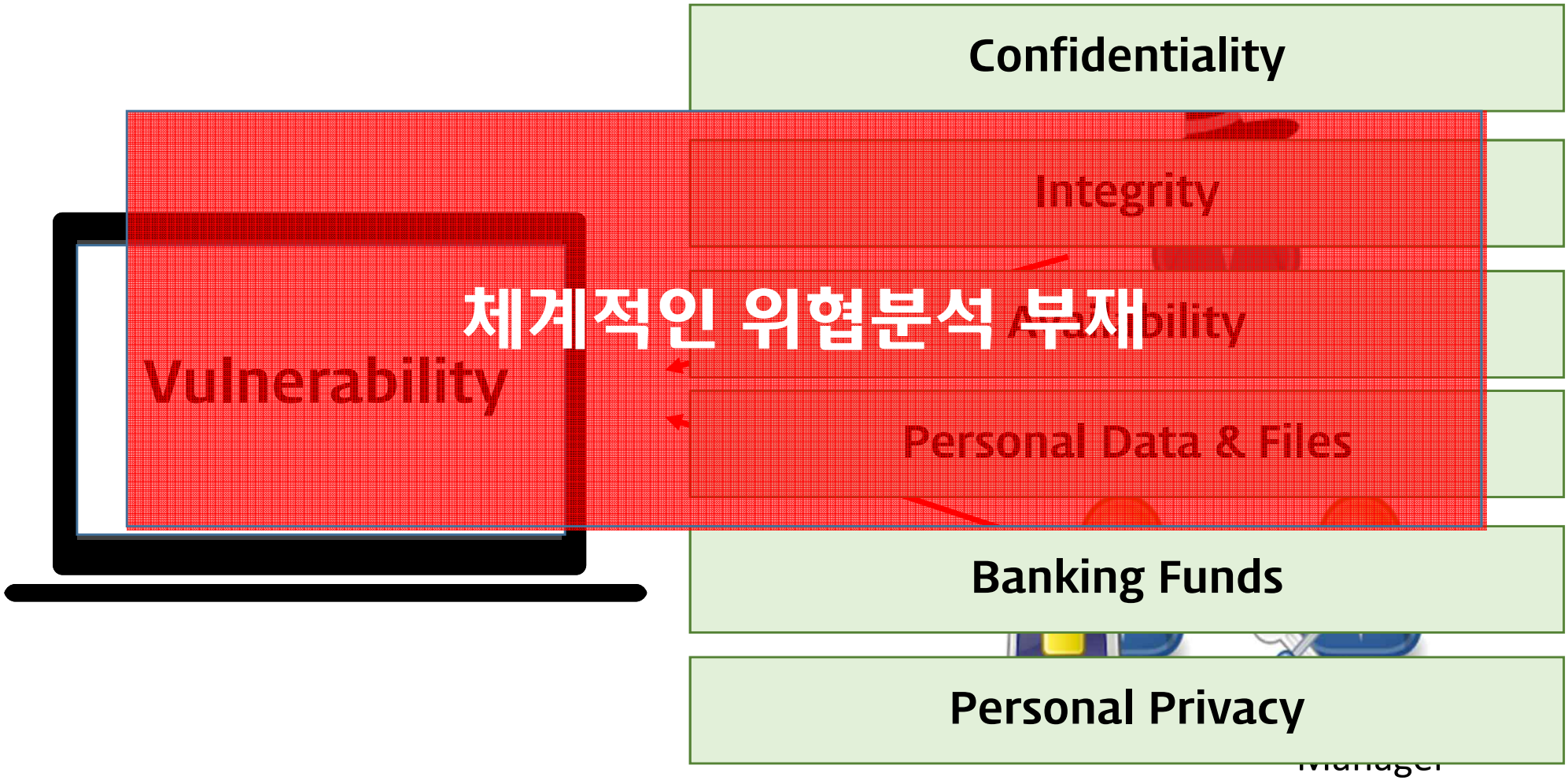
……??????????????

2. How do we Secure?



2. How do we Secure?

- 공격자와 개발자/보안 관리자 모두 공격/방어에 대한 수 많은 경우의 수를 생각

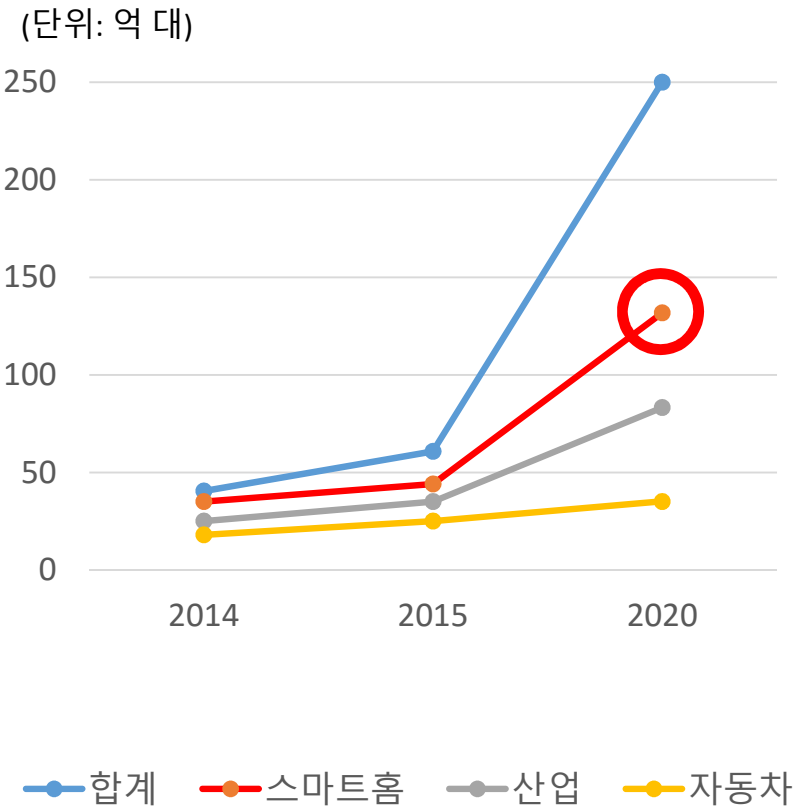


3. What did I do?

스마트홈에 존재하는 위협을 체계적으로 분석

4. What is SmartHome?

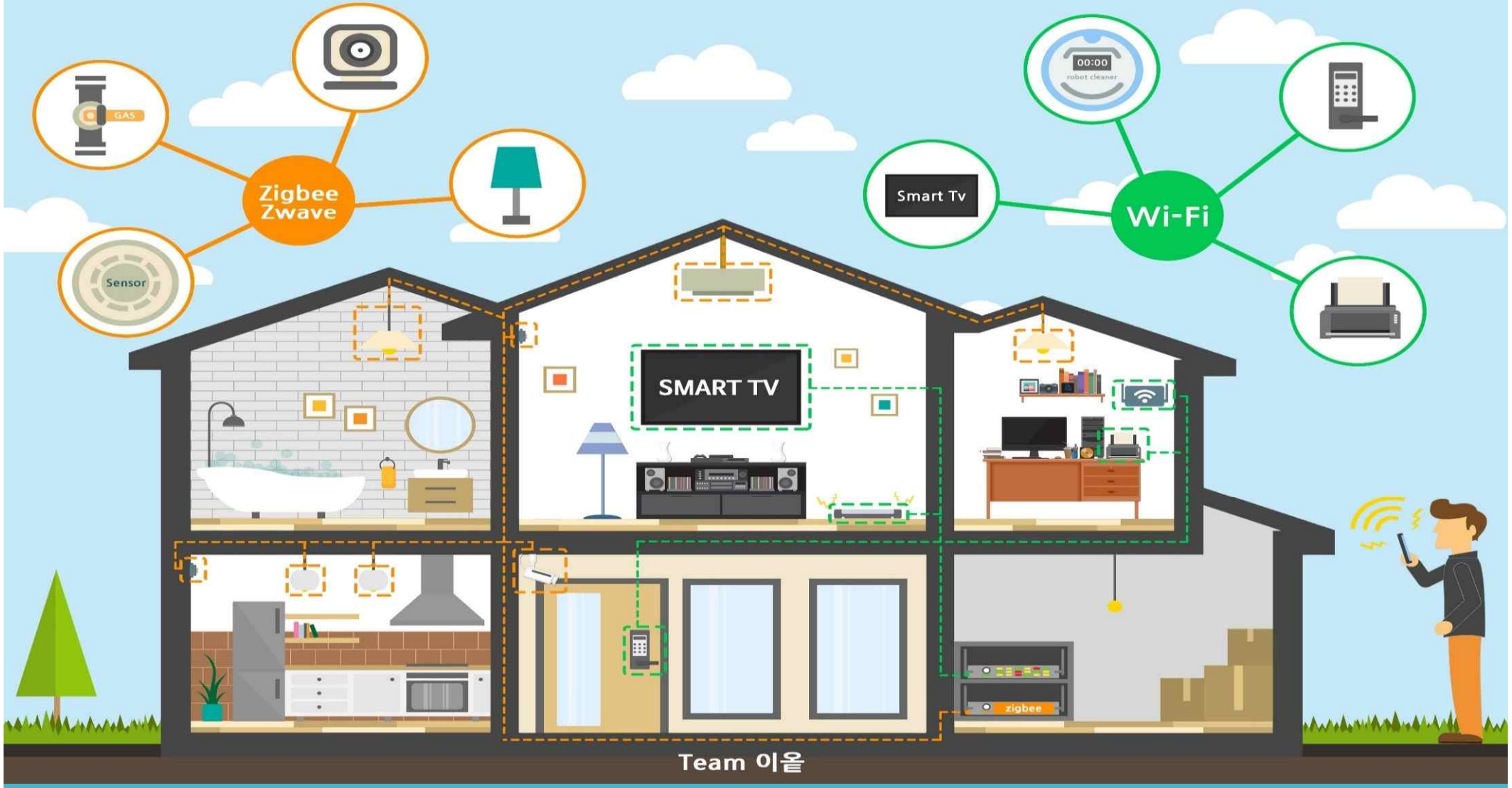
- 급격히 떠오르는 IoT, 그 중 생활에 가장 밀접한 스마트홈
- 경량화와 빠른 시장점유의 이유로 보안 미흡
- 단순한 서비스 프로토콜 사용, 미흡한 인증, 보안기술 결여



< IoT분야별 기기 증가전망 (자료 : Gartner) >

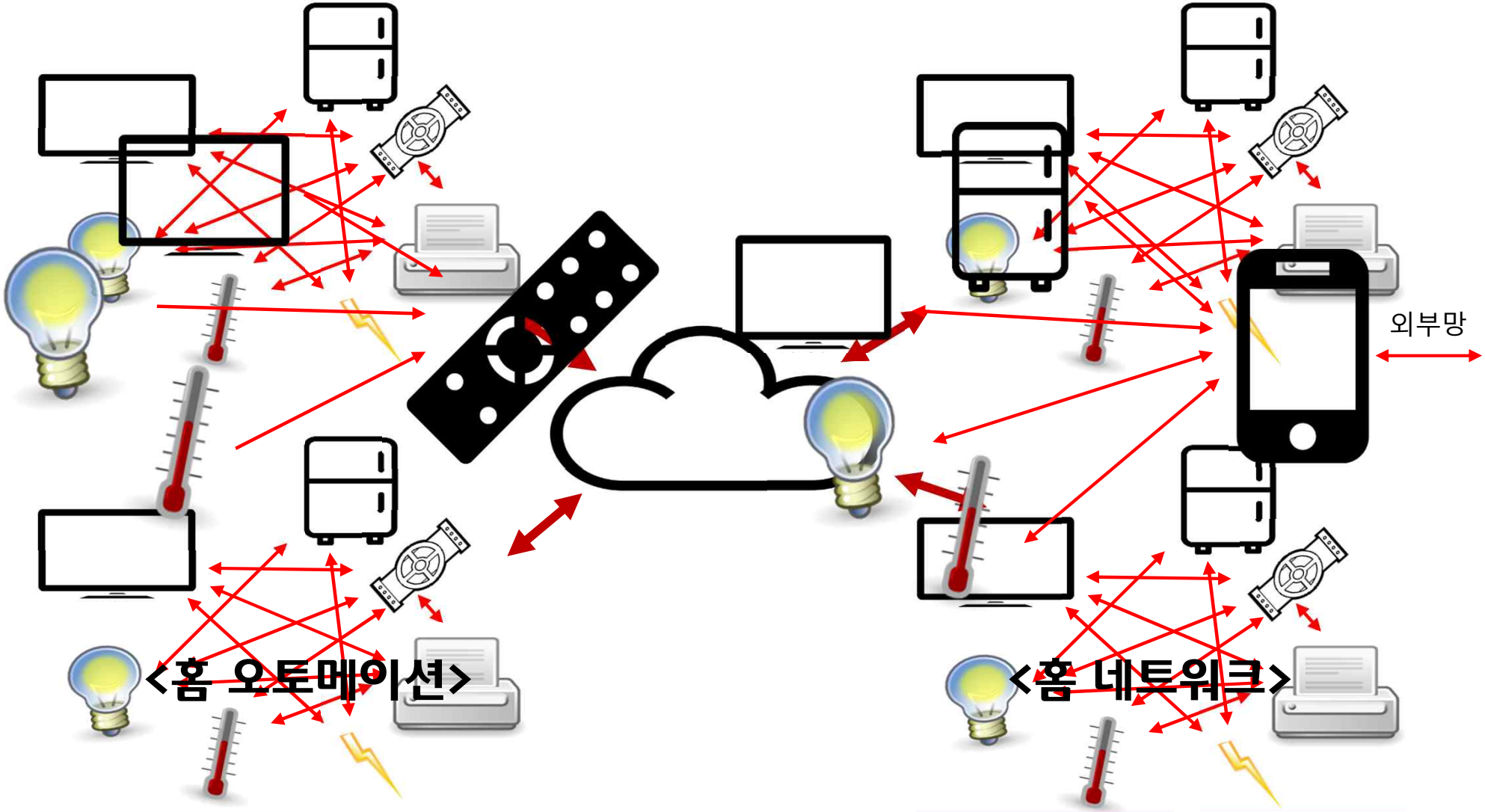
4. What is SmartHome?

- 사용자는 **애플리케이션**을 이용해 스마트홈 내부의 **중계기**로 제어신호를 보내며각 **기기**들과 통신



4. What is SmartHome?

- 홈 오토메이션과 홈 네트워크는 통신방향과 외부 망에 대한 차이
- 스마트 홈은 보다 성숙한 홈 네트워크로 IoT와 Cloud가 결합된 형태



4. What is SmartHome?

Samsung Smartthings

[제품 구성]
허브
모션 센서
위치 센서
열림감지센서
[특징]
2012.08 런칭
2014.08 삼성인수

Xiaomi Home kit

[제품 구성]
게이트웨이(허브)
열림감지센서
무선원격스위치
인체센서
[특징]
2015.06 런칭
국제 시장에서 중국 IoT기기 시장 이 가장 가파른 상승세를 보임

LG U+ IoT@Home

[제품 구성]
허브
온도조절기
가스락
열림감지센서
스위치
플러그
맘카
도어락

[특징]
2015.08 런칭
출시 40일만에 가입자 2만 명 달성

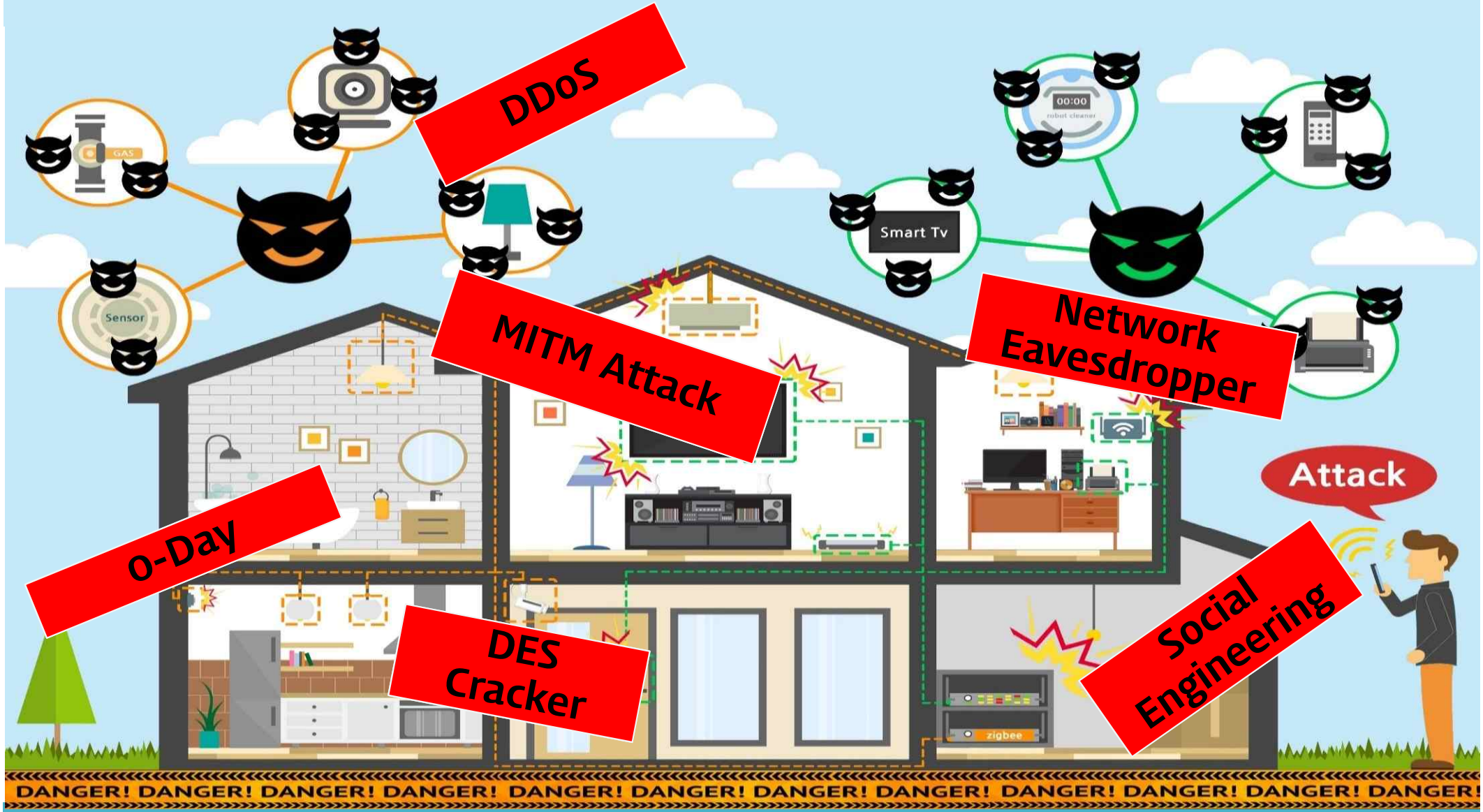
II. Security

1. What is House Security?
2. What is TMA?
3. Theat Modeling Process
4. Threat Modeling
5. Demo
6. What is solution?
7. Conclusion

이 올

1. What is House Security?

- 스마트홈 Element 의 보안위협 존재



2. What is TMA?

- 존재하는 위협들을 분석하기 위해 Threat modeling을 사용

방법

Threat Model Analysis

제품, 응용프로그램, 네트워크 또는 환경에 대한 보안 위협 및 공격이
수행되는 방식을 확인하는 데 도움이 되는 분석

① 자산식별 → ② 데이터흐름도 작성 → ③ STRIDE 적용 → ④ AttackTree 작성 → ⑤ DREAD 적용

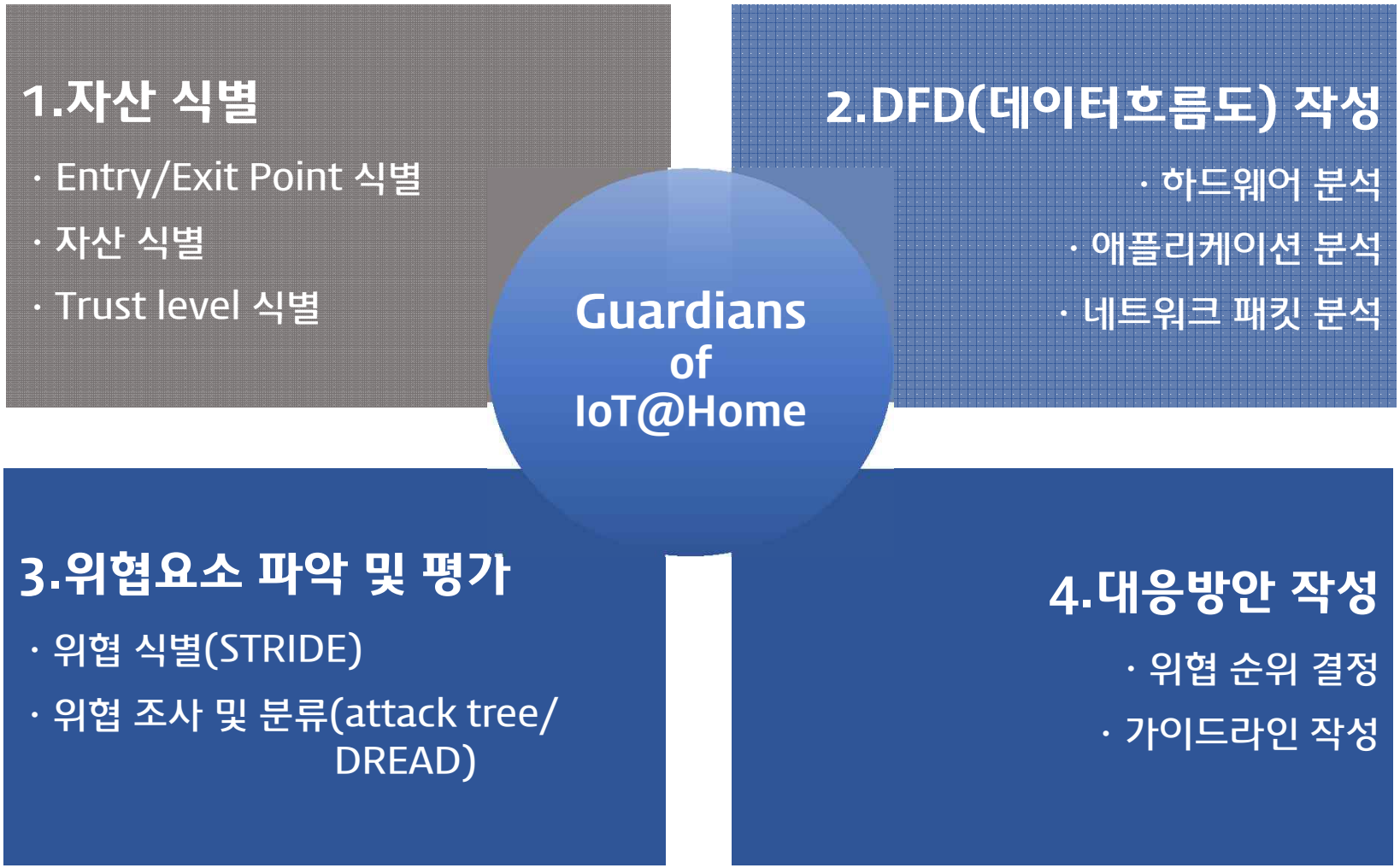
사례

기대효과

막연한 취약점 분석이 아닌
위협 식별을 통한
체계적인 분석이 가능

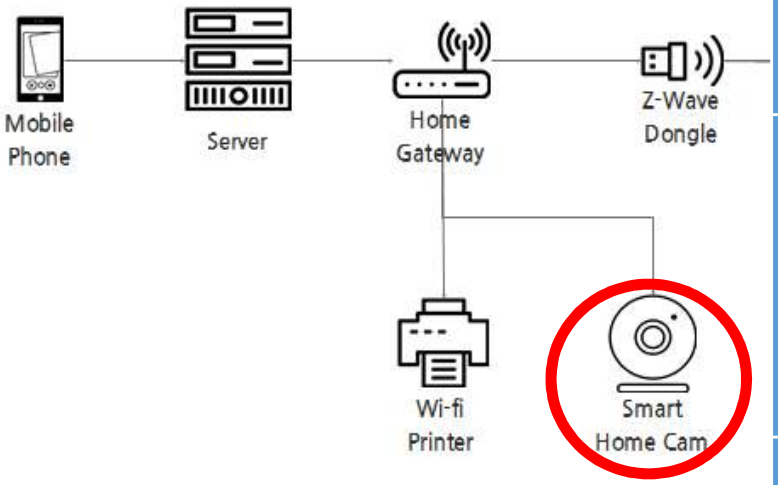
3. ThreatModeling Process

- 자산식별, DFD작성, 위협요소 파악 및 평가, 대응방안작성을 통해 보다 안전한 스마트홈을 구성



4. Threat Modeling ①자산식별

- 구성도를 통해 자산의 범위 식별



<스마트홈 서비스 구성도>

Asset	Smart Home Cam
Reasoning	집 내부를 모니터링 할 수 있어 침해되었을 경우 감지가 어려워 개인정보가 노출.
External Dependency	네트워크 연결이 요구됨. 공격자가 악성 펌웨어를 기기에 탑재하였을 시 이를 감지하기 어려움. 물리적인 보안이 고려가 되지 않아 공격자가 기기에 접근하게 되면 실제 사용자의 이용이 불가.
Security Assumptions	항상 네트워크 연결이 요구되며, 기기간의 통신은 기밀성을 유지하고 있다고 가정. 기기로부터 사용자에게까지 송신되는 데이터는 무결성 유지된다 가정. 펌웨어 수정이 어렵다고 가정. 기기를 사용하기 위해 사용자는 자신의 모바일 기기와 서비스 기기 간의 인증과 등록 절차를 수행.
Security notes	1. 사용자와 기기 간 데이터 송수신 과정의 기밀성이 훼손된 경우 – 도청 가능 2. 기기와 어플리케이션 사이의 무결성이 훼손되는 경우 – 데이터 변조 가능 3. 기기와 어플리케이션 사이 데이터 송수신의 가용성 문제 – 통신 장애 유발 가능
Contains Assets	사용자 개인정보 및 사생활 정보, Smart Home Cam의 시야 각 속에 있는 모든 기기 및 가구

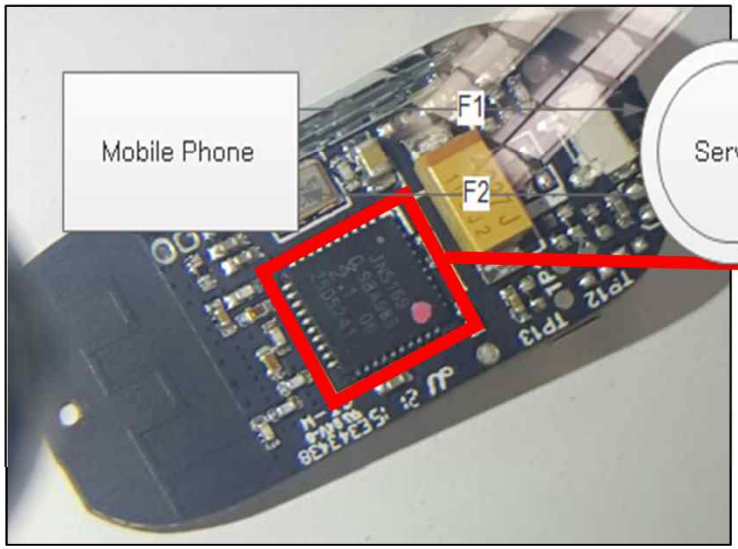
4. Threat Modeling ②DFD작성

- 스마트홈 서비스의 하드웨어,애플리케이션, 네트워크 패킷 분석을 통한 DFD(데이터 흐름도)작성

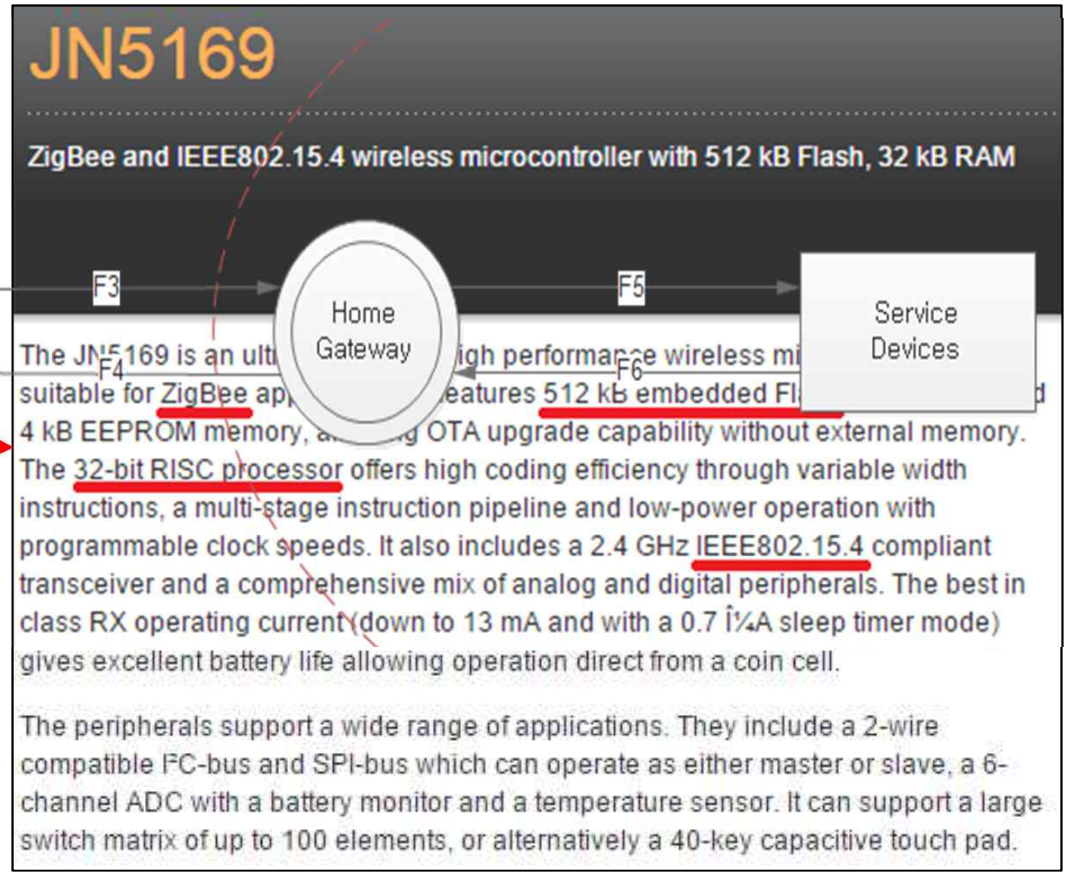
Context Diagram

거 분석

통신방법, 데이터 저장소의 유무, core-process 유무 등



<Xiaomi OpenSensor>

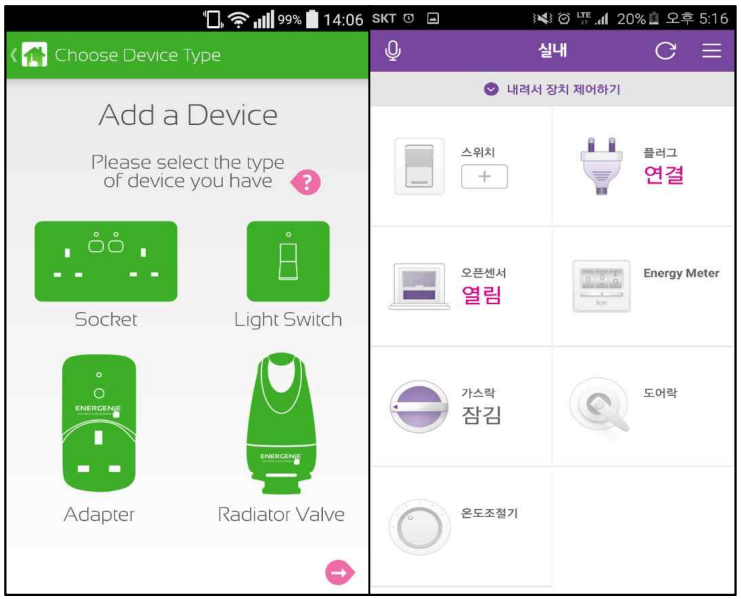


4. Threat Modeling ②DFD작성

- 스마트홈 서비스의 하드웨어,애플리케이션, 네트워크 패킷 분석을 통한 DFD(데이터 흐름도)작성

2) 애플리케이션 분석

암호화 방식, 데이터의 형태, 통신서버의 종류, 서버 주소 등



<Xiaomi . LG U+ Application>

```
    {
      String str = "0" + Integer.toHexString(paramArrayOfByte[i] & 0xFF);
      localStringBuffer.append(str.substring(str.length() - 2));
      i += 1;
    }
    return localStringBuffer.toString();
  }

  public static String convertMD5(String paramString)
  {
    return toHas("MD5", paramString);
  }
```

4. Threat Modeling ②DFD작성

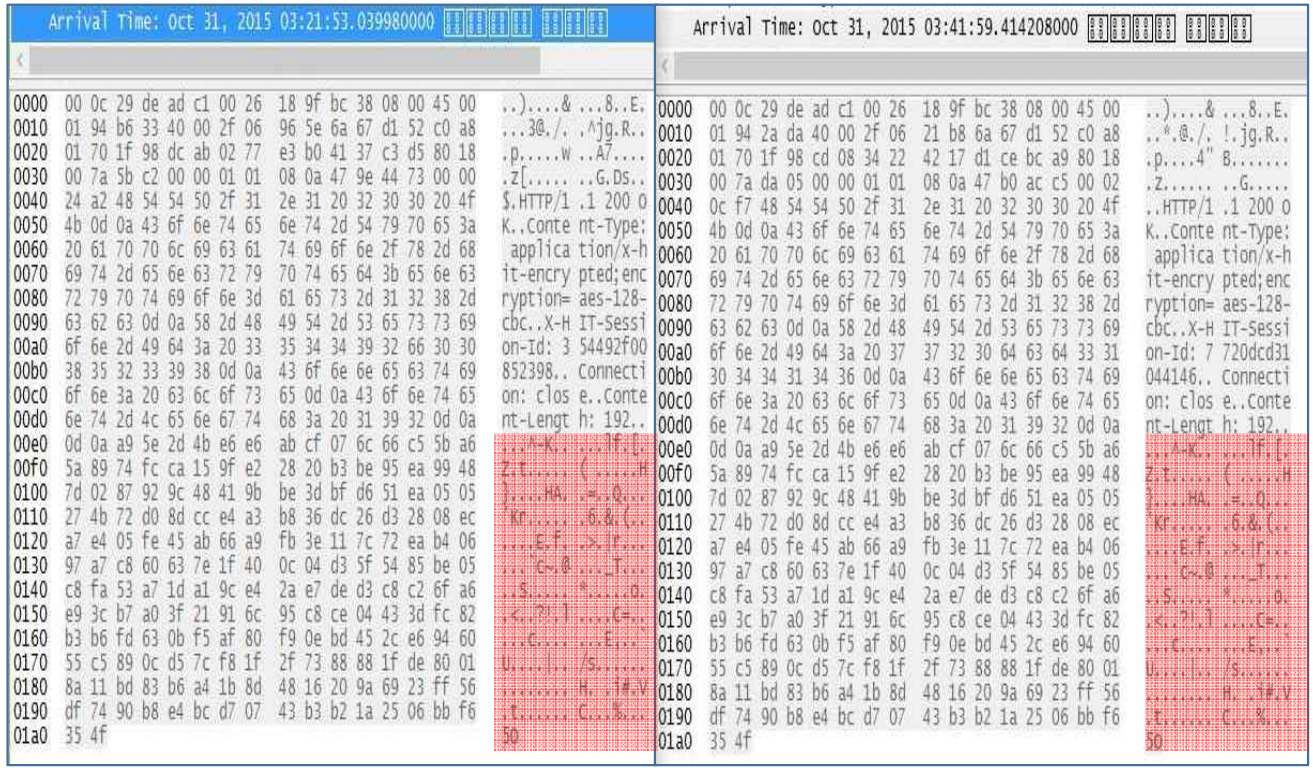
- 스마트홈 서비스의 하드웨어,애플리케이션, 네트워크 패킷 분석을 통한 DFD(데이터 흐름도)작성

3) 네트워크 패킷 분석

통신프로토콜, 암호화 방식, 데이터의 종류 등

- app_login.pcapng
- app_plug_turn_off.pcapng
- app_plug_turn_off_2.pcapng
- app_plug_turn_off_3.pcapng
- app_plug_turn_off_fail.pcapng
- app_plug_turn_on.pcapng
- app_plug_turn_on_2.pcapng
- app_plug_turn_on_3.pcapng
- app_plug_turn_on_fail.pcapng
- gas_connect_close.pcapng
- normal.pcapng
- plug_connect_disconnect2.pcapng
- plug_connect_disconnect.pcapng
- plug_fairing.pcapng
- plug_pairing.pcapng
- plug_turn_off_after_pairing.pcapng
- plug_turn_off_after_pairing_2.pcapng
- plug_turn_off_final.pcapng
- plug_turn_on_after_pairing.pcapng
- plug_turn_on_final2.pcapng
- plug_turn_on_final.pcapng
- sensor_disconnect.pcapng

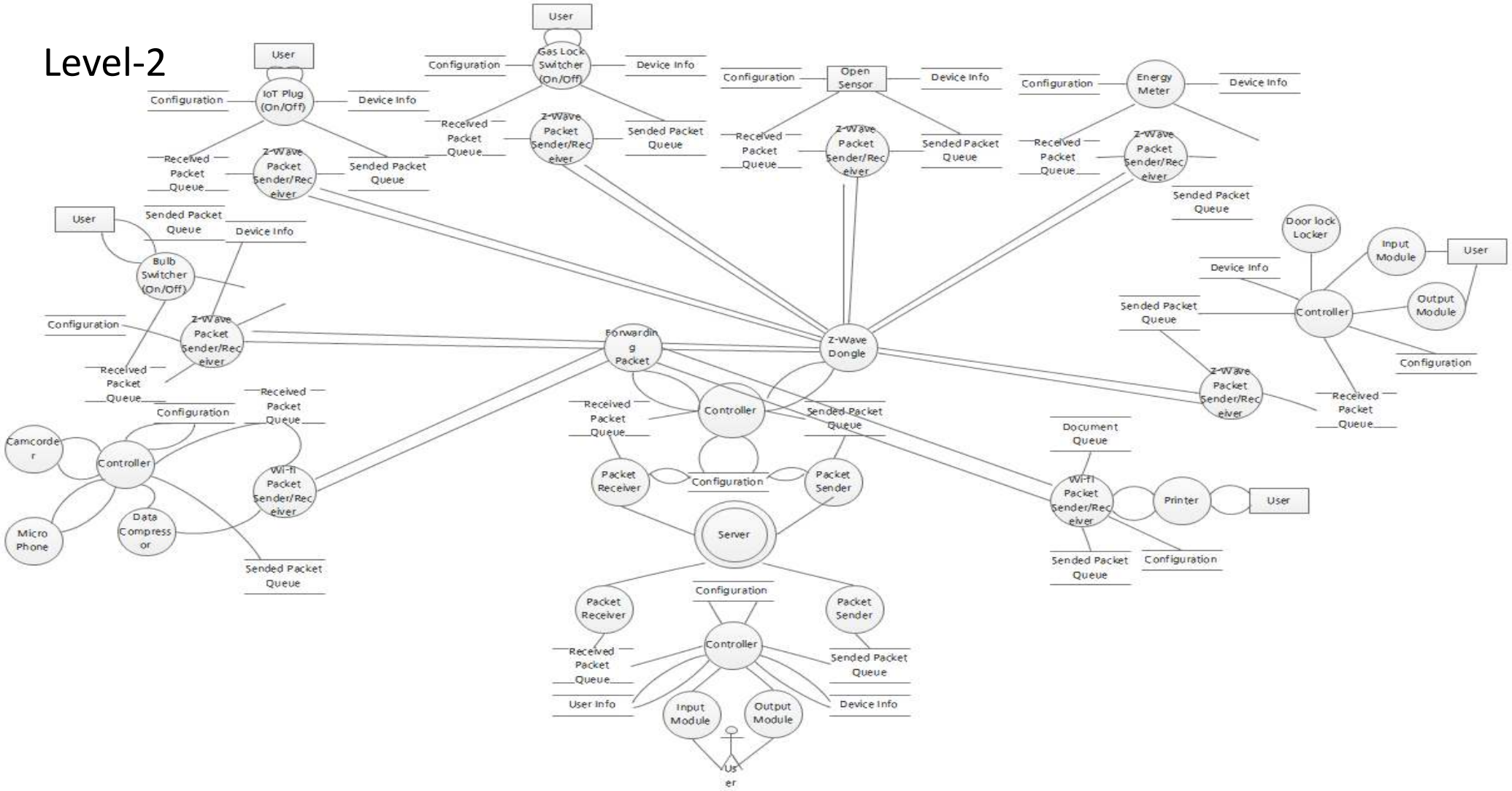
<수행동작 별 패킷>



4. Threat Modeling ②DFD작성

- 심화된 단계의 DFD(Data Flow Diagram)작성을 통해 위협발생 구간 확인

Level-2



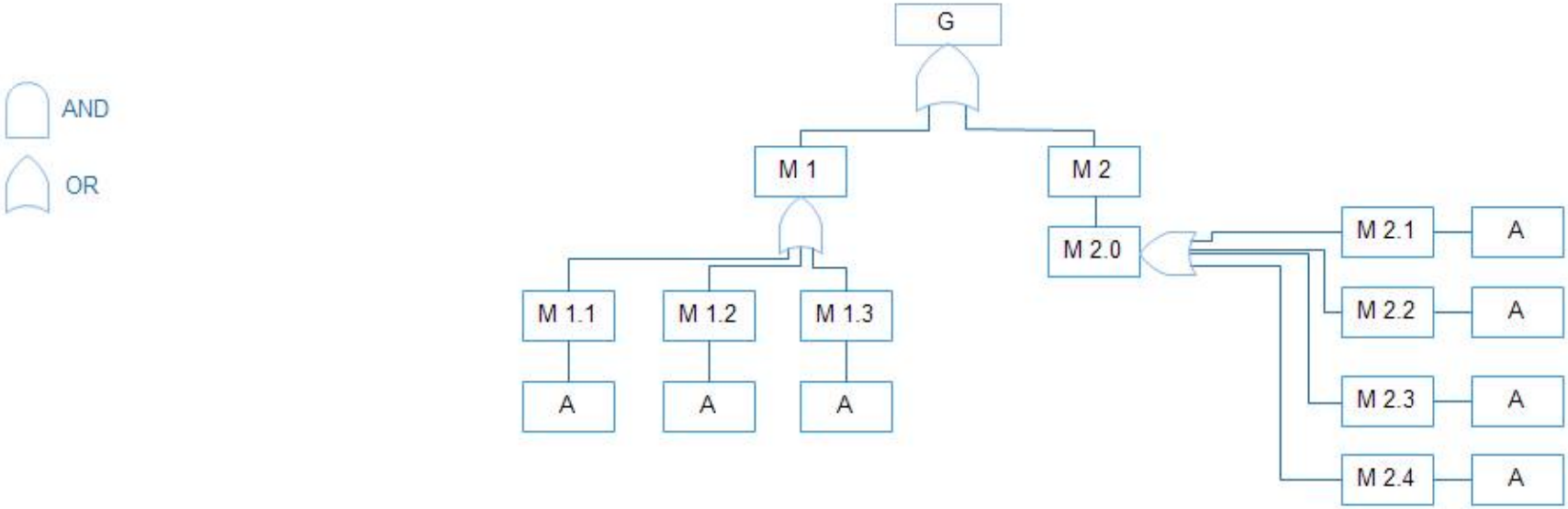
4. Threat Modeling ③STRIDE적용

- STRIDE기법을 사용하여 위협의 대상, 방법을 파악

Asset	Element	Threat	S	T	R	I	D	E
Home Gateway								
	Process	T1 : 공격자의 프로세스가 Home Gateway에 설치되어 실제 수행되어야 하는 프로세스인듯 동작한다	0					
		T2 :공격자의 프로세스가 Home Gateway에 설치되어 실제 수행되는 프로세스가 사용하는 데이터를 변조한다		0				
		T3 : Home Gateway에 설치된 악의적인 프로세스가 자신이 수행한 일련의 행위들을 부인한다.			0			
		T4 : Home Gateway에 설치된 악의적인 프로세스는 정상적인 프로세스가 사용하는 데이터를 획득할 수 있다.				0		
		T5 : Home Gateway에 설치된 악의적인 프로세스는 정상적인 프로세스 수행을 방해하여 사용자에게 적절한 서비스를 제공하지 못하게 한다.					0	
		T6 : Home Gateway에 설치된 악의적인 프로세스가 최고 관리자 권한을 획득한다.						0
	Data Flow	T7 : 공격자가 Home Gateway가 내부의 각 기기 혹은 외부 라우터와 주고받는 데이터를 변조한다.		0				
		T8 : 공격자가 Home Gateway가 내부의 각 기기 혹은 외부 라우터와 주고받는 데이터를 획득한다.				0		
		T9 : 공격자는 Home Gateway와 내부의 각 기기 혹은 외부 라우터와의 데이터 송수신을 방해하여 정상적인 서비스 제공을 막는다.					0	
	Data Store	T10 : 공격자는 Home Gateway 내부 프로세스가 저장하거나 불러오는 데이터를 변조한다.		0				
		T11 : 공격자의 악의적인 프로세스가 Home Gateway에 데이터를 저장하는 일련의 행위를 부인한다.			0			
		T12 : 공격자의 악의적인 프로세스는 Home Gateway의 올바른 프로세스가 저장하는 데이터들을 획득할 수 있다.				0		
		T13 : 공격자의 악의적인 프로세스는 Home Gateway 내부의 올바른 프로세스의 데이터 저장행위를 방해할 수 있다.					0	
	External Entity	T14 : 공격자는 올바른 사용자인 듯 Home Gateway에 접근하여 설정값을 변경하는 행위를 수행할 수 있다.	0					
		T15 : 공격자는 DNS서버를 오염시키거나 ARP Spoofing, IP Spoofing등의 기법을 통해 Home Gateway의 정상적인 동작을 방해할 수 있다.	0					
		T16 : 공격자는 자신이 한 일련의 행위들을 부인 할 수 있다.			0			
Gas Switch Lock								
Door Lock								

4. Threat Modeling④attack tree작성

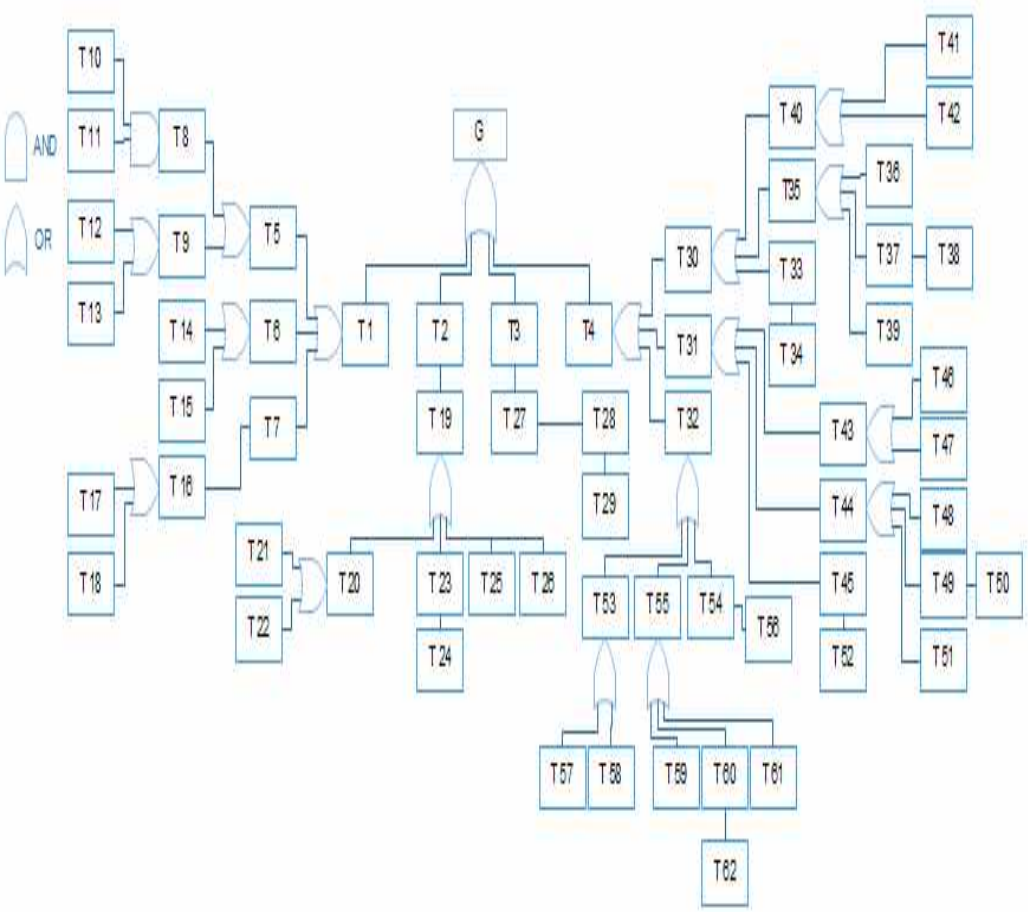
- STRIDE기법에 의거한 Attack Tree
- assumptions on attackers' abilities and resources



G : Invasion of Privacy					
M 1	Direct Invasion	M 2	Indirect Invasion	M 1.1	Door Open
M 1.2	Window Open	M 1.3	Peep into Home	M 2.0	Inference User Life Pattern
M 2.1	Get Data From Bulb Switch	M 2.2	Get Data From Energy Meter	M 2.3	Get Data From Gas Switch Lock
M 2.4	Get Data From IoT Plug	A	Malicious Action	M 2.6	

4. Threat Modeling④attack tree작성

- STRIDE기법에 의거한 Attack Tree
- assumptions on attackers' abilities and resources



G : Malicious Action in Smart Home					
T 1	Compromised Mobile Application	T 2	Compromised Home Gateway	T 3	Compromised Devices in Smart Home
T 4	Contaminated Data Channel	T 5	Compromised App Installation	T 6	U+@Home App's vulnerability
T 7	Android/iOS vulnerabilities	T 8	Authorized Installation	T 9	Unauthorized Installation
T 10	Authenticated Site(App Store/Play Store)	T 11	User Agreement	T 12	Social Engineering
T 13	Fishing	T 14	Weak Authentication	T 15	Weak Encryption
T 16	Get Root Privilege	T 17	0-day Vulnerability	T 18	Known Vulnerability
T 19	Unauthorized Action	T 20	Firmware Modification	T 21	Remote Update
T 22	Physical Access	T 23	Inhibition Availability	T 24	Changing Configuration
T 25	Get Root Privilege	T 26	Malicious Code execution	T 27	Unauthorized Action
T 28	Firmware Modification	T 29	Physical Access	T 30	Mobile To Server Channel Affected
T 31	Server To Home Gateway Channel Affected	T 32	Internal Home Network Channel Affected	T 33	Impersonation
T 34	MIMT	T 35	Get Flowing Data	T 36	Data Tampering
T 37	Data Decryption	T 38	Get Sensitive Data	T 39	Replay Attack
T 40	Inhibition Availability	T 41	Jamming	T 42	Overloaded Packet
T 43	Inhibition Availability	T 44	Get Flowing Data	T 45	Impersonation
T 46	Jamming	T 47	Overloaded Packet	T 48	Data Tampering
T 49	Data Decryption	T 50	Get Sensitive Data	T 51	Replay Attack
T 52	MIMT	T 53	Inhibition Availability	T 54	Impersonation
T 55	Get Flowing Data	T 56	MIMT	T 57	Jamming
T 58	Overloaded Packet	T 59	Data Tampering	T 60	Data Decryption
T 61	Replay Attack	T 62	Get Sensitive Data		

4. Threat Modeling⑤DREAD적용

- DREAD 기법을 사용하여 위협에 대한 점수를 매겨 우선 순위를 결정
- 평가된 지표가 보안대책 수립에 근거가 됨

위협 기준	설명	Score
Damage Potential (잠재적 피해)	피해가 얼마나 클 것인가?	0 = 없음 5 = 개인적 사용자의 데이터가 오염/영향을 받음 10 = 시스템 또는 데이터 전체의 파괴
Reproducibility(재현 용이성)	공격을 재현하기가 쉬운가?	0 = 관리자일지라도 매우 어렵거나 불가능함 5 = 권한이 부여된 사용자가 한 두 단계가 요구됨 10 = 인증 없이 웹브라우저와 주소창으로 가능
Exploitability(공격 용이성)	공격하기 위한 작업량이 얼마나 많은가?	0 = 공격툴이 없어도 프로그래밍과 네트워크에 대한 충분한 지식으로 가능 5 = 악성 프로그램이 인터넷 상에 존재하거나 공격툴을 이용해 공격이 쉽게 됨 10 = 웹브라우저만으로도 가능
Affected users (영향 받는 사용자)	얼마나 사용자가 많은 영향을 받는가?	0 = 없음 5 = 몇몇 사용자 10 = 모든 사용자
Discoverability(발견 용이성)	위협을 얼마나 발견하기 쉬운가?	0 = 소스코드나 관리자 권한이 없으면 매우 어려움 5 = 네트워크를 모니터링하거나 추측함으로써 알아낼 수 있음 9 = 검색엔진을 사용하여 이미 공개된 세부사항을 검색할 수 있음 10 = 정보는 웹브라우저 주소 표시 줄이나 형태로 볼 수 있음

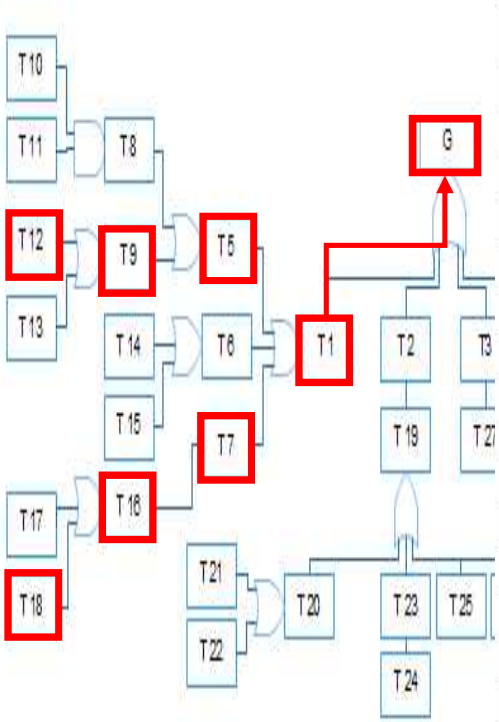
4. Threat Modeling⑤DREAD적용

- DREAD 기법을 사용하여 위협에 대한 점수를 매겨 우선 순위를 결정
- 평가된 지표가 보안대책 수립에 근거가 됨

Threat	D	R	E	A	D	Total
Unauthorized access to Home network	5	5	5	5	5	5
Affected Process in Gateway	10	5	5	10	9	7.8
Get Mobile device root privilege	10	5	5	5	5	6
Get User private information	5	5	5	5	5	5
Change logs in mobile device	5	5	5	5	10	6
Change logs in gateway	5	5	5	5	9	5.8
Affected Process in mobile device	10	5	5	10	9	7.8
Get gateway root privilege	10	5	10	10	9	8.8
Change logs in ISP	10	5	0	10	0	5
Affected process in each small devices	10	0	0	10	5	5
⋮	.	.	.	.	.	.
	.	.	.	.	.	.
	.	.	.		.	.
	.	.	.	.	.	.

5. Demo

- Threat modeling을 통해 얻어진 위협으로 모의해킹 수행



G Malicious Action in Smart Home					
T 1	Compromised Mobile Application	T 2	Compromised Home Gateway	T 3	Compromised Devices in Smart Home
T 4	Contaminated Data Channel	T 5	Compromised App Installation	T 6	U+@Home App's vulnerability
T 7	Android/iOS vulnerabilities	T 8	Authorized Installation	T 9	Unauthorized Installation
T 10	Authenticated Site(App Store/Play Store)	T 11	User Agreement	T 12	Social Engineering
T 13	Fishing	T 14	Weak Authentication	T 15	Weak Encryption
T 16	Get Root Privilege	T 17	0-day Vulnerability	T 18	Known Vulnerability
T 19	Unauthorized Action	T 20	Firmware Modification	T 21	Remote Update
T 22	Physical Access	T 23	Inhibition Availability	T 24	Changing Configuration
T 25	Get Root Privilege	T 26	Malicious Code execution	T 27	Unauthorized Action
T 28	Firmware Modification	T 29	Physical Access	T 30	Mobile To Server Channel Affected
T 31	Server To Home Gateway Channel Affected	T 32	Internal Home Network Channel Affected	T 33	Impersonation
T 34	MIMT	T 35	Get Flowing Data	T 36	Data Tampering
T 37	Data Decryption	T 38	Get Sensitive Data	T 39	Replay Attack
T 40	Inhibition Availability	T 41	Jamming	T 42	Overloaded Packet
T 43	Inhibition Availability	T 44	Get Flowing Data	T 45	Impersonation
T 46	Jamming	T 47	Overloaded Packet	T 48	Data Tampering
T 49	Data Decryption	T 50	Get Sensitive Data	T 51	Replay Attack
T 52	MIMT	T 53	Inhibition Availability	T 54	Impersonation
T 55	Get Flowing Data	T 56	MIMT	T 57	Jamming
T 58	Overloaded Packet	T 59	Data Tampering	T 60	Data Decryption
T 61	Replay Attack	T 62	Get Sensitive Data		

6. What is solution?

- 해당 위협이 발생했을 경우 대응기법 선택

문제점 무시	문제점 알림	문제점 제거	문제점 수정
문제점을 무시하고 아무런 대응도 하지 않는다.	사용자에게 문제점을 알리고 그 기능을 사용여부를 결정할 수 있도록 한다.	문제점을 고칠 시간이 없고, 보안 위험도가 충분히 높다면, 그 기능을 삭제하는 것을 고려해야 한다.	가장 분명한 해결책. 기술적으로 문제를 고치는 것이지만, 현실적으로 가장 어려운 경우도 있다.

6. What is solution?

- 식별된 위협들을 바탕으로 **사전 대응책** 제시

사전 대응

기존에는 방화벽과 같은 별도의 보안장비로 보안을 제공

-> **기획/설계 단계부터의 보안 내재화**

6. What is solution?

- 식별된 위협들을 바탕으로 **실시간 대응** 제시

실시간 대응

IoT기기에 적용되는 실시간 감시체계의 부재

-> **실시간으로 문제점을 알리고 기능 사용여부 선택**

6. What is solution?

- 식별된 위협들을 바탕으로 **사후대응** 제시

사후 대응

저전력/경량형 하드웨어로 인한 저장매체의 부족

펌웨어 기반으로 인한 기록들의 휘발성

-> **침해사고 대응체계 및 책임추적성 확보**

6. What is solution?

- 지속적으로 attack tree를 만들고 대응방안을 만들기 위한 웹사이트 제공

Web Site url :

7.Conclusion

Threat Modeling 을 통해 체계적인 위협 분석 및 대응책 마련 가능

Thank you!