Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.2, Apr. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.2.513

위협 모델링 분석 및 국제공통평가기준을 통한 스마트홈 허브의 보안요구사항에 관한 연구*

박 재 현,† 강 수 영, 김 승 주‡
고려대학교 정보보호대학원

Study of Security Requirement of Smart Home Hub through Threat Modeling Analysis and Common Criteria*

Jae-Hyeon Park,† Soo-young Kang, Seung-joo Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

주거 환경에 IoT 기술을 융합한 스마트홈 환경에서 스마트홈 허브는 다양한 IoT 기기들을 네트워크로 연결하여 사용자에게 편의 기능을 제공한다. 스마트홈 허브는 IoT 기기들을 연결하여 활용하는 과정에서 다양한 데이터가 오고가는 통로의 역할을 하는데, 이 데이터에는 사용자의 생활환경과 밀접한 관련이 있어 개인정보로써 악용될 수 있다. 이러한 개인정보의 악용으로 사용자의 신원 노출 등 피해가 발생할 수 있다. 따라서 본 논문은 스마트홈 허브에 대해 기존에 국내에서 사용하지 않았던 개인정보보호 측면의 위협 모델링 기법인 LINDDUN을 사용하여 위협을 분석하였다. 분석한 위협과 대응하는 보안요구사항을 국제표준인 common criteria를 사용하여 스마트홈 허브에 대한 평가 기준을 제시한다.

ABSTRACT

In a smart home environment that integrates IoT technology into a residential environment, the smart home hub provides convenience functions to users by connecting various IoT devices to the network. The smart home hub plays a role as a gateway to and from various data in the process of connecting and using IoT devices. This data can be abused as personal information because it is closely related to the living environment of the user. Such abuse of personal information may cause damage such as exposure of the user's identity. Therefore, this thesis analyzed the threat by using LINDDUN, which is a threat modeling technique for personal information protection which was not used in domestic for Smart Home Hub. We present evaluation criteria for smart home hubs using the Common Criteria, which is an international standard, against threats analyzed and corresponding security requirements.

Keywords: smart home, privacy, threat modeling, LINDDUN, criteria

I. 서 론

사물인터넷 기술의 발전으로 각종 가전 기기에 통신기능을 추가하여 사용자에게 다양한 편의성을 제공하는 스마트홈 기술이 주목받고 있다. 해외 조사기관 strategy analytics에 따르면 해외 스마트홈

Received(01. 22. 2018), Modified(03. 12. 2018), Accepted(03. 22. 2018)
* "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2017-2015-0-00403)
† 주저자, pjh224@naver.com
‡ 교신저자, skim71@korea.ac.kr(Corresponding author)

시장 규모는 2014년에 480억 달러로 집계되며, 2019년에는 1,115억 달러로 성장할 것으로 추산된다. 또한 국내 스마트홈 시장 규모는 한국스마트홈산업협회에서 조사한 결과에 따르면 2014년에 8조 6천억 원에서 2019년에 23조 4천억 원으로 증가될 것으로 전망되며[1], 해당 자료는 Fig 1.과 같다.

스마트홈 시장이 증대되고 많은 사용자에게 보급되면서 다양한 문제가 발생하며, 특히 사용자의 생활과 밀접한 연관이 있기 때문에 개인정보 유출문제가 증가되고 있다. 위키리크스에서 공개한 문서에서 CIA와 MI5가 삼성 스마트TV를 대상으로 하는 감시도구인 'weeping angel'을 개발하고 이용하여 개인 사용자의 정보를 획득하였다고 발표했다[2]. 위키리크스의 이러한 발표로 인해 Joshua Siegel을 대표로 하여 뉴저지 지방법원에서 삼성을 대상으로 집단 소송이 발생하였다. 원고는 삼성이 허가받지 않는 제3자가 사용자의 사적인 대화에 접근하지 못하도록 보호하기 위한 합당한 조치를 취하지 않았다고 주장하였으며, 징벌적 손해배상을 통한 막대한 양의 배상금을 요구하였다[3].

다른 예로 베이비모니터에 대한 보안 취약점 공개 사례가 있다. 베이비모니터는 영유아를 대상으로 촬영 또는 녹음이 가능한 장비를 말한다. 미국의 보안회사 Rapid 7의 조사에 따르면 미국 내 유통되는 베이비모니터 7종에 대한 조사 결과를 발표하였고, 이를 통해 보안 및 개인정보에 영향을 끼칠 수 있다고 주장하였다[4].

IP 카메라에 대한 해킹 사례도 있다. 최근 IP 카메라를 영유아나 반려동물을 살피거나 가택침입 등의 범죄를 방지하기 위해 많이 사용하는데, 사이버수사대가 검거한 용의자는 2016년 1월부터 2017년 10월 13일까지 1600대의 IP 카메라를 12만 7000번 해킹하여 옷을 갈아입거나 연인, 부부간의 관계 등 민감한 사생활을 훔쳐보고 약 90GB, 888개의 영상물을 불법 촬영한 혐의를 받고 있다[5].

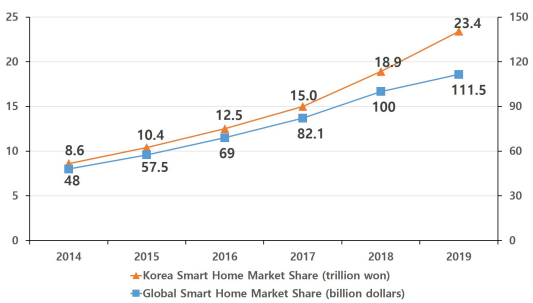

Fig. 1. Smart Home Market Size Trend

이에 본 논문은 스마트홈을 개인정보 유출 관점에

Table 1. Definitions of Smart Home

Reference	Definition
[7]	Using a wireless sensor network with actuator functionality, the system can automatically gather physical sensing information and efficiently control various consumer home devices.
[8]	A residence that uses a Home Controller to integrate the residence's various home automation systems
[9]	A residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment audio & video systems, security, and camera systems that are capable of communicating with one another and can be controlled remotely by a time schedule, from any room in the home, as well as remotely from any location in the world by phone or internet
[10]	A home equipped with lighting, heating, and electronic devices that can be controlled remotely by smartphone or computer
[11]	The smart home is a privately used home (eg home, rented flat), in which the numerous devices of home automation (such as heating, lighting, ventilation), home appliances (such as refrigerator, washing machine), consumer electronics and communication facilities intelligent objects that are based on the needs of the inhabitants. By interlinking these items with each other, new assistance functions and services can be provided for the benefit of the resident and generate added value that goes beyond the individual benefits of the applications in-house.
[12]	A Smart Home device is a thing, whose main functionality is extended with networking abilities to create a new one. The additional infrastructure for those devices, like a base or control station, falls also in Smart Home.

서 연구하고자 한다. 개인정보는 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)를 의미한다[6]. 상기 정의는 개인정보보호법 제2조 1항으로, 법으로써 개인정보를 정의한 이유는 본 논문에서 제안할 평가 기준이 국내법에 부합하게 만들기 위함이다.

스마트홈에 대한 다양한 연구가 진행되고 있으며, 연구별로 조금씩 다른 스마트홈에 대한 정의를 실시하고 있다. 대표적인 예는 Table 1.과 같다.

상기 스마트홈 정의의 공통점은 두 가지 정도로 볼 수 있다. 첫째, 가전 등의 기기에 통신기능을 추가하여 일종의 네트워크를 구성한다. 둘째, 네트워크를 구성하는 것으로 기기의 개별 기능보다 개선되거나 추가적인 기능을 제공한다. 이를 참고하여 본 논문에서는 스마트홈을 다음과 같이 정의한다.

스마트홈은 가정용 기기에 통신기능을 추가하고 기기들을 통제하는 기기를 이용하여 소규모 네트워크를 구성하는 것으로 다양한 편의기능을 제공하는 시스템을 가리킨다. 이 중, 통신기능이 추가된 가정용 기기를 스마트홈 기기라고 지칭하며, 이를 통제하는 기기를 스마트홈 허브라고 정의한다. 스마트홈 기기들과 스마트홈 허브에 대한 구성도는 Fig 2.와 같다.

이 연구를 통하여 기존의 일반적인 보안 관점에서 도출된 요구사항에 추가하여 개인정보 관점에서 분석한 요구사항을 추가적으로 도출하였다. 또한 이러한 연구결과를 토대로 실제로 발생 할 수 있는 위협에 대한 식별이 가능하였으며, 새로이 식별된 위협과 공통평가기준을 통하여 실제 인증 기준에 적합한 보안요구사항을 확인했다.

본 논문은 스마트홈을 구성하는 주요 기기인 스마트홈 허브를 개인정보 유출 관점에서 위협 분석을 실시하고 스마트홈 허브에 대한 평가 기준을 작성하였다. 2장은 관련연구로서 스마트홈에 대한 보안성 연구와 위협 모델링 기법에 대한 연구를 설명한다. 3장에서는 위협 모델링 기법을 적용하여 보안요구사항을 도출하기 위한 과정을 설명하고, 이 결과를 바탕으로 4장에서 평가 기준을 위한 보안요구사항을 작성한다. 5장에서 차후 연구와 결론을 내린다.

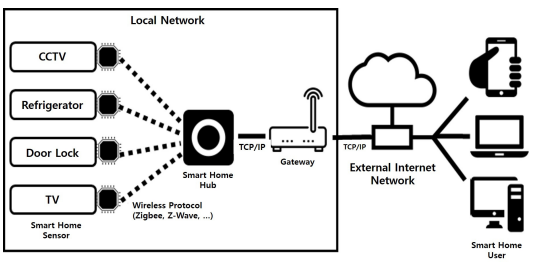

Fig. 2. Architecture of a Smart Home

II. 관련 연구

2.1 스마트홈 보안

최근 IoT 기기에는 IP 카메라나 인공지능 스피커 등 개인정보를 수집할 수 있고, 이를 다루는 기기들이 증가하고 있다. 2015년 IEEE에서 주최한 국제 컨퍼런스인 Computer Communication and Networks에서 Ali Tekeo˘glu과 Ali Saman Tosun이 'Investigating Security and Privacy of a Cloud-Based Wireless IP Camera : NetCam'라는 주제로 IP 카메라 해킹을 통한 개인정보 유출을 다루었다[13].

스마트홈 시스템에 대한 보안 연구는 증가하고 있는 추세이다. Black Hat USA 2015에서 Tobias Zillner가 Zigbee 프로토콜을 사용하는 스마트홈 허브 SmartThings와 SmartBulb에 대한 취약점을 발표하였으며[14], ShmooCon 2016에서 "Breaking Bulbs Briskly by Bogus Broadcasts"를 주제로 Z-Wave 프로토콜을 사용하는 스마트홈의 제어권을 획득하여 개인정보 탈취 및 물적 피해 유발 등이 가능한 사례를 제시하였다[15]. Black Hat USA 2017에서는 Billy Rios와 Jonathan Butts가 생활 전반에서 사용되고 있는 IoT 가전을 통해 재산피해와 인명피해가 일어날 수 있음을 주장하였다[16].

Thomas Brandstetter는 스마트홈 서비스의 기반이 되는 건물 자동화 시스템를 주제로 발표하였으며, 건물 자동화 시스템에서 발생할 수 있는 공격 시나리오에 대하여 서술하고 침투 테스트를 위한 도구의 제안과 기존 보안 조치와 서술한 문제들을 비교하였다[17]. Dimitris Geneiatakis 외 5명은 MIPRO 2017에서 사물인터넷 기반 스마트홈에 대해 개인정보와 관련된 보안이슈에 대해 논문을 발표하였다[18].

취약점 분석 이외에도 정책, 설계 등 스마트홈의

제작단계부터 보안을 적용하는 연구도 증가하고 있다. 한 예로 2012년에 Kristian Beckers가 새로운 요구사항 분석 방법론을 제안하고, 그 방법론을 기존의 LINDDUN과 같은 개인정보 중심의 요구사항 방법론과 비교하였다[19]. 그리고 2017에 Annanda Thavymony Rath와 Jean-Noel Colin이 스마트홈의 보안성을 강화하기 위해서 ABAC(Attributed-Based Access Control) 기반의 접근 통제 기법을 제안하였다[20].

스마트홈의 위협 및 취약점 연구는 지속적으로 진행된 반면, 사용자의 민감한 정보를 다루는 스마트홈을 개인정보 유출 관점에서 연구는 더딘 편이다. 그렇기 때문에 개인정보 유출 관점으로 스마트홈을 다각적으로 연구하는 것이 필요하다.

2.2 위협 모델링

위협 모델링은 임의의 공격자의 관점에서 잠재적 위협(threat)을 식별하고 분석하는 방법론이다. 다시 말해서, 위협 모델링은 한 대상에 대한 위험(risk)을 식별하기 위하여 모델을 통해 추상적으로 표현하는 과정이다. 설계부터 구현 및 운용에 이르는 소프트웨어 개발주기에서 최초 설계 단계부터 위협 모델링을 적용하여 보안 취약점을 사전에 제거하기 위해 사용한다. 위협 모델링은 자산을 식별, 발생 가능한 위협을 발견하고, 위험에 우선순위를 결정하여 위험에 대한 대응책을 결정하는 과정을 수행한다[21].

최근 정보보안 이슈 중 하나로 단순히 정보가 노출되거나 변조되는 것을 막는 것뿐만 아니라 사용자의 개인정보의 유출을 막는 것이 주목받고 있다. 이 시기에 LINDDUN은 위협 모델링을 개인정보(privacy)의 관점에서 실시하는 대표적인 기법이다. LINDDUN은 개인정보 위협의 유형 7가지의 영문 두문자를 통한 약어로 표기된다. 각 요소는 연결성(linkabiltiy), 식별성 (idetifiability), 부인 방지 (non-repudiation), 추적성(detectability), 정보 유출(disclosure of information), 미인지(unawareness), 정책 불이행(non-compliance)이다[22]. LINDDUN의 각 요소에 대한 정의는 Table 2.와 같다.

본 논문에서는 보안요구사항을 도출하여 스마트홈 허브의 평가기준을 제시하기 위하여 다소 변형된 LINDDUN 기법을 사용하였다. 적용한

Table 2. Definitions of LINDDUN element

Element	Definition
Linkability	Being able to sufficiently distinguish whether 2 IOI (Items Of Interest) are linked or not.
Identifiability	Being able to sufficiently identify the subject within a set of subjects
Non-repudiation	Having irrefutable evidence concerning the occurrence or non-occurrence of an event or action
Detectability	An attacker can sufficiently distinguish whether an item of interest (IOI) exists or not
Disclosure of information	Exposing information to someone not authorized to see it
Unawareness	Not understanding the consequences of sharing personal information in the past, present, or future
Non-compliance	Not following the (data protection) legislation, the advertised policies or the existing user consents

LINDDUN의 작업 흐름은 Fig 3.과 같다.

3장에서 각 단계별로 서술할 것으로 3.1장에서는 DFD(Data Flow Diagram)의 작성, 3.2장은 위협과 LINDDUN 요소의 매핑, 3.3장은 위협 트리(threat tree) 작성, 3.4장은 misuse case 작성이다. 상기 4가지 과정은 문제를 식별하는 과정으로 남은 세 단계는 문제를 해결하는 과정이다. 3.5장에서는 위협 우선순위 지정에 대해 논하고, 마지막으로 3.6장에서 완화 전략(mitigation strategy) 및 요구사항 도출에 대해 서술할 것이다.

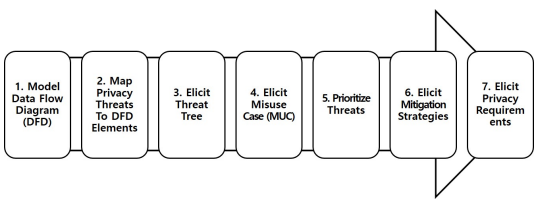

Fig. 3. Work Flow of LINDDUN

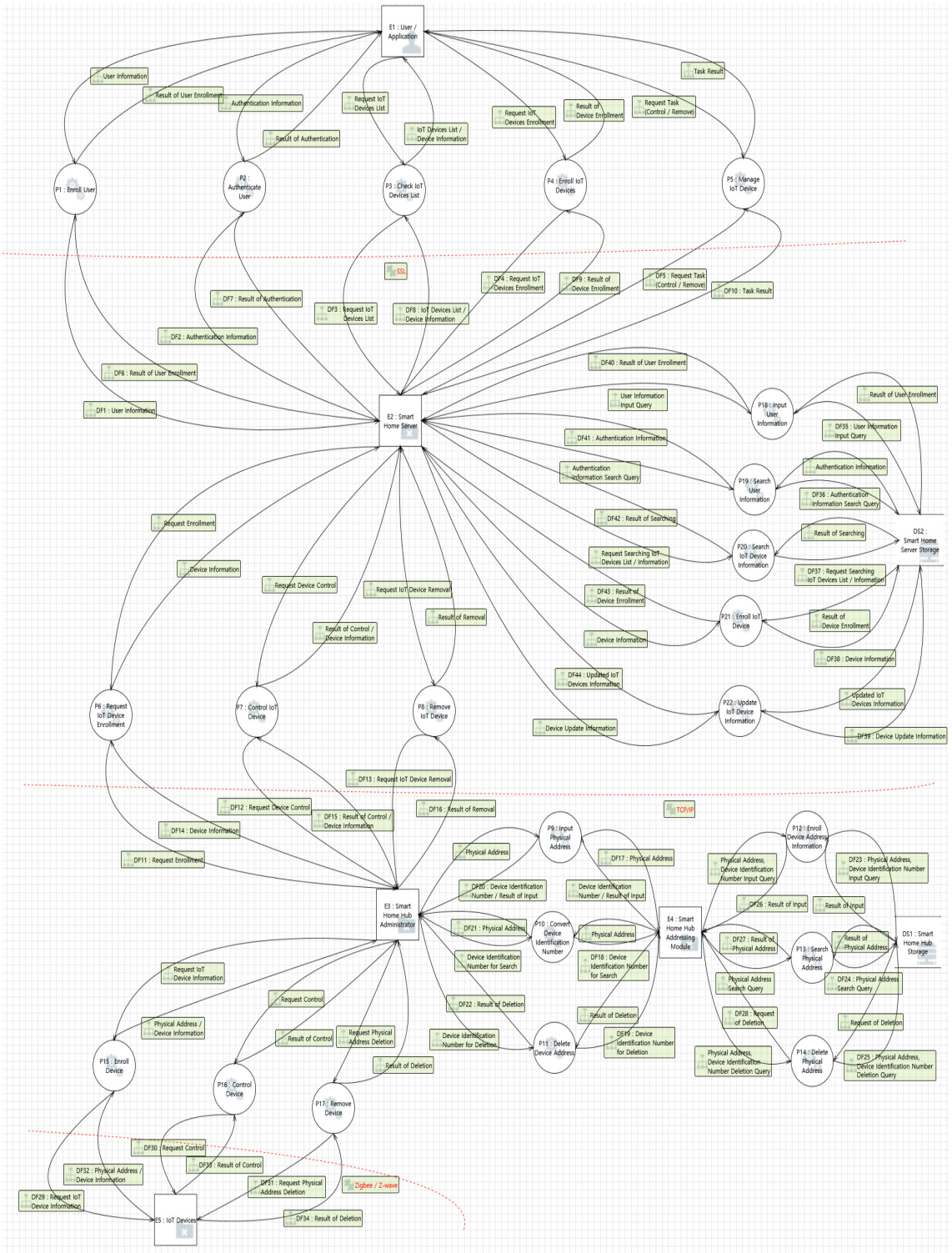

Fig. 4. Data Flow Diagram

III. 스마트홈 허브 위협 모델링

스마트홈 허브는 사용자의 생활환경과 밀접하게 연관되어 있다. 스마트홈이 사용자에게 편의를 제공하는 과정에서 스마트홈 허브를 통한 개인정보 유출이 발생할 수 있다. 그래서 본 논문에서는 LINDDUN을 통해 전체적인 개인정보 관련 위협 모델링을 수행한다. DFD를 작성하고 위협 트리를 통해 misuse case를 분석한다. 그리고 위협의 우선순위를 결정하고 완화 전략을 작성 후, solution을 결정한다.

LINDDUN 실시 간 고려사항은 위협 트리를 가능한 최소로 작성하는 것이다. DFD 요소를 선별하거나 그룹화하여 작성하는 위협 트리를 최소화한다. 이는 중복되는 작업을 제거하고 개인정보에 관련하여 위협을 모델링하기 위해 실시한다[23].

3.1 DFD 작성

DFD는 시스템에서 데이터의 흐름을 보여주기 위하여 작성하는 그림이다. 가시화된 데이터 흐름을 통해서 DFD는 정보 유출과 같은 보안문제가 발생하는 지 여부를 확인시켜 준다. 이러한 DFD의 주요 요소로 외부 객체(external entity), 데이터 저장소(data store), 프로세스(process), 데이터 흐름(data flow)으로 구성된다. 추가적으로 신뢰 경계(trust boundary) 요소가 있다. 신뢰 경계는 데이터 흐름이 발생하는 영역의 신뢰 수준이 변경되는 경계를 가리키는 것으로 해당 경계를 지나가는 데이터 흐름은 보안 위협이 발생할 가능성이 있는 것으로 판단된다.

스마트홈 허브에 대한 DFD는 Fig 4.과 같다. DFD 작성 결과로 5개의 외부 객체와 2개의 데이터 저장소, 22개의 프로세스와 44개의 데이터 흐름을 도출하였다. 신뢰 경계는 총 3개로 사용자와 서버 간의 경계, 서버와 스마트홈 허브의 경계 그리고 스마트홈 허브와 IoT 기기의 경계이다.

사용자 측에는 사용자가 어플리케이션을 통해 실시할 수 있는 작업들이 해당된다. 스마트홈 서버 측에는 사용자 인증을 위한 정보와 스마트홈과 관련된 데이터를 저장하며, 사용한다. 스마트홈 허브 영역은 IoT 기기와 연결하기 위한 물리주소와 논리주소를 치환하는 장비와 저장소가 있으며, 마지막으로 IoT 기기는 해당 기기가 실시하는 작업과 데이터 흐름이 해당된다.

3.2 DFD 요소와 LINDDUN 위협 매핑

DFD에서 작성된 모든 DFD 요소는 LINDDUN의 요소를 매핑하여 위협을 식별한다. Table 3.는 DFD 요소가 LINDDUN의 각 요소에 매핑되는 모든 경우를 나타냈다.

Table 3. Available DFD elements per LINDDUN

	L	I	N	D	D	U	N
External Entity	X	X				X	
Data Store	X	X	X	X	X		X
Process	X	X	X	X	X		X
Data Flow	X	X	X	X	X		X

이 표를 근거로 해당 DFD 요소가 해당 위협에 해당하는지 판단하고 매핑을 실시하였다. 그 결과는 Table 4.와 같다.

Table 4. Smart Home LINDDUN mapping

DFD elememt	ID	L	I	N	D	D	U	N
Data Store	DS1	X	X		X	X		X
	DS2	X	X		X	X		X
External Entity	E1	X	X				X	
	E2	X	X				X	
	E3	X	X				X	
	E4	X					X	
	E5	X					X	
Process	P1	X	X		X	X		X
	P2	X	X			X		X
	P3	X	X		X	X		X
	P4	X			X	X		X
	P5	X			X	X		X
	P6	X			X	X		X
	P7	X			X	X		X
	P8	X			X	X		X
	P9	X				X		X
	P10	X			X	X		X
	P11	X				X		X
	P12	X				X		X
	P13	X			X	X		X
	P14	X				X		X
	P15	X			X	X		X
	P16				X	X		X
	P17	X			X	X		X
	P18	X	X		X	X		X
	P19	X	X			X		X
	P20	X	X		X	X		X
	P21	X			X	X		X
	P22	X			X	X		X

DFD elememt	ID	L	I	N	D	D	U	N
Data Flow	DF1	X	X		X	X		X
	DF2	X	X			X		X
	DF3				X	X		X
	DF4					X		X
	DF5	X			X	X		X
	DF6					X		X
	DF7					X		X
	DF8	X	X		X	X		X
	DF9	X			X	X		X
	DF10	X			X	X		X
	DF11				X	X		X
	DF12	X			X	X		X
	DF13	X			X	X		X
	DF14	X			X	X		X
	DF15	X			X	X		X
	DF16	X			X	X		X
	DF17	X				X		X
	DF18	X				X		X
	DF19	X				X		X
	DF20	X				X		X
	DF21	X				X		X
	DF22					X		X
	DF23	X				X		X
	DF24	X				X		X
	DF25	X				X		X
	DF26	X				X		X
	DF27	X				X		X
	DF28	X				X		X
	DF29					X		X
	DF30				X	X		X
	DF31				X	X		X
	DF32	X			X	X		X
	DF33				X	X		X
	DF34	X			X	X		X
	DF35	X	X		X	X		X
	DF36	X	X			X		X
	DF37	X	X			X		X
	DF38	X			X	X		X
	DF39	X			X	X		X
	DF40					X		X
	DF41					X		X
	DF42	X	X		X	X		X
	DF43					X		X
	DF44	X			X	X		X

3.3 위협 트리 작성

위협 트리는 이전 단계에서 확인한 LINDDUN 위협요소별로 발생할 수 있는 위협을 트리형태로 작성한 결과물을 말한다. 위협 트리 작성 간에 중복되는 결과물이 다수 발생할 수 있다. 불필요한 작업을 줄이기 위해 DFD 요소 간의 그룹화나 트리를 그릴 요소를 선별한다. Table 5.와 Table 6.는 전체 위협 트리 중 data store와 external entity에 대한 위협 트리 중 일부이다.

Table 5. Data Store Threat Tree

Disclosure of Information			
1.			ID_ds
AND	1.1		ID_ds1 : Bypass protection scheme
	OR	1.1.1	ID_ds6 : Canonicalization failure
	OR	1.1.2	ID_ds7 : No protection
	OR	1.1.3	ID_ds8 : Weak permissions
	OR	1.1.4	ID_ds9 : Other consumers
AND	1.2		ID_ds2 : Data intelligible
	OR	1.2.1	ID_ds10 : Unencrypted
	OR	1.2.2	Spoofing external entities
OR	1.3		ID_ds3 : Extra-monitor access
OR	1.4		ID_ds4 : Side channels
OR	1.5		ID_ds5 : Storage management
	OR	1.5.1	ID_ds11 : oCCLUDED DATA
	OR	1.5.2	ID_ds12 : Failure to initialize storage correctly
	OR	1.5.3	ID_ds13 : Failure to clear storage correctly
Non-Compliance			
1.			NC
OR	1.1		NC_1 : Attacker tampering with privacy policies and makes consents inconsistent
	1.1.1		Tampering with policy Data Store
OR	1.2		NC_2 : Incorrect or insufficient privacy policies
	OR	1.2.1	NC_3 : Inconsistent or insufficient policy management
	OR	1.2.2	NC_4 : Insufficient notice

Table 6. External Entity Threat Tree

Unawareness			
1.			U
OR	1.1		U_1 : Providing too much personal data
	OR	1.1.1	U_3 : No-insufficient feedback and awareness tools
	OR	1.1.2	U_4 : No user-friendly privacy support
OR	1.2		U_2 : Unaware of stored data
	OR	1.2.1	U_5 : Unable to review personal information (data accuracy)

3.4 misuse case 작성

misuse case는 각 위협 트리별로 해당 위협이 발생하기 위해 실시하는 행동의 시나리오를 서술한 중간문서를 의미한다. misuse case에는 위협 트리를 통해 위협을 구체화한 이후에 해당 위협이 실제로 어떻게 적용되는지의 시나리오를 작성해야 한다. misuse case 작성 시에는 최소한으로 필요한 정보가 양식 형태로 주어져 있다[24]. 해당 사항을 참고하여 misuse case를 작성한다. Table 7.은 non-compliance에 관한 misuse case를 서술한 Table이다.

Table 7. Misuse Case

Misuse Case	Specification
MUC 26	Tree : NC Summary : The system providing the service does not comply with the security policy or the user agreement, and the user's personal information is leaked. Primary misactor : A competent inner / outer person, Security policy maker, system operator Basic Flow : bf1. Attacker accesses data store related to compliance bf2. Modify the compliance and consent stored in the repository bf3. Modified Compliance Leaks User's Personal Information bf4. Personal information can be leaked if the security policy is determined but wrong or insufficient in the implementation process Result : Security policy errors can affect all non-individual users

3.5 위협 우선순위 지정

LINDDUN 위협모델링 기법에서는 도출되는 위협이 상당히 많은 수가 도출된다. 모든 위협에 대한 대응책을 구비하는 것은 많은 시간과 자본이 소모된다. 노력대비 최대의 성과를 위해 대처할 위협의 우선순위를 선정하여 먼저 처리할 위협을 선택하는 과정을 실시한다.

본 논문에서는 마이크로소프트의 DREAD를 기준으로 우선순위를 결정하였다[25]. DREAD는 측정 대상을 5가지 기준으로 점수를 매기고 그 합계를 통해 우선순위를 결정하는 기법이다. 이름은 각 속성의 두문자의 약어이며 그 요소는 피해 규모(damage), 공격 재생성(reproducibility), 공격 유용성(exploitability), 피해 대상자(affected user), 공격 발견성(discoverability)이다. 각 요소별로 0 ~ 3점의 점수를 매기고 모두 더하여 점수를 산출한다. 산출한 점수가 크면 클수록 높은 우선순위를 설정한다. 본 논문에서 실시한 DREAD의 결과는 Table 8.과 같다.

Table 8. DREAD

Misuse Case	D	R	E	A	D	Score
MUC 01	2	1	2	2	2	9
MUC 02	2	2	1	1	2	8
MUC 03	1	1	2	2	2	8
MUC 04	3	3	1	3	2	12
MUC 05	2	1	2	2	2	9
MUC 06	2	2	2	1	2	9
MUC 07	3	0	2	2	1	8
MUC 08	2	1	2	2	2	9
MUC 09	2	2	1	1	2	8
MUC 10	1	1	2	2	2	8
MUC 11	3	3	1	2	2	11
MUC 12	2	1	2	2	2	9
MUC 13	2	1	2	2	1	8
MUC 14	1	2	2	2	2	9
MUC 15	1	2	3	1	2	9
MUC 16	1	3	3	1	2	10
MUC 17	2	3	2	2	2	11
MUC 18	3	3	1	2	2	11
MUC 19	2	1	2	2	2	9
MUC 20	2	2	1	1	2	8
MUC 21	1	1	2	2	2	8
MUC 22	2	1	2	2	2	9
MUC 23	1	1	1	2	1	6
MUC 24	2	1	1	2	1	7
MUC 25	1	1	1	2	1	6
MUC 26	3	0	0	3	0	6

3.6 완화 전략 및 요구 사항

위협의 우선순위까지 선정하였다면, 해당 위협에 대해 대응하기 위한 완화 전략을 결정한다. 완화 전략은 위험을 최소화하기 위하여 대응하는 조치의 방

향성을 의미한다. 이 과정은 각 misuse case가 어떠한 전략을 통해서 완화될 수 있는지 확인한 후, 해당 시나리오를 대처하기 위한 구체적인 방법론에 대해 확인하는 과정이다. misuse case 별로 도출된 완화 전략을 통해 요구사항을 도출하는 것이 가능하다. 해당 과정에서 요구사항은 어떤 위협에 대응하는지에 대한 명세를 가리킨다. misuse case별 완화 전략과 요구사항의 일부는 Table 9.과 같다.

Table 9. Mitigation Strategy

Misuse Case	Threat Tree Leaf Node	Mitigation Strategy	Requirement to respond
MUC 06	I_e9 : Weak password	Use Pseudonym / Changing Personal Authentication Method	Random login / Password guessing
	I_e10 : Weak username		Random login / Password guessing
	I_e11 : Software token is weakly implemented	Change of personal certification system	APK repacking / Deploying phishing apps
	I_e6 : Untrustworthy receiver	Message integrity vulnerability / No message integrity / Message observation / Channel observation	Message integrity vulnerability / No message integrity / Message observation / Channel observation
	Information Disclosure at Data Flow	Changing the individual certification scheme for anonymit	Message observation / Channel observation
	Identifiability at Data Store		Message observation / Channel observation
		y / Use Pseudonym to improve personal authentication	/ Password guessing / Password stealing
MUC 22	Information Disclosure of Data Flow	Information Hiding	Message observation / Channel observation
	L_g2_df8 : (future) receiver untrusted		Message integrity vulnerability / No message integrity / Message observation / Channel observation
	L_g2_ds4 : Linkability of content		Message observation / Channel observation / Capture control packet
	L_g2_df9 : Based on session ID	Information Hiding / Normalization	Message observation / Channel observation
	L_g2_df10 : Based on behavioral patterns (time, frequency, location)		Message observation / Channel observation / Capture control packet
	L_g2_df11 : Traffic analysis possible		Message observation / Channel observation / Capture control packet
	L_g2_df12 : Passive attacks possible		Message observation / Channel observation

IV. 스마트홈 허브 평가 기준

상기 과정을 통하여 완화 전략과 각 위협에 대한 보안요구사항을 도출하였다. 스마트홈 허브의 평가 기준을 도출하기 위해서 국제표준인 CC(Common Criteria)를 참고하였다[26]. 도출한 보안요구사항과 연관되는 보안기능요구사항과 보증요구사항을 확인하고 이를 통해 스마트홈 허브 평가 기준을 도출한다.

4.1 보안기능요구사항

도출한 보안요구사항을 만족하기 위한 기능을 상세히 명세한 항목이 보안기능요구사항(Security Functional Requirements, SFR)이다[27]. 이러한 SFR은 CC에서 서술하고 있으며, 본 논문에서는 SFR을 통해 스마트홈 허브의 평가 기준을 작성하였다. 위협 모델링을 실시하여 도출한 보안요구사항 별 SFR을 연결한 결과는 Table 10.와 같다.

Table 10. Security Functional Requirements

Requirement to respond	SFR	Description
Account lockout	FIA_AFL.1	When the administrator authentication failure reaches the set number of times (default is 5 times or less), the identification and authentication function should be deactivated for the time set by the authorized administrator (default 5 minutes or more).
	FTA_SSL.1 FTA_SSL.3	If there is no activity for a certain period of time (default 10 minutes or less) after login, you must perform session lock or session termination.
Account identification	FIA_UID.1	Identification and authentication functions should be provided to verify the identity of the administrator.
Basic resource consumption	FPT_FLS.1 FRU_FLT.2	Even if an error occurs due to the consumption of the basic resource, the function operation must be accurately maintained and the state of safety must be maintained.
	FRU_RSA.2	The maximum and minimum quotas for the base resource should be defined so that basic resource consumption does not occur.
Application resource consumption	FPT_FLS.1 FRU_FLT.2	Even if an error occurs due to the consumption of application resources, the function operation must be precisely maintained and maintained in a safe state.
	FRU_RSA.2	You should define maximum and minimum quotas for application resources so that basic resource consumption does not occur.
Network resource consumption	FPT_FLS.1 FRU_FLT.2	Even if an error occurs due to the consumption of network resources, the function operation must be accurately maintained and the state must be maintained in a safe state.
	FRU_RSA.2	The maximum and minimum allocation values for network resources should be defined so that basic resource consumption does

		not occur.
Message integrity vulnerability	FDP_SDI.2	The data stored in the smart home hub and the external IT entity must be provided with integrity, and the integrity check and the corresponding action must be performed.
No message integrity	FDP_SDI.2	The data stored in the smart home hub and the external IT entity must be provided with integrity, and the integrity check and the corresponding action must be performed.
Password stealing	FIA_SOS.1	You must verify that your passwords meet the security criteria (consisting of at least 9 combinations of three or more of the following upper and lower case letters / numbers / special characters).
	FIA_UAU.4	The administrator's password should not be hard-coded into the product or stored in plain text (including simple encoding).
	FIA_UAU.7	In case of identification and authentication failure, feedback on the reason for failure (eg ID error, password error, etc.) should not be provided.
Password guessing	FIA_SOS.1	You must verify that your passwords meet the security criteria (consisting of at least 9 combinations of three or more of the following upper and lower case letters / numbers / special characters).
	FIA_UAU.4	The administrator's password should not be hard-coded into the product or stored in plain text (including simple encoding).
	FIA_UAU.7	In case of identification and authentication failure, feedback on the reason for failure (eg ID error, password error, etc.) should not be provided.
Random login	FIA_SOS.1	You must verify that your passwords meet the security criteria (consisting of at least 9 combinations of three or more of the following upper and lower case letters / numbers / special characters).
	FIA_UAU.7	In case of identification and authentication failure, feedback on the reason for failure (eg ID error, password error, etc.) should not be provided.
APK repacking	FPT_TST.1	You should provide the ability to verify the integrity of the app itself through an app self-test.
	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	Securely generate, distribute and dispose of the encryption key to be used for the app's electronic signature.
	FCS_COP.1	When distributing an app, it must be verified that it is a secure app through digital signature creation and verification.
Deploying phishing	FPT_TST.1	You should provide the ability to verify

apps		the integrity of the app itself through an app self-test.
	FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	Securely generate, distribute and dispose of the encryption key to be used for the app's electronic signature.
	FCS_COP.1	When distributing an app, it must be verified that it is a secure app through digital signature creation and verification.
Data collection in plain text	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Session acquisition	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Message observation	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Channel observation	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Memory reuse	FPT_RPL.1	When smart home hubs reuse memory, they should detect replay attacks and take action.
Metadata	FDP_RIP.1	It should not be able to acquire the basic information existing in the store of the smart home hub and protect the residual information.
RF signal capture	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
RF signal modulation	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Control packet capture	FPT_ITC.1 FPT_ITT.1	Confidentiality and integrity must be ensured through encryption of transport data (security policies, control commands, audit data, etc.) between physically separated product components.
Elevation of privilege through system vulnerability	FDP_ACC.2	Unauthorized privilege elevation should not occur through full access control between subject and object.
	FDP_ACF.1	The access control

		function should be performed based on the security attributes so that unauthorized privilege elevation should not occur.

4.2 보증요구사항

보증요구사항(Security Assurance Requirements, SAR)은 평가 대상의 보안기능이 보안목적 달성 여부를 확인하기 위하여 최소한으로 필요한 요구사항을 서술한다. CCRA 협정서 개정으로 2015년 이후 평가보증등급(EAL) 기반 상호인정 방식에서 공동보호프로파일(cPP) 기반 상호인정으로 변경되는 것으로 인해 상호인정을 하는 수준이 EAL4에서 EAL2로 변경된다. 따라서 본 논문에서는 보증등급을 EAL2로 지정하고, 그에 따른 보증요구사항을 도출하였다. Table 11.은 스마트홈 허브에 대한 보증요구사항을 나타낸다[28].

Table 11. Security Assurance Requirements

Class	Component	Description	Document
ADV	ADV_ARC.1	Security architecture description	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification	Functional specification
	ADV_TDS.1	Basic design	TOE design documentation
AGD	AGD_OPE.1	Operational user guidance	Manual
	AGD_PRE.1	Preparative procedures	
ALC	ALC_CMC.2	Use of a CM system	CM documentation
	ALC_CMS.2	Parts of the TOE CM coverage	
	ALC_DEL.1	Delivery procedures	Delivery document
ASE	ASE_CCL.1	Conformance claims	security objectives
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
ATE	ATE_COV.1	Evidence of coverage	Test documentation
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing - sample	
AVA	AVA_VAN.2	Vulnerability analysis	Vulnerability analysis documentation

Table 10.와 Table 11.의 SFR과 SAR을 평가기준으로 해당 스마트홈이 SFR을 만족하는 기능을 포함하고 있는지와 해당 기능을 SAR에 만족하는 문서를 통해 증명하는지를 평가한다.

V. 결론 및 향후과제

스마트홈은 개선된 편의 기능을 제공하기 때문에 그 시장규모가 확대되고 있는 추세이다. 스마트홈은 IoT 기기들을 통해 사용자의 정보를 수집하고 활용한다. 이 과정에서 스마트홈 허브는 기기들에서 정보들을 송, 수신하는 기능을 수행하고 있기 때문에 사용자 정보 유출을 통해 개인정보가 침해될 수 있다. 그래서 본 논문은 스마트홈 허브에 대해 개인정보 침해 관점에서 연구를 실시하였다.

기존의 국내 위협 모델링 연구는 마이크로소프트

의 STRIDE를 통하여 진행되었다. 본 논문은 개인정보보호 측면에 집중하여 위협을 분석하고 요구사항을 도출하고자 LINDDUN 위협 모델링 기법을 국내에서 최초로 사용하였다.

또한 최근 업계에서 시판되고 있는 스마트홈 허브에 대한 공통적인 표준이나 요구사항에 대한 연구가 미비하여 보안위협에 대한 체계적인 대비가 제한된다. 따라서 본 논문은 분석한 보안요구사항을 통해 보안기능요구사항과 보증요구사항을 도출하여 스마트홈 허브의 평가 기준을 제시하는 것을 통하여 스마트홈 허브 개발에 대한 공통적인 기준을 제안하고자 하였다.

본 논문의 평가 기준은 공통평가기준의 EAL2 등급을 만족시키는 요구사항들을 토대로 작성되었다. 따라서 제작 단계에서 본 평가 기준을 참고로 하여 제작을 실시하는 경우 국제표준에 따르는 보안인증을 위하여 필요한 작업을 줄일 수 있을 것으로 기대한다. 향후 과제로 작성한 평가 기준을 다양한 스마트홈 허브에 대해 평가를 실시하고 미비점을 보완하여 평가 기준의 실효성을 개선하는 것이 향후 과제로 남아있다.

References

[1] National Information Sociery Agency, "Home IoT Market Analysis and Implications," [Internet], Oct. 2016. http://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=39485&bcIdx=18078&parentSeq=18078

[2] WikiLeaks, "Weeping Angel (Extending) Engineering Notes," [Internet], June 2014. https://wikileaks.org/ciav7p1/cms/page_12353643.html

[3] Anne Bucher, "SAMSUNG CLASS ACTION LAWSUIT SAYS SMART TVS SPY ON CONSUMERS," TOP CLASS ACTIONS, Mar. 2017. https://topclassactions.com/lawsuit-settlements/lawsuit-news/543320-samsung-class-action-lawsuit-says-smart-tvs-spy-consumers/

[4] Christopher Burgess, "How Easy Is It to Hack Your Baby's Monitor? Very Easy!," Huffingtonpost, Sep. 2015. https://www.huffingtonpost.com/entry/how-easy-is-it-to-hack-your_b_8173274.html

[5] Huffingtonpost, "They take pictures with a peek at their private lives... 30 Prosecutions for hacked IP Camera," Huffington post, Nov. 2017. http://www.huffingtonpost.kr/2017/11/01/story_n_18443668.html

[6] Ministry of the Interior and Safety, "Personal Information Protection Act," Act No. 14107, July 2017.

[7] Dae-man Han, Jae-hyun Lim, "Smart Home Energy Management System using IEEE 802.15.4 and Zigbee", IEEE Transactions on Consumer Electronics, vol. 56, no. 3, pp. 1403-1410, Oct. 2010.

[8] Rosslin John Robles, Tai-hoon Kim, "Application, Systems and Methods in Smart Home Technology: A Review", International Journal of Advanced Science and Technology, vol.15, pp. 37-48, Feb. 2010.

[9] Smart Home USA, "WHAT IS A SMART HOME?," [Internet], https://www.smarthomeusa.com/smarthome/

[10] Oxford University Press, "Definition of smart home," [Internet], https://en.oxforddictionaries.com/definition/smart_home

[11] H. Strese, U. Seidel, T. Knape, and A. Botthof, "Smart Home in deutschland," Institut für Innovation und Technik (iit), pp. 8-11, May 2010.

[12] Michael Schiefer, "Smart Home definition and security Threats," 2015 9th IEEE International Conference on IT Security Incident Management & IT Forensics(IMF), pp. 114-118, May 2015.

[13] A. Tekeo˘glu, A.S. Tosun, " Investigating Security and Privacy of a Cloud-Based Wireless IP Camera : NetCam," 2015 24th IEEE International Conference on Computer Communication and Networks (ICCCN), pp. 1-6, Aug. 2015.

[14] Tobias Zillner, Sebastian Strobl, "Zigbee

Exploited : The Good, the Bad, and the Ugly," [Internet], Aug. 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf

[15] Joseph Hall, "Breaking Bulbs Briskly by Bogus Broadcasts," [Internet], Feb. 2016. https://www.youtube.com/watch?v=EDzxMfx1v5Q

[16] Billy Rios, Jonathan Butts, "WHEN IOT ATTACKS : UNDERSTANDING THE SAFETY RISKS ASSOCIATED WITH CONNECTED DEVICES," [Internet], July 2017. https://www.blackhat.com/docs/us-17/wednesday/us-17-Rios-When-IoT-Attacks-Understanding-The-Safety-Risks-Associated-With-Connected-Devices.pdf

[17] Thomas Branstetter, "(IN)SECURITY IN BUILDING AUTOMATION : HOW TO CREATE DARK BUILDINGS WITH LIGHT SPEED," July 2017. https://www.blackhat.com/docs/us-17/wednesday/us-17-Brandstetter-insecurity-In-Building-Automation-How-To-Create-Dark-Buildings-With-Light-Speed.pdf

[18] Dimitris Geneiatakis, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini, "Security and Privacy Issues for an IoT based Smart Home," 2017 40th IEEE Internatioal Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 1292-1297, May 2017.

[19] Kristian Beckers, "Comparing Privacy Requirements Engineering Approaches," 2012 7th IEEE International Conference on Availability, Reliability and Security(ARES), pp. 574-581, Aug. 2012.

[20] Annanda Thavymony Rath, Jean-Noel Colin, "Strengthening Access Control in case of Compromised Accounts in Smart Home," 2017 IEEE Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1-8, Oct. 2017.

[21] Adam Shostack, Threat Modeling : Designing for Security, John Wiley & Sons, 2014.

[22] Kim Wults, Wouter Joosen, "LINDDUN privacy threat modeling : a tutorial," CW685, Department of Computer Science, KU Leuven, July 2015.

[23] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen, "A privacy threat analysis framework : supporting the elicitation and fulfillment of privacy requirements," Requirement Engineering - Special Issue on Digital privacy : theory, policies and technologies, vol. 16, no. 2, pp. 3-32, Mar. 2011.

[24] Kim Wults, Riccardo Scandariato, and Wouter Joosen, "LINDDUN privacy threat tree catalog," CW675, Department of Computer Science, KU Leuven, Sep. 2014.

[25] Microsoft, "Chapter 3. Threat Modeling," [Internet], https://msdn.microsoft.com/en-us/library/ff648644.aspx, June 2003.

[26] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model," CCMB-2017-04-001, Apr. 2017.

[27] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 2 : Security functional components," CCMB-2017-04-002, Apr. 2017.

[28] Common Criteria Recognition Arrangement, "Common Criteria for Information Technology Security Evaluation Part 3 : Security assurance components," CCMB-2017-04-003, Apr. 2017.

〈저자소개〉

박 재 현 (Jae-Hyeon Park) 학생회원
2014년 8월: 홍익대학교 컴퓨터공학과 공학사
2017년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 보안성 평가/인증, 위협 모델링

강 수 영 (Soo-Young Kang) 학생회원
2006년 2월: 순천향대학교 컴퓨터공학부 공학사
2008년 2월: 순천향대학교 컴퓨터공학부 공학석사
2008년 5월~2010년 10월: 한국인터넷진흥원(KISA) 연구원
2010년 10월~2014년 10월: 안랩(Ahnlab) 주임연구원
2013년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 보안성 평가/인증, 위협 모델링, 소프트웨어 보안

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2017년~현재: 고려대학교 사이버무기시험평가연구센터(CW-TEC) 부센터장
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: (사)화이트해커연합 HARU 및 국제해킹대회 SECUINSIDE 설립자 및 이사
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 국방보안연구소 정보보호분야 자문위원
2017년~현재: 여신금융협회 신용카드 단말기 시험 인증위원회 위원
〈관심분야〉 보안공학 및 SDL, 위협 리스크 모델링, 보안성 평가/인증, 암호학, Usable Security