https://doi.org/10.33778/kcsa.2020.20.4.169

‘스마트홈 서비스’의 보안취약요인에 관한 연구★

전 정 훈*

요 약

최근 스마트 기기를 이용한 다양한 서비스들이 사용되는 시대를 소위 “스마트 시대”라 부르기도 한다. 이러한 가운데 스마트홈 서비스는 주거 환경과 문화에 큰 변화를 가져왔을 뿐만 아니라, 매우 빠르게 진화해 가고 있다. 그리고 스마트홈 서비스는 일반 가정에서 다양한 전자제품들 간의 통신을 통해 사용자에게 보다 편리한 서비스를 제공해주며, 향후 밝은 미래를 보이고 있다. 특히 ‘스마트홈 서비스’는 각종 기기들 간의 연결에 있어, IoT 기술과 유▪무선 통신을 기반으로 결합된 다양한 서비스들을 제공하고 있다. 그러나 이와 같은 ‘스마트홈 서비스’는 사물 인터넷과 유▪무선 통신기술 같은 기반 기술들의 보안 취약점들을 상속하고 있어, 개인정보의 유출이나 사생활침해 등으로 이어지는 사고가 지속적으로 발생하고 있다. 이에 기반기술의 취약요인에 대해 예방과 대응방안의 마련이 필요한 상황이다. 따라서 본 논문에서는 스마트홈 서비스의 다양한 보안취약요인들을 알아봄으로써, 향후 응용기술의 개발 및 대응기술의 기초 자료로 활용될 것으로 기대한다.

A Study on Vulnerability Factors of The Smart Home Service

Jeon Jeong Hoon*

ABSTRACT

Recently, the era in which various services using smart devices are used is sometimes referred to as the so-called “smart era”. Among these, Smart Home Service′ have not only brought about significant changes in the residential environment and culture, but are evolving very rapidly. and The ‘Smart Home Service′ provides more convenient services to users through communication between various electronic products in general homes, and has a bright future in the future. In particular,′Smart Home Service′ provides various services combined based on IoT(Internet of Things) technology and wired/wireless communication in connection between various devices. However, such a “smart home service” inherits the security vulnerabilities of the underlying technologies such as the Internet of Things and wired and wireless communication technologies, and accidents that lead to the leakage of personal information and invasion of privacy continue to occur. So, it is necessary to prepare a countermeasure and prevention against the weak factors of the underlying technologies. Therefore, this paper is expected to be used as basic data for future application technology development and countermeasure technology by examining various security vulnerability factors of ′Smart Home Service′.

Key words : ‘Smart Home Service’, Wireless Network, IoT(Internet of Things), AI(Artificial Intelligence), Vulnerability Factors

접수일(2020년 9월 18일), 수정일(1차: 2020년 10월 14일), 게재확정일(2020년 10월 23일)

★ 본 논문은 2019년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교/컴퓨터학과(주저자)

1. 서 론

최근 스마트 홈(smart home) 기술은 4차 산업혁명 기술들과 함께 진화해 가고 있으며, 사물인터넷(internet of things)과 유·무선통신 기술을 기반으로 클라우드(cloud)나 SNS(Social Network Service)와 같은 서비스들과 연계해 다양한 서비스들을 제공하고 있다. 스마트홈 서비스는 대부분 무선통신을 기반으로 서비스 영역의 확장이 용이하고, 높은 편의성 제공이 특징이다. 그리고 다양한 기기들 간의 연결을 기반으로 사용자가 원하는 정보들을 제공받을 수 있도록 하고 있다. 스마트폰은 컨트롤하는 디바이스로서 스마트홈 서비스를 일상생활 속 깊숙이 자리 잡을 수 있도록 견인차 역할을 했다고 해도 과언이 아니다. 또한 스마트홈 서비스는 기존의 주거문화에 있어 생활 패턴을 크게 변화시킨 기술이라고도 할 수 있다. 앞으로 스마트폰을 이용한 다양한 스마트홈 서비스가 개발될 것으로 예상되며, 더욱 확산을 가속화할 것으로 전망된다. 그러나 스마트홈 서비스는 보안에 취약한 단점을 갖고 있다. 사물인터넷과 유·무선 통신과 같은 기술들을 기반하고 있어, 기존의 취약점들을 그대로 상속하고 있기 때문이다. 이러한 이유로 보안 취약성과 문제점들이 계속해서 발생하고 있으며, 보안에 대한 요인분석과 대응기술의 마련이 필요한 상황이다.

따라서 본 논문은 스마트홈 서비스가 일상생활 속 일부로 자리잡아가고 있는 상황에서 함께 진화하고 있는 보안취약요인들을 알아봄으로써, 향후 스마트홈 서비스의 개발뿐만 아니라 대응기술의 개발에 부합하는 기초 연구자료로 활용될 수 있을 것으로 기대한다. 본고의 논리적 구성을 위해 2장은 스마트홈 서비스의 기술동향에 대해 알아보고, 3장은 취약점 및 사례들을 알아본다. 그리고 4장의 보안취약요인 및 대응방안과 마지막 5장의 결론 부분으로 이글을 마치도록 한다.

2. 관련연구

2.1 기술동향

스마트홈 서비스는 기존의 '홈 오토메이션(home automation)'이나 '유비쿼터스 아파트' 기술에 스마트 기기를 이용한 인터넷 연결과 4차 산업혁명기술들인 사물인터넷이나 센서 네트워크, 클라우드, 빅 데이터(big data), 인공 지능(artificial intelligence)과 함께 진화해 가고 있다. 이러한 기술들의 진화는 건설사와 통신사 그리고 가전 제조사 등이 주체가 되어 스마트홈 서비스 관련 비즈니스 모델들을 새롭게 개발 및 전개하고 있다[1]. 스마트홈 서비스는 얼마 전까지만 해도 스마트폰을 이용한 단순 제어서비스에만 그쳤으나, 점차 음성인식을 이용한 인공지능 기술과의 결합 형태로도 진화해 가고 있다. 이와 같은 변화에 대해 [2]는 점차 인구감소와 더불어 1인 가구에 맞는 서비스들로 변화해 갈 것임을 전망하고 있다. 또한 스마트 하우징 플랫폼 및 주거 서비스에 대한 기술개발도 이미 진행중에 있으며, 기반기술로 사물 인터넷과 무선통신, 센서 네트워크, 인공지능 등에 대한 지원이 활발히 진행되고 있다[3]. 특히, 인공 지능은 다양한 분야에서 응용범위를 넓혀가고 있으며, 프라이버시의 비식별화 기술과도 더불어 발전해 가고 있다.

(그림 1) A.IoT 플랫폼'의 개념도/삼성물산 제공[4]

(그림 1)은 국내 기업에서 제공할 사물인터넷과 인공 지능이 결합한 스마트홈 플랫폼의 개념도로서, 스마트홈 서비스가 음성 인식과 웨어러블, 홈패드, 스마트폰 등의 간단한 통제장치들을 이용해 조작만으로 서비스들을 이용할 수 있어, 향후 활용도는 더욱 높아질 것로 전망되며, 점차 주거공간과 편의시설을 대상으로 사물인터넷과 인공 지능, 플랫폼 등이 결합한 형태로 진화해 갈 것으로 기대하고 있다[4]. 여기서 스마트홈 서비스의 시장동향에 대해 [5]를 살펴보면, 내비건트 리서치(Navigant Research)에서 실시한 조사

<표 1> 스마트홈 산업 부문별 국내시장 전망[7]

구분	스마트 융합가전		스마트TV & 홈엔터테인먼트		스마트홈 시큐리티		스마트홈 오토메이션		스마트그린홈	
	시장규모(억원)	성장률	시장규모(억원)	성장률	시장규모(억원)	성장률	시장규모(억원)	성장률	시장규모(억원)	성장률
2017년	70,121		62,839		7,818		6,587		2.248	
2018년	74,012	5.5%	77,945	24.0%	8,248	5.5%	6,817	3.50%	3.164	40.8%
2019년	77,712	5.0%	92,133	18.2%	9,114	10.5%	7,124	4.5%	3.381	6.9%
2020년	81,539	4.9%	106,933	16.1%	9,689	6.3%	7,380	3.6%	3.770	11.5%
2021년	85,335	4.7%	121,580	13.7%	10,338	6.7%	7,648	3.6%	4.007	6.3%
2022년	89,130	4.4%	136,227	12.0%	10,986	6.3%	7,917	3.5%	4.201	4.8%
2023년	92,926	4.3%	150,874	10.8%	11,634	5.9%	8,186	3.4%	4.365	3.9%
2024년	96,721	4.1%	165,521	9.7%	12,282	5.6%	8,454	3.3%	4.507	3.3%
2025년	100,517	3.9%	180,168	8.8%	12,930	5.3%	8,723	3.2%	4.632	2.8%
CAGR (17-25)		4.6%		14.01%		6.5%		3.6%		9.5%

결과, 전 세계 스마트홈 플랫폼의 연간 매출액은 2019년 약 32억 달러에서 2028년 약143억 달러로 18.1%의 연평균 성장률(CAGR)을 보일 것으로 전망하였다. 그리고 스마트홈 분야에서 2020년 한 해 동안, 주목받을 만한 여섯 가지 동향에 대해 다음과 같이 발표하였다. 첫 번째로 '스마트'에서 '인텔리전트'로 진화와 두 번째 '다중 프로토콜 연결'로의 가속화, 세 번째 사용자 경험의 향상, 네 번째는 인공 지능 사용자의 증가, 다섯 번째 디바이스 제조회사의 차별화된 지원, 마지막 여섯 번째는 갈수록 높아져 가는 보안성의 중요성에 대해 언급하였다. 이는, 스마트홈 서비스의 인공지능화가 불가피하며, 함께 보안이 지원되어야 함을 알 수 있다.

한편 글로벌 시장조사 업체인 가트너에 따르면, 전 세계 스마트홈 서비스 시장은 2025년까지 70억 달러를 넘길 것으로 예상하였으며, 앞으로도 지속적인 성장을 전망하였다[6]. 반면, 국내 스마트홈 서비스 산업에 대해서는 <표 1>을 통해 부문별 성장세를 확인해 볼 수 있는데, 국내 일반 소비자를 대상으로 한 조사결과에 따르면, 스마트홈에 대한 인지도는 약 75.2%로 높은 편이지만, 스마트홈 제품 및 서비스 이용률은 약 68%로 인지도에 비해 활성화가 다소 저조한 것으로 분석되었다. 이러한 원인으로 [7]에서는 AI 스피커와 사물인터넷 기기 등 보급이 확산됨에 따라 스마트홈에 대한 인지도는 높았지만, 서비스의 부족이 원인인 것으로 파악하였다. 이에 앞으로 다양한 서비스 개발이 병행되어야 할 것이다.

2.2 국내 동향

국내 스마트홈 서비스는 사물인터넷 기술을 기반으로 하고 있으며, 사물인터넷 기술은 통신사를 기반으로 잠금장치나 조명, 가전 등을 인터넷과 연결한 다양한 상품들을 출시하고 있다. 그리고 인공지능 서비스의 일환으로 인공지능 스피커를 통해 사람의 음성으로 사물인터넷 기기들을 제어하고 있다[8][9].

최근에는 코로나 시대를 겨냥해 바이러스를 제거해주는 첨단 제균 서비스도 속속 선보이고 있다. 이와 유사하게 국내 건설회사 중에 한 기업은 바이러스 살균·환기시스템인 'H클린알파 2.0'을 도입하여, 초미세먼지를 줄여주면서 바이러스·박테리아·곰팡이 등을 동시에 제거하는 환기 시스템 서비스를 선보이고 있다[10]. 그리고 스마트폰에 이어 스마트워치나 스마트밴드와 같은 휴대하기 편리한 기기들을 통해 무선통신을 기반 한, 인터넷 통신 및 기기 간 통신으로 정보들을 교환함으로써 스마트홈, 핼스케어, 스마트팜, 스마트팩토리 등 다양한 서비스들을 제공하고 있다. 이러한 스마트홈 기술들의 생태계 및 진화단계에 대해 <표 3>은 스마트홈 구성요소 6가지를 나열하고 있다[11].

2.3 스마트홈의 기반기술

<표 2> 출처: 산업통상자원부, '2017-2018 산업통상자원백서', NICE평가정보(주) 재구성[11]

구분	스마트홈 1.0	스마트홈 2.0	스마트홈 3.0	스마트홈 4.0
개념	홈 오토메이션	홈 네트워크	IoT 홈	커넥티드 홈
통신방식	유선	유선	무선	무선
제어기기	스마트TV	월패드	IoT 가전	AI가전, 로봇 등
주요기능	VOD 서비스	가정 내 제어	외부 원격 제어, 모니터링	자율동작, 개인 맞춤, 플랫폼 간 연동
관련업종	가전사	가전사, 건설사, 홈넷사	가전사, 건설사, 통신사	SW,센서, 자동차, 의료, 에너지등

스마트홈을 구성하는 기술로 [11]의 <표 3>은 통신과 디바이스, 사물인터넷, 플랫폼, 콘트롤 디스플레이, 콘텐츠의 6가지 기술들을 구분하고 있다. 각각의 특징들을 살펴보면, 통신은 100Mbps에서 Giga의 속도로 향상됨에 따라, 무선통신의 경우, 점차 사용률이 증가하고 있으며, 스마트 TV와 같은 일상생활 기기들은 기기 간 또는 플랫폼 간 연동이 가능해졌다. 그리고 '컨트롤 디스플레이'는 스마트폰에서 '모션 인식'이나 '웨어러블' 형태로 발전하였으며, 가전제품과 청소 로봇 등은 AI가 결합된 서비스로 체계로 한층 기능이 업그레이드되었다. 마지막으로 콘텐츠는 분리와 통합 과정을 거쳐 세분화하는 형태로 발전하고 있으며, 이러한 배경에는 사물인터넷의 대량의 정보 생산과 활용이라는 변화가 전제되어 있다. 향후 스마트홈은 사물인터넷을 기반 한 인공지능기술의 활용도를 높여 응용분야를 넓혀갈 것으로 기대하고 있다[11]. 결과적으로 <표 2>와 <표 3>을 통해, 사물인터넷 기술이 스마트홈 서비스를 구성하는 핵심 기반 기술들임을 알 수 있다.

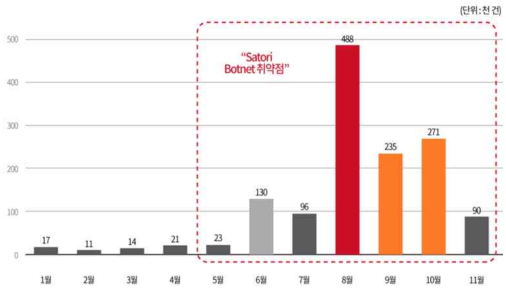
3. 취약점 및 사례

3.1 취약점

스마트홈 서비스는 다양한 관점에서 취약요인들을 구분해 볼 수 있다. [12]는 스마트홈 애플리케이션의 보안위협들로 위조된 디바이스 ID와 데이터 가로채기, 데이터 변조, 멀웨어(malware)의 감염 등 공격기법들을 언급하고 있다. 그러나 스마트홈 서비스가 앞서 언급한 기반기술들의 종합체라는 점을 고려해 볼 때, 기존 기술의 보안 취약점들을 그대로 상속함으로써, 기반 기술이 갖고 있는 취약요인들을 통해 스마트홈 서비스의 취약요인들을 구분해 볼 수 있다. 유·무선 통신은 전송데이터의 가로채기(intercept)와 주파수 간섭 공격에 취약하며, 사물인터넷의 경우에는 유·무선 통신 기술의 취약점을 포함하고 있을 뿐만 아니라 이를 이용해 기기에 대한 공격과 기기를 이용한 공격 모두에 취약하다.

3.2 사례

스마트홈 서비스의 기반 기술로는 앞선 2.3절에서와 같이 사물인터넷기기와 유·무선 통신으로 열거해 볼 수 있다. 그러나 사물인터넷기기들은 무선통신을 기본적으로 사용하기 때문에 별도의 구분 없이, 사물인터넷만의 보안취약점으로 스마트홈 서비스의 취약요인들을 구분해 볼 수 있다. 사물인터넷기기는 종류 및 통신환경에 따라 원인분석 및 역추적이 어렵고, 다양한 공격이 가능하다. 이에 대해서는 [13]의 사고사례를 통해 확인해 볼 수 있다.



Target Port	
37215	29%
52869	28%
23(TELNET)	22%
22(SSH)	11%
Other	5%

IoT Malware	
Satori	53%
Mirai	26%
Hajime	6%
Amnesia	6%
Bricker	6%
Other	3%

(그림 2) 사물인터넷 기기에 대한 주요 공격 통계 및 발생한 사고[14]

<표 3> 출처: 디지에코, '스마트홈(홈IoT) 생태계 6대 구성요소', NICE평가정보(주) 재구성[11]

구분	가전/비가전 디바이스 분리	가전/비가전 디바이스 통합	차세대 기술/디바이스 및 AI컨트롤 도입	스마트홈 디바이스 및 AI컨트롤 최적화
	도입기	성장기	성숙초기	성숙후기
유무선 네트워크 속도	100Mbps/4G	100Mbps/4G	유무선 GiGA	GiGA/5G
스마트디바이스	가전/비가전(일상기기)	가전/비가전(일상기기)	일상기기/차세대 기술	일상기기/차세대 기술
IoT 표준화	개별사업자별 표준화	컨소시엄별 표준화	다 표준지원	지배적사업자표준화
플랫폼	개별사업자 단말/OS	단말/OS 통합화	지배적사업자 통합화	지배사업자 통제력강화
컨트롤 디스플레이	스마트폰/ TV	스마트폰/ TV	웨어러블	웨어러블/음성/ 모션인식
콘텐츠	가전/비가전 분리	가전/비가전통합	차세대 콘텐츠/세분화	응용 콘텐츠/세분화

세계적인 백신회사인 '카스퍼스키 랩'의 보도 자료에 따르면, 주유소 펌프들은 주인이 변경하지 못하는 비밀번호로 인터넷을 연결하고 있어, 공격자는 비밀번호를 이용해 펌프 조작과 신용카드 정보를 훔치거나 펌프탱크의 압력과 온도를 조절해 폭발의 위험성을 포함하고 있다. 그리고 병원의 경우에도 사물인터넷 기기를 선호하고 있어, 의료기기가 아닌 전자기기도 연결하여 백도어를 만들 수 있었으며, 전등조절시스템, 에어컨, 프린터 등이 보안에 취약함을 연구소는 언급하였다[13].

<표 4> OWASP 선정 IoT의 10대 취약점[15]

취약점	내용
1	쉬운 암호, 유추할 수 있는 암호 또는 하드코딩된 암호
2	안전하지 않은 네트워크 서비스
3	안전하지 않은 생태계 인터페이스
4	안전한 업데이트 메커니즘의 부재
5	안전하지 않거나 오래된 구성요소 사용
6	불충분한 개인정보 보호
7	안전하지 않은 데이터 전송 및 저장
8	디바이스 관리의 부재
9	안전하지 않은 기본 설정
10	물리적 보호 수단의 부재

이밖에도 교통 관제시스템과 홍수 관리시스템, 가로등 관리시스템을 공격하여 통제 불능으로 만들었으며, 아파트는 중앙난방과 온수시스템을 포함한 자동 온도조절시스템에 디도스(DDoS) 공격을 감행한바 있다. 그리고 '클라우드 펫'은 온라인 앱과 연동되어 말할 수 있는 IoT 스마트 토이의 일종으로 해커들은 이를 이용해 사용자의 이 메일 주소, 비밀번호, 음성녹음이 있는 '클라우드 펫'의 데이터베이스를 악용해 80만 명이 넘는 사용자에게 금전을 요구하는 사고가 발생하기도 하였다.

<표 5> 5G로 인한 IoT 보안의 7가지 변화[16]

	변화 내용
1	5G 네트워크 트래픽 암호화 및 보호
2	취약한 디바이스 보호 및 격리
3	더 큰 규모의 DDoS 공격에 대비
4	IPv6으로 전환할 경우 사설 인터넷 주소가 공용 주소로 바뀔 수 있음
5	엣지 컴퓨팅으로 인해 늘어나는 공격 표면
6	신규 IoT 업체, 보안이 아닌 시장 선점에 집중
7	누군가 IoT 보안을 책임

또한 이와 같은 공격에 사용되는 유형 및 포트에 대해서는 (그림 2)의 사물인터넷 기기의 통계자료를 통해 공격에 악용되는 공격 포트(37215, 52869)나 공격용 봇(bot)프로그램(사토리(satori), 미라이(mirai) 등)들을 알 수 있다[13]. 그리고 (그림 3)은 2018년 사물인터넷기기에 대한 주요공격 및 사고별 통계자료로서, 사물인터넷 기기에 의한 공격뿐만 아니라, 기기에 대한 공격이 증가하고 있음을 알 수 있다. 자료에 따르면, 공격의 80%는 사토리(satori)나 미라이(mirai)이와 같은 악성코드에 의해 CCTV나 스마트 장남감, IP 카메라, 디지털 도어락 등의 공격사례들을 통해 사생활 침해가 증가하고 있다. 이와 같은 공격들은 스마트홈 기기인 사물인터넷 기기들을 임의로 조작할 수 있다는 점을 시사하고 있으며[14], 다양한 취약점들이

(그림 3) IoT 기기의 해킹을 통한 사생활 침해 사례[14]

존재함을 알 수 있다. 이러한 취약점들에 대해서는 <표 4>의 OWASP가 선정한 사물인터넷 취약점 10가지를 통해 정리해 볼 수 있다[15]. 또한 <표 5>의 5G로 인한 사물인터넷 보안의 변화들을 통해 향후 사물인터넷의 취약부분을 예상해볼 수 있다[16].

4. 보안취약요인 및 대응방안

이장에서는 기존에 알려진 취약점들 이외의 보안취약요인들을 알아본다.

4.1 보안취약요인

4.1.1 기기 호환 및 보안성에 따른 요인

<표 6> 사물인터넷 기기의 취약요인[15][16]

구분	취약요인	공격 유형
통신	무선 네트워크의 트래픽	가로채기, 방해
	유무선 주소 공격	위•변조
	잘못된 명령	위•변조
	무선 주파수 간섭	방해
	고속화에 따른 데이터 증가	방해
디바이스	디바이스의 관리 권한	위•변조
	펌 업그레이드	관리 공격
	디바이스 간 통신	가로채기 위•변조
	디바이스 보호 수단 부재	관리 공격
	디바이스 인증 등록 취약	위•변조 관리 공격
	디바이스 경쟁개발 따른 호환	관리 공격
	디바이스 통신 영역	관리 공격 방해

스마트홈은 다양한 사물인터넷기기들로 구성되어 있다. 예를 들어 냉장고나 세탁기와 같은 생활가전이나 노트북과 프린터 같은 컴퓨터의 주변기기, 스마트폰과 같은 통신기기, 생활에 필요한 운동기기 및 헬스기기 등이 있다. 이러한 기기들은 [1]에서처럼 제조사나 건설사, 통신사에 의존적이기 때문에 데이터의 활용 및 기기 호환, 보안기술 적용 등에 따른 다양한 문제점들이 취약요인으로 작용하게 된다. 3.2절의 취약사례들처럼 제조사가 다른 기기들의 구성은 2.1절에서처럼 특정회사의 제품만으로 구성된 경우의 보안성과 대비된다. 반면, 기기 간의 호환성은 효율적인 보안 및 관리에 필수불가결한 요소이기는 하나, 또 다른 위장공격에 악용될 수 있으며, <표 6>에서처럼 보안에 취약한 다른 기기들 간의 결합이 더 큰 취약요인[15][16]으로 작용할 수 있다.

4.1.2 통신방식에 따른 요인

스마트홈은 유·무선통신을 모두 사용하기 때문에 유선이냐 무선이냐, 어떤 무선통신기술이냐에 따라 보안성을 결정짓게 된다. 이는 <표 6>의 통신방식과 디바이스 간 통신에 따른 취약요인들을 고려해 볼 때, 통신방식과 기술은 공격자가 사전 수집해야할 중요정보로서, 스마트홈 네트워크의 보안취약요인이 된다.

4.1.3 기기의 다중 연결에 따른 요인

<표 7>은 <표 6>의 취약요인들을 공격유형으로 분류해 한 것으로, 대응(mapping)된 정보보호요소들을 통해, 스마트홈 내에 어떤 보안기술들이 필요한지 알 수 있다. 이에 보안성과 성능간의 관계를 고려해볼 때, 4.1절에서 스마트홈 네트워크의 보안성을 높일수

록 성능저하의 요인이 되며, 이는 오히려 공격의 효과를 얻을 수 있게 된다. 스마트홈 네트워크 내에 의도적으로 접근하는 기기들과의 보안 및 연결협상 요청들이 오히려 공격이 될 수 있다는 것을 의미한다.

<표 7> 공격유형과 정보보호 요소의 매핑

공격 유형	정보보호 요소
가로채기	기밀성
위•변조	무결성
방해	가용성
관리 공격	접근통제, 인증, 부인방지

특히 아파트와 같이 무선통신의 경계가 불분명한 곳에서는 이러한 연결요청이 발생할 수 있으며, 기기의 수가 증가할수록 3.2절의 사례에서와 같이 의도하지 않은 공격[13]이나 (그림 3)의 DDoS와 같은 의도적인 공격으로[14] 악용될 수도 있다.

4.1.4 스마트홈 네트워크의 규모에 따른 요인

앞서 4.1~4.3절까지 언급했던 취약요인들을 살펴보면, 스마트홈 네트워크의 다양한 서비스와 기기, 통신방식, 보안기술, 기기 호환으로 인해 보안취약점들이 증가함을 알 수 있었다. 이에 스마트홈 네트워크의 규모가 작을수록, 기기의 수가 적을수록 보안성은 높아지고, 반대일 경우에는 낮아지게 됨에 따라 공격을 결정하게 하는 요인이 된다. 따라서 스마트홈 네트워크의 규모는 보안취약성을 결정하는 요인이 됨을 알 수 있다.

4.2 대응방안

<표 8> 보안취약요인들

분류	보안취약요인
기기 및 장치	호환성
	보안성
	이기종간의 연결
통신방식	유무선 통신
	무선통신 기술
다중 기기연결	보안연결
	연결협상
스마트홈 네트워크 규모	기기의 수
	구성 규모

4.1~4.4절의 보안취약요인들을 <표 8>과 같이 종합해보면, 스마트홈은 기기와 통신방식에 매우 의존적이며, 호환성 및 보안성이 오히려 보안취약요인이 될 수 있음을 알 수 있다. 그리고 <표 8>의 취약요인들은 기기들 간의 연결문제로 요약해 볼 수 있다. 따라서 [16]에서 언급하고 있는 디바이스의 통신영역제한과 인증기술의 적용을 고려해 볼 때, 스마트홈 네트워크의 독립성 보장이 궁극적인 대응목표가 되며, 이에 대한 대응방안들을 다음과 같이 나열해 볼 수 있다.

1) 기기
- 네트워크의 독립성 보장을 위해 기기들 간의 호환 기능의 배제(기기 호환의 최소화)
- 기기들의 관리 및 관제
- 기기 인증(새로운 기기 인증)
- 이상 기기 연결요청 배체

2) 통신방식
- 단일 무선통신매체의 사용(최소 무선통신방식의 사용을 원칙으로 함)
- 무선통신의 암호화(성능을 고려한 최소 암호 키 이상의 사용을 원칙으로 함)
- 무선 방사거리의 최소화

3) 네트워크
- 네트워크간의 연결을 차단(기본 정책으로)
- 네트워크 영역의 최소화
- 기기간 거리의 최소화

결과적으로 스마트홈의 보안취약점들에 대한 대응방안으로 기기와 통신방식, 네트워크의 독립성 보장이 기존의 취약점뿐만 아니라, 새로운 공격에도 대응할 수 있음을 알 수 있다.

5. 결 론

최근 스마트홈 서비스는 일상생활에 자연스럽게 흡수되면서 없어서는 안 될 서비스로 점차 자리잡아가고 있다. 그리고 다양한 서비스들은 편의성과 정확성, 신속성, 연동성 등을 목적으로 초기 홈오토메이션 서비스를 시작으로 진화를 거듭하면서, 최근 인공지능과 결합한 인간 친화적인 서비스로 부상하여 많은 관심을 갖고 있다. 반면, 스마트홈을 구성하는 기반기술들의

취약점들로 인해, 다양한 보안 사고들이 발생하고 있다. 그리고 이에 기반기술 중 비중을 크게 차지하는 사물인터넷 기술의 보안취약요인들과 스마트홈 서비스가 갖고 있는 잠재적인 취약요인들에 대한 대응방안 마련이 절실히 필요함을 알 수 있었다.

따라서 본 논문은 스마트홈 서비스의 보안취약요인을 알아봄으로써, 보다 긍정적인 해결방안 마련과 향후 대응기술 개발에 기여할 수 있을 것으로 기대한다. 그러나 기반기술의 진화에 따른 응용기술들의 개발이 활발히 진행될 것으로 전망되고 있는 가운데, 지속적인 연구를 통해 보다 다양한 기술들에 따른 취약요인들에 대해 대응방안을 마련해 나아가야 할 것이다.

참고문헌

[1] 김학용, “4차 산업혁명 시대의 스마트홈 전략”, 쌍용건설 특집기획, 2018.

[2] 김민상, “1인 가구시대, 진화하는 스마트홈 서비스”, 정보통신산업진흥원(NIPA) 이슈리포트, 2018.

[3] 국토교통부, “AI기반 스마트하우징 기술개발”, 기획보고서, 2019.

[4] 허지윤, “주거공간에 '사물인터넷+인공지능' 플랫폼 결합 '스마트홈'으로”, 조선일보, 2020.

[5] 요한 페데르센(Johan Pedersen), “2020년 스마트홈 시장의 여섯 가지 동향”, 반도체네트워크 2020.

[6] 이혜진, “발전하는 미국 스마트홈 시장동향”, KOTRA, 2019.

[7] 정종길, “국내 스마트홈 산업, 2025년 31조원 시장 전망”, ITDaily, 2019.

[8] 한국국토정보공사, “인공지능과 사물인터넷 기술의 만남! '스마트홈(Smart Home)”, LX한국국토정보공사, 2020.

[9] 박성환, “[AI가 미래다.]“언제, 어디서든 스마트홈” 첨단 기술 품은 아파트 진화”, 서울 뉴시스, 2020.

[10] 김민정, “코로나시대 달라진 ‘스마트홈’ 기술…”, 조선비즈, 2020.

[11] 김경훈, “스마트홈서비스플랫폼”, 한국IR협의회, 2019.

[12] “스마트홈” 보안위협 http://wiki.hash.kr/index.php/%EC%8A%A4%EB%A7%88%ED%8A%B8%ED%99%88

[13] 원병철, “‘쇼단’으로 더욱 불거진 IoT 보안취약점, 정부 대책 마련에 분주”, 보안뉴스, 2018.

[14] SK인포섹, “스마트홈 IoT보안 취약한 IoT기기의 해킹위협과 사생활 침해”, SK인포섹, 2019.

[15] Fredric Paul, “OWASP 선정 IoT의 10대 취약점”, ITWorld, 2019.

[16] Maria Korolov, “5G 네트워크로 인한 IoT 보안의 7가지 변화와 대응 방법”, ITWorld, 2019.

〔저자소개〕

전 정 훈 (Gil-dong Hong)
2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수
email : nerdrandy@dongduk.ac.kr