http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.24, No.2, May 2019, pp.113-124
https://doi.org/10.7838/jsebs.2019.24.2.113

Home IoT 가전의 보안위협모델링을 통한 보안요구사항 분석에 관한 연구

A Study on Security Requirments Analysis through Security Threat Modeling of Home IoT Appliance

윤석진(Suk-Jin Yun)*, 김정덕(Jungduk Kim)**

초 록

최근 많은 기업은 IoT가 적용된 제품들을 개발하여 판매하고 있으며, 외부의 위협으로부터 제품 및 사용자 정보를 보호하기 위해 기획 단계서부터 보안을 고려하고 있다. 그러나 IoT의 다양성으로 인해 제품별 보안요구사항 개발을 하기 위해 투자되는 시간과 인력의 한계가 있어 현재 낮은 수준의 보안이 적용되어 있다. IoT가 적용된 제품에서 취약점이 지속적으로 발표되고 있고, 이에 실제 Home IoT에 대한 보다 상세한 보안요구사항이 필요하게 되었다. 이를 위해 본 논문에서는 Microsoft사의 Threat Modeling Tool을 사용하여 Home IoT의 위협을 도출하였으며, 도출된 위협과 국내·외 취약점 평가 기준 및 논문 등과 비교 분석하여 실제 보안성 점검에 사용할 수 있는 항목을 개발하여 Home IoT 제품의 보안성 강화방안을 제시하였다. 또한 도출된 보안요구사항과 기존의 보안요구사항을 바탕으로 점검을 실시하여 효과성 검토를 하였으며, 그 결과 본 논문에서 도출된 보안요구사항의 취약점 발견 효과성이 대체로 높은 것으로 나타났다.

ABSTRACT

Today many companies are offering IoT-enabled products and place emphasis on security from the planning stage to protect their products and user information from external threats. The present security levels, however, remain low because the time and resources invested in developing security requirements for each device are far from enough to meet the needs of a wide range of IoT products. Nevertheless, vulnerabilities of IoT devices have been reported continuously, which calls for more detailed security requirements for home IoT devices. In this context, this research identified threats of home IoT systems by using Microsoft Threat Modeling Tool. It then suggested measures to enhance the security of home IoT devices by developing security assessment items through comparative analysis of the identified threats, domestic and global vulnerability assessment standards and related research. It also verified the effectiveness of the developed security requirements by testing them against the existing ones, and the results revealed the security requirements developed in this research proved to be more effective in identifying vulnerabilities.

키워드 : 홈 사물 인터넷, 위협 모델링, 홈 IoT 가전, 취약점 진단 항목, 보안요구사항
Home IoT, Threat Modeling, Appliance, Security Checkpoint, Security Requirement

* First Author, Graduate school of Industry Security, ChungAng University(suk-jin.yun@kr.ey.com)
** Corresponding Author, Professor, Department of Industry Security, ChungAng University (jdkimcau@gmail.com)
Received: 2019-03-12, Review completed: 2019-05-14, Accepted: 2019-05-23

1. 서 론

IoT 제품은 2010년부터 소비자에게 본격 적으로 선보인 이래로 지속적으로 시장이 확대되고 있다. 리서치 기관인 Machina에 따르면 글로벌 사물인터넷 시장은 2025년까지 전체 3조 달러 규모까지 성장할 것이라 예측하였으며, 생활가전과 직・간접적으로 관련이 있는 시장의 규모는 1조 3,000억 달러 규모까지 성장할 것이라 예측하였다[2]. 또한 국내 논문에 따르면, IoT를 사용하는 목적중 개인적인 목적으로 사용하는 IoT가 45.3%나 차지하는 것을 알 수 있다[7].

그러나 IoT 시장이 발전하기 위해서는 여러 문제점을 해결해야만 한다. 그중 가장 중요한 문제는 해킹(Hacking)이다. IoT 제품의 특징인 휴대성을 만족하기 위해 크기, 무게, 디자인 등을 고려하여 제작되기 때문에 보안을 위한 기능을 적절하게 적용하지 못하는 경우가 많다. 산업연구원의 조사에 따르면 IoT 제품의 해킹 등 보안 피해 규모는 2020년 17조 7,000억 원, 2030년 26조 700억 원으로 증가할 것으로 예상하고 있다[8]. 또한 한국인터넷진흥원에서는 2019년 7대 사이버 공격 전망으로 '사물인터넷을 겨냥한 신종 사이버 위협'을 선정하였다[9].

대표적인 예로 자동차 회사인 크라이슬러는 보안 전문가들이 지프 체로키 차량을 해킹하여 마음대로 차량을 조작할 수 있는 상황을 보여주고 약 140만 대의 차량을 리콜한 사태를 들 수 있다. 실제 발생된 해킹은 2016년 10월 미국에서 악성코드 '미라이(Mirai)'에 감염된 50만 개 이상의 IoT 기기들을 통해 대규모 DDoS 공격을 통해 아마존, 트위터, 넷플릭스 등 1,200여 개 사이트를 2시간 이상 마비된 사례가 있다.

이와 같이 IoT가 적용된 제품의 보안 위협 요소를 제거하기 위해 현재보다 더 강화된 보안이 적용되어야 할 필요성이 대두되고 있으며 이에 따른 사회적 요구 또한 커지고 있다. 이에 따라 국내 글로벌 기업들인 삼성 및 LG전자는 제품에 IoT 보안을 적용하고 있으며, 국제 인증 규격을 획득하는 등 IoT 제품의 보안을 강화하는 추세이지만, Home IoT 보안요구사항에 대한 상세한 항목이 없어 상세한 보안요구사항 가이드가 필요하다.

이를 위해 본 논문에서는 MS사의 Threat Modeling Tool을 사용하여 Home IoT의 위협을 도출하고, 도출된 위협과 국내외 취약점 평가 기준 및 논문 등과 비교분석하여 실제 모의 해킹 점검에 사용할 수 있는 항목을 개발함으로써 Home IoT 제품의 보안성 강화방안을 제시하며, 개발한 보안요구사항을 실제 업무에 적용하여 도출된 결과를 가지고 효과성 검증을 할 것이다.

2. 선행 연구

현재 국・내외 논문에서는 IoT의 보안을 위해 IoT 프레임워크에 관한 연구가 많이 이루어지고 있다. 논문 "IoT Privacy and Security Challenges for Smart Home Environments"[11]와 "Security in Internet of Things: Challenges, Solutions and Future Directions"[10]에 따르면 IoT 환경을 구성하는 프레임워크에 대한 보안성 문제점을 분석 한 후, 보완하여 업그레이드 된 프레임워크를 제안한다. 해당 논문들에서 제안하고 있는 IoT 프레임워크의 보안성을

강화하기 위해서는 프레임워크에 포함되는 IoT 제품에 대한 보안성 강화가 이루어져야 하므로 IoT 제품에 대한 보안성을 확인할 수 있는 보안 요구사항들을 분석할 것이다.

〈Table 1〉 Home IoT Security Checklist

category	division	Check list
S/W Security	Secure Coding	Check for weak functions which are vulnerable to buffer overflow attacks usage
		Check for validating about user input value(Command from external input is executable on the server side)
		Check whether sensitive information is exposed to script/critical information is exposed to the source code in plain text
		Check application compiles with symbol information when compiled
	Fuzzing test	Check that more data can be entered because there is no buffer area limit specified in the variable
	hidden Mode	Ensure that the hidden mode is implemented properly(S/W, H/W system)
H/W Security	Block Access Interface	Check for blockages on interfaces such as Jtag, UART, ISP and so on that can be directly connected to the device.
	Block H/W disassembly	Check if there is any detection logic for disassembling the external case on the device.
Authenti -cation	User Authentication	Use Default ID and Password
		Confirms that the forced credentials have changed on initial authentication of the service
		Password Policy: No Limit on Failed Authentication
		Password Policy: 8 Characters or Less, The Password Can Be Set.
		Password Policy: Easy-To-Guess Passwords Set
		Password Policy: Possible Changes To The Password And The Same Password That You Used Previously
		Password Policy: No Limit on Password Period
		Password Policy: Insufficient Password Combination(special characters, english characters, letters)
		Password Policy: Insufficient Additional Authentication Methods (Privacy and financial services only)
	Managing Permissions	Check appropriate permission separations if separation is required for access
		Ensure that user IDs and Device IDs are uniquely used and that authentication is implemented accordingly (Excluding the use of the 1:N, N:1, N:N method for service operation purposes)
		Ensure that device is restricting access to administrator privileges when accessing device remotely
	Debugging interface authentication	Ensure that proper authentication is implemented when accessing the device(Jtag, UART, etc.) (powerful password policy, authentication information for each device, access key implementation for access, and so on)

〈Table 1〉 Home IoT Security Checklist(Continued)

category	division	Check list
Encryption	Encryption strength	Check the strength of keys and algorithms used to encrypt critical information(Decryption is possible without key when using low encryption algorithm)
	Authentication information encryption	Check whether to save hash when saving user authentication information
	Important file encryption	Checking for encryption of Critical Information
	Key management	Ensure that the key used for encryption is properly protected (Decryptionable if key is exposed)
	Weak private key	Check whether the encryption keys are unique for each product
	Standard encryption method	Ensure that the encryption method uses the standard method
	Prevent secondary channel attacks	Ensure that the same operation time is required for an incorrect request when performing an encryption operation
Critical information exposure	secure transmission protocol	Ensure that the encryption/protocol is validated when sending critical information
	Protect storage and transmission data	Ensure proper encryption is used for storing and transferring sensitive information
	Gathering critical information	Check if minimum personal information has been collected
		Whether to apply non-identifiable technology
		Check if used personal information has been deleted
	Critical information exposure	Check personal information and sensitive information exposure through log
Platform security	Preferences	Ensure that the initial platform settings are set appropriately for security (Access to default commands, folders, and files)
	Opened unnecessary ports	Ensure that only the required ports are exposed and used
	Fuzzing test	Fuzzing attack test for open ports
	Insufficient security patch	Check for the well-known vulnerabilities when using public libraries and applications
	Application integrity verification	Check for forgery and modulation in the operation of major applications
	security update	Online security patch function
	log collection & transmission	Ensure that log collection and remote transmission capabilities exist for the running applications, opening ports, and errors
Firmware security	Firmware encryption	Ensure that firmware is protected with proper encryption
	Firmware integrity verification	Check whether updates are in operation after verifies appropriate validation of images and files during firmware update(Verification of the sign value of the image file.)

2.1 IoT 제품 보안요구사항에 관한 연구

IoT 제품 보안요구사항 항목 개발에 대한 연구는 IoT 원칙, 논문 조사, 국내・외 가이드 연구 등의 방법으로 진행되었다. 조사 대상은 IoT 얼라이언스에서 발표한 IoT 공통보안 7대 원칙[5]과 해당 원칙을 기준으로 'IoT 공통보안 가이드[4]', 'OWASP Top 10[12]', 'IoT 보안성 검

토에 관한 논문[3, 6]'에서 공통적인 보안항목을 도출하여 세분화 시켜 IoT 제품 보안요구사항 43개를 수립하였다. 도출된 43개의 보안요구사항은 크게 'S/W보안', 'H/W보안', '인증', '암호화', '중요정보 노출', '플랫폼 보안', '펌웨어 보안'으로 구성되어 있으며 이는 통합 IoT 제품 보안요구사항이라고 할 수 있다.

2.2 Microsoft 위협 모델링

보안위협모델링에 대한 연구는 1990년대부터 진행되었으며 1999년 Microsoft사의 Jason Garms 등은 내부 문서인 "The threats to our product"에서 자체적으로 사용하는 보안위협모델링의 방법을 정리하여 STRIDE 방법론을 소개하였다[13]. 또한 Michael How ard, James A. Whittaker은 2005년 Torr[15]에서 잠재적인 공격에 대비하여 제품의 위협 환경을 이해하기 위한 방안으로 위협모델링을 이용하는 것에 대해 각 분석 과정별로 구체적으로 소개하였다. Adam Shostack은 Shostack[14]에서 소프트웨어 및 시스템을 개발할 때 발생할 수 있는 잠재적인 위협을 분석하고 해결하기 위해 사용가능한 위협모델링기법을 소개하고 있으며 위협모델링을 수행하는 구체적인 방법과 기대 효과 등에 대해 설명하였다. 본 논문에서는 Home IoT의 분야별 구성도를 가지고 특정 위협을 도출해 낼 수 있는 MS 위협 모델링 기법을 사용하여 보안요구사항을 도출하기 위해 적극 활용하였다.

2.3 IoT 보안요구사항의 한계점

기존에 존재하는 가이드와 논문을 활용하여 IoT 보안요구사항을 도출했지만, 전체 항목을 활용하여 보안성 점검을 실시한 결과 많은 시간이 소요되며 효과성이 떨어졌다. 따라서 Home IoT의 특정 도메인을 분류하여 도메인만의 특정 보안요구사항을 도출하여 보안요구사항에 대한 우선순위를 정하는 것이 중요하다. 따라서 제3장에서는 Home IoT 제품에 대한 보안요구사항 효과성을 위해 분야별 도메인을 분리하고, 위협 모델링을 통하여 각 도메인별 위협을 도출 후 도메인별 특화된 보안요구사항을 도출 할 것이다.

3. Home IoT 보안요구사항

3.1 Home IoT 도메인 분리

Home IoT의 효과적인 보안요구사항을 도출하기 위하여 비슷한 기능과 구성을 가지는 4가지 도메인으로 나눴다. Home IoT 도메인은 생활에 기본이 되는 TV, 냉장고 등을 공통 도메인 '생활'로 분류하고 나머지 3가지 도메인을 기본 생활 이외에 분야로 나누었다.

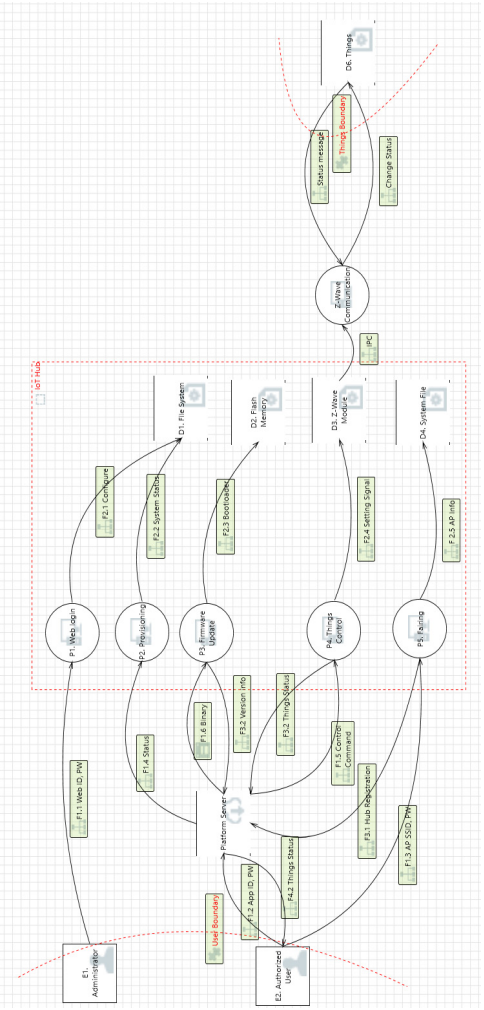
〈Table 2〉 Home IoT Domain

Life	Smart TV, Washer, Refrigerator, Robotic Vacuum, Smart Air Cleaner, Air Conditioner
Security & Digital Media	Home CCTV, IP Camera, Smart DoorLock, IoT Safe
Health & Finance	Smart Watch, AI Speaker, Smart Chair, Smart Band
Energy	Remote Meter, Smart Boiler, IoT Home ESS

3.2 위협 모델링을 통한 도메인별 보안요구사항 도출

3.2.1 도메인 1(생활_Home IoT 공통)

'생활' 도메인의 제품 대상은 생활 가전의 공통적으로 포함되는 TV, 냉장고 등이 포함되며 도메인 1은 가전 IoT의 공통 위협모델링으로 정의할 수 있다. 다음 <Figure 1>은 마이크로소프트사의 위협모델링 소프트웨어인 Microsoft Threat Modeling Tool 2016을 사용하여 생활 도메인의 구조를 모델링 한 것이다. 이처럼 도메인 2부터 4까지 모든 도메인을 대표적인 구조로 위협모델링을 구조화하였다.



〈Figure 1〉 Domain1('Life')

도메인 1은 Home IoT의 기본이 되는 구조를 적용했으며, 이 도메인은 다른 도메인 2, 3, 4에도 공통으로 포함되는 구조이다. 위의 <Figure 1>을 보면 크게 USER, Things를 컨트롤 할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결 해주는 IoT Hub Zone 그리고 Things 이렇게 4개 구간으로 나누었다. Microsoft Threat Modeling Tool을 사용하여 4개의 구간의 위협들을 도출한 결과, 도출된 주요 위협은 보안 이벤트 관리, 네트워크 구간 접근제어, 세션 및 토큰관리, 재생공격, 중간자공격, 상호인증 미흡이 있으며, 도출된 위협들과 선행연구 결과물인 43개의 체크리스트와 비교하여 '도메인 1'에 대한 새로운 보안요구사항을 개발하였으며, 본 논문 제4장 "보안요구사항 효과성 검토"에서 확인할 수 있다.

3.2.2 도메인 2(보안&디지털영상)

'보안&디지털영상' 도메인의 제품 대상은 Home CCTV, IP Camera, Smart 도어락 등이 포함되며 도메인 2의 위협모델링은 영상에 관련된 시스템이나 기능을 포함한 Home CCTV를 대상으로 진행 했다. 앞서 언급한바와 같이 도메인 1은 가전 IoT의 공통 위협 모델링이며, 현재 도메인 2에서 도출되는 위협들과 도메인 1에서 도출된 위협들을 추가하면 도메인 2의 전체 위협항목이 된다.

도메인 2는 Home IoT의 보안&디지털영상의 주제에 관한 구조를 적용했다. 도메인 2는 USER,

Things를 컨트롤 할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결 해주는 IoT Hub Zone이 존재하며, 영상과 관련된 IoT Things들과 많이 사용되는 DVR (Digital Video Recording Platform)을 추가하였다.

Microsoft Threat Modeling Tool을 사용하여 각 구간의 위협을 도출한 결과, 주요 위협은 영상정보에 관한 데이터 무결성 위협, 영상보관 기간에 관한 위협이 있으며 도출된 위협들과 선행연구 결과물인 43개의 체크리스트와 비교하여 '도메인 2'에 대한 새로운 보안요구사항을 개발하였으며, 본 논문 제4장 "보안요구사항 효과성 검토"에서 확인할 수 있다.

3.2.3 도메인 3(건강&금융)

'건강&금융' 도메인의 제품 대상은 심박수, 체온 등을 체크할 수 있는 스마트워치, 음성 금융거래가 가능한 AI 스피커 등이 포함되며 도메인 3의 위협모델링은 중요정보가 전달되는 기능을 포함한 AI 스피커를 대상으로 진행했다. 앞서 언급한바와 같이 도메인 1은 가전 IoT의 공통 위협 모델링이며, 현재 도메인 3에서 도출되는 위협들과 도메인 1에서 도출된 위협들을 추가하면 도메인 3의 전체 위협항목이 된다.

도메인 3는 Home IoT의 '건강&금융'의 주제인 AI 스피커에 관한 구조를 적용했다. 도메인 3은 USER, Things를 컨트롤 할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결 해주는 IoT Hub Zone이 존재하며, 금융결제와 관련되어 IoT Things들과 많이 사용되는 금융권 서버와 연결되는 부분을 추가하였다.

Microsoft Threat Modeling Tool을 사용하여 각 구간의 위협을 도출한 결과, 주요 위협은 결제에 관련된 조작, 정보노출, 암호화 관련 위협이 있으며 도출된 위협들과 선행연구 결과물인 43개의 체크리스트와 비교하여 '도메인 3'에 대한 새로운 보안요구사항을 개발하였으며, 본 논문 제4장 "보안요구사항 효과성 검토"에서 확인할 수 있다.

3.2.4 도메인 4(에너지)

'에너지' 도메인의 제품 대상은 요즘 많이 확산되고 있는 원격검침, 태양열, 공조기, 보일러 등이 있으며, 도메인 3의 위협모델링은 LTE 통신으로 이루어지는 Home 원격검침기를 대상으로 진행 했다. 앞서 언급한 바와 같이 도메인1은 가전 IoT의 공통 위협 모델링이며, 현재 도메인 4에서 도출되는 위협들과 도메인 1에서 도출된 위협들을 추가하면 도메인 4의 전체 위협항목이 된다.

도메인 4는 Home IoT의 '에너지'의 주제인 Home 원격검침기에 관한 구조를 적용했다. 도메인 4는 USER, Things를 컨트롤 할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결 해주는 IoT Hub Zone이 존재하며, 원격검침기에 USIM을 사용하여 LTE 망 통신을 하는 구조를 추가 하였다.

Microsoft Threat Modeling Tool을 사용하여 각 구간의 위협을 도출한 결과, 도출된 주요 위협은 비 허가자의 LTE 데이터 접근 및 사용이 있으며 도출된 위협들과 선행연구 결과물인 43개의 체크리스트와 비교하여 '도메인 3'에 대한 새로운 보안요구사항을 개발하였으며, 본 논문 제4장 "보안요구사항 효과성 검토"에서 확인할 수 있다.

4. 보안요구사항 효과성 검토

4.1 Home IoT 도메인별 보안요구사항

Microsoft사의 Threat Modeling Tool을 사용하여 도출된 위협들과 앞에서 도출된 보안요구사항들을 비교하여 추가적인 보안요구사항을 도출했다. <Table 3> 항목들은 각 도메인에서 우선적으로 점검해야 할 항목들이며 실제 Home IoT 점검 시 각 도메인에 맞게 적용하여 사용이 가능하다. 또한 도메인별 특화된 보안요구사항이기 때문에 우선순위를 높게 설정하여 점검하여 점검 효과성을 높일 수 있다.

〈Table 3〉 Security Checklist for Each Domain

Domain	Check list	Description
Life	Check whether memory protection technique is applied	Check whether memory protection techniques are applied to prevent attacks caused by buffer flow
	Network interval access control settings	Ensure that access control settings for services that communicate with the network controls unauthorized access
	Safe session and token Management	Check whether sessions/tokens are generated by arbitrary values and are easily exposed/calculated
	Network replay attack prevention	Check whether encrypted data sent over the network is preventing attacks that are performed without decrypting
	insufficient to prevent Man-in-the-Middle attacks	Check whether a secure encryption channel is implemented to prevent forgery of important information by 3rd parties
	Inadequate mutual authentication between IoT system configuration	Check whether the server /device performs mutual authentication to prevent sensitive information leakage such as product control or personal information by unauthorized user
Security & digital media	Whether data integrity is ensured	Data integrity must be verified and whether countermeasures are implemented in case of integrity errors
	Set the appropriate video storage period	Checking whether there is a policy for setting up the video storage period
Health & Finance	Payment amount manipulation	When attempting to pay, service needs to identify vulnerabilities that can be paid through the amount of the manipulated payment
	Charges other users for payment	When paying, service needs to identify vulnerabilities that can be charged to other users due to insufficient authentication and session processing
	Unencrypted financial information	When financial information is sent and received via communication channel in a plain text, an attacker is available to acquire sensitive data from other users through sniffing.
	Unencrypted bio information	When bio information is sent and received via communication channel in a plain text, an attacker is available to acquire sensitive data from other users through sniffing.
Energy	Access and use of LTE data by non-authenticated user	It is necessary to verify that USIM usage detection and access control settings exist by unauthorized person after USIM capture

4.2 Home IoT 도메인별 보안요구사항에 대한 효과성 검토

도메인별 보안요구사항에 대하여 효과성 검토를 하기 위하여 본 논문에서는 앞에서 제시했던 기존의 보안요구사항들인 'OWASP TOP 10', 'IoT 공통 보안가이드', '관련 논문 검토 항목'과 새로 도출된 43개의 항목들을 기반으로 실제 L사의 Home IoT 보안 전문가 인력 5명에게 1년간 L사의 Home IoT에 대한 보안성 점검을 의뢰 하였다. 전문가들은 같은 직급의 고급 기술 인력들을 투입하였으며, 동일한 제품으로 각각 다른 보안요구사항 항목을 적용하여 실시한 후 결과에 대해 비교분석 하였다.

<Table 5>는 보안성 점검에 대한 결과 이며, 결과에 대한 효과성 측정을 위해 간단한 공식을 정의하였다. 점검 기간 별 취약점 개수 효과성측정 공식은 "일별 평균 취약점 발견 개수"로 정의했으며, "취약점 개수/점검기간(일)"이다.

〈Table 4〉 Penetration Testing Target & Description

Domain	Target	Description
Domain 1 (Life)	Air conditioner	- Test period: 20 Days - Target description: Supports power conditions and setting functions such as operation or temperature control at external
	Refrigerator	- Test period: 20 Days - Target description: Real-time check of the inside of the refrigerator and support history of using the refrigerator
	Smart TV	- Test period: 40 Days - Target description: User can download and use real-time content through internet connection. Check news, weather, email, etc.
Domain 2 (Security& digital media)	Door lock	- Test period: 15 Days - Target description: Enable remote door open/lock function and view history
	IP Camera	- Test period: 20 Days - Target description: Real-time streaming and data temporary storage via wireless video transmission
	Home CCTV	- Test period: 20 Days - Target description: Enables real-time monitoring, intrusion detection, and automatic mass storage of images
Domain 3 (Health & Finance)	Smart band	- Test period: 10 Days - Target description: Provides heartbeat measurement, sleep measurement, step measurement, and health care functions
	Smart chair	- Test period: 10 Days - Target description: Supports informational functions such as posture changes, postural time, correct posture ratio and seating time
	Smart speaker	- Test period: 20 Days - Target description: Supports functions such as music, life/information, search, shopping/Order, finance, etc. through the speech recognition function of speakers
Domain 4 (Energy)	Home ESS	- Test period: 20 Days - Target description: A function that stores solar energy in a battery pack with an energy storage system.
	Remote meter	- Test period: 10 Days - Target description: Support for remote automatic meter function using LTE network
	Smart boiler	- Test period: 15 Days - Target description: Checking the condition and temperature of the boiler from outside and supporting timer setting function

〈Table 5〉 Result of Effectiveness Evaluation of Security Checkpoints by Domain (Average Daily # of Vul.)

Target \ Guide		OWASP			IoT Common Security Guide			Related papers 1 (한정진)			Related papers 2 (강준모)			NEW		
		result	period	effectiveness	result	period	effectiveness	result	period	effectiveness	result	period	effectiveness	result	period	effectiveness
Domain 1 (Life)	Air conditioner	4	21	0.2	2	8	0.3	11	23	0.5	2	10	0.2	12	20	0.6
	Refrigerator	4	21	0.2	2	8	0.3	11	23	0.5	2	10	0.2	12	20	0.6
	Smart TV	9	34	0.3	3	17	0.2	20	37	0.5	4	20	0.2	22	40	0.6
Domain 2 (Security & digital media)	Smart Door Lock	2	14	0.1	1	6	0.2	6	15	0.4	2	8	0.3	7	15	0.5
	IP Camera	12	21	0.6	6	10	0.6	20	23	0.9	6	10	0.6	30	20	1.5
	Home CCTV	11	19	0.6	6	10	0.6	17	21	0.8	5	10	0.5	30	20	1.5
Domain 3 (Health & Finance)	Smart Band	2	9	0.2	1	4	0.3	6	10	0.6	2	5	0.4	4	10	0.4
	Smart Chair	2	9	0.2	1	4	0.3	6	10	0.6	2	5	0.4	4	10	0.4
	Smart Speaker	13	28	0.5	6	15	0.4	18	30	0.6	6	10	0.6	30	20	1.5
Domain 4 (Energy)	Home ESS	16	29	0.6	6	15	0.4	22	31	0.7	4	10	0.4	32	20	1.6
	Remote Meter	2	9	0.2	1	3	0.3	5	10	0.5	2	5	0.4	4	10	0.4
	Smart Boiler	8	14	0.6	1	6	0.2	7	15	0.5	4	8	0.5	16	15	1.1
Average				0.4			0.3			0.6			0.4			0.9

<Table 4>를 보면 도메인마다 3개의 다른 점검대상을 정하여 점검을 진행 하였으며, <Table 5>과 같이 기존에 참고했던 보안요구사항들과 새로 도출한 보안요구사항을 각각 같은 점검대상을 통해 점검을 실시했으며 앞에서 정의했던 효과성 측정 공식을 활용하여 결과를 도출했다. <Table 5>의 효과성 측정 결과는 취약성이 도출된 개수를 점검 기간으로 나누어 일별 평균 취약점 개수를 도출한 것이다. 예를 들어 OWASP의 보안요구사항을 기반으로 도메인 1의 “에어컨” 제품을 점검하였을 경우는 21일의 점검기간이 소요 되었으며 취약점이 총 4개가 발견된 것이다. 따라서 효율성 측정값, 즉 일평균 취약점 발견 개수는 0.2개가 되는 것이다. 각 보안요구사항 항목별 평균값을 비교해보면, 일평균 0.9개의 평균 효율성 측정값으로 본 논문을 통해 도출된 Home IoT 보안요구사항이 가장 평균적인 효율성이 높은 것으로 판단된다. 하지만 도메인 3, 도메인 4의 일부 세부적 도메인을 확인하면 효율성 값이 비슷하거나 참고 논문에서 보여줬던 보안요구사항이 높은 것으로 측정되었다.

5. 결 론

최근 IoT 보안 검토 항목에 관한 여러 가이드, 논문들이 제시되고 있지만, 현재 가장 많이 확산되고 있는 Home IoT 보안요구사항에 관한 국내 관련 연구가 없었다. 이에 본 논문에서는 기존에 존재하는 보안요구사항 가이드, 논문 등을 분석하여 통합적 IoT 보안요구사항을 도출 하였다.

또한 Home IoT를 4개의 도메인으로 나누고, MS Threat Modeling을 통해 각 도메인별 위협을 도출하였으며, 도출된 위협과 통합 IoT 보안 요구사항을 추가하여 Home IoT 도메인별 보안 요구사항을 도출 하였다. 연구를 통해 도출된 항목들을 검증하기 위해 다른 항목들과 비교 분석하여 효과성 검토를 실시하였다. 효과성 검토는 실제 기업의 Home IoT 점검 대상으로 보안전문가들을 통해 진행이 되었으며, 진행이 되어 도출된 보안요구사항을 실제 제품에 적용하는 것이 효율적이라고 판단되었다.

하지만 보안요구사항 점검에 대한 기간 효율성 향상, Home IoT 제품 자체의 취약점을 근본적으로 줄이는 방안이 필요하다. 점검 기간 효율성과 제품 자체의 취약점을 줄이는 방안은 Security Development Lifecycle을 도입하여 Home IoT 개발 단계에서부터 보안성 검토가 필요하므로, 이에 대한 연구가 향후 과제로 남아있다.

References

[1] Choi, J. W., “The status and prospect of the IoT market,” Kotra, 2016.

[2] Gartner, “Press Release: Global Internet of Things Market to Grow to 27 Billion Devices, Generating USD 3 Trillion Revenue in 2025,” Gartner, 2016.

[3] Han, J. J., “Configuring the design and inspection item for reviewing the Internet of Things (IoT) security,” Master’s thesis in Yonsei University, pp. 41-57, 2016.

[4] IoT Security Alliance, “IoT Common Security Guide,” IoT Security Alliance, p. 3 2016.

[5] IoT Security Alliance, “IoT Common Security Principles,” IoT Security Alliance, pp. 1-10, 2016.

[6] Kang, J. M., “How to Validate Smart TV Security in an Internet of Things,” Master’s thesis at Soongsil University, pp. 28-29, 2016.

[7] Kim, E. A., “A Study on Development and Application of Taxonomy of Internet of Things Service,” The Journal of Society for e-Business Studies, Vol. 20, No. 2, pp. 107-123, 2015.

[8] Korea Institute for industrial Economics & Trade, “Safety Net in the Age of Internet of Things, Convergence Security Industry,” KIET, pp. 1-8, 2014.

[9] Korea Internet & Security Agency. “Seven Cyber Attacks Forecasts of 2019,” KISA, p. 13, 2018.

[10] Kumar, S. A. and Vealey, H. S., “Security in Internet of Things: Challenges, Solutions and Future Directions,” IEEE, pp. 1-9, 2016.

[11] Lin, H. and N. W. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” Information, pp. 1-13, 2016.

[12] OWASP, “OWASP IoT Top 10,” OWASP, 2014.

[13] Shostack, A., “Experience Threat Modeling at Microsoft,” Microsoft, 2008.

[14] Shostack, A., Threat Modeling: Design for Security, WILEY, pp. 1-30, 2014.

[15] Torr, P., “Demystifying the Threat modeling process,” IEEE Security & Private, Vol. 3, No. 5, pp. 66-70, 2005.

저 자 소 개

윤석진 (E-mail: suk-jin.yun@kr.ey.com)
1988년 고려대학교 행정학과 졸업
2005년 서강대학교 경영대학원(MBA) 졸업
2010년 서울종합과학대학원 산업보안전문가 과정 수료
2018년 중앙대학교 대학원 산업보안 박사과정 수료
2019년 EY한영회계법인 부대표(現)
(사)한국 클라우드 보안협회 회장(現)
(사)한국 정보시스템 감사통제협회 회장(前)
관심분야 정보보호/감사, 거버넌스 및 내부통제, 기업가정신 확산

김정덕 (E-mail: jdkimcau@gmail.com)
1979년 연세대학교 정치외교 학과 (학사)
1981년 연세대학교 경제학과 대학원 (석사)
1986년 Univ. of S. Carolina, MBA
1990년 Texas A&M Univ., Ph. D. in MIS
1995년~현재 중앙대학교 산업보안학과 교수
관심분야 디지털 비즈니스 보안, 사이버 보안 거버넌스 및 보안관리