



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

제 105 회 박사학위논문
지도교수 김 정 덕

Home IoT 가전기기의 보안성 향상을 위한
Security Development Lifecycle 적용 연구

중앙대학교 대학원
융합보안학과 산업보안전공
윤 석 진
2019년 8월

Home IoT 가전기기의 보안성 향상을 위한 Security Development Lifecycle 적용 연구

이 논문을 박사학위논문으로 제출함

2019년 8월

중앙대학교 대학원
융합보안학과 산업보안전공
윤 석 진

윤석진의 박사학위논문으로 인정함

심사위원장 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

심 사 위 원 _____ (인)

중앙대학교 대학원

2019년 8월

목 차

제1장 서 론	1
제1절 연구의 배경 및 필요성	1
1. 연구의 배경	1
2. 연구의 필요성	4
제2절 연구의 목표 및 범위	5
1. 연구의 목표	5
2. 연구의 범위	6
제3절 연구의 방법 및 절차	7
1. 연구의 방법	7
2. 연구의 절차	7
제2장 선행연구 분석	10
제1절 IoT 보안 관련 요구사항 분석	10
1. 기존 보안 요구사항 분석	10
2. 위협모델링 분석	22
제2절 Security Development Lifecycle 분석	24
1. MS-SDL 방법론	24
2. CLASP 방법론	27
3. Seven-Touchpoint 방법론	28
4. TSP-Secure 방법론	29
제3절 시사점	30

제3장 연구의 설계	32
제1절 Home IoT 가전기기 보안 요구사항 설계	32
1. IoT 가전기기 보안 요구사항 설계	32
2. 위협모델링 분석	35
제2절 Home IoT SDL 프로세스 설계 및 적용	41
1. SDL 관련 용어 및 책임 정의	42
2. 준비 단계의 Home IoT 보안 전문가 양성 교육 프로세스	45
3. 요구사항 정의 단계의 보안활동 프로세스	47
4. 설계 구현 단계의 보안활동 프로세스	52
5. 테스트 단계의 보안활동 프로세스	63
6. 릴리즈 단계의 보안활동 프로세스	66
7. 대응 단계 프로세스	68
제4장 연구 결과 및 분석	71
제1절 Home IoT 가전기기 보안 요구사항 검증	71
제2절 Home IoT SDL 프로세스 적용	74
제5장 결 론	83
참고문헌	85
국문초록	88
Abstract	90

표 목 차

[표 1] 산업혁명의 특징	2
[표 2] OWASP IoT Top 10 항목	11
[표 3] IoT공통 보안 가이드 항목	13
[표 4] Global 컨설팅 기업 IoT 보안 점검 항목	15
[표 5] IoT 보안성 검토를 위한 디바이스, 펌웨어, 앱 점검 항목	17
[표 6] IoT 보안성 검토를 위한 플랫폼 점검 항목	18
[표 7] IoT 보안성 검토를 위한 사용자(단말기) 관련 점검 항목	20
[표 8] IoT 주요 보안 점검 항목	21
[표 9] 데이터 흐름 다이어그램 요소	23
[표 10] STRIDE 분석	23
[표 11] IoT 보안 요구사항	32
[표 12] 위협모델링 대상 Home IoT 가전기기	35
[표 13] Home IoT 도메인	36
[표 14] 도출된 도메인별 보안 요구사항 항목	36
[표 15] SDL 관련 용어	42
[표 16] SDL 관련 책임과 권한	43
[표 17] 시큐어코딩 가이드	55
[표 18] 보안 요구사항 점검 대상 및 설명	71
[표 19] 도메인별 보안 요구사항 항목 탐지율 검증 결과	73
[표 20] 연구 대상 및 기간	75
[표 21] 효율성 검증 공식	76

[표 22] Home IoT SDL 프로세스 적용 결과	76
[표 23] Home IoT SDL 프로세스 적용 후 취약점 분석 결과	77
[표 24] Home IoT SDL 프로세스 스마트TV 적용 결과	79
[표 25] NIST 시큐어코딩 효과성	84

그림목차

[그림 1] 전 세계 IoT 시장 전망	3
[그림 2] Home IoT 가전기기의 보안성 향상을 위한 연구방법	7
[그림 3] 연구의 수행 절차	9
[그림 4] OWASP IoT Top 10	11
[그림 5] MS-SDL	25
[그림 6] CLASP의 6가지 관점	28
[그림 7] Seven-Touchpoint 방법론	29
[그림 8] TSP-Secure 주요요소 및 팀 구축 방법	30
[그림 9] 도메인1 데이터 흐름도	38
[그림 10] 도메인2 데이터 흐름도	39
[그림 11] 도메인3 데이터 흐름도	40
[그림 12] 도메인4 데이터 흐름도	41
[그림 13] Home IoT Security Development Lifecycle 프로세스	42
[그림 14] Home IoT 보안 교육 설계	46
[그림 15] 보안 등급 정의 프로세스 설계	47
[그림 16] 보안 대상기기별 분류 기준	48
[그림 17] 보안 등급별 SDL 활동 정의	49
[그림 18] SDL 계획 수립 프로세스 설계	50
[그림 19] 보안 요구사항 분석 프로세스 설계	51
[그림 20] 보안설계 검토 프로세스 설계	53
[그림 21] SW설계서 예시	53

[그림 22] 보안 구현 프로세스 설계	55
[그림 23] 오픈소스 보안 취약점 분석 프로세스 설계	58
[그림 24] 보안 정적 분석 프로세스 설계	60
[그림 25] 보안 기능점검 프로세스 설계	61
[그림 26] 퍼지 점검 프로세스 설계	63
[그림 27] 취약점 분석 프로세스 설계	65
[그림 28] 최종 보안 검토 프로세스 설계	67
[그림 29] 가전기기 보안 대응 프로세스 설계	69

제1장 서론

제1절 연구의 배경 및 필요성

1. 연구의 배경

사물 인터넷(Internet of Things: 이하 “IoT”)이란 일상생활에서 사용하는 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 말하며, 1999년 케빈 애쉬튼(Kevin Ashtonin)에 의하여 최초로 정의되었다. IoT는 유무선 네트워크에 연결된 사물들은 물론 사람과 환경을 구성하는 물리적인 모든 것을 구성요소에 포함하고 있다. IoT는 네트워크를 통해 사람과 사람(P2P: People to People), 사람과 사물(P2M: People to Machine), 사물과 사물(M2M: Machine to Machine) 등 다양한 방식으로 언제 어디서나 상호 소통하는 초연결 사회의 기반을 제공하게 된다^[1].

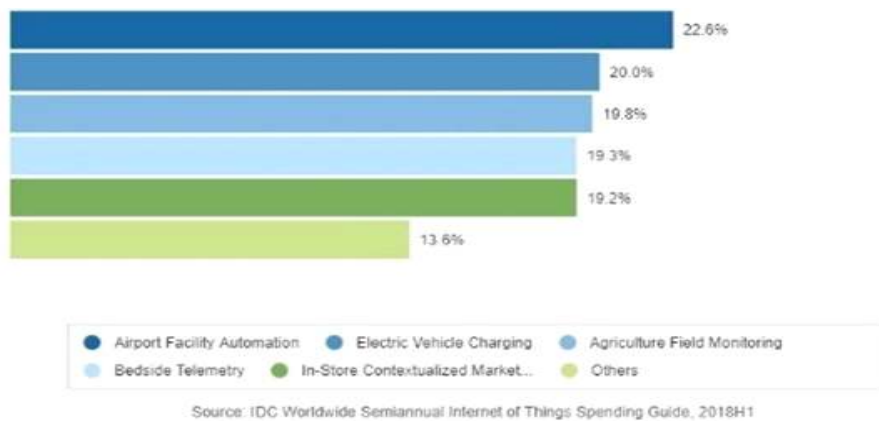
제4차 산업혁명에서는 AI(Artificial Intelligence, 인공지능), IoT, 3D 프린터, 자율 주행 자동차, Nano 기술, 양자 컴퓨팅과 생명 공학 등 새로운 ICT 신기술이 확산될 것으로 전망하고 있다. 이러한 기술 중에 특히 IoT는 여러 신기술들과 조합하여 사용하면 높은 효과성을 볼 수 있고 다양한 분야에도 활용할 수 있는 중요한 분야라고 할 수 있다.

[표 1] 산업혁명의 특징

구분	특징	생산방식
제1차 산업혁명	증기기관	생산설비 기계화
제2차 산업혁명	전기에너지, 분업화	대량 생산
제3차 산업혁명	전자기기, 정보통신	자동화
제4차 산업혁명	Big Data(빅데이터), AI(인공지능), IoT(사물인터넷)	컴퓨터를 활용한 스마트, 최적화

출처: KISDI

IoT 제품은 2010년부터 소비자에게 본격적으로 소개되었고 이후 지속적으로 시장이 확대되고 있다. IT 시장분석 및 컨설팅 기관인 IDC Korea의 보고에 따르면, 사물인터넷 시장 규모는 2019년 7,450억 달러에 이를 것으로 전망했다. 또한, 이는 2018년의 6,460억 달러보다 15.4% 증가한 수치이며, 2017년부터 2022년까지 연간 두 자릿수의 성장률을 유지하여 2022년에는 1조 달러를 넘어설 것으로 예측하고 있다^[2].



[그림 1] 전 세계 IoT 시장 전망

출처: IDC: IDC, Top Use Case Based on 5Year CAGR(2017-2022)

IoT 기술의 발전은 Home 가전기기에도 접목되어 우리의 일상생활 형태를 변화시키고 있으며, 스마트TV, 에어컨뿐만 아니라 가스, 전기 등 에너지 모니터링에 활용 가능한 IoT가 적용된 모든 기기에 접속할 수 있도록 네트워크 환경이 형성되어 있고, 모바일, PC 등의 단말기를 통해 Home IoT의 모든 제품을 제어 할 수 있게 되었다.

Home IoT 시장이 성장하고 발전하기 위해서는 여러가지 문제점들이 해결되어야 한다. 그 중에서도 가장 중요한 것은 해킹(Hacking)이라고 할 수 있다. 특히 IoT제품을 개발할 때 크기, 무게, 디자인 등을 고려하게 되므로, 보안을 위한 필수적인 기능을 적절하게 적용하지 못하는 경우가 발생하며, 여러 기술과 가전기기가 결합됨으로써 보안에 취약한 부분이 나타나는 것을 예측하지 못할 수가 있다. 따라서 확산되고 있는 Home IoT 제품에 관한 정확한 보안 요구사항이 매우 중요하게 요구되고 있다.

Home IoT 시장이 성장하고 발전함에 따라 최근 많은 기업은 IoT가 적용된 제품들을 개발하여 판매하고 있으며, 외부의 위협으로부터 제품 및 사용자 정보를 보

호하기 위해 노력하고 있다. 그러나 IoT의 다양성으로 인해 각 제품별로 적합한 보안 요구사항을 개발하고 실행하는 것은 리소스와 비용의 이슈로 현재 낮은 수준의 보안이 적용되어 있는 것이 현실이다. 따라서 IoT가 적용된 제품에서 취약점이 지속적으로 발표 되고 있고 실제 사례를 통해 보안 위험은 계속 증가되고 있음을 확인할 수 있다^{[3][4]}. 글로벌 시장조사 기관인 가트너, ABI 리서치 등에서는 2020년에 250억 개 이상의 사물들이 상호 연결될 것으로 전망하고 있으며, 이러한 시장의 활성화와 함께 중요하게 재인식되고 있는 부분이 바로 IoT 보안이다^[5]. 우리의 실생활과 매우 밀접하게 연관되어 있는 Home IoT 가전기기의 보안위협은 그 파급력 또한 매우 커지게 될 것으로 예상된다.

2. 연구의 필요성

산업연구원의 조사에 따르면, IoT 제품의 해킹 등 보안 피해 규모는 2020년 17조 7,000억원에서 2030년에는 26조 700억원으로 증가할 것으로 예상하고 있다^[6]. 또한 한국인터넷진흥원에서는 2019년 7대 사이버 공격 전망으로 “사물인터넷을 겨냥한 신종 사이버 위협”을 선정한 바 있다^[7].

이와 같이 IoT가 적용된 제품의 보안 위험 요소를 제거하기 위해 현재보다 더 강화된 보안이 적용되어야 할 필요성이 대두되고 있으며 이에 따른 사회적 요구 또한 커지고 있다. 이에 따라 국내 글로벌 IoT 제조사는 제품을 개발할 때 IoT 보안을 적용하고 있으며, 다양한 국내외 표준 기구 및 사설 표준 기구에서도 보안 기술들이 논의되고 있고^{[8][9][10][11]}, 국제 인증규격을 획득하는 등 IoT 제품의 보안을 강화하는 추세에 있다.

그러나 일상에서 접할 수 있는 IoT 제품 유형이 다양해진 만큼 노출될 수 있는 보안 위협 또한 다양하게 발생할 수 있다. 또한 IoT 기술 자체가 인터넷을 기반으로 구현되어 있기 때문에 모든 IoT 제품은 해킹의 대상이 될 수 있고 IoT 디바이

스의 종류와 기능이 각각 다르기 때문에 다양한 보안 위협이 존재할 수 밖에 없다. IoT 기기의 대표적 해킹사례로는 크라이슬러 자동차의 지프 체로키 차량을 예로 들 수 있으며, 약 140만대의 차량을 리콜한 바 있다. 또한 2016년 10월 미국에서는 악성코드 “미라이(Mirai)”에 감염된 50만개 이상의 IoT 기기들의 대규모 디도스 공격으로 아마존, 트위터, 넷플릭스 등 1,200여개 사이트를 2시간 이상 마비시킨 사례도 있다.

따라서 Home IoT 가전기기의 보안강화를 위해 정확한 보안 요구사항이 매우 중요하게 요구되고 있으며, 보다 근본적인 보안 취약점을 줄여줌으로써 사생활 침해나 해킹의 위협으로부터 더 나은 삶을 영위할 수 있도록 연구할 필요가 있다.

제2절 연구의 목표 및 범위

1. 연구의 목표

Home IoT는 우리의 일상생활에 편리함을 가져다주고 삶의 질을 더욱 높여주는 효과를 가져오고 있지만, 보안사고 발생의 파급력은 막대할 것으로 예상되어 IoT 기기에 대한 보안이슈 해결은 무엇보다도 우선 되어야 할 것이다. 현재 Home IoT 가전기기 제조사들은 증가하고 있는 IoT 보안 사고에 대하여 보안 전문가를 통한 IoT 취약점 분석을 진행하여 도출된 보안 이슈를 줄여 나가고 있으나, 보안지식이 없는 개발자가 구현한 프로그램에는 다양한 보안취약점들이 발생할 수 있으며, 이는 IoT 기기와 서비스에 심각한 오동작, 결함을 야기할 수 있고 잠재 되어 있는 위험 요소는 공격자의 주요 대상이 될 수 있다^[12]. 따라서 도출된 취약점을 모두 개선하기에는 상당한 추가 개발 기간이 소요되어 제품이 출시되기까지 효율성은 매우 떨어지고 있다고 할 수 있다.

본 연구에서는 Home IoT 가전기기의 취약점 분석 및 제품 출시에 대한 효율성을 높이하고자, 실무환경에서 Home IoT 가전기기의 개발단계에 Security Development Lifecycle(이하 “SDL”) 프로세스를 적용함으로써 그 보안성 향상과 제품 출시 효율성을 향상 시키고자 한다. 세부적인 연구 목표는 첫째, Home IoT의 SDL에 대한 이론적 토대를 마련하고 둘째, 실제 Home IoT 제조사에 직접 적용하여 보안성이 실제로 향상되었는지 검증하고자 한다.

2. 연구의 범위

Home IoT 환경이 고도화 될수록 개인화 서비스는 더욱 더 발전할 것이며, 이에 따른 사생활 침해와 새로운 빅브라더의 등장이 우려되기도 한다. 현재 Home IoT 가전기기를 통한 사생활 침해 및 보안위협을 예방하기 위해 Home IoT 제조사들은 자체적인 취약점 분석 및 모의해킹을 주기적으로 실행하고 있다. 그러나 Home IoT 가전기기의 종류와 적용 분야는 급속하게 증가하고 있으며 이러한 보안 문제를 적시에 전부 해결하기에는 명확한 한계가 있어 보인다. 따라서 Home IoT에 최적화된 보안 요구사항을 재정립하고 개발단계부터 “Security by Design”의 개념을 적용한 Home IoT SDL 프로세스를 적용할 필요가 있다. 이러한 보안 요구사항 분석을 통해 SDL을 적용할 때 발생 가능한 취약점을 근본적으로 감소시킬 수 있을 것이다. 본 논문에서는 SDL 방법론 중에서 Microsoft-Security Development Lifecycle(이하 “MS-SDL”)을 선택하여 실무환경에 맞춰 세부 프로세스를 설계하고 적용하였다. 금번 연구에서 모든 Home IoT 가전기기에 대해 SDL을 적용하고 검증하기에는 현실적인 어려움이 있으므로, 대표적인 Home IoT 가전기기 12개를 대상으로 선정하여 연구를 진행하였다.

제3절 연구의 방법 및 절차

1. 연구의 방법

선행 연구 분석을 바탕으로 Home IoT 가전기기에 특화된 보안 요구사항을 재정립하고 근본적인 문제 해결을 위해 취약점 분석의 효율성도 높일 수 있는 SDL 프로세스를 설계하고 적용하여 빠르게 증가하고 있는 Home IoT 가전기기에 대한 보안 위협 리스크를 방지하고자 한다.

이를 위해 각 단계별로 필요한 보안 요구사항이 정의되어야 하며, Home IoT 가전기기에 특화된 요구사항을 기술하고 설계된 SDL의 효율성을 보안 전문가 그룹의 검토를 통해 검증하고자 한다.



[그림 2] Home IoT 가전기기의 보안성 향상을 위한 연구방법

2. 연구의 절차

본 연구의 절차는 Home IoT 가전기기에 특화된 보안 요구사항을 도출하고 MS-SDL 방법론을 활용하여 SDL 세부 프로세스를 설계하고 파일럿 테스트 및 보안 전문가 검토를 통해 연구의 실무적 기여와 이론적 기여도를 확인하는 것이다. MS-SDL 방법론을 활용한 이유는 첫째, Microsoft사에서 자체 적용한 결과 실제로

많은 효용성을 얻고 있으며, 글로벌 제조 기업들이 많이 적용하고 있기 때문이다. 둘째, MS-SDL은 위협모델링을 적용할 수 있는 도구를 지원해주어 실무에서 쉽게 활용이 가능하기 때문이다.

본 연구에서 설계된 SDL 프로세스에 대한 효율성 검토는, Home IoT 제조사의 보안취약점 분석 전문가들의 검토에 의해 이루어졌다. 본 논문은 총 5장으로 구성되며 연구에 대한 세부적인 내용 및 수행 절차는 [그림 3]과 같다.

제2장 선행연구 분석에서는 IoT 공통 보안원칙, IoT 공통 보안가이드, OWASP Top 10, Global 컨설팅 기업의 IoT 보안 요구사항, 몇 가지 논문들의 보안 요구사항을 분석한 결과, 제공하고 있는 보안 요구사항들의 범위와 목적이 각각 상이하고 해당 항목에 대한 검증이 없다는 문제점을 확인하게 되었다.

제3장에서는 선행연구의 문제점을 개선하기 위해 보안 요구사항의 재정립을 진행하여 새롭게 도출한 IoT 보안 요구사항이 Home IoT 가전기기의 모든 위협을 수용할 수 있는지를 검증한다. 검증방법으로는 Microsoft사의 위협모델링을 활용하고 검증을 통해 새롭게 도출되는 위협의 특징을 재분류하여, Home IoT 가전기기에 최적화된 새로운 보안 요구사항으로 도출한다. 기존에 존재하는 가이드 및 논문에서 제시하는 보안 요구사항과 새롭게 도출한 Home IoT 가전기기에 특화된 보안 요구사항을 비교하여 탐지율을 확인한다. 탐지율 확인 후 근본적인 Home IoT 가전기기 보안의 한계에 대한 시사점을 도출한다. 시사점을 보완하기 위해서는 Home IoT 가전기기에 특화된 SDL 프로세스를 적용해야 하며 이를 위해 여러 가지 SDL 방법론을 검토한 후 각 단계별 SDL 프로세스를 만들고 실무에서 적용하게 된다.

제4장에서는 설계된 Home IoT SDL 프로세스를 제조사에 적용하여 도출된 연구 결과에 대한 분석을 실시한다.

마지막으로 제5장에서는 연구결과 분석사항을 종합하여 연구의 활용 방안 및

제언을 하며, 본 연구의 한계점을 토대로 향후 연구 방향을 제시하고자 한다.



[그림 3] 연구의 수행 절차

제2장 선행연구 분석

제1절 IoT 보안 관련 요구사항 분석

Home IoT 가전기기의 보안성 향상을 위한 선행연구로는 기존에 존재하는 위협 모델링을 분석하여 보안 요구사항과 제3장 연구의 설계에 반영하고자 한다.

1. 기존 보안 요구사항 분석

4차 산업혁명의 큰 부분을 차지하는 기술로써 IoT 제품이 증가하면서, IoT 보안에 대한 다양한 보안 요구사항들이 국내·외 가이드, 논문 등으로 발행되고 있다. Home IoT의 보안 요구사항을 도출하기 위해 조사한 대상은 IoT얼라이언스에서 발표한 “IoT 공통 보안 7대 원칙^[13]”과 해당 원칙을 기준으로 “OWASP Top 10^[14]”, “IoT공통 보안 가이드^[15]”, “Global 컨설팅 기업 IoT 점검 항목”, “IoT 보안성 검토에 관한 논문”을 종합하여 분석하였다.

1.1 OWASP IoT Top 10

OWASP(The Open Web Application Security Project)는 국제 웹 표준기구로 정보 노출, 악성 파일 및 보안 취약점 등을 다양하게 연구하고 있다. 그 중 IoT 서비스에서 발생 빈도가 높고 보안상 영향을 많이 줄 수 있는 보안취약점 10개를 2014년에 처음으로 발표하였다. 본 논문은 2014년 버전을 기준으로 사용하였으며 10대 보안 취약점은 다음과 같다.



[그림 4] OWASP IoT Top 10

OWASP에서 정의한 “IoT 취약점 Top 10”은 가상화와 클라우드, 빅데이터와 IoT로 서비스 환경이 급격하게 이동함에 따라 IoT 기기 자체가 가지는 취약점이 크게 문제가 되고 있으며, 세부 항목은 [표 2]와 같다.

[표 2] OWASP IoT Top 10 항목

No	구분	세부 항목
I1	웹 인터페이스 취약점	웹 인터페이스에서 발생하는 일반적인 취약점 에 대한 항목 인젝션, 인증 및 세션 관리 취약점, 크로스 사이트 스크립트, 취약점 접근 제어, 보안 설정 오류, 민감 데이터 노출, 공격방어 취약점, 크로스사이트 요청 변조(CSRF), 알려진 취약점이 있는 컴포넌트 사용, 취약한 API
I2	인증 / 권한 부족	강력한 암호가 필요한 요소에 적절한 암호화 사용 확인 접근에 대한 분리가 필요한 경우 세분화 된 액세스 제어 확인 자격에 대한 증명이 올바르게 보호되는지 확인 필요한 경우 두 가지 요소 인증 구현 중요한 기능을 수행하는 경우 재 인증 구현 암호 제어 구성 옵션 사용여부 자격 증명의 취소(계정삭제) 가능여부 서비스 제공 시 필요한 모든 포인트 별로 인증이 구현되어 있는지 확인 (앱, Device, 서버 등)

No	구분	세부 항목
		각 EndPoint로 보내는 인증 토큰/세션(사용자 확인)키가 항상 다른지 확인 사용자 ID, 앱 ID, Device ID가 고유한지 확인
I3	네트워크 보호	필요한 포트만 노출되고 사용하는지 확인 포트에 대한 퍼지 공격 테스트 도스 공격 테스트 비정상 트래픽에 탐지 및 차단 기능
I4	전송 암호화	SSL 및 TLS를 사용하여 암호화 하고 있는지 확인 SSL 및 TLS를 사용할 수 없는 경우 중요 정보에 대해서 적절하게 암호화 하고 있는지 확인 표준 암호화를 사용하고 있는지 확인
I5	개인 정보 보호	필요한 정보만 수집되고 있는지 확인 수집되는 정보는 데이터가 식별되지 않게 익명으로 처리되고 있는지 확인 수집 된 데이터가 암호화로 올바르게 보호되는지 확인 앱, Device, 서버 등 모든 구성 요소가 개인정보를 적절히 보호하는지 확인 인가된 사람만 개인정보에 접근할 수 있도록 구현되어있는지 확인 수집 된 개인정보에 대해서 보존 제한 설정이 되어 있는지 확인 수집된 데이터가 필요이상 많은 경우 “통지 및 선택”이 가능한지 확인 수집 및 분석된 데이터에 대한 역할 기반 액세스 제어 및 권한 부여가 적절하게 적용되어 있는지 확인 분석된 데이터가 오남용 되었는지 확인할 수 있는 기능이 구현되어 있는지 확인
I6	보안이 적용 되지 않은 클라우드 인터페이스	기본 사용자 자동 변경 기능 확인 클라우드 서비스 생성 시 자동 암호 재설정 기능을 적용하여 타 사용자의 계정을 사용할 수 없도록 구축되어 있는지 확인 계정 잠금 기능 여부(3~5회) 확인 XSS, SQL인젝션, CSRF 취약점 확인 자격 증명이 인터넷을 통해 노출되지 않도록 보장(SSL 등) 두 가지 요소로 인증되도록 구현되어 있는지 확인 비정상 요청 및 시도 감지
I7	모바일 인터페이스 취약점	서버에서 발생할 수 있는 취약점 확인(파라미터 변조) 중요 정보들이 스마트폰 내에 저장되는지 확인 민감한 정보 평문 전송 확인 의도하지 않은 데이터 누출 확인 인증 및 인가 검증 미흡 취약한 암호화 Client 사이트 인젝션 신뢰할 수 없는 입력 값에 의한 보안 의사 결정 (신뢰할 수 없는 어플리케이션이나 외부 프로세스와 통신을 할 때 발생) 부적절한 세션 관리 확인 바이너리 보호 미흡 여부 확인

No	구분	세부 항목
		(바이너리 변조, 어플리케이션 디컴파일, 리버싱 등)
I8	보안 환경 구성 취약점	일반 사용자와 관리 사용자의 분리 기능이 제공되는지 확인 인증 등의 강력한 Secure Boot로 구성되어 있는지 검증
I9	SW 펌웨어 취약점	업데이트 기능이 있으며, 안전을 보장받고 있는지 검증(안전한 메커니즘) 표준 암호화 방식을 사용하여 업데이트 파일이 암호화되어 있는지 검증 업데이트 시 암호화된 프로토콜을 사용하는지 검증 업데이트 파일의 위변조를 별도의 서명을 통해 확인되고 있는지 검증 Secure Boot로 구성되어 있는지 검증
I10	물리적 보안	쉬운 저장장치 제거 여부 검증 Device 내부 데이터가 안정적으로 암호화되어 있는지 검증 USB 포트 및 다른 외부 포트를 사용하여 악의적으로 장치에 액세스 여부 검증 제품의 관리 기능을 제한 할 수 있는 기능 존재 확인

1.2 IoT 공통 보안 가이드

2016년 10월 발행된 IoT 공통 보안 가이드로 “IoT 공통 보안 원칙”을 기준으로 IoT 제품 및 서비스의 설계, 개발, 설치, 운영관리, 폐기까지 모든 주기에 걸쳐 발생할 수 있는 보안위협에 대응하기 위해 고려해야 하는 기본적인 보안 요구사항을 제시하고 있다.

[표 3] IoT공통 보안 가이드 항목

No	구분	세부 항목
1	정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계	IoT 장치의 특성을 고려하여 보안 서비스의 경량화 구현 IoT 서비스 운영 환경에 적합한 접근권한 관리 및 인증, 종단 간 통신 보안, 데이터 암호화 등의 방안 제공 SW보안기술과 하드웨어 보안 기술의 적용 검토 및 안전성이 검증된 보안기술 활용 IoT 제품 및 서비스에서 수집하는 민감 정보(개인정보 등) 보호를 위해 암호화, 비식별화, 접근관리 등의 방안 제공 IoT 서비스 제공자는 수집하는 민감 정보의 이용목적 및 기간 등을 포함한 운영정책 가시화 및 투명성 보장
2	안전한 SW 및 HW	소스코드 구현 단계부터 내재될 수 있는 보안 취약점을 사전에 예방

No	구분	세부 항목
	개발기술 적용 및 검증	하기 위해 시큐어코딩 적용 IoT 제품·서비스 개발에 사용된 다양한 SW에 대해 보안 취약점 분석 수행 및 보안패치 방안 구현 펌웨어/코드 암호화, 실행코드 영역제어, 역공학 방지 기법 등 다양한 하드웨어 보안 기법 적용
3	안전한 초기 보안설정 방안 제공	IoT 제품 및 서비스 (재)설치 시 보안 프로토콜들에 기본으로 설정되는 파라미터 값이 가장 안전한 설정이 될 수 있도록 “Secure by Default” 기본 원칙 준수
4	보안 프로토콜 준수 및 안전한 파라미터 설정	안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라미터 설정
5	IoT제품·서비스 취약점 패치 및 업데이트 지속이행	IoT 제품·서비스의 보안 취약점 발견 시, 이에 대한 분석 수행 및 보안패치 배포 등의 사후조치 방안 마련 IoT 제품·서비스에 대한 보안취약점 및 보호조치 사항은 홈페이지, SNS 등을 통해 사용자에게 공개
6	안전 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련	최소한의 개인정보만 수집·활용될 수 있도록 개인정보보호정책 수립 및 특정 개인을 식별할 수 있는 정보의 생성·유통을 통제할 수 있는 기술적·관리적 보호조치 포함
7	IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련	다양한 유형의 IoT 장치, 유·무선 네트워크, 플랫폼 등에 다양한 계층에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행 침해사고 발생 이후 원인분석 및 책임추적성 확보를 위해 로그기록의 주기적 저장·관리

1.3 Global 컨설팅 기업 IoT 보안 점검 항목

Global 컨설팅 기업에서 적용하고 있는 IoT 보안점검 세부항목을 살펴보면 [표 4]와 같다.

[표 4] Global 컨설팅 기업 IoT 보안 점검 항목

No	구분	세부항목
1	웹 인터페이스 취약점	알려진 웹 인터페이스 취약점 존재 여부 확인(웹 체크리스트 사용)
2	모바일 인터페이스 취약점	알려진 모바일 인터페이스 취약점 존재 여부 확인 (모바일 체크리스트 사용)
3	사용자 인증	강력한 패스워드 정책: 일정 횟수 이상의 인증 실패에 대한 제한이 없음
4		강력한 패스워드 정책: 길이가 8자 이하 비밀번호 지정 가능
5		강력한 패스워드 정책: 일련번호, 주민번호, 아이디 등 추측하기 쉬운 비밀번호 지정
6		강력한 패스워드 정책: 이전에 사용했던 비밀번호와 동일한 비밀번호로 변경 가능
7		강력한 패스워드 정책: 비밀번호 사용 기간에 제한이 없음
8		강력한 패스워드 정책: 특수문자, 영문자, 숫자로 이루어지지 않음
9		강력한 패스워드 정책: 아이디/비밀번호 외 공인인증서 등 추가 인증수단 미흡 (단, 개인정보취급자 및 금융서비스만 해당) two-factor 인증
10		사용자 계정/패스워드의 자동완성기능 제한이 없음
11		사용자 정보 변경 후, 재인증 절차가 없음
12		디폴트 계정 및 패스워드 사용
13		사용자 인증 정보 평문 저장
14		사용자 및 노드 인증 로직 우회 (ID/Pwd인증, Setup 코드, 기타 인증 etc...)
15		취약한 암호화 알고리즘 사용
16	불필요한 파일 노출 및 중요정보 노출	단말기 내 중요정보 (개인정보, 인증정보 등) 평문 저장
17		중요정보 평문 전송
18		단말기 내 로그 파일 및 임시 파일 확인 (예: 이벤트 로그 및 임시 파일 (tmp) 내 민감 정보 저장 여부 확인)
19		단말기 내 로컬 데이터 베이스 내 민감 정보 저장 여부 확인
20		백업 및 임시 파일 노출 (중요정보 포함)
21		백업 및 임시/샘플 파일 노출 (중요정보 미포함)
22		펌웨어 내 중요정보 노출 (예: 펌웨어 정보 내 암호화 키 및 기타 중 요정보 노출 등)
23		디버깅 정보 노출

No	구분	세부항목
24	개인정보 및 중요정보보호	최소한의 개인정보 수집여부
25		중요정보 (개인정보, 인증정보, 기기제어 등) 암호화 전송 미흡: TCP 프로토콜
26		중요정보 (개인정보, 인증정보, 기기제어 등) 암호화 전송 미흡: UDP 프로토콜
27		중요정보 (개인정보, 인증정보, 기기제어 등) 암호화 전송 미흡: HTTP 프로토콜
28		중요정보 (개인정보, 인증정보, 기기제어 등) 암호화 전송 미흡: ZigBee 프로토콜
29	부적절한 환경 설정	부적절한 에러 처리
30		단말기설정 미흡: 불필요한 포트 오픈
31		단말기설정 미흡: 보안 패치 미흡
32		단말기설정 미흡: 서버 종류/버전 정보 노출
33		단말기설정 미흡: 기타
34	취약한 물리적 보안	하드웨어 포트(UART, Jtag, Serial) 접근 가능 및 악의적인 목적으로 활용 가능 여부 확인
35		저장된 데이터 암호화 여부 확인
36		펌웨어 다운로드 및 업로드 가능 여부 확인
37	기타	히든 모드가 적절한 방법으로 구현되어 있는지 확인
38		프로세스 및 비즈니스 로직 우회 가능 여부 확인
39		부적절한 API 사용 (예: 히든 API 및 민감정보수집 등)
40		펌웨어/어플리케이션 무결성 검증 (예: 펌웨어/어플리케이션 위변조 탐지 등)

1.4 관련 연구 논문

한정진은 “사물인터넷(IoT) 보안성 검토를 위한 보안아키텍처 설계와 점검항목^[16]”에서 ITU-T(International Telecommunications Union-Telecommunication)의 SG13 (클라우드 컴퓨팅, 모바일, 차세대 네트워크 등을 포함한 미래네트워크 연구그룹)에서 2011년 5월에 제정된 Y.2060(Overview of IoT)^{[17][18]}, IETF 표준화 기술 및 OneM2M^[19], IoT 보안 아키텍처^{[20][21][22]}등을 연구하여 [표 5,6,7]과 같이 3개 영역에

대한 IoT 보안 점검 항목을 제시하였다.

[표 5] IoT 보안성 검토를 위한 디바이스, 펌웨어, 앱 점검 항목 (제조/개발 단계)

No	구분	세부 항목
1	인증 및 권한관리	개체 상호 간 Challenge-Response 인증 절차가 존재하는가? *Challenge-Response 인증방식: 질문("challenge")를 전송하면 상대 측에서 올바른 답("response")을 회신하는 방식으로 이루어지는 인증 방식
2		패스워드 복구, 찾기, 변경 절차 시 안전한 추가 인증을 적용하고 있는가?
3		패스워드 정책(패스워드 복잡도, 변경 주기 등)을 강제화하고 있는가?
4		원격으로 디바이스로 접근할 경우, 관리자 권한으로의 접근을 제한하고 있는가?
5		관리자 계정이 각 role에 맞추어 권한이 주어져 있는가?
6	네트워크 보안	사용하지 않는 불필요한(취약한) 서비스 포트가 오픈되어 있는가?
7		공인 IP 사용으로 인하여 외부에서 각 디바이스로의 접근이 가능한가?
8		사용되고 있는 프로토콜에 대한 취약점 검토를 수행하고 있는가? (eg-UPnP 등) 또는 경량화 장비에 맞는 표준화된 프로토콜을 적용하고 있는가? *UPnP: 홈 네트워크 내 PC, 주변 장치, 모바일 디바이스, 지능형 가전제품 등의 네트워크 장치들이 서로 연동될 수 있도록 하는 범용 표준 프로토콜을 적용하고 있는가?
9		2개 이상의 Ethernet Card를 사용하는 디바이스가 Weak-End Model로 제작되어 있는가?
10		플랫폼, 모바일 단말기와 통신 시 민감한 제어 데이터 혹은 정보를 암호화하도록 하고 있는가? (SSL/TLS 적용 등)
11	암호화	COA 환경에서 KPA, CPA, CCA 환경으로 암호문에 대한 공격을 쉽게 만드는 환경 또는 서비스가 존재하는가? * 암호의 안전성을 확인하기 위한 Attack model의 대표적인 4가지 환경 COA(Ciphertext-onlyattack): 도청된 암호문만 공격자에게 주어지는 상황 KPA(Known-plaintextattack): 몇 쌍의 평문과 그에 해당하는 암호문이 공격자에게 주어지는 상황 CPA(Chosen-plaintextattack): 공격자가 선택한 평문에 해당하는 암호문을 얻을 수 있는 상황 CCA(Chosen-ciphertextattack): 공격자가 선택한 암호문에 해당하는 평문을 얻을 수 있는 상황
12		디바이스에 저장되는 암호화 키에 대한 접근을 차단하고 있는가?
13		암호화 방식은 임의의 방식이 아닌 안전하다고 권고 되는 표준 방식을 사용하고 있는가?
14		초기 디바이스 설정 시, 초기 기본 ID와 Password를 변경하도록 하고 있는가?

No	구분	세부 항목
15	로그관리	관리자 인터페이스에 보안 이벤트에 대한 로깅이 이루어지고 있는가?
16		디바이스에 적용되고 있는 서비스에 대한 보안설정은 검토되고 있는가?
17		디바이스 커널에 임의 코드실행을 방지하기 위한 설정이 되어 있는가?
18		디바이스에 대한 패치를 적용하기 전 별도로 이상 유무 테스트를 수행하고 있는가?
19	앱/ 펌웨어 관리	디바이스 내 프로그램이 실행될 때 root와 같은 관리자 권한으로 실행되는 것을 제한하고 있는가?
20		USB와 같은 외부의 포트를 이용하여 디바이스 내 데이터에 접근할 수 있는가?
21		펌웨어, 어플리케이션 개발 시, 시큐어코딩을 적용하고 있는가?
22		앱, 펌웨어에 대한 무결성 검증을 수행하도록 하고 있는가?
23		펌웨어, 어플리케이션 개발 후, 취약점 분석을 수행하고 있는가?
24	물리적 보안	암호화 연산을 수행하는 디바이스의 경우 부채널 공격에 대한 보안성 검토가 이루어 졌는가? * 부채널 공격: 암호알고리즘이 처리하는 시간이나 기타 다른 전자적 특성 등을 고려하여 암호키 값 또는 평문을 알아내는 공격기법을 의미
25		JTAG, Serial Pin 등 Debugging 을 위한 Pin을 숨기거나, Disable 혹은 특수한 인풋이 들어올 때만 동작하도록 처리되어 있는가?
26	예외상황 조치	디바이스에 대한 오작동 발생가능성에 대해 검토하고 있으며, 고장 발생 시 수동으로 디바이스를 제어할 수 있게 되어 있는가?
27	(사고대응)	A/S 단계에서 테스트 계정 혹은 설정이 외부에 공개되지 않도록 관리되고 있는가?

[표 6] IoT 보안성 검토를 위한 플랫폼 점검 항목

No	구분	세부 항목
1	인증 및 권한관리	패스워드 복구, 찾기, 변경 절차 시 안전한 추가 인증을 적용하고 있는가?
2		불필요한 관리자 계정에 대한 주기적인 검토를 수행하는가? (사용기간이 오래된 계정(90일~120일 이상), 탈퇴한 회원 계정 등)
3		패스워드 정책(패스워드 복잡도, 변경 주기 등)을 강제화하고 있는가?
4		플랫폼의 관리자 계정이 각 역할에 맞게 부여되어 있는가?
5		관리자 권한 부여에 대한 주기적인 검토가 이루어지고 있는가?
6	네트워크 보안	사용하지 않는 불필요한(취약한) 서비스 포트가 오픈되어 있는가?
7	통신 암호화	플랫폼, 모바일 단말기와 통신 시 민감한 제어 데이터 혹은 정보를 암호화하여 전송하는가? (SSL/TLS 적용 등을 포함하여)

No	구분	세부 항목
8	인터페이스 관리	특정 계정의 로그인 3-5회 실패 시 계정 잠금 정책이 존재하는가? (관리자 계정의 로그인 실패의 경우, 담당자에게 별도의 통보가 되도록 설정되어 있는가?)
9		사용되는 API의 취약점에 대한 검토가 이루어 졌는가?
10		개발자에 의해 플랫폼으로 upload되는 앱 또는 펌웨어에 대한 악성코드 감염 여부 또는 보안성 검토를 수행하고 있는가?
11		Cloud based web interface 또는 디바이스 web interface 가 있을 시 XSS, SQL injection 등 웹 기반 취약점에 대한 검토가 주기적으로 이루어지고 있는가?
12	보안 설정 및 로그관리	관리자 인터페이스에 보안 이벤트에 대한 로깅이 이루어지고 있는가?
13		일반 사용자의 보안 이벤트 발생 시 관리자 인터페이스에 경고 혹은 공지가 발생하도록 설정되어 있는가?
14		플랫폼 시스템(서버)에서 적용되고 있는 서비스에 대한 보안성 검토가 이루어지고 있는가?
15		관리자 및 사용자의 Session Timeout 설정이 존재하는가?
16	업데이트 관리	업데이트 서버에 대한 설정 및 오픈된 포트, 인터페이스의 보안성 검토가 이루어 졌는가?
17	개인정보 보호	연동 규격서에서 정의된 정보만 수집되는가?
18		개인정보가 암호화 및 마스킹 되지 않은 채 노출되는가? 예시) A) 고객명 두번째 자리, B) 주민등록번호 뒤 7자리, C) 여권번호 뒤 4자리, D) 휴대 전화번호 가운데 4자리, E) 비밀번호 전체, F) 계좌번호 뒤에서 5자리, G) 카드 번호 16자리 중 가운데 8자리와 유효기간 등
19		개인정보가 DB에 암호화되어 저장되어 있는가? Ex) 1급(일방향 암호화 적용): 비밀번호, 바이오정보(지문, 얼굴, 홍채 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보) 2급: 개인식별번호(주민등록번호, 면허번호, 외국인등록번호), 금융정보(계좌번호, 카드번호), 위치정보, 기기정보(IMEI)
20		해당 플랫폼은 표준 규격을 준수하여 관리되고 있는가?
21	사고대응	플랫폼에 대한 침해사고 발생 시, 침해사고 대응절차가 마련되어 있는가?

[표 7] IoT 보안성 검토를 위한 사용자(단말기) 관련 점검 항목

No	구분	세부 항목
1	단말기 보안	단말기(모바일)의 경우, 루팅(Rooting) 또는 탈옥(jailbreak)된 단말기를 사용이 제한되고 있는가?
2		단말기에 패턴 또는 암호입력을 통한 잠금 설정이 적용되도록 하고 있는가?
3		단말기에 백신이 설치되어 있으며, 주기적인 점검 및 업데이트를 수행하고 있는가?
4		단말기에 설치된 OS에 대한 패치 및 업데이트를 수행하고 있는가?
5	통신암호화	모바일 단말기 통신 시 민감한 제어 데이터 혹은 개인정보를 암호화하여 전송하는가? (SSL/TLS 적용 등을 포함하여)
6	개인정보 관리	연동 규격서가 정의한 정보만 사용하고 있는가?
7		개인정보가 DB에 암호화되어 저장되어 있는가? Ex)1급(일방향 암호화 적용): 비밀번호, 바이오정보(지문, 얼굴, 홍채 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보) 2급: 개인식별번호(주민등록번호, 면허번호, 외국인등록번호), 금융정보(계좌번호, 카드번호), 위치정보, 기기정보(IMEI)
8	디바이스 보호	IoT 디바이스에 대한 물리적 보호조치를 수행하고 있는가?
9		디바이스 초기 설정 시, 취약한 기본(default)설정을 변경하여 사용하고 있는가?
10	패스워드 관리	패스워드를 특수문자를 포함하여 8자리 이상으로 설정하고 있는가?
11		패스워드를 주기적(60일~90일)으로 변경하고 있는가?
12	로그기록 확인	사용자 접속 로그 및 등록된 디바이스 사용기록을 주기적으로 점검하여 이상 유무를 점검하고 있는가?

강준모는 “사물인터넷 환경에서 스마트TV 보안성 검증방안^[23]”에서 기존에 발행된 OWASP IoT Top 10과 사물인터넷의 특성 및 유형에 따른 점검 항목들을 연구하여 [표 8]과 같은 IoT 보안 점검 항목을 제시하였다.

[표 8] IoT 주요 보안 점검 항목 (강준모)

No	구분	세부항목
1	취약점 대책	개발 단계에서 취약점 방생 방지 운영 단계에서 발견된 취약점 해결
2	보안개발	구현 시 보안 프로그램을 실행하여 보안 테스트를 실시(바이러스 감시)
3	서버보안	서버보안(설정정보)을 정기적으로 확인
4	FW기능	연결 IP 주소를 제한 (ACL)
5	서버인증	상호 인증을 통해 부정 접속 방지
6	필터링	신뢰할 수 없는 웹사이트 및 메일 수신 금지
7	IDS/IPS	입출력 데이터 모니터링
8	도스 대책	Dos 공격을 차단하기 위한 대책 실시
9	안티바이러스	바이러스 탐지 및 제거하여 바이러스 감염 방지
10	가상패치	SW업데이트를 실시할 수 없는 경우 취약점 유입 전면 차단
11	유저인증	사용자 인증을 통해 허가된 사용자만 액세스 가능하도록 구현
12	메시지 인증	메시지 인증을 통해 정보의 위변조 방지
13	암호화 통신	데이터 통신 경로를 암호화
14	데이터 암호화	데이터 자체 암호화를 통해 정보 유출 차단
15	데이터 재사용 금지	데이터의 목적 외 이용 금지
16	화이트리스트 제어	허가된 프로그램만 동작하도록 구성
17	SW서명	서명된 SW만 동작하도록 구현
18	출하 시 상태 재설정	디바이스 출하 시 초기 상태로 재설정하여 데이터와 출하 후 모든 설정 삭제
19	보안삭제	삭제된 데이터는 복구 불가능하도록 삭제
20	HW변조	케이스 개봉을 감지하여 내부 정보를 자동으로 삭제하는 등의 하드웨어 보호기능
21	SW변조	프로그램과 데이터 구조 난독화 및 패킹 등을 통해 내부 구조와 데이터 보호
22	원격잠금	원격 조작에 의해 디바이스의 기능을 잠그고 제삼자에 의한 부정 이용 방지
23	원격삭제	원격조작에 의해 디바이스 내의 중요 정보를 삭제하고 정보유출 방지
24	로그분석	각종 로그를 분석하여 무단 액세스 감지 및 부정 기록 확인
25	사용자 동의	사용상 주의사항이나 사용자 동의 없는 동작의 실행 방지



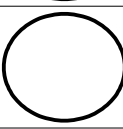



2. 위협모델링 분석

디지털 보안을 위한 단일한 해결책은 없다. 더 안전해지기 위하여 무엇을 보호할 것인지, 누구로부터 보호할 것인지를 생각해 보아야 된다. 이러한 위협모델링은 개인 차원에서뿐만 아니라 단체 차원에서도 수행할 필요가 있다. 위협모델링은 가능한 모든 취약 위험을 파악하고 추출하는 활동이며 설계단계에서 보안 문제에 대한 체계적인 접근 지원이 가능하다. 1990년대 초반부터 진행되고 있으며 Microsoft 내부 문서인 “The threats to our product”에서 보안 위협모델링의 STRIDE 방법론을 소개하고 있다^[24]. 또한 Michael Howard, James A. Whittaker은 제품 위험을 사전에 도출하기 위한 방법으로 위협모델링을 사용하였고 각 단계별로 상세하게 그 내용을 소개하였다^[25]. Adam Shostack은 시스템 개발 시, 위험을 사전에 도출하여 해결하기 위한 방법으로 위협모델링을 사용하였고 위협모델링에 대한 상세 방법과 효과 등을 설명하였다^[26]. 본 논문에서는 Home IoT의 분야별 구성도를 가지고 특정 위험을 도출해 낼 수 있는 Microsoft사의 위협모델링 기법을 사용하여 보안 요구사항을 도출하기 위해 활용하였다.

2.1 데이터 흐름 다이어그램

데이터 흐름 다이어그램(Data Flow Diagram: DFD)은 Process, Entity, Device, Trust Boundary 등으로 구체적인 데이터 흐름을 표현할 수 있기 때문에 시스템이나 서비스 방식의 보안위험을 파악하는데 도움을 줄 수 있으며 서비스 방식에 대한 파악도 용이하다.

[표 9] 데이터 흐름 다이어그램 요소

구성요소	기호	설명
Entity		사용자 혹은 프로그램
Process		데이터를 처리하는 작업
Multiple Process		다중 작업
Device		저장장치
Data Flow		요소 간 데이터 흐름
Trust Boundary		신뢰경계

2.2 STRIDE 분석

Microsoft사의 STRIDE는 시스템 분석 시 고려해야 할 보안속성 6가지에 대해 대응되는 위협들을 식별하는 방법이다^[27]. [표 10]은 STRIDE의 각 속성을 설명하는 것으로 STRIDE를 이용하기 위해서는 이에 대한 정확한 이해가 요구된다.

[표 10] STRIDE 분석

위협 분류	설명
신분 위장 (Spoofing)	신분을 속이는 위협은 공격자가 다른 사용자인 것처럼 위장하거나, 진짜 서버를 진짜 서버처럼 위장하는 것이다. 사용자 신분을 속이는 위협은 사용자 계정 및 패스워드와 같은 다른 사용자의 인증 정보를 취득하여 사용하는 것이다.
데이터 변조 (Tampering)	악의를 가지고 데이터를 변조하는 것을 말하며, 데이터베이스와 같은 데이터를 변조하거나, 인터넷과 같은 공개된 네트워크를 통과하는 데이터를 변조하는 경우가 있다.

위협 분류	설명
부인 (Repudiation)	상대방이 증명할 방법이 없는 상황에서 자신이 한 조작이나 행위를 부인하는 것이다. 예를 들어, 금지된 조작에 대한 추적 기록을 할 수 없는 시스템에서 금지된 조작을 행하고 이를 부인하는 경우를 들 수 있다.
정보 유출 (Information Disclosure)	정보 유출 위협은 정보의 취득이 허가되지 않은 사람에게 정보가 유출되는 것으로, 접근 권한이 없는 파일을 읽을 수 있거나, 데이터가 컴퓨터 간에 전송될 때 중간에 가로채 읽을 수 있는 경우를 들 수 있다.
서비스 거부 (DoS, Denial of Service)	정당한 사용자에게 대한 서비스를 못하게 만드는 위협으로, 웹 서버를 일시적으로 사용 불가능하게 만드는 것을 들 수 있다. 시스템이 가용성 및 안정성 측면에서도 이러한 위협에 대응해야 할 필요가 있다.
권한 상승 (Elevation of Privilege)	자신의 권한을 상승시켜 관리자 권한을 획득함으로써, 시스템을 손상시키거나 완전히 파괴하는 것이 가능하게 되는 위협을 말한다. 예를 들어, 공격자가 취약점이 있는 시스템에 실행파일을 복사하는데 성공하고, 다른 사람이 로그인 할 때 그 실행파일이 실행되도록 할 수 있는 상황에서, 관리자가 로그인하여 그 실행파일이 관리자 권한으로 실행되는 경우를 들 수 있다.

제2절 Security Development Lifecycle 분석

현재 많은 기업들은 SDL 프로세스를 적용한 안전한 SW개발을 진행하고 있으며 대표적인 SDL 방법론으로는 MS-SDL, CLASP, Seven-Touchpoint, TSP-Secure 등이 있다.

1. MS-SDL 방법론

Microsoft사는 보안이 적용된 안전한 SW를 개발하기 위해 자체적으로 만든 MS-SDL방법론을 적용하였으며, SDL이 적용된 SW는 이전 버전에 비해 50% 이상 취약점이 감소되었다고 발표했다. 또한 안전한 SW를 개발하기 위한 기본 원리로써 Secure by Design, Secure by Default, Secure in Deployment, Communication을 언급하였다^[28].

Secure by Design 은 SW의 구조 설계 시 위협모델링을 통한 위협을 도출하여 완화 방법을 제공하고 제작된 코드의 보안성을 강화하며, 기존에 알려진 취약점을 모니터링하여 제거한다는 내용을 포함한다. Secure by Default는 사용하지 않는 디폴트 기능, 위협을 야기할 수 있는 디폴트 세팅 등에 관한 내용이 포함되며, 최소한의 권한으로 실행하고 위협에 관해서 여러 개의 솔루션을 제공해야 한다는 내용이 포함되어 있다.

Secure in Deployment는 SW패치에 관련한 도구와 가이드를 생성해서 제공해야 한다는 내용이 포함되어 있다. Communication은 SW보안 취약점에 관련된 내용과 업데이트 정보를 지속적으로 제공하며, 보안과 관련된 문의사항에 대하여 항상 적극 대응해야 한다는 내용을 포함하고 있다.



[그림 5] MS-SDL

MS-SDL은 교육 단계, 요구사항 단계, 설계 단계, 구현 단계, 검증 단계, 릴리즈 단계, 대응의 총 7단계로 구성되어 있다. 각 단계별 보안활동의 적용 수준을 두 가지로 구분하고 있는데, 필수 보안활동의 경우는 반드시 수행해야 하며, 권고 보안활동은 상황에 따라 선택적으로 적용할 수 있는 활동이라 볼 수 있다. 각 단계별 세부 내용은 다음과 같다.

1.1 교육 단계

SW개발과 관련된 팀의 구성원들이 개발 보안과 보안에 관한 동향 등에 대해 매년 1회 교육을 받을 수 있도록 하는 단계이다. 또한 개발팀의 보안교육은 시큐어 설계, 프라이버시, 위협모델링, 보안테스팅, 시큐어코딩 등이 포함되어 있다.

1.2 요구사항 단계

신뢰성 있는 SW를 개발하기 위하여 프라이버시 요구사항 및 기본적인 보안 요구사항을 정의하는 단계이다. 요구사항 단계에서 필수로 적용해야 할 항목은 SDL 방법론 적용 여부 결정, 보안책임자 선정, 보안팀 선정, 보안 위험 평가, 보안 계획서 작성, 버그 추적 시스템 정의 등이 포함되어 있다.

1.3 설계 단계

SDL 설계 단계는 Home IoT 가전기기의 구현에서부터 릴리즈에 이르기까지 수행해야 하는 작업에 대한 계획을 수립하는 단계이다. 설계 단계에는 보안 사항 문서화, 위협모델링을 통한 위협 목록 작성, 안전하지 않은 코딩 패턴 알림, 소스코드의 보안성 검토 수행, 보안이 적용된 인스톨 실행, 보안 설계서 작성, 위협 모델의 검토 및 승인, 위협 모델 품질 보증, 방화벽 정책 준수여부 확인 및 보안 설계서 검토 등이 포함된다.

1.4 구현 단계

SDL 구현 단계는 SW의 보안 및 프라이버시에 관련된 문제점을 사전에 발견하고 해결하기 위해 개발 Best Practice를 수립하고 실행하도록 한다. 구현 단계에는 최신 버전의 개발 도구를 사용해야 하며 금지된 API 사용 회피, Excute 허가를 통

한 안전한 SQL 사용, 저장된 프로시저에서의 SQL 사용, 안전한 SW사용을 위한 사용자 정보 식별, 보안 형상관리에 대한 정보 생성, 정책에 대한 정의 및 문서화 등 많은 단계가 포함되어 있다.

1.5 검증 단계

검증 단계는 SW의 보안성을 검증하는 단계로써, 코딩단계에서 설정한 보안과 프라이버시가 잘 지켜지고 있는지를 프라이버시 테스트와 보안 푸쉬, 문서 리뷰를 통해 확인한다.

2. CLASP 방법론

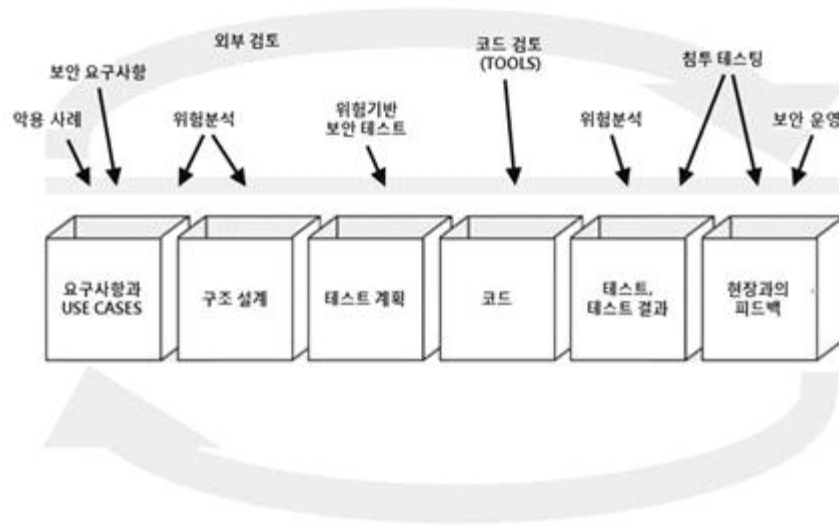
CLASP(Comprehensive, Lightweight Application Security Process)^[29] 방법론은 Secure Software사에서 개발하였으며, SW개발 생명주기의 초기단계에서 보안을 강화하기 위한 목적을 가진 프로세스이다. 활동중심, 역할기반의 프로세스로 구성된 집합체로 시스템이 코드를 작성하기 전에 적절한 애플리케이션 문제점을 명시하고 접근하도록 하기 위한 일련의 기법과 실천 방법들을 제시하고 있다. CLASP는 프로젝트관리자, 보안감사책임자, 개발자, 설계자, 테스트책임자 등 프로젝트 참여자에 대한 보안에 관한 지침을 제공한다. 또한 CLASP는 프로그램 오류로 인한 취약점 목록을 제공하며, 취약점들을 점검하기 위하여 자동화 툴을 사용하기도 한다.



[그림 6] CLASP의 6가지 관점

3. Seven-Touchpoint 방법론

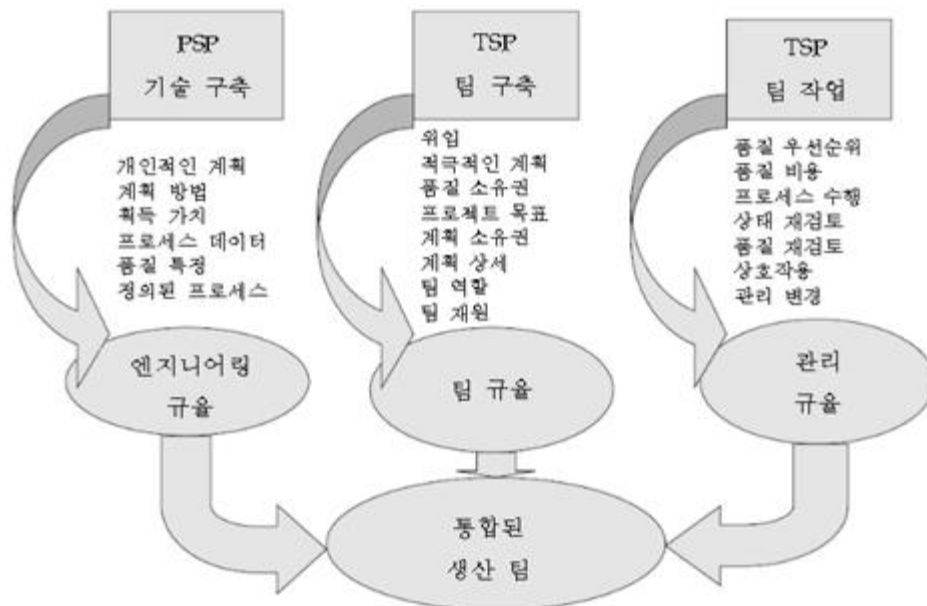
Seven-Touchpoint 방법론^[30]은 보안 강화를 하기 위한 기법으로 실무적으로 검증된 방법 중 하나이다. 이것은 [그림 7]과 같이 요구사항과 USE CASES, 구조 설계, 테스트 계획, 코드 검증, 테스트 및 결과 도출, 현장과의 피드백 총 7개의 프로세스로 이루어져 있으며 각각의 활동들이 별도로 관리되어 SW의 보안성을 더욱 강화 시킬 수 있다는 포인트를 가지고 있다. 각각의 활동들을 관리해야 하므로 각 터치 포인트에 관하여 개발자에게 더욱 주의 깊은 관리를 하도록 요구한다.



[그림 7] Seven-Touchpoint 방법론

4. TSP-Secure 방법론

TSP-Secure 방법론^[31]은 Team Software Process 로써 애플리케이션의 보안을 위한 설계 원칙이며, 보다 안전한 SW개발을 돕기 위해 설계되었다. TSP-Secure는 [그림 8]과 같이 PSP(Personal Software Process) 기술 구축과 PSP 팀 구축, 그리고 PSP 팀 작업의 구성으로 이루어져 있다.



[그림 8] TSP-Secure 주요요소 및 팀 구축 방법

제3절 시사점

선행 연구에서 IoT 보안 요구사항의 가이드, 글로벌 IT 컨설팅 기업의 가이드, 논문 등을 상세 분석한 결과, 각 가이드와 논문에서 제시하는 IoT 보안 요구사항은 모두 상이한 것을 확인할 수 있었고 빠른 속도로 시장이 성장하고 발전하고 있는 Home IoT 가전기기에 대해 특화된 보안 요구사항으로 적용하기에는 검증 과정이 부재하여 신뢰성이 부족한 문제점을 확인할 수 있었다.

이에 대한 해결 방안으로 Home IoT 가전기기에 대하여 위협 모델링을 진행하고 기존 보안 요구사항에 대한 재정립 및 새로운 보안 요구사항 도출을 진행하고 도출된 보안 요구사항의 취약점 탐지를 실시하여 그 효과성을 확인하는게 필요하였다.

그러나 새롭게 정립한 보안 요구사항의 취약점 탐지율이 기존 가이드 또는 논문 등의 보안 요구사항보다 효과적인 것이 검증될 경우라 하더라도 다음과 같은 문제가 발생하게 된다. 첫째, 발견된 취약점이 많을수록 가전기기에 대해 보완하는 기간이 길어지게 되므로 출시가 지연되고 따라서 기업에서 가전기기를 생산하는데 전체적인 비용이 증가하게 된다. 둘째, 출시한 가전기기에서 해킹사고가 발생할 경우 기업의 브랜드 가치하락은 물론 막대한 금전적 손실이 발생할 수 있다. 마지막으로 고객의 입장에서 구입한 가전기기를 통해 사생활과 개인정보가 노출되어 2차 피해를 야기할 수 있고 생명의 위협까지 직면하게 될 수도 있다. 따라서, 출시되는 Home IoT 가전기기의 근본적인 취약성 문제를 해결할 수 있는 방법이 필요하고 취약성 분석 기간의 효율성 또한 높여 전체 비용을 낮추는 연구의 필요성을 확인하게 되었다.

제3장 연구의 설계

제1절 Home IoT 가전기기 보안 요구사항 설계

Home IoT 가전기기에 특화된 보안 요구사항을 설계하기 위하여 선행연구에서 분석한 IoT 국내·외 가이드 및 논문을 바탕으로 IoT 보안 요구사항을 재정립하였다. 추가적으로 위협모델링 분석을 통하여 Home IoT 가전기기에 특화된 위협과 보안 요구사항을 도출하였다.

1. IoT 가전기기 보안 요구사항 설계

보안 요구사항 항목을 분석하여 IoT 기기의 통합적인 보안 요구사항 7개 항목 43개 세부항목을 도출하였다. 이를 대분류로 살펴보면 “SW보안”, “HW보안”, “인증”, “암호화”, “중요정보 노출”, “플랫폼 보안”, “펌웨어 보안”으로 구성되어 있으며, 각 항목의 세부 내용은 [표 11]과 같다.

[표 11] IoT 보안 요구사항

대분류	중분류	세부 항목
SW 보안	시큐어코딩	버퍼오버플로우 등의 공격에 취약한 함수 사용 여부 확인
		사용자 입력 값에 대해서 적절한 처리 여부 확인 (외부입력이 직접적인 명령어 실행이 이루어지는 경우)
		스크립트 언어에 중요 정보 노출 여부확인 소스코드에 중요정보 평문 노출 여부 확인
		응용 프로그램 컴파일 시 심볼정보 등의 포함되어 컴파일 되는지 확인
	퍼지 점검	변수에 지정된 버퍼 영역의 제한이 없어 더 많은 데이터의 입력 가능 여부 확인
	히든 모드	히든 모드가 적절한 방법으로 구현되어 있는지 확인 (SW방식, HW방식)

대분류	중분류	세부 항목
HW 보안	접근인터페이스 차단	JTAG, UART, ISP 등 Device와 직접 연결 가능한 인터페이스에 대한 차단 여부 확인
	HW분해 차단	외부 케이스 오픈 시 탐지하여 프로그램 정상동작 제어 여부 확인
인증	사용자인증	Default ID 및 Password 사용 여부 확인
		서비스 최초 인증 시 강제 인증 정보 변경 여부 확인
		강력한 패스워드 정책: 일정 횟수 이상의 인증 실패에 대한 제한이 없음 확인
		강력한 패스워드 정책: 길이가 8자 이하 비밀번호 지정 가능 확인
		강력한 패스워드 정책: 일련번호, 주민번호, 아이디 등 추측하기 쉬운 비밀번호 지정 확인
		강력한 패스워드 정책: 이전에 사용했던 비밀번호와 동일한 비밀번호로 변경 가능 확인
		강력한 패스워드 정책: 비밀번호 사용기간에 제한이 없음 확인
		강력한 패스워드 정책: 특수문자, 영문자, 숫자로 이루어지지 않음 확인
		강력한 패스워드 정책: 아이디/비밀번호 외 공인인증서 등 추가 인증 수단미흡 (단, 개인정보 취급자 및 금융 서비스만 해당), Two-Factor인증 확인
	권한 관리	접근에 대한 분리가 필요한 경우 적절한 분리 여부 확인
		사용자 ID 및 Device ID 가 고유하게 사용되며, 그에 따른 인증기능이 구현되어 있는지 확인 (서비스 운영 목적 1:N, N:1, N:N 방식으로 사용하는 경우 제외)
		원격으로 디바이스에 접근할 경우 관리자 권한의 접근을 제한하고 있는지 확인
	디버깅 인터페이스인 중	Device 접근 시 적절한 인증 기능 구현 여부 확인 (JTAG, UART 등) (강력한 패스워드 정책 부여 확인 및 Device별 인증정보 상의, 접속을 위한 Access Key 구현 등)
암호화	암호화강도	중요정보를 암호화 시 사용되는 키 및 알고리즘의 강도확인 (낮은 암호화 알고리즘 사용 시 Key 없어도 복호화 가능)
	인증정보 암호화	사용자 인증 정보 저장 시 해쉬 저장 여부 확인
	중요파일 암호화	중요정보 암호화 여부 확인
	키 관리	암호화에 사용되는 Key가 적절하게 보호되고 있는지 확인 (Key가 노출된 경우 복호화 가능)
	취약한 대칭키	제품별 암호화 키 동일 여부 확인

대분류	중분류	세부 항목
	표준 암호화 방식	암호화 방식은 표준 방식을 사용하고 있는지 확인
	부채널 공격방지	암호화 연산 수행 시 잘못된 요청을 하는 경우에도 동일한 연산 시간이 소요되는지 확인
중요 정보 노출	안전한 전송프로토콜	중요정보 전송 시 검증된 암호화 프로토콜 사용여부 확인
	저장 및 전송데이터 보호	중요정보 저장 및 전송 시 적절한 암호화 방식 사용 여부 확인
	중요정보 수집	최소한의 개인정보 수집 여부 확인
		개인정보 비식별화 기술 적용 여부 확인
		사용 완료된 개인정보 삭제 여부 확인
	중요정보 노출	Log를 통해 개인정보 및 중요정보 노출 확인
플랫폼 보안	환경설정	초기 플랫폼 설정이 보안에 적절하게 설정되어 있는지 확인 (기본 명령어, 폴더, 파일에 대한 접근 권한)
	불필요한 포트오픈	필요한 포트만 노출되고 사용하고 있는지 확인
	퍼지 점검	오픈된 포트에 대한 퍼지 공격 테스트 확인
	보안패치 미흡	공개된 라이브러리 및 응용프로그램 등 사용 시 현재까지 알려진 취약점 존재 여부 확인
	응용프로그램 무결성검증	주요 응용프로그램 동작 시 위·변조 확인 여부
	보안 업데이트	온라인 보안패치 기능 여부 확인
	로그수집 및 전송	응용 프로그램 실행, 포트 오픈 및 에러에 대한 수집 기능 및 원격 전송 기능 존재 여부 확인
펌웨어 보안	펌웨어 암호화	적절한 암호화를 통해 펌웨어를 보호하고 있는지 확인
	펌웨어 무결성검증	펌웨어 업데이트 진행 시 이미지 및 파일에 대한 적절한 검증 후 업데이트 기능 동작 여부 확인 (이미지 파일 사인 값 검증 등)

IoT 보안 요구사항의 가이드, 글로벌 IT 컨설팅 기업의 가이드, 논문 등을 분석하여 재정립을 진행하였고, 새롭게 도출한 IoT 보안 요구사항이 Home IoT 가전기기의 모든 위협을 수용할 수 있는지에 대한 확인과 검증이 필요하게 된다. 본 연구에서는 MS 위협모델링을 활용하여 Home IoT 가전기기들의 전체 위협에 대한 검토를 진행하였다.

2. 위협모델링 분석

Home IoT 가전기기들의 전체 위협 수용 여부를 확인하기 위해 기업에서 출시되고 있는 대표적인 가전기기 12개를 선정하였고 해당 Home IoT 가전기기는 [표 12]와 같다.

[표 12] 위협모델링 대상 Home IoT 가전기기

Home IoT 가전기기	설 명
에어컨	외부에서도 전원상태를 확인 및 작동 또는 온도 조절 등의 기능 설정 지원
냉장고	실시간 냉장고 내부 상태 확인 및 냉장고 사용 이력 지원
스마트TV	인터넷에 연결되어 실시간 콘텐츠를 다운로드하여 이용이 가능하며, 뉴스·날씨·이메일 등 확인 가능
스마트도어락	원격 문 열림/잠금 기능 사용 및 사용 이력 확인 가능
IP 카메라	무선영상 송출을 통한 실시간 스트리밍 및 데이터 임시 저장 기능 지원
Home CCTV	실시간 모니터링, 침입 감지 및 영상을 자동으로 대용량 저장 기능 지원
스마트밴드	심장박동측정, 수면 측정, 걸음 측정, 건강관리 기능 제공
스마트의자	자세의 변화, 자세 별 시간, 자세비율에 대한 정보, 착석 시간 등의 정보 제공 기능 지원
스마트스피커	스피커의 음성인식 기능을 통해, 음악, 생활/정보, 검색, 쇼핑/주문, 금융 등의 기능 지원
Home에너지 저장 시스템	에너지 저장 시스템으로 태양광 에너지를 배터리 팩에 저장해주는 기능
원격 검침기	LTE 망을 활용한 원격 자동 검침 기능 지원
스마트보일러	외부에서 보일러 상태 확인 및 온도 조절, 타이머 설정 기능 지원

Home IoT 가전기기 12개를 대상으로 위협모델링을 진행한 결과, IoT 보안 요구사항 7개 항목, 43개 세부항목 외 추가적인 위협이 도출되었다. 추가로 도출된 위협들을 위협의 특징별 재분류를 진행한 결과, Home IoT 가전기기에 대한 보안 요구사항과는 별도로 4개의 도메인으로 추가 분류되었고, 분류된 도메인 범위에 포함되는 Home IoT 가전기기는 [표 13]과 같다.

[표 13] Home IoT 도메인

도메인	설 명
도메인1 (Home IoT 공통)	에어컨, 냉장고, 스마트TV
도메인2 (보안&디지털 영상)	스마트도어락, IP 카메라, Home CCTV
도메인3 (건강&금융)	스마트밴드, 스마트의자, 스마트스피커
도메인4 (에너지)	Home 에너지 저장 시스템, 원격 검침기, 스마트보일러

위협모델링을 통해 도출된 위협에 대해 추가 분류된 도메인별 보안 요구사항은 [표 14]와 같다.

[표 14] 도출된 도메인별 보안 요구사항 항목

도메인	보안 요구사항	세부 항목
도메인1. (Home IoT 공통)	메모리 보호기법 적용 여부 확인	버퍼오버플로우로 인한 공격을 방지하기 위해 메모리 보호기법 적용여부 확인
	보안 이벤트 관리	사용자의 금전적 손실 및 사생활 침해, 안전에 영향을 미칠 수 있는 가전기기의 경우 보안이벤트 로그를 생성해야 하며 관리, 경고 절차를 구현 했는지에 대한 여부 확인
	네트워크 구간 접근 제어 설정	네트워크 통신을 하는 서비스에 대한 접근 제어 설정을 통해 비인가 접근을 제어 하는지에 대한 여부 확인
	안전한 세션 및 토큰 관리	세션/토큰이 임의의 값으로 생성되며, 쉽게 노출/추측이 가능한지 여부 확인
	네트워크 재생공격 방지 미흡	네트워크를 통해 전송되는 암호화된 데이터를 해독하지 않고 행해지는 공격을 방지하는지에 대한 여부 확인
	중간자 공격 방지 미흡	중요정보를 제 3자가 위변조하는 것을 방지하기 위해 안전한 암호화 통신 채널을 구현하는지에 대한 여부 확인

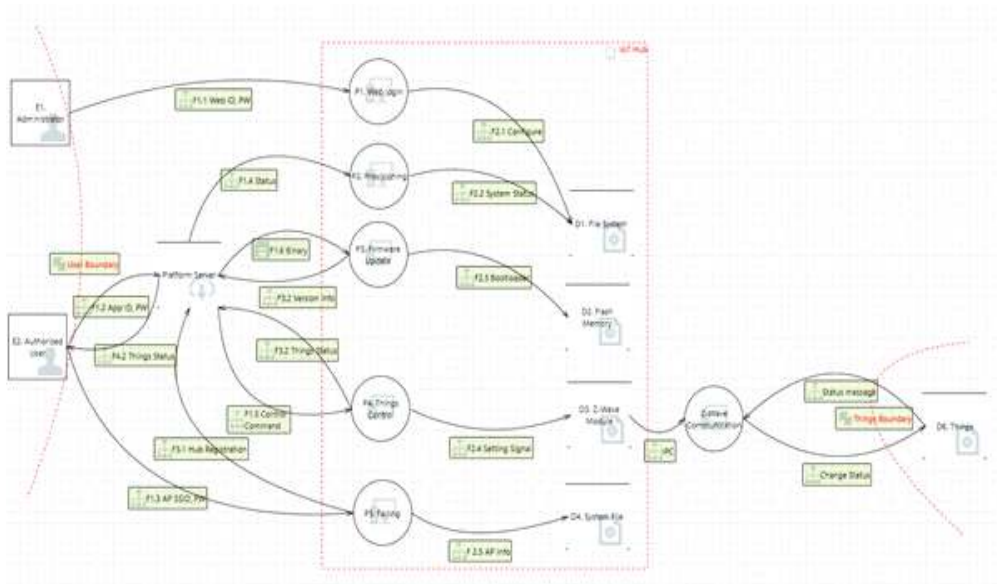
도메인	보안 요구사항	세부 항목
	IoT시스템 구성 간 상호인증 미흡	비 인가된 사용자에게 의한 가전기기 제어나 개인정보 등 민감 정보 유출을 방지하기 위한 상호인증 수행여부 확인
도메인2. (보안 & 디지털 영상)	데이터 무결성 확보 여부	데이터 무결성을 검증해야 하며 무결성 오류 발생 시 대응방안 구현 여부 확인
	적절한 영상보관 기간 설정	영상보관 기간 설정에 대한 정책 존재 여부 확인
도메인3. (건강 & 금융)	결제 금액 조작	서비스 내 결제 시도 시, 조작한 결제 금액을 통해 결제할 수 있는 취약점 확인 필요
	타 사용자에게 결제 금액 부당 부과	서비스 내 결제 시 인증 및 세션처리 미흡으로 타 사용자에게 결제 금액 부당 부과가 가능한 취약점 확인 필요
	암호화 되지 않은 금융정보	금융정보가 평문으로 통신채널을 통해 송수신 될 경우 공격자가 스니핑을 통해 다른 사용자의 민감한 데이터를 획득할 수 있는 취약점 확인 필요
	암호화 되지 않은 바이오정보	바이오정보가 평문으로 통신채널을 통해 송수신 될 경우 공격자가 스니핑을 통해 다른 사용자의 민감한 데이터를 획득할 수 있는 취약점 확인 필요
도메인4. (에너지)	비 허가자의 LTE 데이터 접근 및 사용	USIM 탈취 후 비인가자에 의한 USIM사용 여부 탐지 및 접근제어 설정이 존재하는지 확인 필요

2.1 도메인1 (Home IoT 공통)

“Home IoT 공통” 도메인의 가전기기 대상은 생활 가전을 대표하는 에어컨, 냉장고, 스마트TV가 포함되었다. 위협모델링 진행 결과, 도출된 위협이 점검 대상 12개 Home IoT 가전기기에서 공통으로 포함되었다. [그림 9]는 Microsoft사의 위협모델링 도구를 사용하였고 Home IoT 가전기기의 기본이 되는 구조를 적용했으며, 다른 도메인2,3,4에도 공통으로 포함되는 구조이다. 크게 USER, Things를 컨트롤 할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결해주는 IoT Hub Zone 그리고 Things 이렇게 4개 구간으로 나누었다.

위협모델링 도구를 사용하여 도출된 4개 구간의 주요 위협은 보안 이벤트 관리,

네트워크 구간 접근제어, 세션 및 토큰관리, 재생공격, 중간자공격, 상호인증 미흡으로 나타났다. 이러한 위협들과 선행연구 결과물인 43개의 점검 항목을 비교하여 “도메인1”에 대한 새로운 보안 점검 항목을 개발하였으며, 본 논문 3장 2절의 2. “Home IoT 가전기기 보안 요구사항 검증”에서 확인할 수 있다.



[그림 9] 도메인1 데이터 흐름도

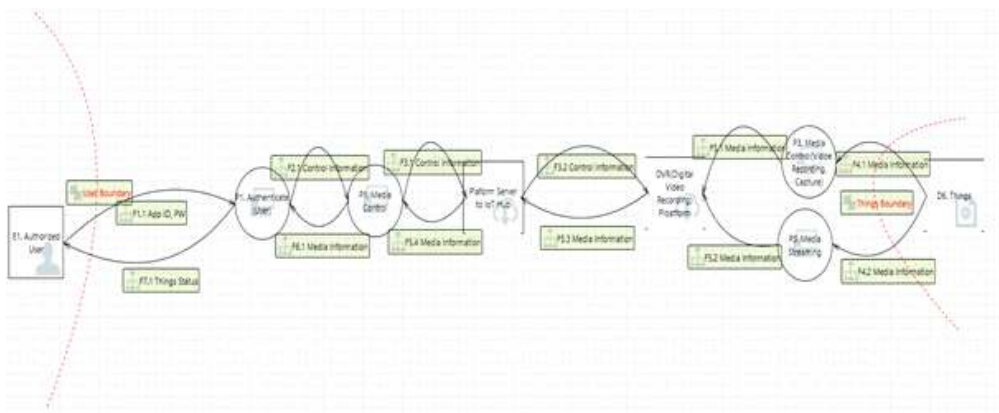
2.2 도메인2 (보안&디지털영상)

“보안&디지털영상” 도메인의 가전기기 대상은 IP 카메라, Home CCTV, 스마트 도어락이 포함되며 도메인2의 위협모델링 진행 결과 영상과 관련된 시스템이나 기능을 포함하고 있는 Home IoT 가전기기를 대상으로 위협이 도출되었다. 앞서 언급한 바와 같이 도메인1은 가전 IoT의 공통적으로 포함되는 위협모델링이므로, 도메인2에서 도출된 위협들을 추가하면 도메인2의 전체 위협항목이 된다.

[그림 10]과 같이 USER, Things를 컨트롤할 수 있게 해주는 Platform Server, 사

용자와 Platform Server를 연결해주는 IoT Hub Zone이 존재하며, 영상과 관련된 IoT Things들과 많이 사용되는 DVR (Digital Video Recording Platform)을 추가하였다.

위협모델링 도구를 사용하여 각 구간의 위협을 도출한 결과, 영상정보에 관한 데이터 무결성 위협, 영상보관 기간에 관한 위협이 추가로 도출되었고 점검 결과 값에 대해서는 본 논문 3장 2절의 2. “Home IoT 가전기기 보안 요구사항 검증”에서 확인할 수 있다.



[그림 10] 도메인2 데이터 흐름도

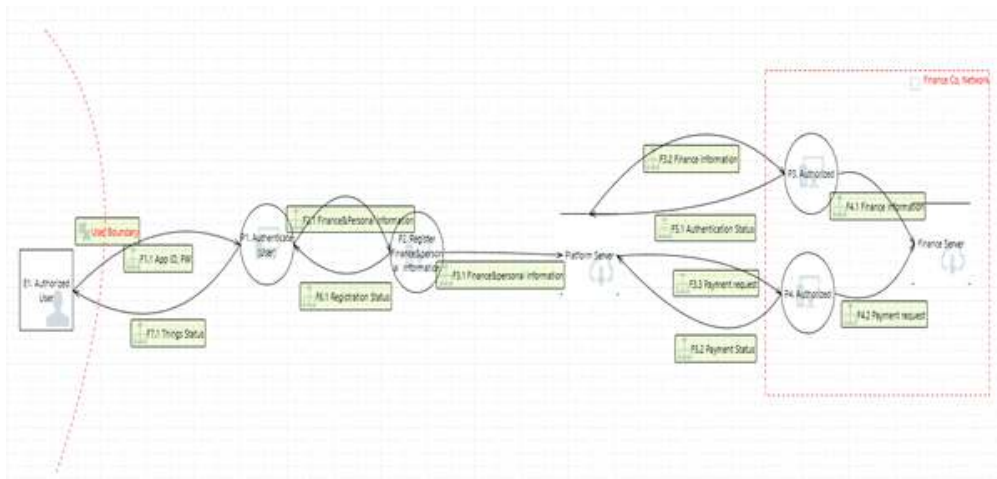
2.3 도메인3 (건강&금융)

“건강&금융”도메인의 가전기기 대상은 스마트밴드, 스마트의자, 음성 금융거래가 가능한 스마트스피커가 포함되며 도메인3의 위협모델링 진행 결과 중요정보를 전달하고 Hub역할을 수행하는 기능을 Home IoT 가전기기를 대상으로 위협이 도출되었다.

[그림 11]과 같이 USER, Things를 컨트롤할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결해주는 IoT Hub Zone이 존재하며, 금융결제와 관련

되어 IoT Things들과 많이 사용되는 금융권 서버와 연결되는 부분을 추가하였다.

위협모델링 도구를 사용하여 각 구간의 위협을 도출한 결과, 주요 위협은 결제와 관련된 조작, 정보노출, 암호화 관련 위협이 있으며, 선행연구 결과 43개의 점검 항목을 포함하여 점검한 결과 값은 본 논문 3장 2절의 2. “Home IoT 가전기기 보안 요구사항 검증”에서 확인할 수 있다.



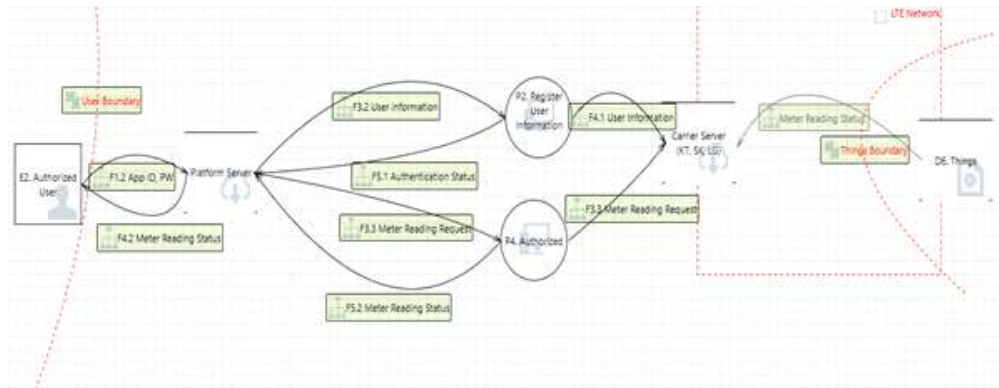
[그림 11] 도메인3 데이터 흐름도

2.4 도메인4 (에너지)

“에너지” 도메인의 가전기기 대상은 최근 많이 확산되고 있는 Home 에너지 저장 시스템, 원격 검침기, 스마트보일러가 포함되었으며, 위협모델링 진행 결과 LTE 통신으로 이루어지는 Home IoT 가전기기를 대상으로 위협이 도출되었다.

[그림 12]와 같이 USER, Things를 컨트롤할 수 있게 해주는 Platform Server, 사용자와 Platform Server를 연결해주는 IoT Hub Zone이 존재하며, 원격 검침기에 USIM을 사용하여 LTE 망 통신을 하는 구조를 추가하였다.

위협모델링 도구를 사용하여 각 구간의 위협을 도출한 결과, 도출된 주요 위협은 비 허가자의 LTE 데이터 접근 및 사용이 있으며, 점검 결과 값에 대해서는 본 논문 3장 2절의 2. “Home IoT 가전기기 보안 요구사항 검증”에서 확인할 수 있다.



[그림 12] 도메인4 데이터 흐름도

제2절 Home IoT SDL 프로세스 설계 및 적용

Home IoT 가전기기를 만드는 제조사가 Home IoT SDL 프로세스를 설계하기 위해서는 그에 합당한 목적과 표준 지침을 만들어 전사적으로 적용시켜야 한다. SDL 프로세스 설계 목적으로는 Home IoT 가전기기의 보안 향상을 목표로 개발 프로세스에 보안활동을 추가하여 가전기기를 표준화하는 것이다. 이러한 프로세스를 전사 표준지침으로 만들고 SDL과 관련된 부서에 전파하고 적용시켜야 된다. 본 논문에서는 MS-SDL을 기반으로 세부 프로세스를 설계하고 적용하였다.

제3장에서는 Home IoT 가전을 만드는 제조사가 SDL 프로세스를 설계하고 적용함으로써 가전기기의 보안성을 향상시킬 수 있도록 구체적인 보안활동 프로세스

를 제시하였다.



[그림 13] Home IoT Security Development Lifecycle 프로세스

1. SDL 관련 용어 및 책임 정의

Home IoT SDL 프로세스를 기업에 적용시키기 위해서는 SDL에 관련한 정확한 용어 정의와 관련된 부서의 책임 정의가 정확히 이루어져야 한다. 다음은 본 논문의 연구범위와 관련된 Home IoT SDL 적용을 위해 필요한 용어와 부서별 책임과 권한을 정리한 테이블이다.

[표 15] SDL 관련 용어

용어	설명
퍼지 점검 (Fuzzy Test)	분석가들이 SW에 존재하는 버그를 효과적으로 찾아낼 수 있는 보안 취약점 발굴 기술 중 하나로 다량의 유효하지 않거나 임의의 무작위 데이터를 시스템(웹, 파일, 네트워크프로토콜, 메모리)에 수행해보고, 메모리누수, 크래시, 기타 보안 이슈가 발생하지 않는지 모니터링하기 위해 랜덤, 네거티브 자동화 형식으로 수행되는 점검
취약점 분석 (Vulnerability Assessment)	가전기기의 SW보안향상을 목적으로 SW에 공격시나리오 및 정형화된 점검항목을 기반으로 프로그래머와 시스템분석가가 참여하여 모의 취약점 분석 테스트를 수행하여 가전기기의 보안취약점을 발견하는 단계
PRD(Product Requirements Description)	가전기기에 탑재되는 SW의 개발 및 구현 가능성을 검토 또는 판단하여, 기능적/비기능적, 공통 및 모델 요구사항에 대해 검토 가능한 수준으로 구체화한 명세서

용어	설명
PRS(Product Requirements Specification)	사업자, 상품기획, 기술 Spec. 형태의 상위 특징들을 SW개발 요구사항으로 세분화하여 정의된 SW상세요구사항
보안 기능 테스트 케이스(Functional Security Test Case)	SW보안 요구사항으로 명세된 보안기능 및 보안설계 검토 시 발견된 보안 위협요소 완화방안을 제대로 구현하고 있는지 확인하는 테스트케이스
보안 설계 (Security Design)	SW보안 요구사항을 반영하여 보안이 고려된 SW설계
제품최고책임자	제품 기획/개발 담당 최고 책임자

SDL 관련 책임과 권한에는 SDL 관련 주요 부서인 “기획부서”, “개발부서”, “품질관리부서”, “검증부서”, “최고 책임자”, “취약점 분석 수행 주체”, “보안부서”를 중심으로 한 책임과 권한을 명시하고 있다. 각 부서는 해당 책임과 권한에 관하여 숙지하고 업무 수행 시 보안에 관한 부분이 누락되지 않도록 유념해야 된다. 특히 개발부서와 품질관리 부서는 SDL 보안활동의 핵심 역할을 수행함으로 담당자 교육에 만전을 기해야 한다. 상세 책임과 권한은 [표 16]과 같다.

[표 16] SDL 관련 책임과 권한

부서	책임과 권한
기획 부서	보안 등급 결정에 영향을 미치는 특징과 시나리오들을 도출한다.
개발 부서	보안 등급 결정에 영향을 미치는 특징과 시나리오들을 도출한다. 제품 보안 등급을 분류한다. 결정된 보안 등급 기준으로 SDL 계획서를 작성하고, 협의된 SDL 계획서를 개발 관리 시스템에 등록한다. SDL 계획 수립 시 취약점 분석 범위 및 일정을 수립하여 취약점 분석 수행 주체에게 전달하고, 취약점 분석 일정을 협의한다. SW보안 요구사항을 이해하고, SW요구명세서에 SW보안 요구사항을 명세한다. 요구사항 분석 결과와 보안부서의 검토 결과를 바탕으로 SW보안 요구사항을 SW요구명세서에 보완한다. 보완된 SW요구명세서를 확정하고, SW요구명세서에 확정내용을 기록하고, 관련부서와 커뮤니케이션 한다.

부서	책임과 권한
	<p>데이터 흐름도(DFD: Data Flow Diagram)를 작성하여 실제적 보안 위협 요소를 도출하고, 이에 대한 완화 방안을 수립한다.</p> <p>보안부서와 논의하여 보안 위협 요소 완화 방안을 최종 결정하고, 이를 바탕으로 SW 보안 요구사항을 보완하여 작성한다.</p> <p>보안 구현 가이드를 기반으로 SW개발 및 자가 검토를 수행한다.</p> <p>사용중인 오픈소스에 대한 정보를 수집하고, 오픈소스 보안취약점 분석을 수행한다.</p> <p>도출된 오픈소스 보안 취약점에 대하여, 취약점 수정 계획을 수립하고 해당 취약점을 수정하여 반영한다.</p> <p>탐지된 보안 정적 분석 취약점을 수정한다.</p> <p>SW보안 요구사항을 검증할 수 있는 보안 기능 테스트 케이스를 설계하고, 이를 기반으로 보안 기능 테스트를 자가 수행한다.</p> <p>탐지된 보안 기능 테스트 취약점, 퍼지 점검, 취약점 분석에서 도출된 취약점에 대한 수정 방안을 반영한다.</p> <p>SW승인단계 시험 진입 시, SDL 활동 결과서를 작성한다.</p> <p>해결되지 않은 잔존 보안 이슈는 미해결 이슈 승인서를 작성하여, 검증부서 합의하여 개발부서 제품 최고 책임자의 승인을 획득해야 한다.</p> <p>보안부서와 SDL 활동 검토 완료 후, 보안 검토서를 작성하여 개발 관리 시스템 입력 및 결재를 요청한다.</p> <p>결재 완료된 보안 검토서와 필수 제출 문서를 개발 관리 시스템에 등록한다.</p>
품질관리 부서	<p>보안 정적 분석 도구와 정적 분석 룰 셋을 바탕으로 보안 정적 분석 자동화 환경을 구축한다.</p> <p>구축된 보안 정적 분석환경을 기반으로 주기적으로 보안 정적 분석을 수행한다.</p> <p>수행된 보안 정적 분석 결과를 바탕으로 정적 분석 결과서를 작성하고, 주기적으로 개발팀에 보안 정적 분석 결과서를 송부한다.</p> <p>개발팀의 보안 정적 분석 취약점 수정 사항을 점검한다.</p> <p>개발 조직 내 품질관리부서의 보안 정적 분석 취약점 수정 사항 검토 결과에 따라 취약점 수정 활동을 반복 수행할 수 있다.</p> <p>개발부서가 설계한 보안 기능 테스트 케이스를 검토 및 보완한다.</p> <p>보안 기능 테스트 케이스를 별도 구역으로 분리하여 관리한다.</p> <p>작성된 테스트 케이스를 기반으로 SW개발 단계에서 보안 기능 테스트를 수행한다.</p> <p>보안 기능 테스트를 수행한 후, 보안 기능 테스트 결과서를 개발부서로 전달한다.</p> <p>보안 기능 테스트 취약점 조치 결과를 바탕으로 기능 충족 여부를 판단한다.</p> <p>퍼지 점검 대상을 검토하여 퍼지 점검 범위를 파악하고, 해당되는 퍼지 점검 도구를 검토 및 선정한다.</p> <p>선정한 퍼지 점검 도구에 대해 수행조건과 통과기준을 수립한다.</p> <p>선정된 도구를 기반으로 퍼지 점검 자동화 환경을 구축한다.</p> <p>퍼지 점검 자동화 환경을 기반으로 점검을 수행하고, 개발부서로 결과를 송부한다.</p> <p>잔존 보안 이슈 중 해결이 불가능한 보안 이슈(미해결 이슈)가 존재하는 경우, 품질 부서장은 미해결 이슈 승인서를 검토 및 합의한다.</p>
검증	<p>품질부서에서 전달 받은 테스트 케이스 기반으로 SW검증 단계에서 보안 기능 테스트</p>

부서	책임과 권한
부서	를 실시한다. 보안 기능 테스트 결과에 대한 SW검증단계 완료 기준 충족 여부를 판단한다. 보안 검토서를 확인하여 결재를 최종 완료한다.
최고 책임자	보안 등급을 검토 및 승인한다. 잔존 보안 이슈 중 해결이 불가능한 보안 이슈(미해결 이슈)가 존재하는 경우, 미해결 이슈 승인서를 검토 및 승인한다.
취약점 분석 수행 주체	SDL 계획 수립 프로세스에서 취약점 분석 범위 및 일정(시험 차수)을 개발부서와 협의한다. 취약점 분석 대상에 대한 정보를 수집하고 구조를 파악하여 보안 취약점을 도출하고 분석한다. 협의된 일정에 따라 SW검증 단계에서 공격 시나리오 및 점검항목을 바탕으로 취약점 분석을 수행한다. SW검증 마지막 시험에서 취약점 분석으로 탐지된 취약점이 잘 수정되었는지 취약점 이행 분석을 수행한다.
보안 부서	도출된 보안 관련 특징 및 시나리오를 바탕으로 보안 등급을 결정한다. SDL 계획서를 검토 및 합의하고, 필요 시 SDL 계획서의 재작성을 요청한다. SW보안 요구사항을 검토한다. 보안 요구사항 분석프로세스를 통해 보완된 SW요구명세서에 대한 확정 여부를 모든 이해관계자(기획부서, 개발부서, 품질부서, 검증부서, 보안부서)의 동의를 통해 결정한다. '보안 위협 요소 분석 및 완화 방안 결과서'를 통해 개발부서에서 작성한 보안 위협 요소 분석 결과를 검토한다. 보안 위협 요소 분석 결과를 통해 도출된 완화 방안을 검토한다. '보안 구현 가이드'를 개발하여 개발부서에게 배포하고, 지속 관리한다. 기능 선언 시점에서 오픈소스 보안 취약점 수정 결과를 검토하고 수정된 결과를 재분석하여 보안 취약점 완화 유무를 확인한다. SDL 활동 결과서를 바탕으로 질의 응답을 통해 SDL 활동 별 보안 활동 수행 결과를 점검한다. SDL 활동 검토 결과 통과 기준이 충족되면 최종 보안 검토를 완료한다. SW보안 정책을 수립 및 관리한다. SDL 활동을 모니터링한다.

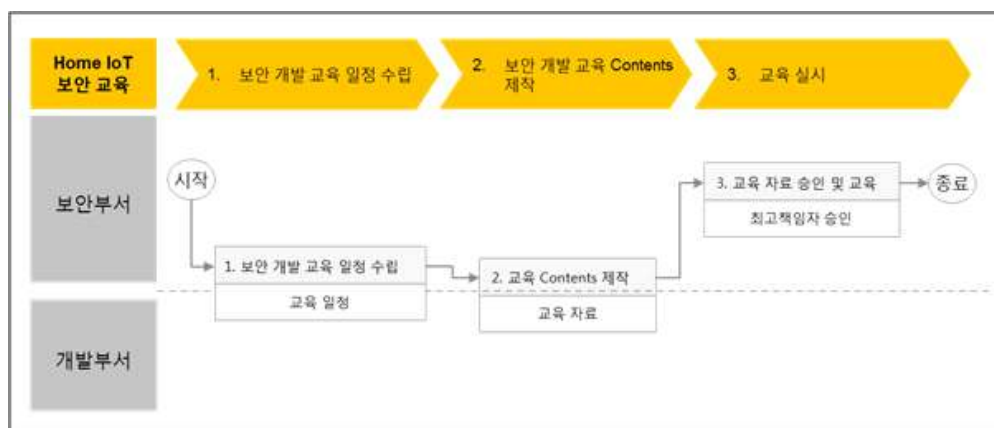
2. 준비 단계의 Home IoT 보안 전문가 양성 교육 프로세스

2.1 Home IoT 보안 교육

1) Home IoT 보안 교육 프로세스

Home IoT 가전기기의 개발 시, 개발자들이 Home IoT 개발 보안에 대한 전문

적인 이해를 바탕으로 가전기기의 잠재적 보안 취약점을 제거하기 위한 주요 활동으로써, Home IoT 개발 보안 교육을 실시한다. 보안부와 개발부서의 협의하에 교육일정 계획을 수립하고 교육에 활용될 Contents를 개발하여 최고책임자 승인을 득한다. 그 후 보안부서에서 Home IoT 개발과 관련된 임직원들을 대상으로 교육을 실시하는 과정이다. 상세 프로세스는 [그림 14]와 같다.



[그림 14] Home IoT 보안 교육 설계

2) Home IoT 보안 교육 프로세스 별 상세 업무

개발 보안 교육 일정 수립: 보안부와 개발부서 협의 하에 개발과 관련된 임직원들을 대상으로 실시할 개발 보안 교육 일정을 수립한다.

교육 Contents 제작: 보안부와 개발부서는 현재 Home IoT 보안에 관한 리서치를 통하여 현재 보안에 관련된 트렌드를 반영한 교육 Contents를 제작한다.

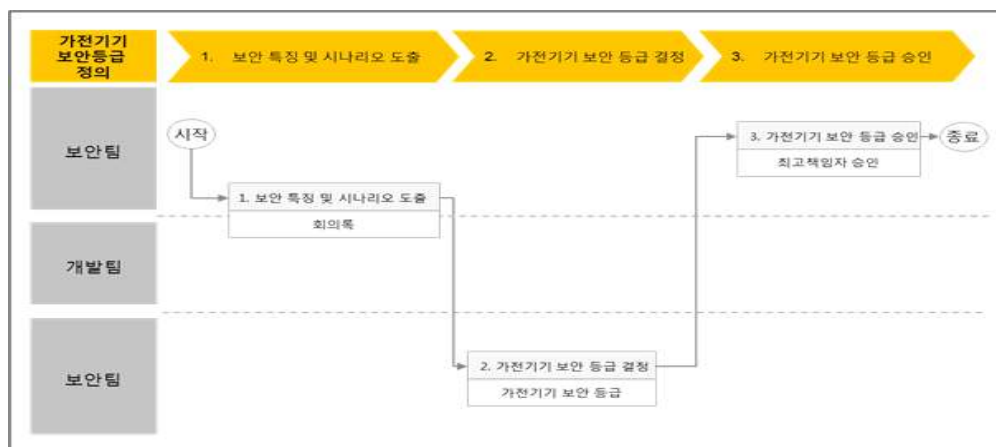
교육자료 승인 및 교육 실시: 보안부와 개발부서가 제작한 교육 Contents에 관하여 보안부서 최고책임자의 승인을 받아야 하며, 그 후 일정에 맞춰 Home IoT 가전기기 개발에 관련된 임직원들의 교육을 실시한다.

3. 요구사항 정의 단계의 보안활동 프로세스

3.1 보안 등급 정의

1) 보안 등급 정의 프로세스

보안 등급 정의 시에는 보안 관점에서 검토하여 등급을 결정하고 이를 바탕으로 보안 검증을 위한 SDL의 활동 범위를 결정하며, “IoT의 사물인터넷 기기 등급 분류 및 보안 요구사항”을 참고한다^[32]. “보안 특징 및 시나리오 도출” 단계에서 기획부서와 개발부서간의 논의를 통해 보안 등급 결정에 영향을 미치는 요소들을 도출할 것이다. “보안 등급 결정” 단계에서는 기획부서와 개발부서에서 도출된 “보안 특징 및 시나리오”를 바탕으로 검토하여 보안부서에서 보안 등급을 결정한다. 마지막으로 “보안 등급 승인” 단계는 보안부서에서 결정한 보안 등급을 제품 기획의 최고 책임자가 검토하고 최종적으로 승인한다. 상세 프로세스는 [그림 15]와 같다.



[그림 15] 보안 등급 정의 프로세스 설계

2) 보안 등급 정의 프로세스 별 상세 업무

기획부서와 개발부서는 보안등급 결정에 영향을 미치는 “보안 특징 및 시나리오”를 도출한다.

보안 등급 결정

보안 등급 검증 대상 여부 판단: A급, B급 기기의 경우 기본 검증 대상으로 지정하고 C급, D급 가전기기는 개발부서와 기획부서의 자체적인 판단 기준에 따라 결정한다.

보안부서는 개발부서와 기획부서에서 도출된 “보안 특징 및 시나리오”를 바탕으로 검토하여 보안등급을 결정한다.

보안 대상 제품군	보안 대상 기기별 분류 기준
A	<ul style="list-style-type: none"> 네트워크 기능이 존재하는 가전기기 중요정보, 개인정보 송수신(O), 가전기기 내 중요정보, 개인정보 저장(O)
B	<ul style="list-style-type: none"> 네트워크 기능이 존재하는 제품 중요정보, 개인정보 송수신(O), 가전기기 내 중요정보, 개인정보 저장(X) 중요정보, 개인정보 송수신(X), 가전기기 내 중요정보, 개인정보 저장(O)
C	<ul style="list-style-type: none"> 네트워크 기능이 존재하는 제품 중요정보, 개인정보 송수신(X), 가전기기 내 중요정보, 개인정보 저장(X)
D	<ul style="list-style-type: none"> 네트워크 기능이 없는 단순 편의 기능 가전기기

[그림 16] 보안 대상기기별 분류 기준

결정된 보안 대상 기기 내에서 선택 가능한 보안 등급을 요구사항 확정, 회의에서 유관 부서와 협의하여 결정한다. 각 보안 대상 기기별로 받아야 할 최소한의 보안 등급이 존재하며, 그 이하 보안 등급은 선택할 수 없다. A 제품은 3단계, B 제품은 최소한 2단계, C 제품은 최소한 1단계를 수행한다.

보안 등급의 정의: 특성(보안 대상 기기 분류 기준)에 따라 기기별로 수행해야 할 SDL 활동의 단계가 다르다. 또한 단계별로 수행해야 할 SDL 활동이 정의되어 있으며 단계가 올라갈수록 수행해야 할 SDL 활동이 많아진다.

보안등급	1단계	2단계	3단계
SDL 활동	<ul style="list-style-type: none"> 가전기기 보안 등급 정의 SDL 계획 수립 보안 요구사항 분석 보안 구현 	<ul style="list-style-type: none"> 오픈 소스 보안 취약점 분석 보안 정책 분석 보안 기능 테스트 최종 보안 리뷰/인증 	<ul style="list-style-type: none"> 1단계 활동 포함 퍼지 점검 취약점 분석
			<ul style="list-style-type: none"> 2단계 활동 포함 보안 설계 리뷰

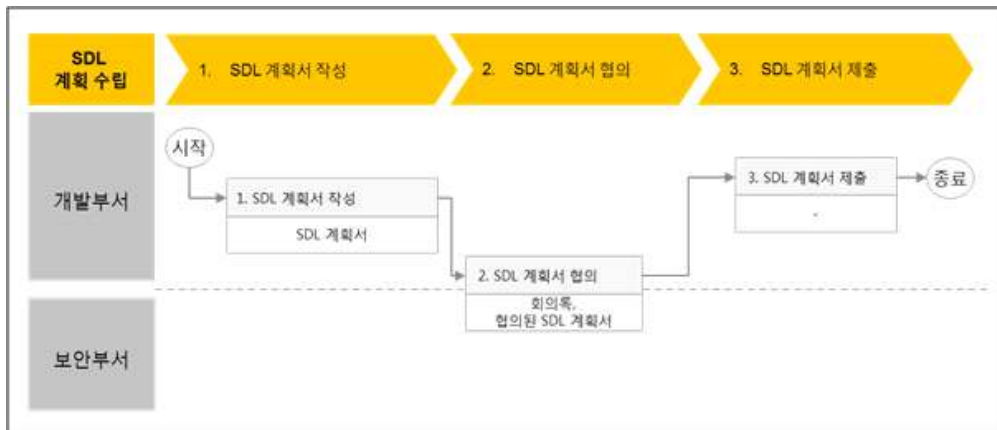
[그림 17] 보안 등급별 SDL 활동 정의

보안 등급 승인: 개발부서는 보안 등급을 명시해서 개발관리시스템에 등록하고 기획부서 최고 책임자는 보안 등급의 타당성을 검토하고 SDL 활동을 승인한다.

3.2 SDL 계획 수립

1) SDL 계획 수립 프로세스

먼저 “SDL 계획서 작성” 단계에서는 결정된 기기의 보안 등급을 기준으로 개발 부서에서 SDL 계획서를 작성한다. “SDL 계획서 협의” 단계에서 보안부서는 작성된 SDL 계획서를 검토하고 협의를 진행한다. “계획서 제출” 단계에서는 최종 협의된 계획서를 개발부서에 발행하도록 한다. 상세 프로세스는 [그림 18]과 같다.



[그림 18] SDL 계획 수립 프로세스 설계

2) SDL 계획 수립 프로세스 별 상세 업무

SDL 계획서 작성: 결정된 보안 등급에 따라 개발부서에서는 관련 부서와 협의를 통해 SDL 활동 계획을 수립한다. 개발부서는 협의한 내용으로 SDL 계획서를 작성하여 보안부서에 전달하며 SDL 계획서 작성 단계에서 취약점 분석 주체와 분석 범위 및 일정을 협의한다.

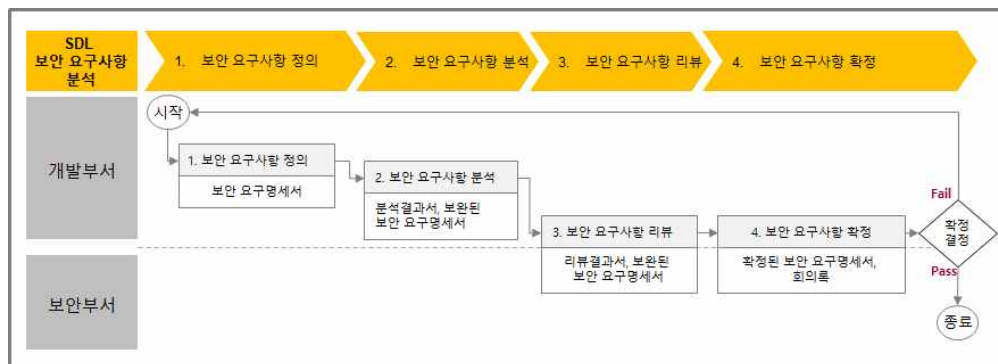
SDL 계획서 협의: 보안부서는 보안 등급을 기준으로 SDL 계획서를 검토하여 협의하고, 만약 협의가 거부될 경우에는 거부 사유를 상세하게 명시한다. 개발부서는 협의된 SDL 계획서를 기반으로 관련부서와 공유하며, 보안부서에서 협의 거부 시에 개발부서는 'SDL 계획서 작성' 활동부터 다시 수행해야 한다.

SDL 계획서 제출: 개발부서 일정 품질 목표 수립 기한 내에 제품 개발 관리 시스템에 보안부서와 협의한 SDL 계획서를 등록한다.

3.3 보안 요구사항 분석

1) 보안 요구사항 분석 프로세스

“보안 요구사항 정의”단계에서는 개발부서 담당자에게 질의 및 분석을 통해 보안 요구사항을 확인한다. “보안 요구사항 분석”단계에서는 확인된 보안 요구사항 점검 항목을 기반으로 요구사항을 분석한다. “보안 요구사항 리뷰”단계에서는 보안 요구사항 분석 점검 항목을 기반으로 전체적인 검토와 수정이 진행된다. 마지막 단계로 “보안 요구사항 확정”단계에서는 개발부서 담당자 등 모든 이해관계자의 동의를 통해 결정한다. 상세 프로세스는 [그림 19]와 같다.



[그림 19] 보안 요구사항 분석 프로세스 설계

2) 보안 요구사항 분석 프로세스 별 상세 업무

보안 요구사항 정의: 개발부서는 유관 부서로부터 요구사항 관련 문서와 보안 정책 문서를 수집하고 이해한다.

보안 요구사항 분석: 보안 요구사항분석 항목을 기반으로 요구사항을 분석하며 분석 결과를 바탕으로 보안 요구사항을 요구명세서에 보완한다.

보안 요구사항 리뷰: 보안부서는 개발부서에게 전달받은 SW보안 요구사항을 보

안 요구사항 검토 항목을 기반으로 검토한다. 개발부서는 검토 결과를 바탕으로 보안 요구사항을 요구명세서에 보완해 작성한다.

보안 요구사항 확정: 보완된 요구명세서에 대해 모든 이해관계자(기획부서, 개발부서, 검증부서, 품질부서, 보안부서)의 동의를 받고 증거를 기록한다. 요구명세서의 확정 동의 거부 정보를 관련부서에 공유한다.

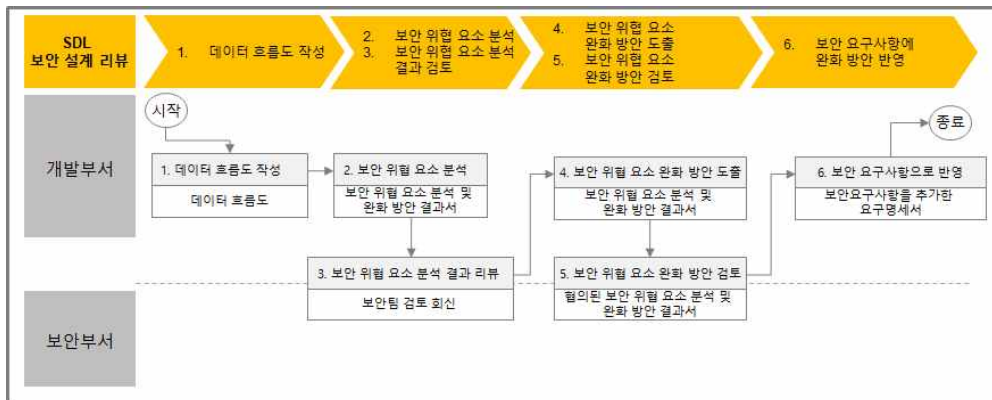
4. 설계 구현 단계의 보안활동 프로세스

4.1 보안설계 검토

1) 보안설계 검토 프로세스

선행연구에서 진행한 위협모델링 도구를 사용하여 각 Home IoT 가전기기의 데이터 흐름도를 통해 전체적인 시스템 흐름상에서의 보안 위협 요소를 파악하고 발견된 위협 요소에 대하여 완화 방안을 결정하고 보안 요구사항에 반영한다.

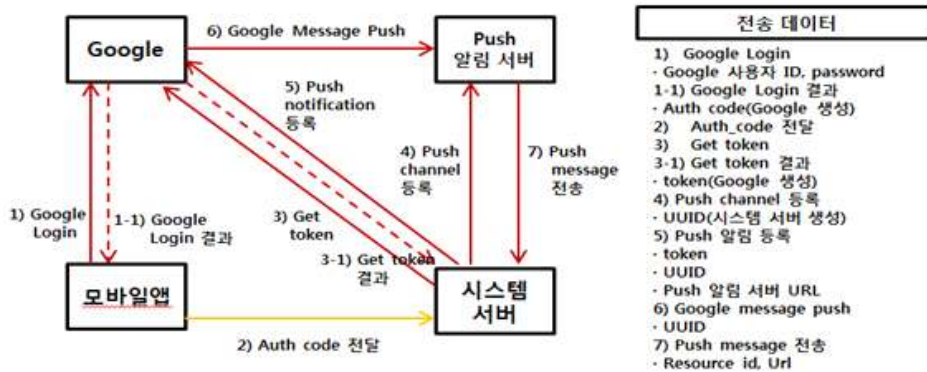
“데이터 흐름도 작성” 단계에서는 전체 시스템의 데이터 흐름을 분석하기 위하여 위협모델링을 활용하여 데이터 흐름도를 작성한다. “보안 위협 요소 분석” 단계에서는 보안 위협 요소를 도출하고 그에 따른 분석 보고서 및 완화 방안 결과서를 작성한다. “보안 위협 요소 분석 결과 검토” 단계에서는 발행된 결과서를 보안팀으로부터 검토 결과를 회신 받는다. “보안 위협 요소 완화 방안 도출” 단계에서는 발견된 보안 위협 요소에 대한 완화 방안을 도출하고 그에 따른 결과서를 발행한다. “보안 위협 요소 완화 방안 검토” 단계에서는 마찬가지로 보안부서에 의해 검토 받으며 최종 방안을 결정한다. 마지막으로 “보안 요구사항에 완화 방안 반영” 단계에서는 최종 결정된 보안 위협 완화 방안을 보안 요구사항으로 반영한다. 상세 프로세스는 [그림 20]과 같다.



[그림 20] 보안설계 검토 프로세스 설계

2) 보안 요구사항 분석 프로세스 별 상세 업무

데이터 흐름도 작성: 개발부서는 전체 시스템의 데이터 흐름을 분석하기 위한 데이터 흐름도를 작성한다. 데이터 흐름도 작성 시 외부 연결 인터페이스를 통해 전달되는 데이터는 필수적으로 표현해야 하며 위협모델링 도구를 사용하여 작성할 수 있다.



[그림 21] SW설계서 예시

보안 위협 요소 분석: 개발부서는 데이터 흐름도를 바탕으로 보안 위협 요소를 도출하며 도출된 보안 위협 요소 중 실제적 보안 위협 요소를 파악하고, 이를 바탕으로 보안 위협 요소 분석 및 완화 방안 결과서를 작성한다. 보안 위협의 분류 및 커뮤니케이션을 위해, STRIDE 분류법의 사용을 권장한다.

보안 위협 요소 분석 결과 검토: 보안부서는 개발부서로부터 전달받은 보안 위협 요소 분석 및 완화 방안 결과서의 보안 위협 요소 분석 결과를 검토하고 개발 부서에게 검토결과를 전달한다. 개발부서는 보안부서에서 받은 검토 결과를 바탕으로 보안 위협 요소 분석 활동을 추가하여 수행할 수 있다.

보안 위협 요소 완화 방안 도출: 개발부서는 보안 위협 요소 분석 결과를 바탕으로 보안 위협 요소 완화 방안을 도출하고, 보안 위협 요소 분석 및 완화 방안 결과서를 작성한다.

보안 위협 요소 완화 방안 검토: 보안부서는 개발부서에서 작성한 보안 위협 요소 분석 및 완화 방안 결과서를 바탕으로 보안 위협 요소 완화 방안이 보안 위협 요소를 적절하게 고려하였는지 검토한다. 개발부서는 검토 결과를 바탕으로 보안부서와 논의하여 보안 위협 요소 완화 방안을 최종 결정한다.

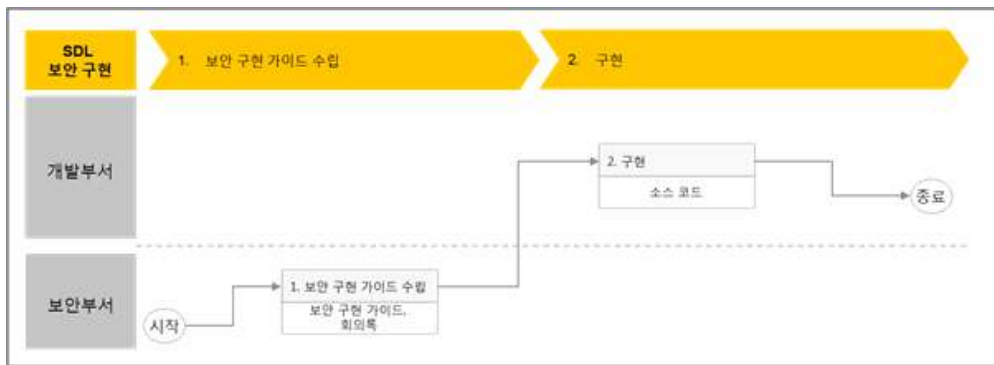
보안 요구사항에 완화 방안 반영: 개발부서는 요구사항 명세서에 최종 결정된 보안 위협 요소 완화 방안을 보안 요구사항으로 반영한다.

4.2 보안 구현

1) 보안 구현 프로세스

SW개발자들이 안전한 SW코딩 규칙을 적용하여 개발한 후 보안 구현 업무 기술서를 통해 실수나 논리적 오류 등으로 인해 발생할 수 있는 SW상의 보안 취약점을 최소화 함을 목적으로 한다. “보안 구현 가이드 수립” 단계에서는 보안 구현 가이드를 개발하여 SW개발팀에게 공유하고 지속적으로 관리한다. “구현” 단계에서

는 보안 구현 가이드를 기반으로 하여 SW개발 및 자가 검토를 수행하도록 한다.
상세 프로세스는 [그림 22]와 같다.



[그림 22] 보안 구현 프로세스 설계

보안 구현 가이드에는 시큐어코딩에 관한 내용이 포함되며 미국의 카네기멜런 대학교의 시큐어코딩 가이드[<https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard>]^{[33][34][35]}를 사용하였다. 카네기멜런 대학교의 시큐어코딩 가이드에는 JAVA, C, C++, Perl 언어 등의 가이드가 포함되어 있으며 [표 17]는 JAVA에 대한 가이드 항목이다.

[표 17] 시큐어코딩 가이드

Sections	Rule	Description
Rule 00	Input Validation and Data Sanitization(IDS)	<ul style="list-style-type: none"> · Prevent SQL injection · Normalize strings before validating them · Canonicalize path names before validating them
Rule 01	Declarations and Initialization	<ul style="list-style-type: none"> · Prevent class initialization cycles · Do not reuse public identifiers from the Java Standard Library · Do not modify the collection's elements during an enhanced for statement
Rule 02	Expressions	<ul style="list-style-type: none"> · Do not ignore values returned by methods

Sections	Rule	Description
	(EXP)	<ul style="list-style-type: none"> · Do not use a null in a case where an object is required · Do not use the Object.equals() method to compare two arrays
Rule 03	Numeric Types and Operations (NUM)	<ul style="list-style-type: none"> · Detect or prevent integer overflow · Do not perform bitwise and arithmetic operations on the same data · Ensure that division and remainder operations do not result in divide-by-zero errors
Rule 04	Characters and Strings (STR)	<ul style="list-style-type: none"> · Don't form strings containing partial characters from variable-width encodings · Do not assume that a Java char fully represents a Unicode code point · Specify an appropriate locale when comparing locale-dependent data
Rule 05	Object Orientation (OBJ)	<ul style="list-style-type: none"> · Limit accessibility of fields · Preserve dependencies in subclasses when changing superclasses · Prevent heap pollution
Rule 06	Methods (MET)	<ul style="list-style-type: none"> · Validate method arguments · Never use assertions to validate method arguments · Do not use deprecated or obsolete classes or methods
Rule 07	Exceptional Behavior (ERR)	<ul style="list-style-type: none"> · Do not suppress or ignore checked exceptions · Do not allow exceptions to expose sensitive information · Prevent exceptions while logging data
Rule 08	Visibility and Atomicity (VNA)	<ul style="list-style-type: none"> · Ensure visibility when accessing shared primitive variables · Ensure visibility of shared references to immutable objects · Ensure that compound operations on shared variables are atomic
Rule 09	Locking (LCK)	<ul style="list-style-type: none"> · Use private final lock objects to synchronize classes that may interact with untrusted code · Do not synchronize on objects that may be reused · Do not synchronize on the class object returned by getClass()
Rule 10	Thread APIs (THI)	<ul style="list-style-type: none"> · Do not invoke Thread.run() · Do not invoke ThreadGroup methods · Notify all waiting threads rather than a single thread
Rule 11	Thread Pools (TPS)	<ul style="list-style-type: none"> · Use thread pools to enable graceful degradation of service during traffic bursts · Do not execute interdependent tasks in a bounded thread pool · Ensure that tasks submitted to a thread pool are interruptible
Rule 12	Thread-Safety	<ul style="list-style-type: none"> · Do not override thread-safe methods with methods that are

Sections	Rule	Description
	Miscellaneous (TSM)	<ul style="list-style-type: none"> not thread-safe Do not let the this reference escape during object construction Do not use background threads during class initialization
Rule 13	Input Output (FIO)	<ul style="list-style-type: none"> Do not operate on files in shared directories Create files with appropriate access permissions Detect and handle file-related errors
Rule 14	Serialization (SER)	<ul style="list-style-type: none"> Enable serialization compatibility during class evolution Do not deviate from the proper signatures of serialization methods Sign then seal objects before sending them outside a trust boundary
Rule 15	Platform Security (SEC)	<ul style="list-style-type: none"> Do not allow privileged blocks to leak sensitive information across a trust boundary Do not allow tainted variables in privileged blocks Do not base security checks on untrusted sources
Rule 16	Runtime Environment (ENV)	<ul style="list-style-type: none"> Do not sign code that perform Microsoft only unprivileged operations Place all security-sensitive code in a single JAR and sign and seal it Do not trust the values of environment variables
Rule 17	Java Native Interface (JNI)	<ul style="list-style-type: none"> Define wrappers around native methods Do not assume object references are constant or unique Do not use direct pointers to Java objects in JNI code
Rule 49	Miscellaneous (MicrosoftC)	<ul style="list-style-type: none"> Do not use an empty infinite loop Generate strong random numbers Never hard code sensitive information
Rule 50	Android (DRD)	<ul style="list-style-type: none"> Do not act on malicious intents Restrict access to sensitive activities Ensure that sensitive data is kept secure

2) 보안 구현 프로세스 별 상세 업무

보안 구현 가이드 수립: 보안부서는 “보안구현 가이드”를 개발하여 개발자들에게 주기적으로 개정하며 지속 관리한다.

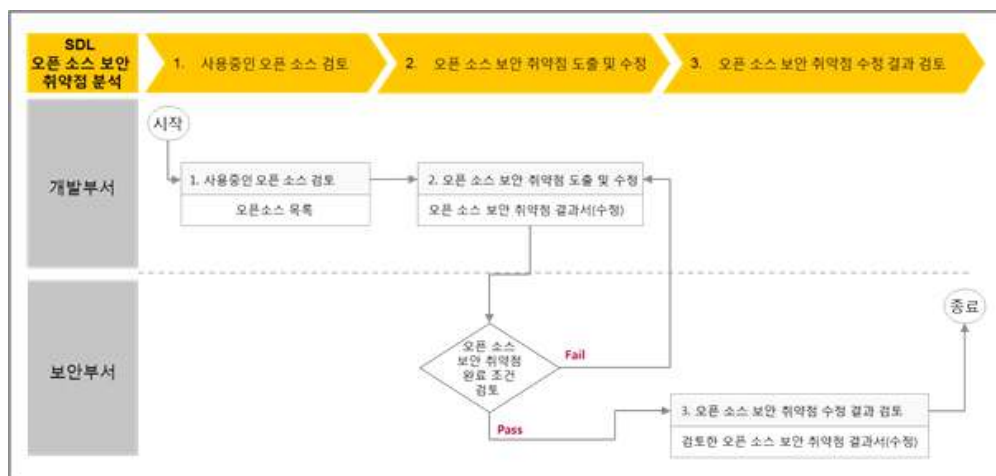
구현: 개발부서에서는 “보안 구현 가이드”를 숙지하여 개발하고 개발 후 소스코

드를 반영하기 전 “보안 구현 가이드”를 기반으로 자가 검토를 수행한다.

4.3 오픈소스 보안 취약점 분석

1) 오픈소스 보안 취약점 분석 프로세스

Home IoT 가전기기에 내재되어 있는 오픈소스를 분석하여 알려진 보안 취약점을 발견하고 해당 취약점을 제거 또는 완화하려는 목적이 있다. “사용 중인 오픈소스 검토” 단계는 오픈소스를 사용하는 Home IoT SW를 관리하기 위한 목적으로 가전기기에서 사용되는 오픈소스 목록을 검토한다. “오픈소스 보안 취약점 도출 및 수정” 단계에서는 오픈소스 취약점 분석 도구를 통해 사용 중인 오픈소스의 보안 취약점을 도출하고 해당 취약점을 수정하여 반영한다. 마지막으로 “오픈소스 보안 취약점 수정 결과 검토” 단계에서는 보안 취약점 수정 결과를 검토하고 오픈소스 관리 취약점 분석 도구를 통해 수정된 결과를 재분석하여 취약점 완화 유무를 확인하는 것이다. 상세 프로세스는 [그림 23]과 같다.



[그림 23] 오픈소스 보안 취약점 분석 프로세스 설계

2) 오픈소스 보안 취약점 분석 프로세스 별 상세 업무

사용 중인 오픈소스 검토: 개발부서는 사용 중인 오픈소스의 이름 및 버전에 대한 정보를 수집하여 목록화한다.

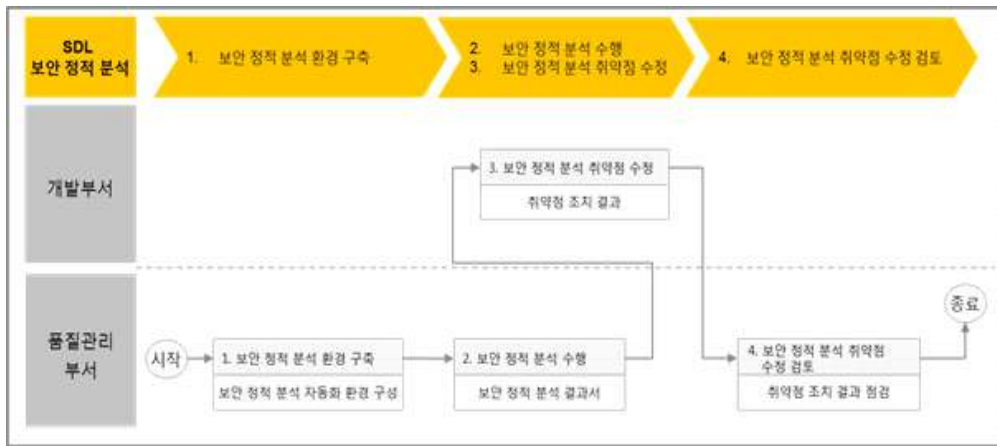
오픈소스 보안 취약점 도출 및 수정: SW개발 단계 동안 오픈소스 취약점 분석 도구를 통해 오픈소스의 보안 취약점 도출 및 수정 단계를 반복적으로 수행한다. 사용 중인 오픈소스의 보안 취약점을 도출하며 발견된 오픈소스 보안 취약점에 대하여 취약점 수정 계획을 수립하고 해당 취약점을 수정 반영한다.

오픈소스 보안 취약점 수정 결과 검토: 보안부서는 "오픈소스 보안 취약점 수정 최종 결과서"를 기준으로 완화 여부를 확인하고 통과기준에 부합하는지 검토한다.

4.4 보안 정적 분석

1) 보안 정적 분석 프로세스

자동화된 보안 정적 분석도구를 사용하는 것은 사람이 찾기 어려운 SW보안 취약점을 검출하고 개발단계에서 취약점을 미연에 제거하며, 이를 통해 안전한 SW개발을 하는 것이 목적이다. “보안 정적 분석 환경 구축” 단계에서는 가전기기에 적합한 보안 정적 분석 도구를 선정하여 자동화 환경을 구축한다. 정적 분석도구는 앞에서 언급했던 “보안구현 가이드”의 시큐어코딩 내용 중 중요한 부분을 자동화로 구현해 놓은 것이다. “보안 정적 분석 수행” 단계에서는 주기적으로 보안 정적 분석을 수행하여 정적 분석 결과서를 발행한다. “보안 정적 분석 취약점 수정” 단계에서는 개발부서에서 탐지된 보안 정적 분석 취약점을 수정한다. 마지막으로 “보안 정적 분석 취약점 수정 검토” 단계에서는 보안 정적 분석 취약점 수정 사항을 검토한다. 상세 프로세스는 [그림 24]와 같다.



[그림 24] 보안 정적 분석 프로세스 설계

2) 보안 정적 분석 프로세스 별 상세 업무

보안 정적 분석 환경구축: 보안 정적 분석 도구를 선정하고 보안 정적 분석 자동화 환경을 구축한다.

보안 정적 분석 수행: 품질관리부서는 구축된 보안 정적 분석환경을 기반으로 주기적으로 보안 정적 분석을 수행한다. 수행된 보안 정적 분석 결과를 바탕으로 정적 분석 결과서를 작성하고 주기적으로 개발부서에 정적 분석 결과서를 송부한다. 개발부서의 정적분석 취약점 수정 사항을 점검하고, 통과기준 충족 여부를 판단한다.

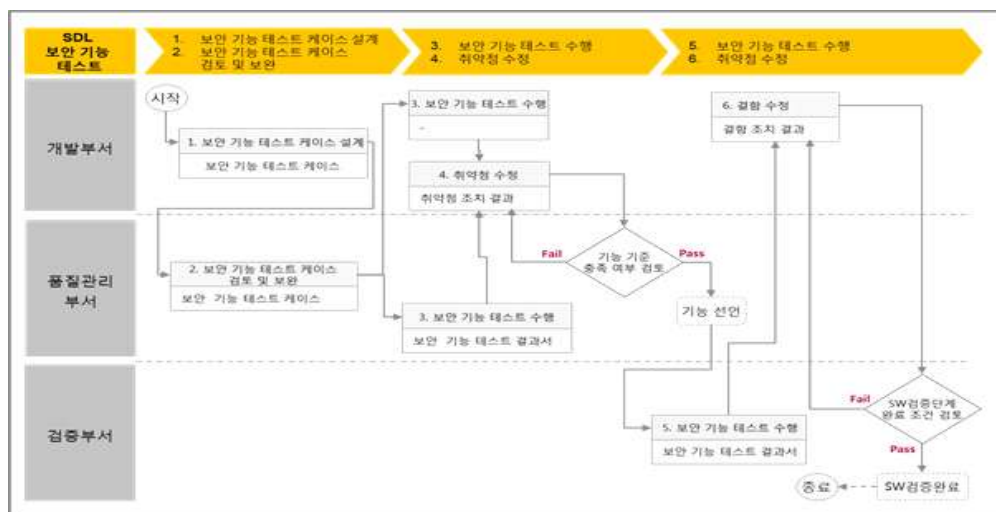
보안 정적 분석 취약점 수정: 개발부서는 탐지된 보안 정적 분석 취약점을 수정한다. 품질관리부서의 취약점 수정 사항 검토 결과에 따라 취약점 수정 활동을 반복 수행할 수 있다.

보안 정적 분석 취약점 수정 검토: 개발부서의 정적 분석 취약점 수정 사항을 검토하고 통과기준 충족 여부를 판단한다.

4.5 보안 기능 점검

1) 보안 기능 점검 프로세스

“보안 기능 점검 케이스 설계” 단계에서는 SW보안 요구사항을 검증할 수 있는 보안 기능 점검 케이스를 설계한다. “보안 기능 점검 케이스 검토 및 보완” 단계에서는 보안 기능 점검 케이스를 검토 및 보완하여, 전수점검 케이스를 설계한다. “보안 기능 점검 수행” 단계에서는 개발부서와 품질관리부서가 함께 작성한 점검케이스를 기반으로 SW개발 단계에서 보안 기능 점검을 수행한다. 점검 케이스로는 “정보 노출”, “인증과 인가”, “세션 관리”, “입력 값 검증”, “취약한 알고리즘 사용”, “펌웨어 업데이트”, “시스템 가용성” 등이 있다. “취약점 수정” 단계에서는 개발부서가 탐지된 보안기능 점검 취약점에 대하여 수정 방안을 가전기기에 반영한다. “보안 기능 점검수행” 단계에서는 수정된 점검케이스를 기반으로 보안 기능 점검을 재 실시한다. 마지막으로 “취약점 수정” 단계에서는 탐지된 보안 기능 점검 취약점에 대한 수정방안을 반영한다. 상세 프로세스는 [그림 25]와 같다.



[그림 25] 보안 기능점검 프로세스 설계

2) 보안 기능 테스트 프로세스 별 상세 업무

보안 기능 테스트 케이스 설계: 개발부서는 요구사항 명세서 내 기술된 보안 요구사항을 검토하여 보안 기능 테스트케이스를 설계한다.

보안 기능 테스트 케이스 검토 및 보완: 품질관리부서는 개발부서가 설계한 보안 기능 테스트 케이스를 검토 및 보완하여, 전수테스트 케이스를 설계한다. 그리고 최종적으로 보안 기능 테스트케이스를 작성하여 완성한다. 보안 기능 테스트 케이스는 별도 섹션으로 분리 관리되어야 한다.

보안 기능 테스트 수행: 개발부서는 완성된 보안 기능 테스트케이스를 이용하여 보안 기능 테스트를 자가 수행하고, 취약점이 탐지되는 경우 취약점에 대한 수정방안을 가전기기에 반영한다. 품질관리부서는 보안 기능 테스트를 수행한 뒤, 보안 기능 테스트 결과서를 작성하여 개발부서에 배포한다.

취약점 수정: 개발부서는 보안 취약점에 대한 수정방안을 가전기기에 반영한 뒤 품질관리부서에 보안 기능 테스트를 재요청한다. 품질관리부서는 개발부서의 취약점 조치 결과를 바탕으로 가전기기 기능 충족 여부를 판단한다. 개발부서는 가전기기 기능이 충족될 때까지 보안 기능 테스트 및 취약점 수정 단계를 반복할 수 있다.

보안 기능 테스트 수행: 검증부서에서는 보안 기능 테스트를 수행하고, 보안 기능 테스트 결과서를 작성하여 개발부서에 배포한다.

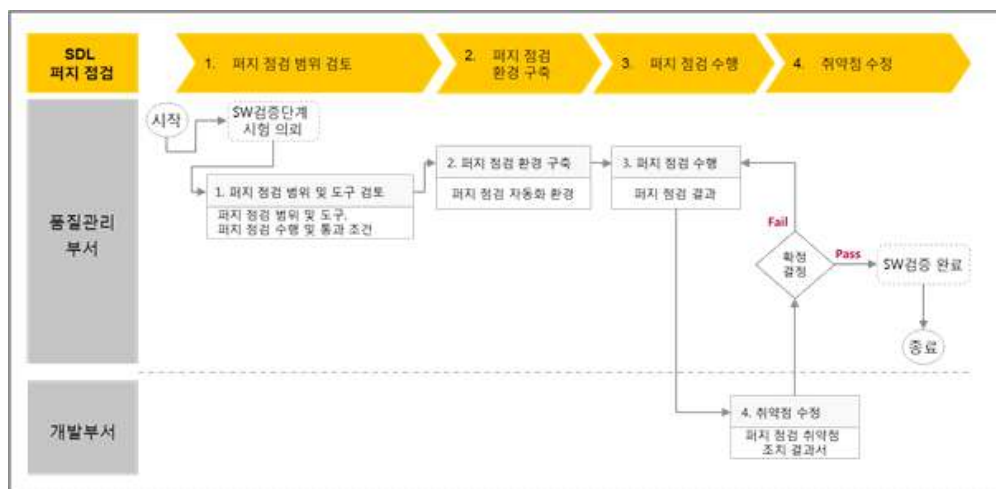
취약점 수정: 개발부서는 보안 취약점에 대한 수정방안을 가전기기에 반영한 뒤 검증부서에 보안 기능 테스트를 재요청한다. 검증부서는 개발부서의 취약점 조치 결과를 바탕으로 SW검증단계 완료 기준 충족 여부를 판단한다. 개발부서는 SW검증 단계 완료 기준 충족 시까지 보안 기능 테스트 및 취약점 수정단계를 반복할 수 있다.

5. 테스트 단계의 보안활동 프로세스

5.1 퍼지 점검

1) 퍼지 점검 프로세스

“퍼지 점검 범위 검토” 단계에서는 점검 대상을 검토하여 수행할 수 있는 퍼지 점검 범위를 산정하고, 퍼지 점검 도구를 검토/선정한다. “퍼지 점검 환경 구축” 단계에서는 선정된 도구를 기반으로 퍼지 점검 자동화 환경을 구축한다. “퍼지 점검 수행” 단계에서는 퍼지 점검 자동화 환경을 통해 점검을 수행한다. 퍼지 점검 항목으로는 “웹퍼지”, “네트워크 프로토콜 퍼지”, “파일 포맷 퍼지”를 포함한다. 마지막으로 “취약점 수정” 단계에서는 개발부서에서 퍼지 점검을 통해 검출된 취약점을 수정하고 취약점 조치 결과서를 발행한다. 상세 프로세스는 [그림 26]과 같다.



[그림 26] 퍼지 점검 프로세스 설계

2) 퍼지 점검 프로세스 별 상세 업무

퍼지 점검 범위 검토: 점검 대상 가전기기의 특성에 따라 적용할 퍼지 점검의 범위를 검토한다. 선정된 도구 별 수행 조건 및 통과 기준을 수립한다.

퍼지 점검 환경 구축: 품질관리부서는 선정된 도구를 기반으로 퍼지 점검 자동화 환경을 구축한다.

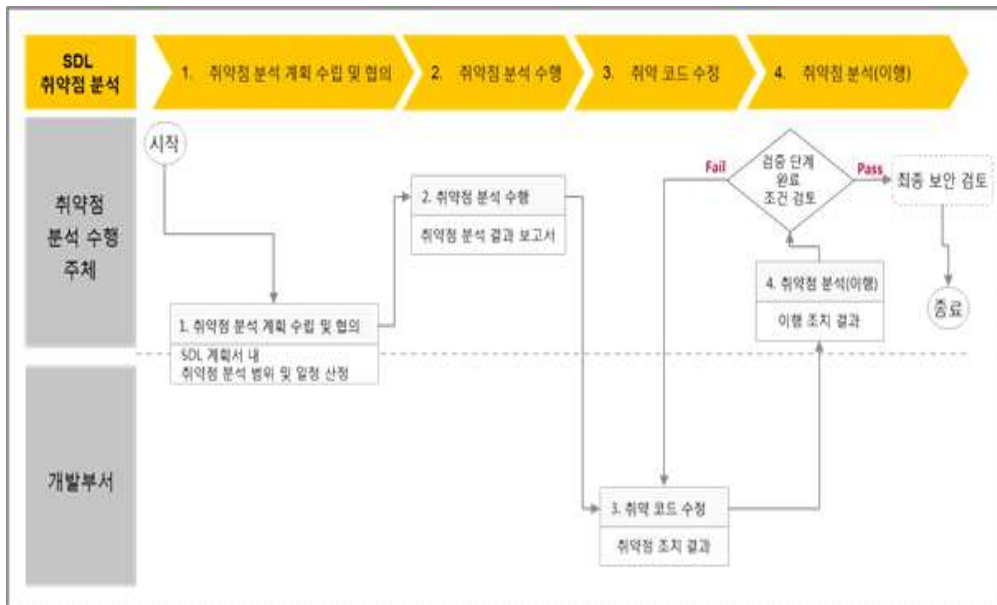
퍼지 점검 수행: 품질관리부서는 자동화 환경을 통해 퍼지 점검을 수행한다. 퍼지 점검 수행 결과를 작성하여 개발부서에 전달한다.

취약점 수정: 개발부서는 탐지된 취약점을 수정하고, "퍼지 점검 취약점 조치 결과서"를 작성한다. 품질관리부서는 통과 기준에 부합하는지 검토 후 승인한다.

5.2 취약점 분석

1) 취약점 분석 프로세스

“취약점 분석 계획 수립 및 합의” 단계에서는 개발부서와 취약점 분석 수행주체가 서로 협의하여 점검 범위와 일정을 산정한다. “취약점 분석 수행” 단계에서는 취약점 분석 대상에 관한 정보를 수집하고 구조를 파악하여 예상 취약점을 도출하고 분석하여 공격 시나리오와 보안 요구사항을 바탕으로 취약점 분석을 수행한다. “취약 코드 수정” 단계에서 해당 개발부서는 전달받은 취약점을 소스코드에 수정 및 반영한다. 마지막으로 “이행점검” 단계에서는 취약점이 조치된 가전기기에 대하여 취약점이 잘 수정되었는지 확인 검사를 받는다. 상세 프로세스는 [그림 27]과 같다.



[그림 27] 취약점 분석 프로세스 설계

2) 취약점 분석 프로세스 별 상세 업무

취약점 분석 계획 수립 및 협의: 취약점 분석은 해당 취약점 분석 수행 주체와 가전기기 개발부서와 협의를 통하여 범위와 시간 등을 산정해야 한다.

취약점 분석 수행: 취약점 분석 수행 주체는 협의된 취약점 분석 일정 및 범위에 따라 보안 취약점을 탐지한다. 취약점 분석의 취약점 영향도 평가는 3단계(High, Medium, Low)로 구분한다. 취약점 분석의 수행 주체는 취약점 영향도에 따른 수정 조치 가이드를 제안한다. 취약점 분석 수행 주체는 취약점 분석 시, 3장 1절 3.5 오픈소스 보안 취약점 분석과 3장 1절 3.6 보안 정적 분석, 3장 1절 4.1 퍼지 점검에 해당하는 점검 범위는 제외한다.

취약점 코드 수정: 개발부서는 탐지된 보안 취약점을 검토하고, 해당 취약점을 완화할 수 있는 방안을 SW에 적용한다. 취약점 코드 수정을 완료하지 못할 경우,

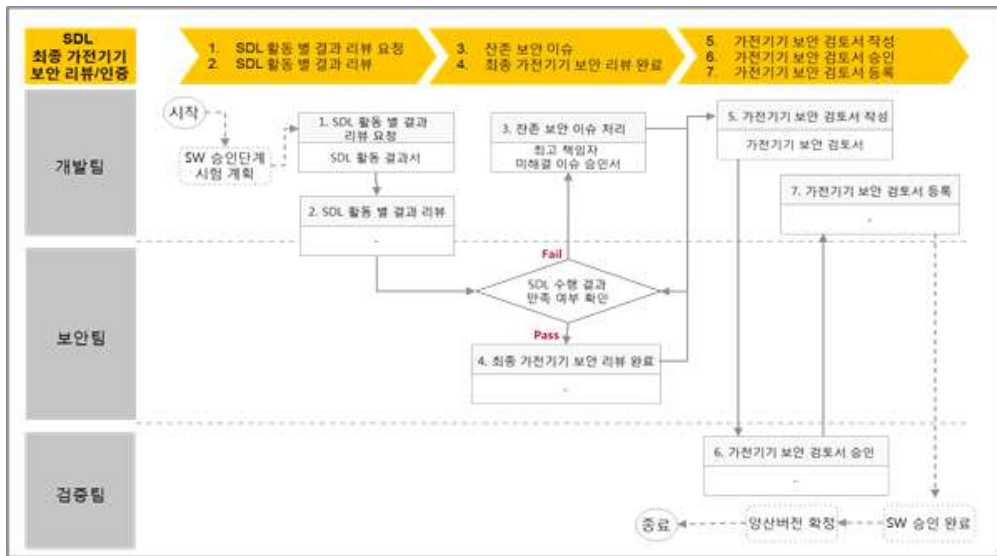
취약점 분석 프로세스의 미해결 이슈 승인 방식을 따른다.

취약점 분석(이행): 개발부서는 보안 취약점을 개선하여, 취약점 분석 수행 주체에게 이행 분석을 의뢰한다. 취약점 분석 수행 주체는 탐지된 보안 취약점이 가전 기기에 제대로 수정 및 반영되었는지 이행 분석을 실시한다. 이행 분석은 최종 가전기기 보안 검토 이전에 완료되어야 한다.

6. 릴리즈 단계의 보안활동 프로세스

6.1 최종 보안 검토 프로세스

“SDL 활동 별 결과 검토 요청”단계에서 개발부서는 품질관리부서에게 SDL 활동 결과서 검토를 요청한다. “SDL 활동 별 결과 검토” 단계에서 품질관리부서와 개발부서는 질의 응답을 통해 SDL 활동 별 보안 활동 수행 결과를 검토한다. “잔존 보안 이슈 처리” 단계에서는 보안 활동 수행 결과를 점검하여 통과 기준에 미달하는 경우, 개발부서는 잔존 보안 이슈를 해결해야 한다. “최종 보안 검토 완료” 단계에서 품질관리부서는 SDL 활동 검토 결과 통과 기준이 충족되면 최종 보안 검토를 완료한다. “보안 검토서 작성” 단계에서는 최종 보안 검토 완료 후, 개발부서는 보안 검토서를 작성하고, 보안 검토서 결재를 요청한다. “보안 검토서 승인” 단계에서는 검증부서에서 검토서 결재를 최종적으로 완료한다. 상세 프로세스는 [그림 28]과 같다.



[그림 28] 최종 보안 검토 프로세스 설계

6.2 최종 보안 검토 프로세스 별 상세 업무

SDL 활동 별 결과 검토 요청: 개발부서는 품질관리부서에게 SDL 활동 결과서 검토를 요청한다.

SDL 활동 별 결과 검토: 품질관리부서와 개발부서는 SDL 활동 결과서를 기반으로 질의/응답을 통해 SDL 활동 별 보안활동 수행 결과를 검토한다.

잔존 보안 이슈 처리: 가전기기 보안활동 수행 결과 검토 시 통과 기준 미달일 경우, 개발부서는 잔존 보안 이슈를 해결해야 한다. 개발부서는 잔존 보안 이슈를 해결하고, 품질관리부서와 협의하여 수정 사항으로 검토를 진행한다. 잔존 보안 이슈 중 해결이 불가능한 보안 이슈가 존재하는 경우, 미해결 보안 이슈의 리스크를 인지하여 리스크가 존재함에도 출시한다는 개발부서 최고 책임자의 승인이 필요하다. SDL 활동 통과 기준 충족 및 잔존 보안 이슈 처리가 완료될 경우, 개발부서는 품질관리부서로 SDL 활동 검토를 요청하고, 품질관리부서의 검토 결과에 따라

개발부서의 잔존 보안 이슈 처리 활동이 반복될 수 있다.

최종 보안 검토 완료: 품질관리부서는 모든 SDL 활동 검토를 수행하여 최종적으로 SDL 활동 별 통과 기준 충족 여부를 확인하고, 최종 보안 검토를 완료한다.

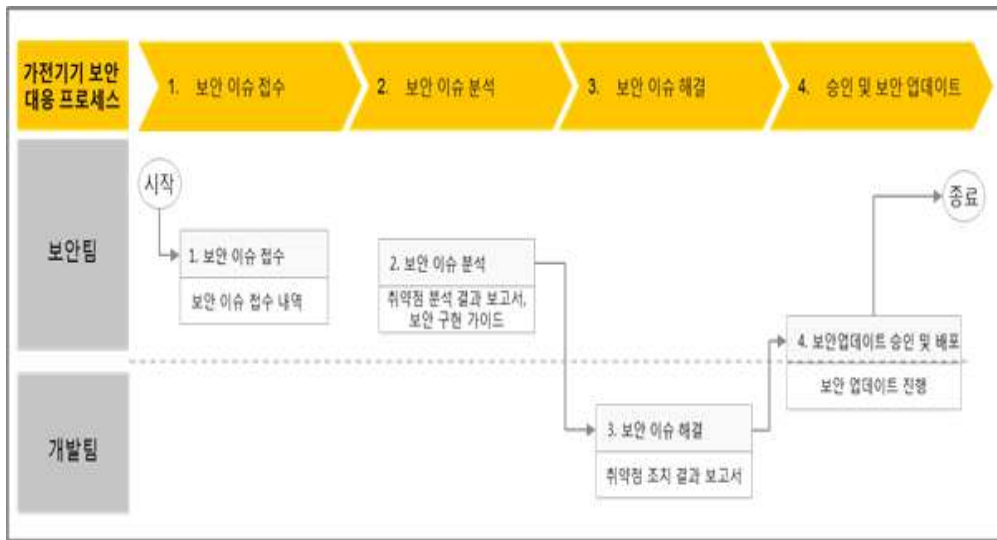
보안 검토서 작성: SW승인 완료 전까지, 개발 관리 시스템 입력을 통해 해당 기기 보안 인증서 결재를 요청한다. 결재 요청 시, SDL 보안 검토서를 첨부하여 내부 지침을 따른다.

보안 인증서 승인: 검증부서는 보안 검토서를 확인하여 보안 검토서 결재를 최종 완료한다. 보안 검토서 등록은 개발부서에 의해 결재 완료된 보안 검토서를 개발 관리 시스템에 등록한다.

7. 대응 단계 프로세스

7.1 보안 이슈대응 프로세스

SDL 프로세스가 적용된 Home IoT 가전기기의 보안 이슈가 발생하였을 때 해당 프로세스가 적용되며 보안 이슈가 접수되는 시점부터 보안 이슈 분석, 보안 이슈 해결, 보안 업데이트 버전 승인 순으로 진행된다. 이슈 접수 단계에서는 보안부서에서 접수를 받은 후 취약점 분석 결과 보고서와 보안 구현 가이드를 제작하여 개발부서에 전달한다. 개발부서는 전달받은 취약점 분석 결과 보고서와 보안 구현 가이드를 바탕으로 보안 이슈를 해결하여 취약점 조치 결과 보고서를 다시 보안팀에 전달하고 보안부서에서는 취약점 조치 결과 보고서를 검토하여 승인한 뒤 개발부서와 협업하여 보안 업데이트를 진행한다. 상세 프로세스는 [그림 29]와 같다.



[그림 29] 가전기기 보안 대응 프로세스 설계

7.2 보안 이슈 대응 프로세스 별 상세 업무

보안 이슈 접수: 보안부서에서 Home IoT 보안 가전기기의 보안 이슈를 접수 받는다.

보안 이슈 분석: 보안부서는 접수된 보안 이슈 정보를 검토한 뒤 취약점 분석을 진행하여 취약점 분석 보고서와 보안 구현 가이드를 제작한다. 단, 보안 이슈 분석 및 책임추적성 확보를 위해 로그기록을 주기적으로 안전하게 저장·관리해야 한다. 또한 저전력·경량형 하드웨어 사양 및 운영체제가 탑재된 IoT 장치의 경우, 그 특성상 로그기록의 생성·보관이 어려울 수 있으므로, 이런 경우에는 서비스 운영·관리시스템에서 IoT 장치의 상태정보를 주기적으로 안전하게 기록·저장할 수 있어야 한다^[36].

보안 이슈 해결: 개발부서는 보안부서에서 전달받은 취약점 분석 보고서와 보안 구현 가이드를 통해 보안 이슈를 해결하고 취약점 조치 결과 보고서를 작성하여

보안부서에게 전달한다.

승인 및 보안 업데이트: 보안부서에서는 전달받은 취약점 조치 결과 보고서를 검토하여 승인한 뒤 개발부서와 협업하여 보안 업데이트를 진행한다.

제4장 연구 결과 및 분석

제1절 Home IoT 가전기기 보안 요구사항 검증

도메인 별 보안 요구사항에 대한 탐지율 검토를 위해 기존의 “OWASP TOP 10”, “IoT공통 보안가이드”, “Global 컨설팅 기업 IoT 보안 점검 항목”, “관련 논문 검토 항목”과 새롭게 도출된 43개의 점검 항목, 그리고 위협모델링을 활용하여 도출된 점검 항목을 확정하였다. 이를 기반으로 보안 전문가 5명에게 2017년도 1년간 제조사의 Home IoT 가전기기에 대한 취약점 분석을 의뢰하였다. 전문가들은 5년 이상의 숙련된 기술 인력으로써, 동일한 가전기기를 대상으로 각각 다른 보안 요구사항 항목을 적용하여 점검한 후 결과에 대해 비교분석을 진행하였다.

[표 19]는 취약점 분석에 대한 결과 값이며, 탐지율 비교를 위하여 간단한 공식을 사용하였다. 탐지율은 각 기기별 탐지 기간 대비 결과 값으로 일 평균 탐지 건으로써 각 논문과 가이드에서 주장하는 보안 요구사항의 평균 탐지율과 비교하였다.

[표 18] 보안 요구사항 점검 대상 및 설명

도메인	대상	설명
도메인1 (Home IoT 공통)	에어컨	점검 기간: 20 대상 설명: 외부에서도 전원상태를 확인 및 작동 또는 온도 조절 등의 기능 설정 지원
	냉장고	점검 기간: 20 대상 설명: 실시간 냉장고 내부 상태 확인 및 냉장고 사용 이력 지원
	스마트TV	점검 기간: 40 대상 설명: 인터넷에 연결되어 실시간 콘텐츠를 다운로드하여 이용이 가능하며, 뉴스·날씨·이메일 등 확인 가능

도메인	대상	설명
도메인2 (보안 & 디지털 영상)	스마트도어락	점검 기간: 15 대상 설명: 원격 문 열림/잠금 기능 사용 및 사용 이력 확인 가능
	IP 카메라	점검 기간: 20 대상 설명: 무선영상 송출을 통한 실시간 스트리밍 및 데이터 임시 저장 기능 지원
	Home CCTV	점검 기간: 20 대상 설명: 실시간 모니터링, 침입 감지 및 영상을 자동으로 대용량 저장 기능 지원
도메인3 (건강 & 금융)	스마트밴드	점검 기간: 10 대상 설명: 심장박동측정, 수면 측정, 걸음 측정, 건강관리 기능 제공
	스마트의자	점검 기간: 10 대상 설명: 자세의 변화, 자세 별 시간, 자세비율 정보와 착석 시간 등의 정보 제공 기능 지원
	스마트스피커	점검 기간: 20 대상 설명: 스피커의 음성인식 기능을 통해, 음악, 생활/정보, 검색, 쇼핑/주문, 금융 등의 기능 지원
도메인4 (에너지)	Home 에너지 저장 시스템	점검 기간: 20 대상 설명: 에너지 저장시스템으로 태양광에너지를 배터리 팩에 저장해주는 기능
	원격검침기	점검 기간: 10 대상 설명: LTE 망을 활용한 원격 자동 검침 기능 지원
	스마트보일러	점검 기간: 15 대상 설명: 외부에서 보일러 상태 확인 및 온도 조절, 타이머 설정 기능 지원

기존에 참고했던 보안 요구사항들과 새로 도출한 보안 요구사항을 각각 동일한 점검대상을 통해 점검을 실시했으며, 앞에서 정의했던 탐지율 산정 공식을 활용하여 결과 값을 도출하였다. 예를 들어 OWASP의 보안 요구사항을 기반으로 도메인 1의 “에어컨”을 점검하였을 경우에는, 21일의 점검기간 동안에 총 4개의 취약점이 발견되었다. 따라서 탐지율 측정값, 즉 일평균 취약점 발견 개수는 0.2개가 되는 것이다. 각 도메인별 점검 결과 평균 값을 비교해 보면, 도출된 점검 항목이 일평균 0.9개로써 본 논문을 통해 제시된 Home IoT 가전기기 보안 요구사항이 가장

탐지율이 높은 것으로 확인이 되었다. 그러나, 도메인3과 4의 일부 점검대상 가전에서는, 다른 논문에서 제시한 보안 요구사항의 탐지율 평균 값이 비슷하거나 높게 측정이 되었다.

[표 19] 도메인별 보안 요구사항 항목 탐지율 검증 결과

점검대상		OWASP			Global 기업			IoT공동 보안가이드			관련논문1 (한정진)			관련논문2 (강준모)			NEW		
		결과	기간	탐지율	결과	기간	탐지율	결과	기간	탐지율	결과	기간	탐지율	결과	기간	탐지율	결과	기간	탐지율
도메인 1	에어컨	4	21	0.2	11	21	0.5	2	8	0.3	11	23	0.5	2	10	0.2	12	20	0.6
	냉장고	4	21	0.2	11	21	0.5	2	8	0.3	11	23	0.5	2	10	0.2	12	20	0.6
	스마트TV	9	34	0.3	19	40	0.5	3	17	0.2	20	37	0.5	4	20	0.2	22	40	0.6
도메인 2	스마트 도어락	2	14	0.1	6	15	0.4	1	6	0.2	6	15	0.4	2	8	0.3	7	15	0.5
	IP 카메라	12	21	0.6	22	21	1.0	6	10	0.6	20	23	0.9	6	10	0.6	30	20	1.5
	Home CCTV	11	19	0.6	19	21	0.9	6	10	0.6	17	21	0.8	5	10	0.5	30	20	1.5
도메인 3	스마트 밴드	2	9	0.2	2	10	0.2	1	4	0.3	6	10	0.6	2	5	0.4	4	10	0.4
	스마트 의자	2	9	0.2	2	10	0.2	1	4	0.3	6	10	0.6	2	5	0.4	4	10	0.4
	스마트 스피커	13	28	0.5	20	22	0.9	6	15	0.4	18	30	0.6	6	10	0.6	30	20	1.5
도메인 4	Home 에너지 저장 시스템	16	29	0.6	20	22	0.9	6	15	0.4	22	31	0.7	4	10	0.4	32	20	1.6
	원격 검침기	2	9	0.2	3	10	0.3	1	3	0.3	5	10	0.5	2	5	0.4	4	10	0.4
	스마트 보일러	8	14	0.6	11	15	0.7	1	6	0.2	7	15	0.5	4	8	0.5	16	15	1.1
탐지율 평균값				0.4			0.6			0.3			0.6			0.4			0.9

IoT기기의 보안 검토 항목에 관하여 여러 가이드와 논문들이 제시되고는 있으나, 현재 가장 빠르게 확산되고 있는 Home IoT 가전기기 보안 요구사항에 관해서는 관련 연구가 많이 없었다. 이에 본 논문의 선행연구에서 기존에 존재하는 보안 요구사항 가이드, 논문 등을 분석하여 통합적인 IoT 보안 요구사항을 도출하였다. 또한 Home IoT 가전기기를 MS 위협모델링을 활용하여 추가로 특화된 위협을 도출하였고 위협 별로 4개의 도메인으로 재분류하였으며, 이러한 과정을 거쳐 Home IoT 가전기기의 도메인별 보안 요구사항을 새롭게 도출하게 되었다.

Home IoT 가전기기 도메인별 보안 요구사항을 검증하기 위해 다른 가이드 및 논문의 보안 요구사항들과 비교하여 탐지율을 검토하였다. 탐지율 검토 방법은 기업에서 출시되는 Home IoT 가전기기를 대상으로 보안 전문가들이 진행하였으며, [표 19] 도메인별 보안 요구사항 항목 탐지율 검증 결과를 통해 새롭게 수립한 보안 요구사항이 높은 탐지율이 나타나고 있음을 확인할 수 있었다.

그러나 이러한 보안 취약점 점검방법은 다음의 한계가 존재한다. 첫째, 취약점이 발견되면 보완하는 기간이 필요하므로 출시가 지연되고 따라서 전체적인 비용이 증가하게 된다. 둘째, 해킹사고가 발생할 경우 브랜드 가치하락은 물론 막대한 금전적 손실이 발생할 수 있다. 마지막으로 고객의 입장에서 사생활과 개인정보가 노출되어 2차 피해를 야기할 수 있고 생명의 위협까지 직면하게 될 수도 있다. 따라서, Home IoT 가전기기의 근본적인 취약점을 줄이고 점검 기간의 효율성 또한 높임으로써 비용을 낮출 필요성이 제기되었다. 이에 대한 해결 방안으로 SDL 도입을 고려하게 되었으며 이의 연구를 진행하였다.

제2절 Home IoT SDL 프로세스 적용

본 논문 제 3장에서 설계한 Home IoT SDL 프로세스를 실제 기업의 제조 프로세스에 적용하였고 보안전문가를 통하여 그 결과 값을 분석하였다. 또한 본 논문

의 선행연구에서 도출된 Home IoT 가전기기에 특화된 보안 요구사항들을 바탕으로 Home IoT 가전기기에 관한 취약점 분석도 진행하였다. Home IoT 가전기기의 범위와 가전기기에 안에 내장된 기능들의 종류가 무수히 많기 때문에, 현실적으로 본 논문에서 모든 대상을 기준으로 Home IoT SDL을 적용하는 것은 불가능했다. 따라서 본 논문에서는 Home IoT 가전기기 12개를 선정하여 취약점 분석을 다시 진행하였다.

[표 20] 연구 대상 및 기간

점검 대상	점검 기간	점검자
에어컨, 냉장고, 스마트TV, 스마트도어락, IP 카메라, HOME CCTV, 스마트밴드, 스마트의자, 스마트스피커, Home 에너지 저장 시스템, 원격 검침기, 스마트보일러	2018년 1월 ~ 2019년 4월	보안전문가 5명 (5년 이상 경력)

점검기간은 2018년 1월부터 2019년 4월까지이며 경력 5년 이상의 보안전문가 5명이 진행하였다. Home IoT 가전기기의 보안 요구사항을 도출하여 취약점 분석의 가이드라인을 만들었고, 최종적으로 Home IoT SDL 프로세스를 적용하였다. 취약점 분석은 기본적으로 SDL 프로세스가 적용된 가전기기에 대해서는 SDL에서 기진행한 “보안 정적 분석”, “오픈소스 취약점 점검”, “퍼지 점검”에 대한 보안 요구사항들은 별도로 분석하지 않는다.

2.1 효율성 평가 방법

본 논문에서는 Home IoT SDL 프로세스의 효율성을 평가하기 위해서 SDL 프로세스 적용 전과 적용 후로 취약점 분석 결과를 비교하여 효율성 평가를 진행하였다. 효율성 평가를 측정하는 요소로써 취약점 탐지율과 취약점 분석 기간 단축율로 효율성을 판단하였으며 검증 공식은 [표 21]과 같다.

[표 21] 효율성 검증 공식

취약점 탐지율	취약점 분석 기간 단축율
$(1 - \frac{SDL \text{ 적용 후 취약점 개수}}{SDL \text{ 적용 전 취약점 개수}}) \times 100$	$(1 - \frac{SDL \text{ 적용 후 취약점 분석 기간}_{(월)}}{SDL \text{ 적용 전 취약점 분석 기간}_{(월)}}) \times 100$

2.2. Home IoT SDL 프로세스 적용 결과 및 분석

Home IoT SDL 프로세스를 제조사에 적용한 결과 SDL 프로세스를 적용하기 전과 SDL 프로세스를 적용한 후의 취약점 분석을 통한 탐지 결과의 개선율과 분석 기간 단축율이 크게 향상된 것을 확인할 수 있다. SDL 프로세스가 적용된 12개의 Home IoT 가전기기는 [표 21]와 같은 방법으로 산정한 결과, SDL 적용 전 대비 평균적으로 76%의 탐지 개선율 향상과 59%의 취약점 분석 기간이 단축된 것을 [표 22]에서 확인할 수 있다.

[표 22] Home IoT SDL 프로세스 적용 결과

분석 대상		SDL 적용 전		SDL 적용 후		평균 결과(%)	
		탐지 결과	분석 기간	탐지 결과	분석 기간	탐지결과 개선율	분석기간 단축율
도메인 1	에어컨	12	20	<u>2</u>	<u>7</u>	83%	65%
	냉장고	12	20	<u>3</u>	<u>9</u>	75%	55%
	스마트TV	22	40	<u>6</u>	<u>15</u>	73%	63%
도메인 2	스마트도어락	7	15	<u>2</u>	<u>7</u>	71%	53%
	IP 카메라	30	20	<u>6</u>	<u>9</u>	80%	55%
	Home CCTV	30	20	<u>7</u>	<u>9</u>	77%	55%
도메인 3	스마트밴드	4	10	<u>1</u>	<u>3</u>	75%	70%
	스마트의자	4	10	<u>1</u>	<u>3</u>	75%	70%
	스마트스피커	30	20	<u>8</u>	<u>11</u>	73%	45%

분석 대상		SDL 적용 전		SDL 적용 후		평균 결과(%)	
		탐지 결과	분석 기간	탐지 결과	분석 기간	탐지결과 개선율	분석기간 단축율
도메인 4	Home에너지 저장시스템	32	20	<u>8</u>	<u>10</u>	75%	50%
	원격 검침기	4	10	<u>1</u>	<u>3</u>	75%	70%
	스마트보일러	16	15	<u>4</u>	<u>7</u>	75%	53%
	평균값	17	18	<u>4</u>	<u>8</u>	76%	59%

[표 23]를 통해 Home IoT SDL 프로세스를 적용한 12개 가전기기에 대해 취약점 분석을 진행한 상세결과를 확인할 수 있다.

보안 전문가 5명이 12개의 가전기기를 대상으로 취약점을 분석한 결과, 탐지 결과는 1개, 분석기간은 1~2일 정도의 상이한 부분들이 존재한다. 탐지 결과와 분석 기간의 경우 보안 전문가들의 개인별 역량에 따라 약간의 차이를 보인 것으로 나타난다.

[표 23] Home IoT SDL 프로세스 적용 후 취약점 분석 결과 (상세)

분석 대상		보안 전문가 A		보안 전문가 B		보안 전문가 C		보안 전문가 D		보안 전문가 E	
		탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간
도메인 1	에어컨	2	7	2	6	2	7	2	7	2	6
	냉장고	3	9	3	9	3	9	3	9	2	8
	스마트TV	5	15	6	14	6	16	6	15	6	15
도메인 2	스마트도어락	2	7	2	6	2	7	2	7	2	6
	IP 카메라	6	9	6	8	6	10	6	9	6	9
	Home CCTV	7	9	7	8	7	10	7	9	7	9
도메인 3	스마트밴드	1	3	1	2	1	3	1	3	1	2
	스마트의자	1	3	1	2	1	3	1	3	1	2
	스마트스피커	8	11	8	10	8	12	7	11	7	11

분석 대상		보안 전문가 A		보안 전문가 B		보안 전문가 C		보안 전문가 D		보안 전문가 E	
		탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간	탐지 결과	분석 기간
도메인 4	Home 에너지 저장 시스템	8	10	8	9	7	11	7	10	8	10
	원격 검침기	1	3	1	2	1	3	1	3	1	2
	스마트보일러	4	7	4	6	4	8	4	7	4	7
	평균값	4	8	4	7	4	8	4	8	4	7

SDL 프로세스를 적용한 Home IoT 가전기기의 경우 보안 전문가의 “취약점 분석” 단계에서 IoT 보안 점검 항목 중 장기간 분석이 필요한 “보안 정적 분석”, “오픈소스 보안 취약점 분석”, “퍼지 점검” 항목이 점검에서 제외되어 전체 취약점 분석 기간을 감소시킬 수 있었다. 그러나 SDL 단계별 점검을 진행한 후에도 취약점이 도출된 이유는, 개발부서와 품질관리부서 담당자가 보안 전문가 집단에 비해 전문성이 부족하기 때문으로 나타났다. [표 24]는 전체 결과 중 “스마트TV”의 취약점 상세 내역을 기술한 표이며 동일한 방법으로 11개 나머지 가전기기도 취약점 분석을 진행하였다.

SDL 적용 이후에 도출된 취약점을 살펴보면 “스크립트 언어에 중요 정보 노출 여부 확인”, “소스코드에 중요정보 평문 노출여부 확인”, “히든 모드가 적절한 방법으로 구현되어 있는지 확인”, “JTAG, UART 등 디바이스와 직접 연결 가능한 인터페이스에 대한 차단여부 확인”, “외부 케이스 오픈 시 탐지하여 프로그램 정상동작 제어여부 확인”, “필요한 포트만 노출되고 사용하고 있는지 확인”, “중요정보를 제3자가 위변조하는 것을 방지하기 위해 안전한 암호화 통신채널을 구현하는지에 대한 여부 확인”이 존재했다. 도출된 취약점들은 대부분 개발자의 지식 부족과 실수 그리고 개발의 편의성을 너무 많이 강조하다가 발생한 취약점이었다. 취약점 항목에 관한 상세 내용은 실제 제조사 가전기기의 취약점이므로 본 논문에서는 언급할 수가 없다.

[표 24] Home IoT SDL 프로세스 스마트TV 적용 결과

선행연구 IoT 보안 점검 항목 (50개)			SDL 프로세스 적용단계	SDL 적용 전 스마트 TV	SDL 적용 후 스마트 TV
SW 보안	시큐어코딩	버퍼오버플로우 등의 공격에 취약한 함수 사용 여부확인	A	O	
		사용자 입력 값에 대해서 적절한 처리 여부 확인 (외부입력이 직접적인 명령어 실행이 이루어지는 경우)	A	O	
		스크립트 언어에 중요 정보 노출 여부확인 소스코드에 중요정보 평문 노출 여부 확인	D	O	O
		응용 프로그램 컴파일 시 심볼정보 등의 포함되어 컴파일 되는지 확인	A	O	
	퍼지점검	변수에 지정된 버퍼 영역의 제한이 없어 더 많은 데이터의 입력 가능여부확인	B	O	
HW 보안	히든모드	히든 모드가 적절한 방법으로 구현되어 있는지 확인 (SW방식, HW방식)	D	O	O
	접근 인터페이스 차단	JTAG, UART, ISP 등 Device와 직접 연결 가능한 인터페이스에 대한 차단여부 확인	D	O	O
	HW분해차단	외부 케이스 오픈 시 탐지하여 프로그램 정상동작 제어 여부확인		O	O
인증	사용자 인증	Default ID 및 Password 사용 여부 확인	D	O	
		서비스 최초 인증 시 강제 인증 정보 변경여부 확인	D		
		강력한 패스워드 정책: 일정 횟수 이상의 인증 실패에 대한 제한이 없음 확인	D	O	
		강력한 패스워드 정책: 길이가 8자 이하 비밀번호 지정 가능 확인	D	O	
		강력한 패스워드 정책: 일련번호, 주민번호, 아이디 등 추측하기 쉬운 비밀번호 지정 확인	D		
		강력한 패스워드 정책: 이전에 사용했던 비밀번호와 동일한 비밀번호로 변경 가능 확인	D		
		강력한 패스워드 정책: 비밀번호 사용기	D	O	

선행연구 IoT 보안 점검 항목 (50개)			SDL 프로세스 적용단계	SDL 적용 전 스마트 TV	SDL 적용 후 스마트 TV
		간에 제한이 없음 확인			
		강력한 패스워드 정책: 특수문자, 영문자, 숫자로 이루어지지 않음 확인	D	O	
		강력한 패스워드 정책: 아이디/비밀번호 외 공인인증서 등 추가 인증 수단 미흡 (단, 개인정보취급자 및 금융서비스만 해당), two-factor인증 확인	D		
	권한 관리	접근에 대한 분리가 필요한 경우 적절한 분리여부 확인	D		
		사용자 ID 및 Device ID 가 고유하게 사용되며, 그에 따른 인증기능이 구현되어 있는지 확인 (서비스 운영 목적 1:N, N:1, N:N 방식으로 사용하는 경우 제외)	D		
		원격으로 디바이스에 접근할 경우 관리자 권한의 접근을 제한하고 있는지 확인	D		
	디버깅 인터페이스 인증	Device 접근 시 적절한 인증 기능 구현 여부 확인 (JTAG, UART 등) 강력한 패스워드 정책 부여 확인, 접속을 위한 Access Key 구현	D		
암호화	암호화 강도	중요정보를 암호화 시 사용되는 키 및 알고리즘의 강도확인 (낮은 암호화 알고리즘 사용 시 Key 없어도 복호화 가능)	D	O	
	인증정보 암호화	사용자 인증 정보 저장 시 해쉬 저장여부 확인	D		
	중요파일 암호화	중요정보 암호화 여부 확인	D		
	키 관리	암호화에 사용되는 Key가 적절하게 보호되고 있는지 확인 (Key가 노출된 경우 복호화 가능)	D		
	취약한 대칭키	제품별 암호화 키 동일 여부 확인	D		
	표준암호화 방식	암호화 방식은 표준 방식을 사용하고 있는지 확인	D		
	부채널 공격방지	암호화 연산 수행 시 잘못된 요청을 하는 경우에도 동일한 연산 시간이 소요	B		

선행연구 IoT 보안 점검 항목 (50개)			SDL 프로세스 적용단계	SDL 적용 전 스마트 TV	SDL 적용 후 스마트 TV
		되는지 확인			
중요정보 노출	안전한 전송 프로토콜	중요정보 전 송시 검증된 암호화 프로토콜 사용여부 확인	D	O	
	저장 및 전송 데이터 보호	중요정보 저장 및 전 송시 적절한 암호화 방식 사용 여부 확인	D	O	
	중요정보 수집	최소한의 개인정보 수집 여부 확인	D		
		개인정보 비식별화 기술 적용여부 확인	D		
		사용 완료된 개인정보 삭제여부 확인	D		
	중요정보 노출	Log를 통해 개인정보 및 중요정보 노출 확인	D		
플랫폼 보안	환경설정	초기 플랫폼 설정이 보안에 적절하게 설정되어 있는지 확인 (기본 명령어, 폴더, 파일에 대한 접근 권한)	D		
	불필요한 포트오픈	필요한 포트만 노출되고 사용하고 있는지 확인	D	O	O
	퍼지 점검	오픈된 포트에 대한 퍼지 공격 테스트 확인	B		
	보안패치 미흡	공개된 라이브러리 및 응용프로그램 등 사용 시 현재까지 알려진 취약점 존재여부 확인	C	O	
	응용 프로그램 무결성검증	주요 응용프로그램 동작 시 위·변조 확인 여부	D		
	보안 업데이트	온라인 보안패치 기능 여부 확인	D		
	로그수집 및 전송	응용 프로그램 실행, 포트 오픈 및 에러에 대한 수집 기능 및 원격 전송 기능 존재 여부 확인	D		
펌웨어 보안	펌웨어 암호화	적절한 암호화를 통해 펌웨어를 보호하고 있는지 확인	D		
	펌웨어 무결성검증	펌웨어 업데이트 진행 시 이미지 및 파일에 대한 적절한 검증 후 업데이트 기능 동작 여부 확인 (이미지 파일 사인 값 검증 등)	D		
도메인 1	메모리 보호기법	버퍼오버플로우로 인한 공격을 방지하기 위해 메모리 보호기법 적용여부 확인	A	O	

선행연구 IoT 보안 점검 항목 (50개)		SDL 프로세스 적용단계	SDL 적용 전 스마트 TV	SDL 적용 후 스마트 TV
적용여부 확인				
보안 이벤트 관리	사용자의 금전적 손실 및 사생활 침해, 안전에 영향을 미칠 수 있는 제품의 경우 보안이벤트 로그를 생성해야 하며 관리, 경고 절차를 구현했는지에 대한 여부 확인	D		
네트워크 구간 접근제어 설정	네트워크 통신을 하는 서비스에 대한 접근 제어 설정을 통해 비인가 접근을 제어하는지에 대한 여부 확인	D		
안전한 세션 및 토큰 관리	세션/토큰이 임의의 값으로 생성되며, 쉽게 노출/추측이 가능한지 여부 확인	D		
네트워크 재생공격 방지 미흡	네트워크를 통해 전송되는 암호화된 데이터를 해독하지 않고 행해지는 공격을 방지하는지에 대한 여부 확인	D	O	
중간자공격 방지미흡	중요정보를 제3자가 위변조하는 것을 방지하기 위해 안전한 암호화 통신 채널을 구현하는지에 대한 여부 확인	D	O	O
IoT시스템 구성간 상호인증 미흡	비 인가된 사용자에게 의한 제품제어나 개인정보 등 민감정보 유출을 방지하기 위한 상호인증 수행여부 확인	D	O	

※ O: 취약점이 발견됨

※ A: 보안 정책 분석, B: 펌웨어 점검, C: 오픈소스 보안 취약점 분석, D: 보안 기능 테스트

제5장 결 론

현재 국·내외적으로 Home IoT 가전들은 일상생활에 급속도로 확산되고 있으며, Home IoT의 기술 또한 빠르게 발전하고 있다. 그러나 Home IoT 가전기기는 다른 디바이스와 연동되면서 보안위협이 급속도로 늘어나고 있는 현실에 직면하고 있다. Home IoT 가전기기에 대한 보안은 개인과 가족의 사생활을 침해할 우려가 있을 뿐만 아니라 안전과 생명까지도 위협하고 있는 실정이어서 Home IoT 가전기기에 대한 근본적인 보안강화가 매우 필요하다고 하겠다.

본 연구에서는 이러한 Home IoT 가전기기의 근본적 취약점을 미연에 방지하는 방안을 제시하고자 SDL을 Home IoT에 특화하여 프로세스를 만들었고 실제로 Home IoT 제조사에 적용하여 그 효율성을 입증하였다. 현실적인 제약조건은 Home IoT SDL 프로세스를 모든 Home IoT 가전기기에 적용하기에는 시간과 인력 등의 한계가 있었다는 점이다. 따라서 대표적인 Home IoT 가전기기 12개를 대상으로 선정하여 특화된 SDL 프로세스를 적용하였다.

본 연구의 선행연구로써 기존에 존재하는 국·내외 가이드, 글로벌 컨설팅 기업의 보안 요구사항과 관련 논문들에서 제시하는 보안 요구사항과 SDL의 4가지 방법론을 상세 비교 분석하였다. 다만 IoT 보안 요구사항들이 상이하고 실제 항목들에 대한 검증이 없는 것과 이에 대한 문제점 개선의 필요성을 확인하였다.

본 연구에서는 선행연구의 문제점 개선을 위해 Home IoT에 적합한 보안 요구사항들을 도출하였다. 보안 요구사항을 도출하기 위해 Home IoT 가전기기 12개를 MS 위협모델링을 통해 추가 위협들을 도출하였고, 총 4개의 도메인으로 분류하여 보안전문가의 점검을 통해 취약점을 확인하였다. 마지막으로 Home IoT 가전기기에 특화된 SDL 프로세스를 실무에 적용할 수 있도록 만들었으며, SDL 프로세스를

실무에 적용하기 전보다 취약점 탐지율은 76% 감소, 취약점 분석 기간은 59%를 개선하게 되었다. 결과적으로 Home IoT 가전기기의 보안성은 높아졌으며 개발단계에서 보안 요구사항을 적용했을 때 취약점을 분석한 결과 효율성을 향상시킬 수 있었다. 실제로 NIST(National Institute of Standards and Technology, 미국 표준 기술연구소)에 따르면, [표 25]와 같이 출시 단계에 취약점을 발견하여 제거하는 것은 설계 단계에서 취약점을 제거하는 것에 비해 30배의 유지보수 비용이 발생한다고 발표된 바 있다.

[표 25] NIST 시큐어코딩 효과성

구분	설계 단계	코딩 단계	통합 단계	베타 제품	제품 출시
설계과정 결함	1배	5배	10배	10배	30배
코딩과정 결함		1배	10배	20배	30배
통합과정 결함			1배	10배	20배

이처럼 본 연구에서 설계된 Home IoT SDL 프로세스는 Home IoT 가전을 생산하는 제조사의 개발단계에 적용할 수 있으며, 설계한 SDL 프로세스가 다수의 기업에 적용될 경우에는 Home IoT 가전기기에 대한 보안 수준을 향상시켜서 급속도로 성장하는 Home IoT 가전기기의 보안성과 경제성 향상에 크게 기여할 것으로 기대된다.

본 연구는 과거에 없었던 Home IoT 가전기기에 특화된 SDL 프로세스를 마련했다는 점에서 학술적인 의미가 있으며, 실무적으로는 Home IoT 가전기기의 취약점을 분석하기 위해 투입된 비용 측면에서 그 효율성을 높였다는 부분에 그 의미가 있다고 할 수 있다.

본 연구에서 설계한 Home IoT 가전기기에 특화된 SDL 프로세스 중 개발부와 품질부서에서 자동화 도구를 사용하여 수행하는 자가 검증 단계가 얼마만큼 보안품질을 확보할 것인가는 향후 연구 과제로 남아 있다.

참고문헌

〈국내 문헌〉

- [1] 공만식, 채홍준, 유보현 (2016). 사물인터넷(IoT) 기술동향과 전망. *기계저널*, 32-33.
- [3] 김호원 (2014). 사물인터넷환경에서의 보안/프라이버시 이슈. *TTA Journal*, Vol.153.
- [4] IITP (2014). *IoT 현황 및 주요이슈*. IITP Insight, 21-24.
- [6] 융합보안산업 (2014). *산업연구원 사물인터넷 시대 안전망*, 7-9.
- [11] 사물인터넷포럼 (2015). *사물인터넷 게이트웨이 보안 요구사항*. 사물인터넷포럼.
- [14] 7대 사이버 공격 전망 (2019), 한국인터넷진흥원, 6-7.
- [13] IoT 공통보안 원칙 (2016). 한국인터넷진흥원.
- [15] IoT 공통보안 가이드 (2016). 한국인터넷진흥원.
- [16] 한정진(2015). *사물인터넷(IoT) 보안성 검토를 위한 보안아키텍처 설계와 점검 항목 구성*. 연세대학교.
- [19] 유주상, 최영환, 홍용근 (2014). *사물인터넷을 위한 IETF 표준화 기술 동향*. 한국전자통신연구원.
- [23] 강준모 (2016). *사물인터넷 환경에서 스마트TV 보안성 검증 방안*. 숭실대학교.
- [32] 사물인터넷포럼 (2015). *사물인터넷 기기 등급 분류 및 보안 요구사항*. 사물인터넷포럼.
- [34] 행정안전부 (2012). *운영자를 위한 C 시큐어코딩 가이드*. 3판.
- [35] 행정안전부 (2012). *운영자를 위한 Java 시큐어코딩 가이드*. 3판.
- [36] 침해사고 분석 절차 안내서 (2010). 한국인터넷진흥원.

〈국외 문헌〉

- [2] Top Use Case Based on 5 year CAGR, <https://www.idc.com/getdoc.jsp?containerId=prAP44660819>
- [5] FTC Staff, *Internet of Things Privacy & security ina connected world*, FTC, 2015
- [7] OWASP (2014). *OWASP IoT Top 10* (<https://www.owasp.org>)
- [8] CoAP (Constrained Application Protocol). [https://coap.technology.IETF\(Internet Engineering Task Force\)](https://coap.technology.IETF(Internet Engineering Task Force)). <http://www.ietf.org>.
- [9] MQTT (Message Queuing Telemetry Transport). <http://mqtt.org>. OASIS (Organization for the Advancement of Structured Information Standards). <http://oasis-open.org/>
- [10] oneM2M Specification Release 1. <http://www.onem2m.org>.
- [12] Security Considerations in the IP-based Internet of Things. <http://www.ietf.org>
- [17] ITU-T Y.2060 (2012). *Overview of the Internet of Things*.
- [18] ITU-T Y.2066. (2014). *Common requirements of the Internet of things*.
- [20] Bing Zhang, Xin-Xin Ma, & Zhi-Guang Qin (2011). *Security Architecture on the Trusting Internet of Things*.
- [21] R. H. Weber (2010). Internet of Things: new security and privacy challenges. *Computer Law and Security Review*. Vol.26, pp.23-30.
- [22] FLAUZAC Oliver, GONZALEZ Carlos, & NOLOT Florent (2015). *New Security Architecture for IoT Network*.
- [24] Adam Shostack (2008). *Experience Threat Modeling at Microsoft*. Microsoft.
- [25] P. Torr (2005). Demystifying the Threat modeling process. *IEEE Security*

&Private, Vol.3, No.5, pp.66-70.

- [26] Adam Shostack (2014). *Threat Modeling: Design for Security*. John Wiley & Sons.
- [27] Microsoft STRIDE Chart, <https://www.microsoft.com/security/blog/2007/09/11/stride-chart/>
- [28] Microsoft Security Development Lifecycle (SDL), <http://msdn.microsoft.com/en-us/security/cc448177.aspx>.
- [29] CLASP (Comprehensive Lightweight Application Security Process), http://searchsoftwarequality.techtarget.com/searchAppSecurity/downloads/clasp_v20.pdf.
- [30] Gary McGraw (2006). *Software Security: Building Security*, In Addison-Wesley Professional, p.448.
- [31] Humphrey, W. S. (1989). *Managing the Software Process*. Reading, MA: Addison-Wesley.
- [33] The CERT Oracle Secure Coding Standard for Java, <https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standard>

국문초록

Home IoT 가전기기의 보안성 향상을 위한 Security Development Lifecycle 적용 연구

윤 석 진

융합보안학과 산업보안전공

중앙대학교 대학원

사물인터넷(IoT: Internet of Things) 기술의 발전으로 사람과 사물, 사물과 사물 간 상호 연결이 급속도로 증가하고 있으며 그 종류 또한 늘어나고 있다. IoT 기술의 발전은 Home 가전기기에 IoT 기능을 탑재하여 사람들에게 수준 높은 삶의 질을 제공해 주고 있지만, 사생활 침해와 생명의 위협 등 심각한 보안에 대한 우려도 높아지고 있다. 현재 Home IoT 제조사들은 이러한 보안 위협을 감소시키기 위해, 자체적으로 Home IoT 가전기기의 보안 취약점 분석을 지속적으로 실시하는 등 많은 노력을 기울이고 있다. 그러나 증가하는 Home IoT 가전기기의 종류와 급속하게 발전하는 기능에 비해, 취약점을 줄이기 위한 시간과 투입되는 리소스는 점점 부족해지고 있는 것이 현실이다. 따라서 Home IoT 가전기기에 대한 근본적인 취약점을 줄임으로써 보안성을 향상시키는 연구가 필요하다고 하겠다.

Home IoT 가전기기에 대한 근본적인 보안의 취약성을 줄이기 위해서는 정책적 연구에서부터 상세한 기술들에 이르기까지 다양하게 연구되어야 한다. 현재 Microsoft사에서는 SW를 개발할 때 Security Development Lifecycle(이하 “SDL”)을 적용하여 실행하고 있다. SDL은 실제로 Microsoft사에 의해서 적용되고 테스트

되어 그 효율성이 입증되었다. 본 연구에서는 Home IoT 가전기기에 특화된 SDL 을 개발하여 Home IoT 제조사의 업무에 해당 프로세스를 적용하고 그에 대한 효율성을 확인하고자 목표를 정하였다.

선행연구로써 여러 가지 IoT 보안 요구사항 가이드와 기 발표된 논문에서 주장한 항목과 글로벌 컨설팅 기업에서 활용하고 있는 가이드를 분석하였고, 본 연구에서는 선행연구의 분석결과를 바탕으로 Home IoT 가전기기에 특화된 보안 요구사항을 추가로 도출하였다. 또한 Microsoft사의 위협모델링 기법을 활용하여 Home IoT 가전기기를 4개의 도메인으로 나누고 각각 도출된 보안 취약점을 추가하여 점검을 실행하였다. 이러한 연구를 기반으로 Home IoT 가전기기에 특화된 SDL 프로세스를 만들었고 보안 전문가로 하여금 효율성 여부를 검증하였다. Home IoT 제조사를 대상으로 한 개발자 인터뷰와 제조사에 산재되어 있는 단편적인 업무 매뉴얼을 집중 분석하여 각 단계별 프로세스와 Action item을 설계하였다. IoT 가전기기는 너무나 다양하여 모든 기기를 대상으로 연구를 진행할 수가 없음으로 가장 대표적 가전기기인 12개를 대상으로 진행하였다.

Home IoT 가전기기에 특화되어 설계된 SDL 프로세스를 실제 업무에 적용하기 전과 후의 보안 취약점 분석 결과는 취약점 탐지율, 취약점 분석기간 효율성 측면에서 상당한 성과가 있었다. SDL 프로세스를 적용한 가전기기에서 취약점 탐지율은 76% 이상 향상되었고, 분석 기간도 59% 감소하였다. 본 연구를 통하여 Home IoT 가전기기의 보안성 향상을 위하여 SDL 프로세스를 설계한 학문적 기여와, 실제 업무에 적용한 후 확인된 보안 취약점이 상당히 감소했다는 실무적 성과도 함께 얻게 되었다. 검증된 SDL 프로세스가 Home IoT 가전기기를 만드는 모든 제조사들에게 적용되어 Home IoT 가전기기의 근본적인 보안 취약점을 줄일 수 있게 되기를 기대한다. 마지막으로 SDL 프로세스상 설계, 구현단계에서 개발부서의 자가 검증을 통한 품질확보를 어떻게 담보할 것인가는 향후 과제로 남겨둔다.

Abstract

A study of Improved Security for Home IoT Devices Using Security Development Lifecycle.

Yun, Suk-Jin

Major in Industrial Security
Dept. of Security Convergence
The Graduate School of
Chung-Ang University

Advances in the Internet of Things (IoT) are enhancing connectivity between people and things and between things and things, spanning an increasing number of areas. The advanced IoT technology is being embedded in home appliances, improving our standards of living. It, however, is faced with a growing concern about security issues regarding threats to privacy and human life. Home IoT device manufacturers are making their own efforts to mitigate security risks by conducting inspections of the security vulnerabilities regarding their devices. However, time and resources invested in addressing such vulnerabilities are not enough to keep up with the increasing number of home IoT devices and their advances. This indicates that a study needs to be conducted to explore ways to enhance security for such devices by minimizing fundamental vulnerabilities.

To address fundamental security vulnerabilities for home IoT appliances, a wide range of efforts, including policy research and more sophisticated technologies, should be made. Microsoft, for example, is currently applying the Security Development Lifecycle (SDL) when developing software. The efficiency of the SDL has already been verified by Microsoft's application and testing. The objective of this study is to develop an SDL exclusively for home IoT appliances, apply it to home IoT appliance manufacturers' practices, and verify its efficiency.

This study analyzed previous studies containing various IoT security requirements or opposing views and took into consideration Global consulting company's guidelines to develop new security requirements exclusively for home IoT appliances. It also divided home IoT appliances into four domains using Microsoft's threat modelling and examined each domain with additional security vulnerabilities. Based on this analysis, this study designed an SDL process exclusively for home IoT appliances and had security specialists verify its efficiency. It also involved interviews with developers at a home IoT appliance manufacturer and intensive analysis of fragmentary work manuals scattered throughout the manufacturer to establish processes at each stage and related action items. Since there are numerous types of IoT appliances, this study focuses on smart TVs, which is a typical home appliance.

This study applied an SDL process designed exclusively for home IoT appliances and compared the security vulnerabilities before and after the application, and the results suggest a significant level of efficiency of the process. Smart TVs with the SDL process applied saw a 70% decrease in security vulner-

abilities and an 63% decrease in the time needed for inspection. This study is meaningful in that it contributes to the academia by designing an SDL process for enhanced security for home IoT appliances and that it achieved practical results that the actual application of the process led to a significant reduction in security vulnerabilities. The SDL process is expected to be adopted by all home IoT appliance manufacturers, reducing their fundamental security vulnerabilities. Lastly, further research should be conducted to explore how to assure the quality through a self-assessment by the development department at the stages of designing and implementing an SDL process.