Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.2, Apr. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.2.213

STRIDE 위협 모델링에 기반한 스마트 TV 보안 요구사항 도출*

오 인 경,[1†] 서 재 완,[1] 이 민 규,[1] 이 태 훈,[1] 한 유 나,[1] 박 의 성,[1] 지 한 별,[1]
이 종 호,[2] 조 규 형,[1] 김 경 곤[3‡]
[1]KITRI 차세대 보안 리더 양성 프로그램(연구원),
[2,3]고려대학교 정보보호대학원(대학원생, 교수)

Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling*

In-Kyung Oh,[1†] Jae-Wan Seo,[1] Min-Kyu Lee,[1] Tae-Hoon Lee,[1] Yu-Na Han,[1]
Ui-Seong Park,[1] Han-Byeol Ji,[1] Jong-Ho Lee,[2]
Kyu-Hyung Cho,[1] Kyounggon Kim[3‡]
[1]KITRI Best of the Best(Researcher), [2,3]Graduate School of Information Security,
Korea University(Graduate Student, Professor)

요 약

스마트 TV가 최근 IoT 생태계의 중심으로 떠오름에 따라 그 중요성은 갈수록 높아지고 있다. 스마트 TV 내 취약점이 발생하는 경우 도청, 도촬로 인한 사생활 침해 및 개인정보 유출의 측면 뿐만 아니라 금전적 피해까지 발생할 가능성이 있다. 본 논문에서는 스마트 TV 취약점 분석의 완전성을 높이기 위해 STRIDE 위협 모델링을 통해 위협을 체계적으로 식별하고 공격 대상에 대한 특성을 파악하였다. 또한 Attack Tree와 취약점 점검리스트를 제작하고 실제 취약점 분석을 통하여 점검리스트의 효과성을 검증하여 안전한 스마트 TV 사용 환경을 위한 보안 요구사항을 도출하였다.

ABSTRACT

As smart TVs have recently emerged as the center of the IoT ecosystem, their importance is increasing. If a vulnerability occurs within a smart TV, there is a possibility that it will cause financial damage, not just in terms of privacy invasion and personal information leakage due to sniffing and theft. Therefore, in this paper, to enhance the completeness of smart TV vulnerability analysis, STRIDE threat classification are used to systematically identify threats. In addition, through the manufacture of the Attack Tree and the actual vulnerability analysis, the effectiveness of the checklist was verified and security requirements were derived for the safe smart TV use environment.

Keywords: Threat Modeling, Smart TV, Security Requirement, STRIDE Threat Classification

Recieved(01. 23. 2020), Modified(04. 02. 2020), Accepted(04. 02. 2020)

* 본 연구는 KITRI 차세대 보안 리더 양성 프로그램(Best of the Best)의 연구 지원으로 수행되었습니다.

† 주저자, inkoh9802@sookmyung.ac.kr
‡ 교신저자, anesra@korea.ac.kr(Corresponding Author)

I. 서 론

기존 TV의 일반적인 사용행태는 방송 '시청'에 초점이 맞춰져 있던 것에 반해, 2008년 인터넷과 연결된 스마트 TV의 등장을 기점으로 TV는 단순한 시청의 개념을 넘어 사용자에게 다양한 콘텐츠를 더욱 편하게 즐길 수 있게 하는 존재로 자리 잡았다[1]. 2012년 스마트 인터랙션이 가능한 스마트 TV로 발전하면서, 스마트 기기는 물론 클라우드에서 지원되는 웹 스토리지로 집 밖에서 태블릿이나 노트북과 같은 스마트 기기 멀티미디어 콘텐츠를 공유하게 되었다. 2016년에는 스마트 허브를 탑재하여 'IoT에 가장 먼저 준비된 TV' 라는 타이틀을 가졌다. 그와 함께 스마트 컨트롤 리모컨을 통해 모든 컨텐츠를 간편하게 즐길 수 있도록 하고, 스마트 허브를 통해 메뉴, 영상, 게임 등 스마트 TV 콘텐츠 간 장벽을 없앴다.

기술적 측면의 발전을 거듭한 결과, 2019년 스마트 TV는 주위 환경과 콘텐츠, 기기 간 연결에 구애를 받지 않는 맞춤형 서비스를 제공하는 것을 핵심으로 하여 음성인식 플랫폼, IoT 서비스 통합 앱과 더불어 사용자의 시청 이력을 분석하여 취향에 맞는 채널과 콘텐츠를 자동으로 추천하는 등, 더욱 똑똑한 인공지능 TV로 거듭났다[5].

스마트 TV가 다양한 서비스를 지원하게 되면서 이를 악용하는 사례 또한 증가하게 되었다. 국내외적으로 스마트 TV의 도입이 증가함과 동시에, 도청, 도촬, 개인정보 유출 등 스마트 TV의 다양한 기술을 보안상 악용하는 사례가 발생하면서 스마트 TV 위협 분석과 관련된 연구의 필요성이 증가하고 있다[6].

따라서 본 논문에서는 임베디드 기기의 특성에 기반한 위협 모델링 기법[22]과 Microsoft 사의 위협 모델링 기법을[12] 중심으로 하여 보안 위협을 식별하고 최종적으로 스마트 TV에 대한 보안 요구사항을 도출하는 것을 목표로 한다.

본 논문의 2장에서는 스마트 TV 보안 연구 동향과 위협 모델링에 대한 기존 연구 사례 및 스마트 TV를 대상으로 제안하는 위협 분석 모델링에 대해 소개한다. 3장에서는 실제 기기에 위협 분석 모델링 절차를 적용하여 데이터 흐름도를 도출하고, 구체적인 위협 분석을 진행한다. 또한 3.5에서는 도출된 위협들을 이용하여 Attack Tree를 작성하고 이를 기반으로 3.6에서 스마트 TV 모의 해킹 시나리오를 제시한다. 3장의 끝으로 취약점 분석을 위한 취약점 점검리스트 제작을 진행한다. 제작된 점검리스트를 바탕으로 취약점 분석을 진행하여 취약점을 도출하였고 이를 통해 취약점 점검리스트의 실효성 테스트 또한 수행하였다. 4장에서는 분석된 위협에 따른 보안 요구사항을 도출하고 마지막으로 5장에서 결론 및 향후 과제를 기술한다.

II. 관련 연구

2.2에서는 위협 모델링 관련 연구 사례를, 2.3에서는 스마트 TV를 대상으로 제안하는 2가지 위협 모델링 기법을 소개한다. 2.2 및 2.3에서 소개할 것은 Klockwork사의 임베디드 소프트웨어 위협 모델링 기법[22]과 MS 위협 모델링[12] 기법에서 사용하는 STRIDE 공격 유형 분류이다.

2.1 스마트 TV 보안 연구 동향

스마트 TV에 대한 공격사례가 발표되면서 현재 여러 기업에서는 스마트 TV가 높은 컴퓨팅 성능과 네트워크 기능, 카메라, 마이크와 같은 하드웨어 자원을 이용하는 공격이 발생할 수 있는 문제에 대해 보안성 향상을 위한 노력이 이루어지고 있다. 제품에 대한 설계 및 구현에 대한 안전성 검증을 위해 보안성 평가 제도를 활용한 제품 인증 및 스마트 TV 해킹에 대한 다양한 관점에서 접근 시도 등, 스마트 TV 보안 위협을 제거하기 위한 심도 있는 연구 내용이 보고서 및 논문[19], 컨퍼런스[18]를 통해 발표되고 있다.

또한, 스마트 TV를 대상으로 한 디지털 포렌식 연구도 이루어지고 있다. 디지털 포렌식의 경우 시스템 내부에 저장된 사용자 데이터를 수집 및 분석하기 매우 적합하다. 여기서 사용자 데이터란 인터넷 사용 기록, 최근 사용한 앱 및 접속한 웹페이지, 저장된 TV 채널, 시스템 설정 정보, 외부 저장장치 연결 정보 등이다. 이를 이용하여 포렌식 분석을 진행함으로써 개인정보를 획득할 뿐만 아니라 사용자의 성향을 파악한다[19].

STRIDE는 가장 널리 알려진 위협 모델링 방법으로, 위협 모델링을 하는 전체적인 과정 측면에서는 유용하다. 그러나, 소프트웨어 중심의 위협 모델링이라는 한계점이 있어 임베디드 기기인 스마트 TV와는 세부적인 사항에서 적합하지 않다. 따라서 스마트

TV 위협 모델링의 전체적인 구성은 Klockwork 사에서 제안한 임베디드 소프트웨어 위협 모델링[22]을 따르고, MS 사의 위협 모델링 기법[12]에서 사용하는 STRIDE 공격 유형 분류를 접목하여 위협 분석 및 분석 방법에 대한 취약점 점검 리스트를 도출하였다.

2.2 위협 모델링 연구 사례

위협 모델링은 임의의 공격자 관점에서 잠재적인 위협을 식별하고 분석하는 방법론이다[2,7,8,10,12,13,16]. 위협 모델링을 통해 자산을 식별하고, 발생 가능한 위협을 발견하고, 위험의 우선순위를 결정하여 위험에 대한 대응책을 결정할 수 있다. 위협 모델링 기법의 특징은 단순히 소프트웨어 관점만이 아닌 공격자와 보안의 관점에서 목적과 요구사항을 반영한다는 점이다. 일반적인 위협 모델링을 활용한 취약점 분석은 제품 분석, 위협 식별, Attack Tree 작성, 취약점 점검 리스트 도출 순으로 진행되며, 이때 각 위협에서 발생 가능한 공격을 식별하기 위해 알려진 기존의 취약점들을 수집한 공격 라이브러리 생성되어야 한다.

최초의 위협 모델링은 요구사항을 수집하는 단계와 설계문서를 통합하는 과정에서 위협을 식별하기 위한 절차로 시작되었다. 위협 트리에 대한 개념은 1994년 'Fundamentals of Computer Security Technology'에서 처음 소개되었다. 이후 1999년에는 도식적인 위협 모델링 방법인 Attack Tree를 사용하는 것이 제안되었고, 비슷한 시기에 Microsoft 제품의 설계 단계부터 다양한 위협을 식별하기 위해 STRIDE 공격 유형 분류가 소개되었다. 나아가 2011년에는 MS 자체 소프트웨어 개발 생명 주기가 만들어 지면서 이를 기반으로 한 자체 위협 모델링 도구가 현재까지 배포되고 있다[14].

MS사에서 제작한 위협 모델링 기법 외에도 여러 다양한 위협 모델링 기법이 존재한다. OWASP에서는 주로 웹 응용 프로그램 설계를 목적으로 한 위협 모델링 기법이 제안되었다. 또한 임베디드 소프트웨어 환경에 맞는 시큐어 임베디드 소프트웨어 개발을 위한 위협 모델 연구가 Klockwork사에 의해 시도되었는데, 위협 모델 생성 시 공격자 모델을 사용하지 않아 체계적이지 못하고 자동화될 수 없는 기법이라는 한계점을 확인하였다[22]. 또한 LINDDUN은 소셜 미디어 네트워크 환경의 응용 소프트웨어를 대상으로 한 privacy 위협 모델링 기법이다.

2.3 임베디드 소프트웨어 위협 모델링 기법

Klockwork사의 임베디드 소프트웨어 위협 모델링 기법은 다음과 같이 5단계로 구성된다[22].

1. Identify Security Objectives

이 단계에서 수행되는 것은 원하는 보안 수준을 명확히 하는 것이다. 모든 보안 침해를 방지하는 것이 목표인지, 특정 공격이 허용되는지 등에 대해 고려해야 한다. 또한, 가능한 모든 공격을 예방하는 것은 가능하나, 비용 효율의 균형을 맞추어 현실적인 보안 목표를 설계해야 한다.

2. Create a System Overview

이 단계에서 수행되는 것은 시스템 개요를 작성하는 것이다. 보안 목표가 명확해지면, 위협 모델링을 적용할 대상을 검토하고 자산 식별을 해야 한다.

3. Isolate and Decompose the Device's Software Design

이 단계에서 수행되는 것은 Abuse Scenario에 대해 고려하는 것이다. Abuse Scenario는 악의적인 사용자의 시스템 공격 시나리오를 의미한다.

4. Identify Threats

이 단계에서 수행되는 것은 위협을 식별하고 공격 유형을 고려한 Attack Tree를 개발하는 것이다. 가능한 많은 위협을 식별하기 위해 각 자산의 기밀성, 무결성 또는 가용성에 영향을 미치는 경우를 고려하는 CIA Method를 사용한다. Attack Tree를 개발하여 사용자를 가장한 공격자가 진행할 수 있는 공격의 유형을 식별하고, 공격이 성공할 수 있는 조건과 기법 또한 나열한다.

5. Identify Vulnerabilities

이 단계에서 수행되는 것은 취약점을 식별하는 것이다. 이를 기반으로 공격 완화 전략을 계획하는데 사용될 수 있는 취약점 목록을 구상한다.

2.4 STRIDE 공격 유형 분류

STRIDE 공격 유형 분류는 기밀성, 무결성, 가

용성의 보안의 3요소에 인증, 부인방지, 권한 부여의 3가지 요소를 추가하여 총 6가지 각각의 목표에 대응하는 위협을 분류한 것이다. 이는 응용프로그램의 취약성 및 잠재적 공격 가능성을 식별하는 데 도움이 된다[3].

1. Spoofing

Spoofing은 보안 속성 중 인증과 관련된 것으로, 거짓된 계정 등을 이용하여 시스템 권한을 획득하는 위협 등을 식별할 수 있다.

2. Tempering

Tempering은 보안 속성 중 무결성과 관련된 것으로, 불법적으로 데이터를 변경하는 위협 등을 식별할 수 있다.

3. Repudiation

Repudiation은 보안 속성 중 부인방지와 관련된 것으로, 특정 서비스를 수행하지 않았다고 부인하거나 책임이 없다고 부인하는 위협 등을 식별할 수 있다.

4. Information Disclosure

Information Disclosure는 보안 속성 중 기밀성과 관련된 것으로 접근 권한이 없는 누군가에게 정보를 제공하는 위협 등을 식별할 수 있다.

5. Denial of Service

Denial of Service는 보안 속성 중 가용성과 관련된 것으로, 서비스 또는 Application이 정상적으로 수행되지 않도록 하는 위협 등을 식별할 수 있다.

6. Elevation of Privilege

Elevation of Privilege는 보안 속성 중 권한 부여와 관련된 것으로 누군가가 권한을 부여받아 권한이 없는 서비스를 수행하도록 하는 위협 등을 식별할 수 있다.

III. 스마트 TV 위협 모델링

스마트 TV 환경에서 정보의 불법 노출 및 수정, 손상 등을 방지하기 위해서는 주요 정보가 반드시 보호되어야 한다. 이에 따라 3.1에서는 전반적인 스마트 TV 위협 모델링 방법론을 제시한다. 그리고 3.2부터 3.4까지는 수집한 스마트 TV 대상 공격 라이브러리를 기반으로 데이터 흐름도를 도출하고 STRIDE 공격 유형 분류를 적용하여 데이터 흐름도의 각 요소 들에서 발생 가능한 위협을 분석한다. 3.5에서는 식별된 위협이 공격에 적용되는 형태를 알아보기 위해 Attack Tree를 작성한다. 3.6에서

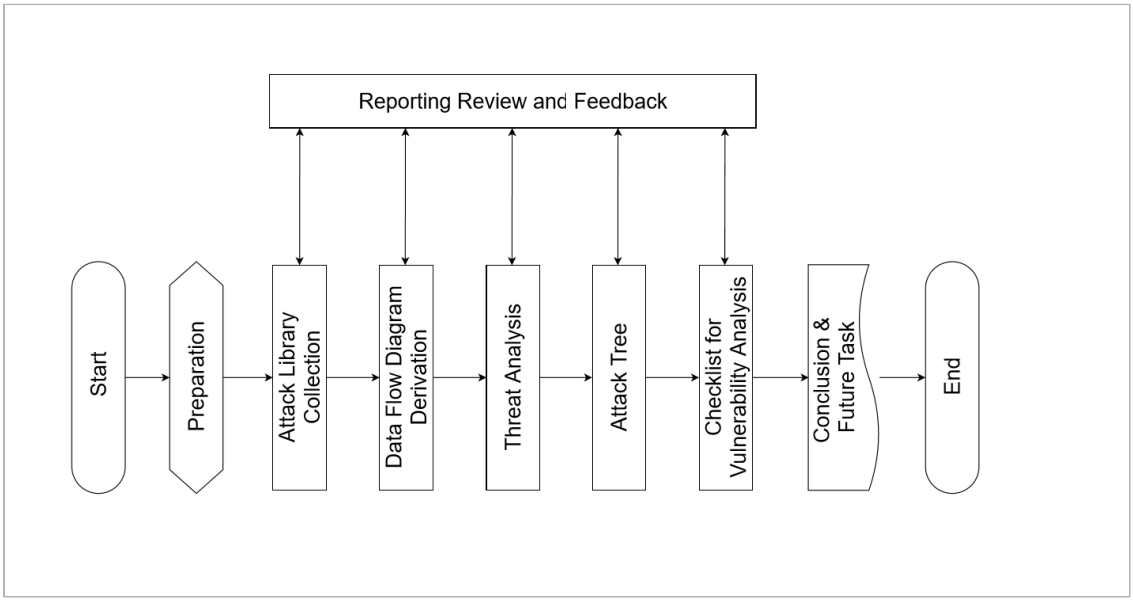


Fig. 1. Threat Modeling Procedure

는 스마트 TV를 공격할 수 있는 방법을 구체화 시키기 위해 스마트 TV 모의 해킹 시나리오를 제시한다. 끝으로 3.7에서는 위협 모델링 기법을 적용하여 도출한 위협 목록에서 실제 취약점이 발생할 수 있는 공격 벡터를 선정한 후 취약점 분석을 위한 취약점 점검 리스트를 제작한다[3].

3.1 위협 모델링 방법론

취약점 분석을 진행하기 앞선 위협 모델링 절차는 Fig.1.과 같은 형태로 진행된다. 공격 라이브러리란 선행된 연구 정보를 모아 놓은 것이다. 사용될 수 있는 정보는 표준, 논문 및 컨퍼런스에서 발표된 선행연구[19], CVE와 같이 공개된 취약점 정보, OWASP와 같은 보안 연구 프로젝트에서 공개한 취약점 항목 등이 있다. 이를 이용하여 데이터 흐름도상의 각각의 요소에서 발생 가능한 위협을 식별할 수 있다. 위협 식별 과정에서는 중복되는 결과를 줄이고, Attack Tree를 통해 스마트 TV를 공격 할 수 있는 방법을 구체화 시킨다. 끝으로 취약점 점검 체크리스트를 기반으로 한 실제 분석 시도 및 보안 요구사항 도출을 결론 및 향후 과제로 제시함으로써 위협 모델링을 마무리한다.

3.2 공격 라이브러리 수집

스마트 TV 공격 라이브러리는 크게 논문, CVE, 컨퍼런스 자료를 수집하였다. 총 36개의 논문 및 컨퍼런스 자료와 총 21개의 CVE를 수집하였고, 이 중 중요 논문, CVE, 컨퍼런스 자료들을 아래의 Table 1, Table 2, Table 3.을 통해 나타내었다.

Table 1. Attack Library: Paper

Vulnerability Analysis Paper			
Author	Title	Year	Ref
Gu-hwan Kwon	Research on the Analysis of Smart TV Vulnerabilities and Verification Methods for Firmware Security	2019	[9]
Min-su Park	Study on Security and Privacy of Smart TV	2018	[3]
Jong-ho Lee	A Study on the Analysis of Smart TV Vulnerabilities Based on WebOS	2017	[1]
Sung-hyuck Hong	Hacking and Countermeasure on Smart TV	2014	[15]
Soo-young Kang	Analysis of Security Requirements for Secure Updates of IVI Using Threat Modeling and Common Criteria	2019	[7]
Suk-jin Yoon	A Study on Security Requirements Analysis through Security Threat Modeling of Home IoT Appliance	2019	[16]
CMU	Threat Modeling: A Summary of Available Methods	2018	[13]
HAL	Smart-TV Security: Risk Analysis and Experiments on Smart TV Communication Channels	2018	[4]
Eun-ju Park	Derivation of Security Requirements of Smart Factory Based on STRIDE Threat Modeling	2017	[12]
Yong-hee Zeon	A Study on the Security Modeling of Internet of Things	2017	[6]
Jae-ki Kim	Study on the Femtocell Vulnerability Analysis Using Threat Modeling	2016	[8]
Jin-ho Lee	Technology Trends of Threat Modeling Technique for Developing Secure Software	2015	[10]
Chan-suk Jeong	Security Measures for Smart TV Service	2013	[5]
Klockwork Company	Threat Modeling for Secure Embedded Software	2011	[22]

Table 2. Attack Library: CVE

CVE		
CVE Number	Abstract	Ref
CVE-2019-5784	Heap Corruption	[23]
CVE-2019-5782	Execute arbitrary code inside a sandbox	[24]
CVE-2019-5755	Remote Attacker to perform arbitrary read/write	[25]
CVE-2019-9871	Remote Code Execution	[26]
CVE-2018-16065	Use After Free	[27]
CVE-2018-6143	Out of Bound	[28]
CVE-2018-6062	An integer Overflow on 32-bit systems	[29]
CVE-2018-6065	Integer Overflow	[30]

Table 3. Attack Library: Conference

Conference			
Presenter	Title	Year	Ref
Pedro Carbrera	SDR Against Smart TVs URL and Channel Injection Attacks	2019	[17]
Min-su Park	LG VS Samsung TV: Which is Better for Tracking You?	2017	[18]
Jong-ho Lee	Are you watching TV Now?	2017	[19]
Seung-ju Kim	Developing a Protection Profile for Smart TV	2014	[20]
Seung-jin Lee	Hacking, Surveilling and Deceiving Victims on Smart TV	2013	[21]

3.3 데이터 흐름도 도출

DFD는 시스템에서 데이터의 흐름을 보여주기 위해 작성하는 그림이다. 가시화된 데이터의 흐름을 기반으로 하여 보안 문제 발생 여부를 확인시켜 주는 역할을 한다. 이러한 DFD의 구성 요소는 Table 4.와 같이 외부 객체(External Entity), 데이터 저장소(Data Store), 프로세스(Process), 데이터 흐름(Data flow), 신뢰 경계(Trust Boundary)의 총 5가지로 구성된다. 스마트 TV에 대한 DFD는 Fig.2.와 같다. DFD 작성 결과로 7개의 외부 객체와 21개의 프로세스, 그리고 59개의 데이터 흐름을 도출하였다. 신뢰 경계는 총 3개로 사용자와 AWS 서버 간의 경계, 사용자와 Payment 서버 간의 경계, 사용자와 Sandbox Trust 공간 간의 경계이다[13].

Table 4. Data Flow Diagram Component

DFD Component		
Element	Description	Shape
External Entity	External Entity generates inputs of data and consume outputs	
Data Store	Data Stores store data temporarily or permanently	
Process	Process get inputs of data and generates outputs	
Data Flow	Data Flow indicates movement of data between the external entity, data store and process	
Trust Boundary	Trust Boundary indicates changes of privilege levels	

3.4 위협 분석

Fig.2.의 DFD Level 2의 요소들을 분리한 후, Microsoft Threat Modeling Tool(이하 MS Tool)을 이용하여 자동 위협 식별 및 도출을 진행한다. STRIDE 요소에 맞게 분류한 결과 Table 5.와 같이 총 379개의 위협을 도출하였다. 또한 MS Tool에 의한 자동 위협 식별 결과 외에, STRIDE 공격 유형 분류를 이용하여 임베디드 기기의 특성에 맞게 Table 6.과 같이 총 41개의 추가적인 위협을 도출하였다.

Table 7.에서 설명하듯이, 악성코드를 실행시키는 앱을 설치함으로써 발생하는 위협, MiTM 공격

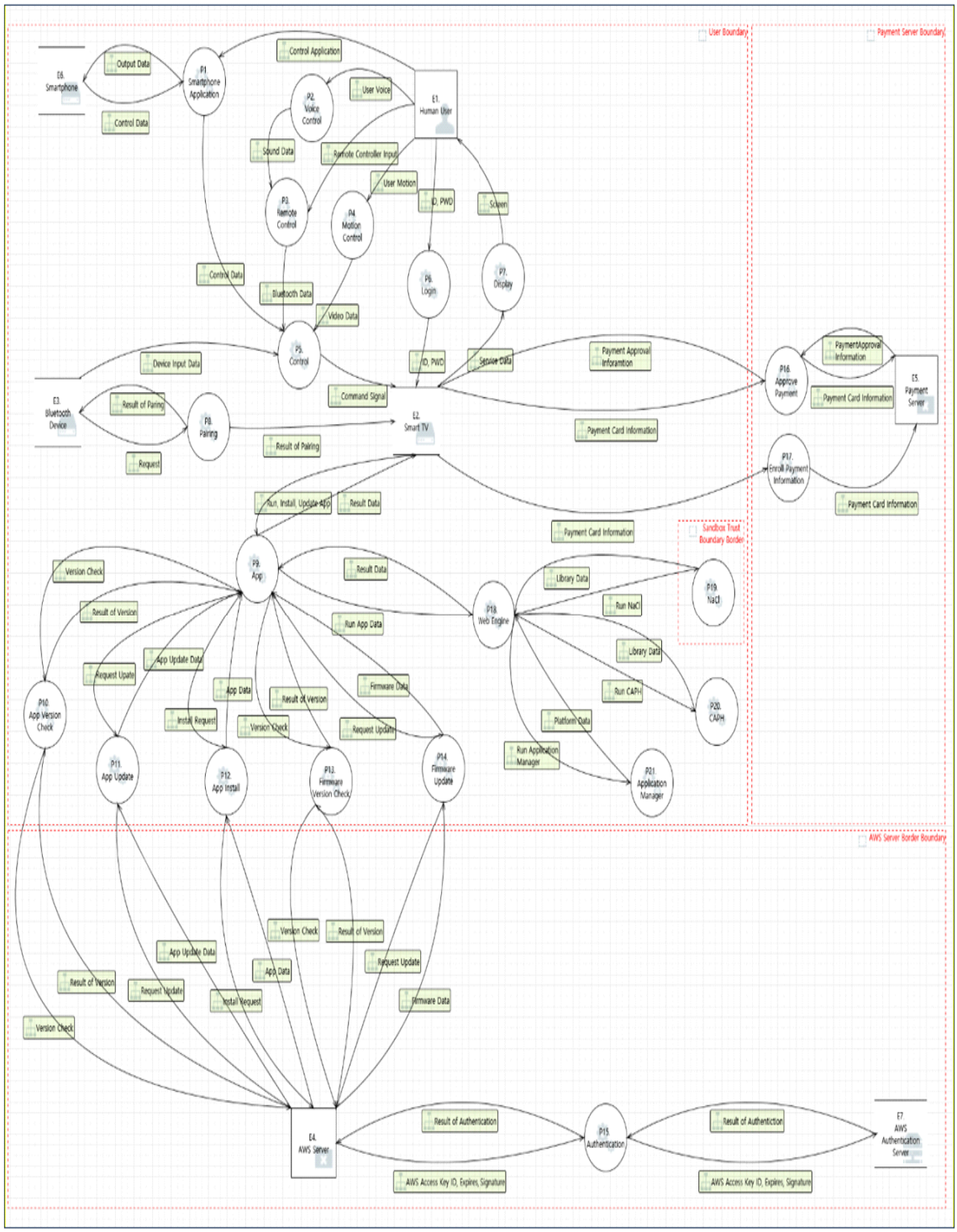


Fig. 2. Level 2 DFD for Smart TV

Table 5. MS Tool Threat Derivation Results

MS Tool Threat Derivation Results							
STRIDE	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	Total
Number	70	84	47	64	49	65	379

Table 6. Additional Threat Derivation Results

MS Tool Threat Derivation Results							
STRIDE	Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	Total
Number	4	10	2	11	5	9	41

을 통한 SSL/TLS Spoofing이 발생 가능한 위협, 스파이캠으로 인한 사생활 침해 위협 등이 있다.

3.5 Attack Tree

Attack Tree란 자산이나 정해진 목표를 공격하는 시나리오를 제시하는 개념도로, 다중 수준으로 구성되어 있다[12].

STRIDE 공격 유형 분류를 이용하여 임베디드 기기의 특성에 맞게 도출한 총 41개의 추가적인 위협을 바탕으로 Table 8.과 같이 공격 대상인 Smart TV를 루트 노드로 한 Attack Tree를 작성하였다. Table 8.은 STRIDE 분석을 통해 식별한 위협과 작성된 Attack Tree 사이의 연관성을 보여준다. Attack Tree를 이용하게 되면 스마트 TV를 공격 할 수 있는 방법을 구체화 시킬 수 있다는 의의가 있다. 이를 통해 3.6과 같이 스마트 TV 모의 해킹 시나리오를 제시할 수 있다.

3.6 스마트 TV 모의 해킹 시나리오

3.4에서는 STRIDE 기법을 통해 위협을 식별하고, 스마트 TV 공격 벡터를 파악할 수 있었다. 이를 기반으로 3.6에서는 Information Leakage 시나리오, MiTM을 이용한 유료 컨텐츠 재생 및 다운로드 시나리오, Third Party Application에 의한 개인정보 유출 시나리오, 악의적인 Application을 이용한 개인정보 유출 시나리오와 같이 4가지 모의 해킹 시나리오를 제시하였다. 각 시나리오 별 구상 목적과 공격 대상에 따른 세부 내용과 그에 따른 예상 피해를 기술하였다.

1. Information Leakage 시나리오

Table 9.에서 설명하듯이, Information Leakage 시나리오에서는 공격자가 Application에 악의적인 코드를 삽입하여 App Store에 배포하고 사용자가 이를 다운로드 하여 사용하는 내용을 다룬다.

공격자가 Application을 제작 시 Information Leakage가 발생 가능한 악의적 코드를 삽입 후 App Store에 등록한다. 사용자는 정상적인 Application으로 위장한 악성 Application을 실행하여 서비스를 이용한다. Application을 실행함과 동시에 공격자의 서버로 TV 디렉토리 정보 및 바이너리, 쉘 스크립트, DB, 구성 파일 등이 전송된다. 이를 통해 공격자는 스마트 TV를 대상으로 다른 공격을 하기 위한 정보를 얻을 수 있으며 DB와 구성 파일에서 사용자의 정보 또한 얻을 수 있다. 이를 통해 스마트 TV 구조 파악 및 개인정보 유출이 가능하다.

2. MiTM을 이용한 유료 컨텐츠 재생 및 다운로드 시나리오

Table 10.에서 보듯이, MiTM 공격은 통신하는 두 주체 사이에 네트워크 통신을 조작하는 중간자가 침입해 한쪽에서 전달된 정보를 도청 및 조작한 후 다른 쪽으로 전달하는 것이다. 이러한 공격은 TLS 통신을 하지 않기 때문에 가능하다. 만약 사용자가 스마트 TV 서비스 중 유료 컨텐츠를 재생하기 위해 결제하는 경우, 영상 전송 패킷을 확인하여 영상을 획득할 수 있다. 또한, 결제하는 회원의 정보를 전송하는 패킷을 확인하여 결제 정보 및 개인 정보를 획득할 수 있다. 이를 통해 공격자는 유료 컨텐츠 URL에 접속하여 파일 직접 다운로드 및 유포가 가능하고, 획득한 결제 정보 및 개인정보를 각종 사기,

Table 7. Additional Threat Derivation

Additional Threat Derivation				
DFD	Name	Detail	Threat	STRIDE
E2	Smart TV	The threat that intercepts and steals passwords through sniffing	T1	I
		The threat that obtains command permissions through firmware modulation	T2	T
		The threat that damages IoT Device systems due to malicious code distribution	T3	D
		The threat that modulates frame buffer through buffer overflow	T4	T
		The threat that caused by Denial of Service attack	T5	D
		The threat that malicious code is installed through USB driver	T6	D,E
		The threat that is likely to cause a general-purpose user to attempt to increase authority through race condition	T7	E
		The threat that can see TV's directory and run file by malcious code	T8	T
		The threat that might occur if log history is cleared and denied	T9	R
		The threat that could result in SSL/TLS spoofing through MiTM Attack	T10	S
E3	Bluetooth Device	The threat that arises from controlling device through Bluetooth spoofing vulnerability	T11	S
		The threat that caused by Denial of Service attack	T12	D
E4	AWS Server	Threats that could use unmanaged open ports as attack vectors	T13	E
		The threat that acquires administrator account permissions through remote access	T14	E
		The threat that caused by server information leakage with sniffing	T15	I
E5	Payment Server	Threats that could use unmanaged open ports as attack vectors	T16	E
		The threat that acquires administrator account permissions through remote access	T17	E
		The threat that caused by server information leakage with sniffing	T18	I
E6	Smart Phone	The threat that unauthorized attackers attempt to bypass Application authentication through MiTM attack	T19	S
		The threat that intercepts and steals passwords through sniffing	T20	I
		The threat that the attacker denies access and connection	T21	R
E7	AWS Authentication Server	The threat that acquires administrator account permissions through remote access	T22	E
		The threat that caused by server corruption because of physical damage	T23	D
		The threat that non-authorized DB access by vulnerable access control	T24	I
P2	Voice Control	The threat that arises from eavesdropping	T25	I
P3	Remote Control	The threat that arises from controlling TV through Bluetooth spoofing vulnerability	T26	S
P4	Motion Control	The threat that caused by camera function	T27	I

Additional Threat Derivation				
DFD	Name	Detail	Threat	STRIDE
P5	Control	The threat that arises from controlling device	T28	T
P6	Login	The threat that intercepts and steals passwords through sniffing	T29	I
		The threat that visualizes personal information through plain text transmission	T30	I
P7	Display	The threat that arises from the transmission of pirated broadcasts	T31	I
P9	App	The threat caused by malicious Application upload	T32	T
P11	App Update	The threat that arises from updating modulated App	T33	T,E
P12	App Install	The threat that arises from installing Apps that execute malicious code	T34	T,E
P14	Firmware Update	The threat that arises from updating modulated firmware	T35	T
P17	Enroll Payment Information	The threat that visualizes payment information through plain text transmission	T36	I
P20	CAPH	The threat that arises because not use a sandbox	T37	T
P21	Application Manager	The threat that arises because not use a sandbox	T38	T

Table 8. Attack Tree

Attack Tree				Threats
1			Application	
OR	1.1	Unauthorized Application Executable		
	OR	1.1.1	Information Leakage	T15, T18
	OR	1.1.2	Denial of Service	T32
OR	1.2	Unauthorized Accessibility		
	OR	1.2.1	API Vulnerability	T33
	OR	1.2.2	Install Malicious Application	T32
	OR	1.2.3	Modulate Existing Application	T32
	OR	1.2.4	Permission Intrusion Between Applications	T21
OR	1.3	Use of Vulnerable Software		
	OR	1.3.1	Execute Malicious Script	T3, T, T8, T34
2			Network	
OR	2.1	Packet Manipulation		
	OR	2.1.1	Network Packet Spoofing	T1, T9, T11, T26, T29, T30, T31
	OR	2.1.2	MiTM	T10, T19, T20, T25, T29, T30, T31
OR	2.2	Packet Analysis		
		2.2.1	Download Paid Video by Free	T30, T31
		2.2.2	Information Leakage	T36
OR	2.3	Denial of Service Attack		T5, T12
3			System	
OR	3.1	Shell Acquisition		
	OR	3.1.1	1-Day Attack	T2, T4, T7, T14, T17, T22, T24
	OR	3,2,2	Escaping Container	T2
OR	3.2	Modified Firmware Updates		
	OR	3.2.1	Modify Firmware using USB	T35
	OR	3.2.2	Modify Firmware Supported by Web	T35

Attack Tree				Threats
OR	3.3	Unauthorized Video Transmission		
OR	3.4	Firmware Acquisition		
4		Hardware		
OR	4.1	Physical Interface		
	OR	4.1.1	eMMC Data Extraction	T23
	OR	4.1.2	JTAG	T13, T16
	OR	4.1.3	UART	T13, T16
	OR	4.1.4	RS232 Port	T13, T16

도박 등 2차 범죄에 악용할 가능성이 있다.

MiTM 공격을 이용하여 스마트 TV에서 정당한 대가를 지불하지 않고 유료 컨텐츠를 재생 및 다운로드 하는 시나리오는 다음과 같다.

첫 번째 시나리오는 스마트 TV에서 무료 컨텐츠의 토큰을 사용하여 인증하고, 유료 컨텐츠를 재생하는 것이다. 이는 스마트 TV에서 유료 컨텐츠를 보기 위해서 해당 컨텐츠가 무료인지 유료인지 인증하는 과정을 거쳐 영상 재생하는 과정이 필요함을 이용하는 시나리오이다. 인증 과정에서 무료 컨텐츠 재생 번호를 유료 컨텐츠 재생 번호로 패킷을 변조하여 시청하고자 하는 유료 컨텐츠를 재생함으로써 결제를 하지 않고도 원하는 유료 영상을 볼 수 있다.

두 번째 시나리오는 스마트 TV의 영상 패킷을 도청하여 해당 영상의 URL에 접속하는 것이다. 실제 무료 컨텐츠의 패킷을 도청하여 확인한 URL에 접속한 결과 영상 재생뿐만 아니라 다운로드가 가능한

Table 9. Information Leakage

Scenario Overview	
Purpose	Acquire and analyze key files in a smart TV to understand the structure of a smart TV
Target	Smart TV Firmware
Attack Step	
Preparation	Insert the malicious code that could cause the Information Leakage into the application and register it in the App Store.
Invasion	Users install malicious applications and run them on smart TVs.
Security Issue	Directories and binaries, shell scripts, DBs, configuration files on the TV are sent to the attacker's server as soon as the app is run.
End	This allows an attacker to obtain information for other attacks on smart TVs and also user information from DB and configuration files.

Table 10. MiTM

Scenario Overview	
Purpose	Does not pay due price for playing and downloading paid content on Smart TVs through MiTM attacks.
Target	Smart TV Network
Attack Step	
Preparation	Users pay to play the paid content of Smart TV.
Invasion	Upon payment, the attacker checks the paid content transmission packet and payment member information packet.
Security Issue	An attacker can acquire paid contents through paid contents transmission packet and obtain payment informations and personal informations through a payment member information packet.
End	In addition to being able to access paid content URLs and directly download and distribute files, an attacker could potentially exploit acquired payment information and personal information for secondary crimes such as fraud and gambling.

것을 확인할 수 있었다. 따라서, 이를 유료 컨텐츠의 경우에 적용한다면 결제를 하지 않고도 영상 재생 및 다운로드 등 악용 가능성이 매우 높을 것이다.

3. Third party application에 의한 개인정보 유출 시나리오

Table 11에서 설명하듯이, 스마트 TV에는 휴대폰과 마찬가지로 타 사의 Third party application이 기본적으로 설치되어 있다. 따라서 스마트 TV자체 보안이 잘 되어 있더라도, 타 사의 Third party application이 취약하다면 고객 정보가 공격자에게 노출될 가능성이 있다.

사용자는 스마트 TV에 기본적으로 설치되어 있는 Third party application을 사용하며 로그인, 결제 등의 통신을 필요로 하는 서비스를 이용한다. 이때 데이터는 TV에서 라우터를 거쳐 해당 Third party vendor server로 전송된다. 공격자는 이 데이터를 중간에서 가로채는 MiTM 공격을 수행한다. 이때 만약 Third party application의 통신 방식이 보안 프로토콜인 TLS 프로토콜을 사용하지 않는다면 패킷이 평문으로 전송되는 문제가 발생하게 된다. 이 과정에서 노출된 데이터를 이용하여 공격자는 스마트 TV에 직접 침투하지 않고도 Third party application을 이용하여 손쉽게 고객의 개인정보를 획득할 수 있다.

Table 11. Third party application

Scenario Overview	
Purpose	Personal Information Leakage
Target	Smart TV Network
Attack Step	
Preparation	Use the third party application installed on smart TV that requires a network such as logging in, paying, etc.
Invasion	On smart TVs, through routers, attackers obtain data sent to third party Vendor Server using MiTM attacks.
Security Issue	If the third party application's network method does not use the TLS protocol, which is a security protocol, there is a problem in which packets are sent in plain text.
End	Attackers can use Third Party Application to obtain customer's personal information without directly invading Smart TVs.

4. 악의적인 Application을 이용한 개인정보 유출 시나리오

2017년 이후 스마트 TV는 .NET Application 업로드가 가능하다. Table 12에서 설명하듯이, App Store에 배포된 악성 .NET Application을 사용자가 실행하는 경우 공격자는 쉘을 획득할 수 있게 된다. 그 후 공격자는 LPE 등 추가적인 공격을 통해 권한을 상승시킬 수 있다. 높은 권한을 얻은 공격자는 Key Logging 프로그램을 업로드 하여 사용자의 키보드 입력 값을 얻거나 사용자의 음성 데이터를 얻는 등 개인정보 유출 및 도용의 피해를 발생시킬 가능성이 있다.

Table 12. Malicious Application

Scenario Overview	
Purpose	Personal Information Leakage
Target	Smart TV Network
Attack Step	
Preparation	Insert a malicious code into the .NET application and register it in the App Store.
Invasion	An attacker will be able to acquire a shell while the user installs a malicious application and runs it on a smart TV.
Security Issue	Attackers can gain control of the TV by increasing their authority through additional attacks, such as LPE, after obtaining the shell.
End	An attacker may upload a Key Logging program to obtain user keyboard input values or to obtain user voice data, causing damage to personal information leakage and theft.

3.7 취약점 분석을 위한 취약점 점검 체크리스트

3.4에서 식별한 위협을 기반으로 Table 14.와

Table 13. Validate Checklist Effectiveness

NO	Checklist Verification Item	Total Number of Items	Vulnerable Number of Items	Verification Rate
1	Application	5	2	40%
2	Network	7	3	43%
3	System	10	4	40%
4	Hardware	4	1	25%

Table 14. Checklist for Vulnerability Analysis

Checklist		
Classification	Check Item	Detail
Application	Unauthorized Application Executable	Information Leakage Vulnerability by unauthorized application
		DoS Attack Depleting Storage Space through File Generation
	Unauthorized Accessibility	API Vulnerability that allows execution permission on decompression
		Acquire Shell by malicious application
		Install Malicious Application
		Modulate the Existing Application
		Permission Intrusion between Applications
	Use of Vulnerable Software	Execute Malicious Script by using well known vulnerable software
Network	Packet Manipulation	Network Packet Spoofing Attacks for Manipulating System Data
		MiTM Attack Using SSL/TLS Certificate Manipulation
	Packet Analysis	Download Paid Video by free
		Leaking User Information by plaintext trasmission
	Denial of Service Attack	DoS Attacks by transferring a large amount of network packets
	Use of Vulnerable Port	RCE by opening a vulnerable port
System	Shell Acquisition	1-Day Attack through existing CVE
		Shell Acquisition through escaping container
	Modified Firmware Updates	Force update using modified firmware
	Unauthorized Video Transmission	Showing Pirate broadcasting
	Firmware Acquisition	Firmware Modulation with USB
		Modulating Using Firmware Update Supported by Web
	Command Injection	Command Injection by setting the name of TV
Hardware	Use of Vulnerable Interface	Check Data in Debug, UART, Logic, FANET mode of RS232 Port
		Shell Acquisition Using JTAG, UART Port
	Data Extract	eMMC Data Extraction

같이 취약점 점검 체크리스트를 도출한다.

이를 통해 Application, Network, System, Hardware에 대한 취약점 점검을 수행할 수 있다. 취약점 점검 체크리스트는 향후 스마트 TV 안전성 검사 및 보안 가이드 라인 제작에 활용될 것으로 기대된다[3]. Table 13.은 체크리스트 실효성 검증 결과를 나타낸 것이다.

IV. 스마트 TV 보안 요구사항 도출

스마트 TV 사용자에게 안전한 서비스를 제공하기 위해, 스마트 TV 내 하드웨어 및 소프트웨어 구성 요소들은 여러 다양한 보안 위협으로부터 견고해야 한다[3]. Table 15.는 STRIDE 위협 도출 결과 및 Attack Tree를 바탕으로 작성한 스마트 TV 환경에서의 보안 요구사항이다.

V. 결 론

스마트 홈의 규모가 커짐에 따라 가장 높은 보급률과 꾸준한 성장률을 갖는 스마트 TV는 향후 스마트 홈의 중심이 되어 타 스마트 기기들의 중추 역할

Table 15. Smart TV Security Requirements

Checklist		
Category	Surface	Detail
Application	Unauthorized Application Executable	Set up the permission of application in order to prevent being read the public key file from others to avoid the Information Leakage vulnerability.
		To prevent Information Leakage vulnerability, add authentication to security setting entry.
		Manage separately both API permissions and internal permission of Smart TV.
	Unauthorized Accessibility	OS should offer safe APIs to prevent exposure of key information.
	Use of Vulnerable Software	By using the tool which inspect inside of Smart TV, the device check installation and executing of programs and should prevent execution of malicious application.
Network	Packet Manipulation	When attacker attempt to authenticate using forged certificate, application or service should close network connection by SSL pinning.
		The functions have to be provided which protect the credential such as key, certifications.
	Packet Analysis	The user information outflow and illegal download of paid image should be prevented through the SSL/TLS encryption.
	Denial of Service Attack	DoS Attack is prevented through various access control such as unnecessary port deactivation, initial authentication information change, etc.
	Use of Vulnerable Port	Device should not provide services that has already known vulnerability to open port.
System	Shell Acquisition	External inputs should not be used as system instructions without validation.
		The instrument authentication management procedure should be implemented in order to prevent the illegal use.
		To prevent the memory operation, the memory protection technique should be applied to binary file.
		It is necessary to devide space by container so that shell acquired inside of container cannot affect the Smart TV.
	Modified Firmware Updates	The integrity verification technology for the firmware must be applied so that the modified firmware file cannot be widely distributed.
	Unauthorized Video Transmission	To prevent unauthorized video transmission, OS should manage display service using another permission.
	Firmware Acquisition	Firmware file for customer support should be encrypted to make analysis difficult, and avoid revealing encryption keys.
	Command Injection	The text which can be edited by user must be encoded to prevent command injection.
Hardware	Physical Interface	Internal debugging ports such as JTAG,UART,RS232 port, etc. should be physically removed or deactivated to prevent information retrieval through firmware extraction and file system analysis.
	Data Extract	Data which is in storagy such as eMMC, Flash Memory, etc. must be encrypted for prevention of physical extraction.

을 할 것이다.

이에 따라 스마트 홈 전체를 제어하는 기능을 맡을 경우, 스마트 TV에 대한 보안은 중요도가 더욱 높아질 것이다. 따라서 스마트 TV에 대한 단기적인 보안 솔루션의 개발 및 도입뿐만 아니라 장기적 측면에서 기기가 가지고 있는 근본적인 위협에 대한 전략적인 대응방안이 필요하다[5]. 그리고 스마트 TV의 구조를 분석하여 DFD를 도출하고, STRIDE 공격 위협 분류를 활용하여 스마트 TV에 존재 가능한 위협 요소를 식별하였다.

이를 기반으로 Application, Network, System, Hardware의 4가지 측면에 대한 취약점 점검 리스트를 제작하였다. 위협 분석 모델링을 통해 스마트 TV에 대한 보안 위협을 식별하고 효과적인 취약점 분석을 위한 취약점 점검 리스트를 작성하는 것은, 추후 안전한 스마트 TV 사용 환경을 구축하는데 도움이 될 것으로 기대된다[2].

향후 진행 방향 및 과제로는 취약점 점검 리스트 기반의 취약점에 대한 구체적인 대응방안 연구가 있다. 취약점 점검 도구를 개발하여 범용적으로 다양한

스마트 TV 제조사가 보안성을 확보할 수 있도록 도울 것이다.

References

[1] Jong-ho Lee, "A Study on the Analysis of Smart TV Vulnerabilities Based on WebOS," Information Security Department, University of Korea, Aug. 2017

[2] Kyoung-gon Kim, Soo-hoon Kim, "Using Threat Modeling for Risk Analysis of SmartHome," Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 378-379, Nov. 2015.

[3] Min-Su Park, "Study on Security and Privacy of Smart TV", Information Security Department, University of Korea, Jan. 2018

[4] Bachy, Yann, "Smart-TV security: risk analysis and experiments on Smart-TV communication channels," Journal of Computer Virology and Hacking Techniques, vol. 15, no. 1, pp61-76, Apr. 2018.

[5] Chan-Suk Jeong, Myung-Ryul Lee and Yong-Tae Sin. "Smart TV security threat analysis and security measures research," Proceedings of the Korean Information Science Society, pp701-703, June. 2013.

[6] Yong-hee Jeon, "A Study on Security Modeling of Internet of Things (IoT)," The Journal of Information Technology of Korea, 15(12), pp17~27, Dec. 2017.

[7] Soo-young Kang and Seung-joo Kim, "Analysis of secure update security threat modeling and Common Criteria," Journal of the Korea Institute of Information Security and Cryptology, 29(3), pp613-628, June. 2019.

[8] Jae-ki Kim, Jeong-Hoon Shin, and Seung-joo Kim, "Study on the Femtocell Vulnerability Analysis Using Threat Modeling," KIPS Transactions on Computer and Communication Systems, 5(8), pp197-210, July. 2016.

[9] Gu-hwan Kwon, "Smart TV vulnerability analysis and study on integrity verification for firmware security enhancement," Hanyang University, Feb. 2019.

[10] Jin-ho Lee, Hyuk Lee, and In-hye Kang, "Technical Trends in Threat Modeling Techniques for Secure Software Development." Journal of Information Security, 25(1), pp32-38, Feb. 2015.

[11] Yun-hwan Lee, and Sang-gun Park, "How to apply threat modeling for security risk analysis in smart home service environment," Korean Institute of Electrical Engineers, 66p(2), pp76-81, June. 2017.

[12] Eun-ju Park, and Seung-joo Park, "Deduced Smart Factory Security Demands Based on STRIDE Threat Modeling," Information Protection Society Journal, 27(6), pp1467-1482, Dec. 2017.

[13] Shevchenko, Nataliya, "Threat Modeling: a Summary of Available Methods," July. 2018.

[14] Shostack, Adam, "Experience Threat Modeling at Microsoft," MODSEC@MoDELS. Oct. 2008.

[15] Sung-hyuck Hong. "Analysis of Smart TV Hacking Threats and Countermeasures," Journal of Digital Convergence, 12(1), pp313-317, Jan. 2014

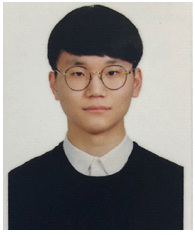
[16] Suk-jin Yoon and Jung-deok Kim, "A Study on the Analysis of Security Demands through Security Threat

Modeling of Home IoT Home Appliances." Korea Electronics Trade Journal, 24(2), pp113-124, May. 2019.
〔17〕 Pedro Carabrera, "SDR Against Smart TVs URL and Channel Injection Attacks," DEF CON Conference, 2019.
〔18〕 Min-su Park, "LG VS Samsung TV: Which is Better for Tracking You?," CODE BLUE Conference, 2017.
〔19〕 Jong-ho Lee, "Are You Watching TV Now?", Hack in Paris Conference, 2017.
〔20〕 Seung-ju Kim, "Developing a Protection Profile for Smart TV", ICCC Conference, 2014.
〔21〕 Seung-jin Lee, "Hacking, Surveilling and Deceiving Victims on Smart TV," Black Hat Conference, 2013.
〔22〕 Klockwork, "Threat Modeling for Secure Embedded Software," SECURITY INNOVATION & KLOCWORK, June. 2011.
〔23〕 Common Vulnerabilities and Exposures, "CVE-2019-5784"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5784
〔24〕 Common Vulnerabilities and Exposures, "CVE-2019-5782"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5782
〔25〕 Common Vulnerabilities and Exposures, "CVE-2019-5755"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5755
〔26〕 Common Vulnerabilities and Exposures, "CVE-2019-9871"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-CVE-2019-9871
〔27〕 Common Vulnerabilities and Exposures, "CVE-2018-16065"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16065
〔28〕 Common Vulnerabilities and Exposures, "CVE-2018-6143"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6143
〔29〕 Common Vulnerabilities and Exposures, "CVE-2018-6062"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6062
〔30〕 Common Vulnerabilities and Exposures, "CVE-2018-6065"〔Internet〕, https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6065

〈저자소개〉

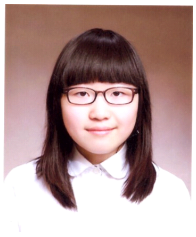
오 인 경 (In-Kyung Oh) 학생회원
2017년 3월~현재: 숙명여자대학교 컴퓨터과학과 학사과정
〈관심분야〉 정보보호, 보안 컨설팅, 모의해킹, 정보보안 교육, 시스템보안

서 재 완 (Jae-Wan Seo) 정회원
2019년 2월: 한신대학교 정보통신학부 졸업
〈관심분야〉 정보보호, 웹보안, 시스템보안, 네트워크보안

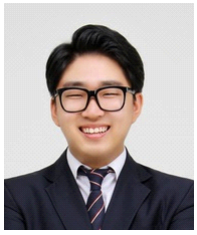


이 민 규 (Min-Kyu Lee) 학생회원
2018년 3월~현재: 인하대학교 컴퓨터공학과 학사과정
〈관심분야〉 정보보호, 시스템보안, 역공학, 웹보안, 네트워크보안

이 태 훈 (Tae-Hoon Lee) 학생회원
2014년 3월~현재: 경희대학교 산업경영공학과 학사과정
2020년 3월~현재: 라온 화이트햇 프로젝트팀
〈관심분야〉 정보보호, 보안컨설팅, 웹보안, 금융보안



한 유 나 (Yu-Na Han) 정회원
2019년 2월: 전북대학교 전자공학부, 컴퓨터공학부 졸업
〈관심분야〉 정보보호, 역공학, 시스템보안



박 의 성 (Ui-Seong Park) 정회원
2019년 08월: 목포대학교 정보보호학과 졸업
2017년 4월~현재: 라온 화이트햇 연구원
〈관심분야〉 웹/앱 보안, 모의해킹

지 한 별 (Han-Byeol Ji) 정회원
2019년 02월: 서울과학기술대학교 산업정보시스템공학과, 컴퓨터공학과 졸업
2017년 4월~현재: 라온 화이트햇 연구원
2019년 2월~현재: 교육부 미래교육위원회 교육위원
〈관심분야〉 보안컨설팅, 웹/앱 보안, 모의해킹

이 종 호 (Jong-Ho Lee) 정회원
2012년 4월~현재: 라온시큐어 핵심연구팀 팀장
2015년 02월: 인하대학교 컴퓨터공학과 졸업
2016년 07월~현재: KITRI Best of the Best 책임멘토
2019년 02월: 고려대학교 정보보호대학원 석사 졸업
2018년: 평창동계올림픽 정보보호전문위원회 기술전문위원
2018년: 육군 정보화기획참모부 사이버기술자문위원
〈관심분야〉 웹/앱 보안, 모의해킹

조 규 형(Kyuhyung Cho) 정회원
2001년 2월: 서울시립대학교 수학과 졸업
2003년 8월: 고려대학교 정보보호대학원 석사
2006년 8월: 고려대학교 정보보호대학원 박사 수료
2008년 8월~2009년 4월: 한국인터넷진흥원 위촉 연구원
2011년 8월~현재: KITRI Best of the Best 센터장
〈관심분야〉 네트워크 보안, CTF, 양자 컴퓨터, 정보보안 교육

김 경 곤 (Kyounggon Kim) 정회원
2008년 2월: 숭실대학교 컴퓨터공학과 졸업
2015년 2월: 고려대학교 정보보호대학원 석사
2019년 3월: 고려대학교 정보보호대학원 박사수료
2003년 8월~2006 2월: A3 시큐리티 컨설턴트
2006년 3월~2007 12월: SK 인포섹 시니어컨설턴트
2008년 1월~2011 12월: 삼일회계법인(Samil PwC) Manager
2011년 12월~2017 8월: 딜로이트 Senior Manager
2014년 7월~현재: KITRI Best of the Best 멘토
2016년 9월~현재: 고려대학교 정보보호대학원 산학협력중점교수
〈관심분야〉 보안컨설팅, 모의해킹, 정보보안 교육, 악성코드분석, 인공지능보안