ISSN(Print) : 1976-5304, ISSN(Online) : 2713-931X
https://kdfs.jams.or.kr, DOI : 10.22798/kdfs.2022.16.2.86

webOS 기반 스마트 TV 아티팩트 분석

송 경 식*, 임 재 혁*, 전 민 재*, 손 태 식**
아주대학교 사이버보안학과 (학부생)*, (교수)**

Artifact Analysis of smart TV based on webOS

Gyeongsik Song*, JaeHyeok Lim*, Minjae Jeon*, Taesik Son**
Dept. of Cybersecurity, Ajou University (Undergraduate Student)*, (Professor)**

요 약

IoT 기술의 발전에 따라 스마트 가전제품들의 사용 빈도도 늘어나고 있다. 특히 스마트TV의 경우 'COVID-19'의 영향으로 실내 활동이 증가함에 따라 그 수요 또한 높아지고 있다. 특히 '넷플릭스'와 같은 OTT (Over The Top media service) 서비스나 다양한 방송, 영상 서비스들을 TV로 이용하기 위해 많은 사람들이 스마트TV를 가정에서 사용하고 있다. 하지만 스마트TV의 수요량이 높아진 만큼 스마트TV를 대상으로 한 해킹 공격의 빈도수가 지속적으로 증가하고 있으며, 이 때문에 일반적인 가정 내의 스마트TV 또한 높은 보안성이 중요시되고 있다. 해당 논문에서는 webOS 기반의 스마트TV에서 수집 가능한 다양한 아티팩트들에 대해 분석, 연구하고, 수집 된 아티팩트들에 대한 디지털 포렌식 관점의 활용 방안에 대한 내용을 다룬다.

주제어 : webOS, 스마트TV, 포렌식, 아티팩트, 해킹

ABSTRACT

With the development of IoT technology, the frequency of use of smart home appliances is also increasing. In particular, in the case of smart TVs, demand for them is also increasing as indoor activities increase due to the influence of 'COVID-19'. In particular, many people use smart TVs at home to use OTT (Over The Top Media Service) services such as 'Netflix' or various broadcasting and video services as TVs. However, as the demand for smart TVs increases, the frequency of hacking attacks on smart TVs continues to increase, and for this reason, high security of smart TVs in general homes is also important. This paper analyzes and researches various artifacts that can be collected on webOS-based smart TVs, and deals with how to utilize the digital forensics perspective on the collected artifacts.

Key Words : webOS, SmartTV, Forensic, Artifacts, Hacking

Ⅰ. 서 론

스마트 TV는 인터넷에 연결되어 기존의 TV 기능뿐만 아니라 게임, 인터넷 검색, VOD(Video On demand)와 같은 다양한 서비스로 사용자에게 편의를 제공하는 TV이다[1]. 2021년 7월, 시장조사업체 "Strategy Analytics"에 의하면 5년 뒤인 2026년에는 전 세계 가구의 절반 이상이 스마트 TV를 보유할 것으로 예측하였다[2]. 수요가 증가함에 따라 전 세계에는 많은 스마트 TV 제조 벤더사가 존재한다.

하지만 스마트 TV에 탑재되는 OS는 극히 한정적이다. 대표적으로 삼성에서 개발한 '타이젠 OS', LG 전자가 인수하여 사용중인 'webOS', 구글 에서 개발한 'Android' 등이 있다.그 중 LG의 webOS는 OS 라이센스

▪ Received 06 May 2022, Revised 11 May 2022, Accepted 6 June 2022
▪ 제1저자(First Author) : Gyeongsik Song (Email : secretpack@ajou.ac.kr)
▪ 교신저자(Corresponding Author) : Taeshik Shon (Email : tsshon@ajou.ac.kr)

를 해외 TV제조 벤더사에 판매하고 있다. webOS는 2020년도 기준으로 전 세계 스마트 TV OS 점유율의 10.5%를 차지하고 있으며, 콩카, 에이온즈(호주) 아이와(일본) 등 해외 TV 제조업체 20여 곳에 판매를 진행하였다.[3]

위와 같이 스마트 TV 보급의 증가에 따라 스마트 TV의 보안에 대한 중요성은 갈수록 높아지고 있다. 특히 TV OS 라이센스를 판매하는 webOS의 경우 취약점이 발생할 경우 도청, 불법촬영으로 인한 사생활 침해 및 개인정보 유출의 측면뿐만 아니라 금전적 피해[4] 가 전 세계적으로 발생할 가능성이 있다. 이와 같은 침해사고가 발생하였을 때 포렌식 관점에서 webOS 스마트 TV는 주요 분석 대상이다.

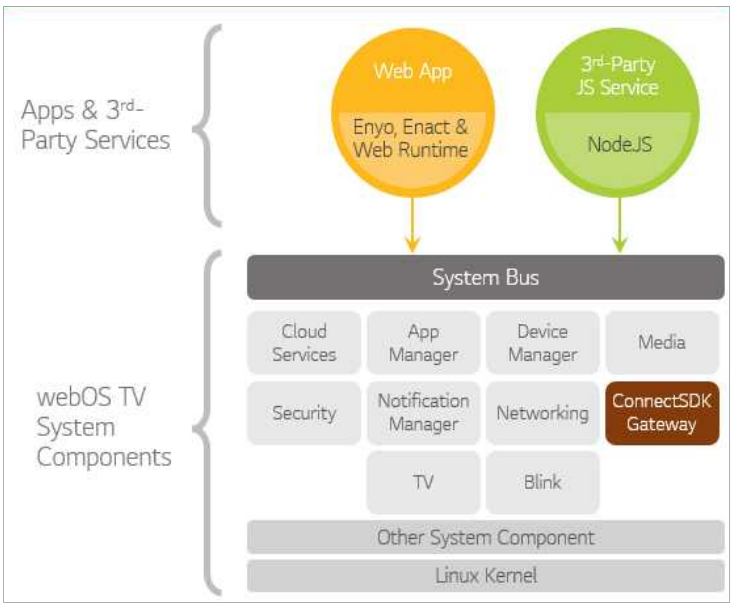
webOS 스마트 TV는 네트워크 연결 및 다양한 어플리케이션을 통해 실시간으로 데이터를 수집하여 저장한다. 수집된 데이터를 추출하여 분석하기 위해 먼저 TV의 관리자 권한을 획득할 필요가 있다. 따라서 TV에서 사용되는 webOS의 권한상승 취약점을 통해 스마트 TV OS의 관리자 권한을 획득한다. 이후 'scp' 명령어를 사용하여 스마트 TV가 수집한 데이터를 획득한다. 획득한 데이터를 분석하여 디지털 포렌식 관점에서 의미 있는 데이터를 선별한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구 대해 서술한다. 3장에서는 webOS 기반의 스마트 TV 포렌식을 위한 환경 구성 및 데이터 수집 방법을 설명한다. 4장에서는 두 개의 시나리오를 기반으로 데이터를 수집하고 유의미한 아티팩트를 분류한다. 끝으로 5장에서 논의와 6장에서 결론을 서술한다.

Ⅱ. 관련 연구

2.1 webOS

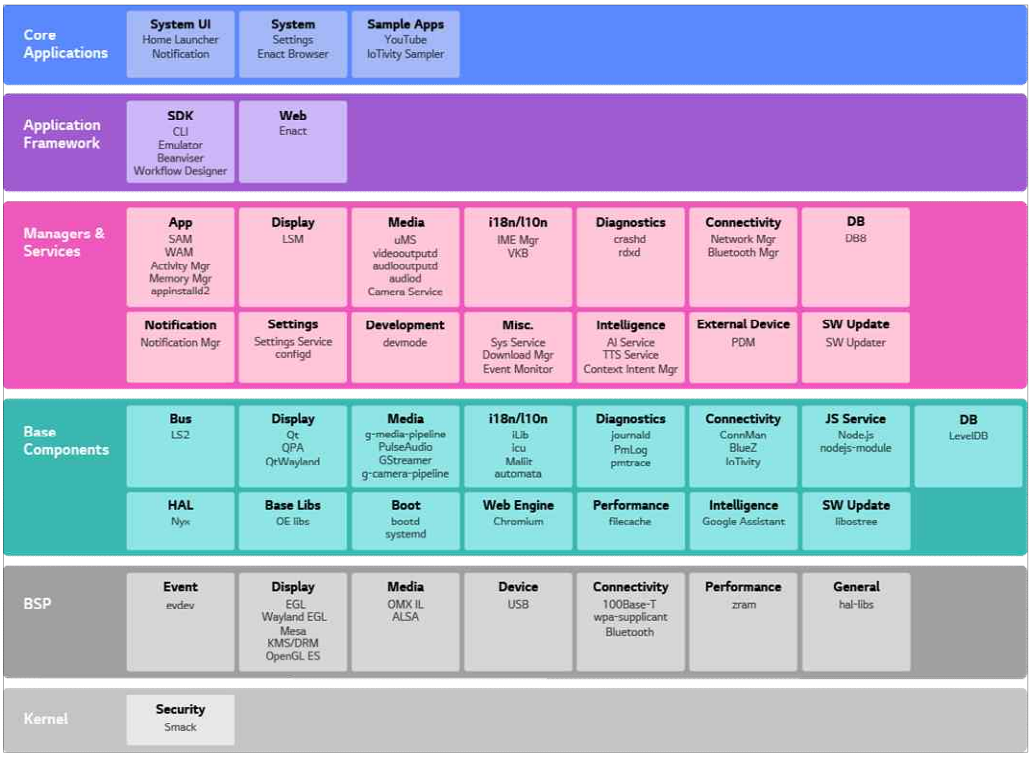
webOS는 Linux 기반 운영체제며 앱을 통해 미디어, 장치, 보안, 네트워킹, TV 기능 등을 관리 한다. webOS에서 사용되는 어플리케이션은 표준의 웹 앱과 매우 유사한 형태로, 'ipk' 확장자를 가지며, HTML(HyperText Markup Language) 및 CSS(Cascading Style Sheets), JavaScript 등과 같은 표준 웹 기술을 활용하여 webOS TV 전용 어플리케이션을 만들 수 있다. 이는 시스템 버스를 통해 webOS 자체적인 내장 컴포넌트들인 클라우드 서비스, App Manager, Device Manager, Device 등과 상호작용하며 이 모든 기반 구성요소들은 커널 위에서 관리된다. 안드로이드 운영체제가 자바로 개발된 모바일 어플리케이션을 동작하기 위해 필요한 컴포넌트들이 추가된 것처럼, webOS 또한 마찬가지로 web App을 구동하고 실행하는데 필요한 필수 컴포넌트들과 웹 브라우저와 같은 앱에서 사용하기 위한 컴포넌트들을 기본적으로 운영체제 내부에 내장하고 있다. 구조는 아래의 그림과 같다.



〈Figure 1〉 webOS TV Architecture[5]

webOS는 내부적으로 어플리케이션들에 대한 관리, UI 등에 대한 상호작용을 용이하게 하고 효율적으로 다루기 위해서 Core Applications, Application Framework, Managers & Services, Base Components, BSP(Board Support Package), Kernel 등과 같은 구체적인 레이어로 구성되어 있으며,

이에 대한 구성요소는 아래의 그림과 같다.



〈Figure 2〉 webOS System Architecture Layer[6]

webOS 는 보안적 요소보다, 신기술 및 기술 향상에 대한 연구가 많이 진행되었다. K.Jeon et al.[7]는 webOS 내에서 병렬처리 가능성에 대한 연구를 제시하였다. webOS Architecture를 분석하여 이에 대한 맞춤형 Profiling 방법을 고안하였으며 WebCore 분석 및 JavaScriptCore 분석을 진행하여 계산 자원을 보다 효율적으로 활용할 수 있는 방법을 제시하였다. J. Lim et al.[8]는 webOS Architecture 분석을 토대로 소프트웨어 설계와 실제 구현 단계에 도달했을 때 발생할 수 있는 차이에 대해 연구하였다. Y.Park et al.[9]는 webOS 환경에서 API Hooking 및 Memory 비교 분석 방법을 사용한 악성 어플리케이션 분석 자동화 방법을 제시하였다.

2.2 SMART TV 취약점

스마트 TV 위협 및 취약점에 관한 연구는 꾸준히 이루어지고 있다. Y. Wi et al.[10]은 국내 및 국외에서 생산된 스마트 TV의 동향과 스마트 TV 에서 발생 가능한 위협 및 이에 대한 대응 방안을 제시하였다. H. Kim et al.[11]은 삼성전자의 스마트 TV에 탑재된 펌웨어 구조 및 발생 가능한 위협 및 취약점을 제시하였다. H. Hong et al.[12]은 전반적인 스마트 TV에서 발생 가능한 해킹 위협 및 이에 대한 대응방안을 제시하였다. K. Oh et al. 2020[4]은 STRIDE 위협 모델링을 기반으로 한 스마트 TV의 전반적인 보안 요구사항에 대한 연구를 제시하였다.

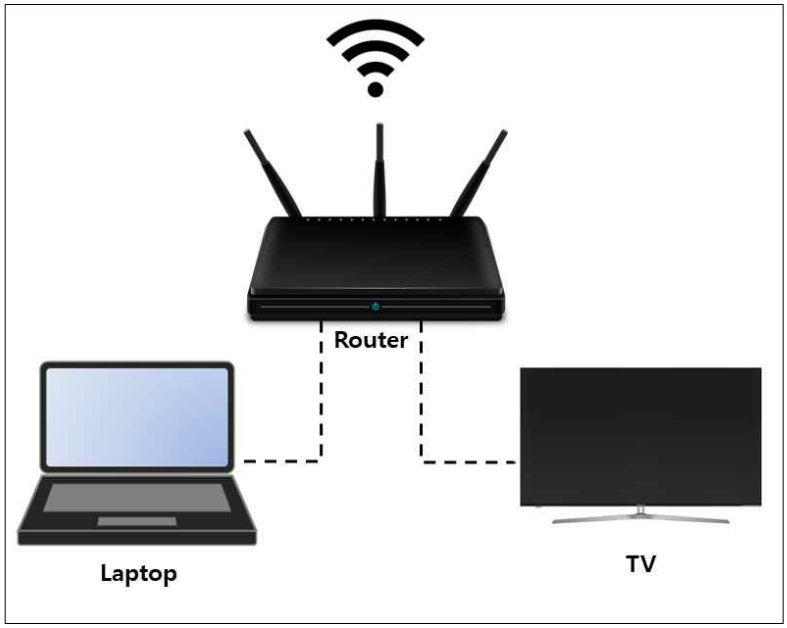
2.3 SMART TV 포렌식

스마트 TV 포렌식과 관련된 연구도 진행된 바 있다. T.Nemayire et al.[13]는 삼성전자 스마트 TV 에 대하여 Chip-off, 네트워크 등 데이터 획득에 대한 다양한 획득 기법에 대하여 제시하였다. S.Kang et al.[14]는 전반적인 스마트 TV 구조와 포렌식의 필요성과 절차를 제시하였으며, 실제 시판된 기기에 대한 분석 등을 통해 유효한 아티팩트의 종류 및 위치 등을 설명하였다. 직접적으로 스마트 TV에 대한 연구는 아니지만 J.Kim[15]에서 네트워크에 연결되는 IoT 장비들에 대한 포렌식의 필요성과 접근 방법에 대하여 제시하였으며, S.Ryu[16]는 IoT 환경에서 디지털 포렌식을 위한 데이터 분류 방법에 대해 제시하였다.

Ⅲ. webOS 기반 스마트 TV 포렌식 환경 구축

3.1 webOS 기반 스마트 TV 포렌식을 위한 환경 구축

스마트 TV는 어플리케이션을 통해 사용자에게 보다 나은 편의성을 제공하기 위해 사용자 정보를 수집한다. 수집되는 정보는 앱 마다 상이하나 ID, 패스워드, 위치정보, 검색 기록 등을 수집하며 수집하는 과정에서 TV의 저장 공간 내에 이를 저장한다. 따라서 스마트 TV의 펌웨어를 직접 획득하여 포렌식을 진행한다. 스마트 TV 포렌식을 진행하기 위해 스마트 TV와 공유기를 연결한 뒤 컴퓨터 혹은 노트북을 통해 TV에 접속 가능해야 한다. 따라서 아래의 그림과 같이 환경을 구성한다.



〈Figure 3〉 Testbed for smart TV firmware extract and analysis

스마트 TV포렌식을 위해 webOS를 사용하는 스마트 TV 기기를 선정하여 분석을 수행하였다. 연구에 사용된 기기는 〔Table. 1〕과 같다. 분석 환경은 Windows 10 PC 환경에서 진행하였으며 분석에 사용된 툴은 〔Table. 2〕와 같다.

〈Table 1〉 List of Device for Smart TV forensic

Device type	Manufacturer	Device	Communication	Remark
Smart TV	LG	LG-43UJ6260	LAN	webOS 6.0
Laptop	-	-	Wi-Fi	Windows 10

〈Table 2〉 List of tools for Smart TV forensic

Tool Name	Manufacturer	Usage	Remark
db browser for sqlite	Digital Ocean	db file analysis	freeware
HxD Editor	mh-nexus	Hex Editor	freeware
Powershell	Microsoft	using SSH	Windows only

3.2 webOS 기반 스마트 TV 포렌식을 위한 쉘 권한 획득

스마트 TV에 사용되는 OS는 제조사 별로 다르기 기기마다 데이터 수집 방법 또한 다르다. 그러므로 벤더사별 기기에 따른 데이터 획득 방법에 대한 연구가 진행되어야 한다. 스마트 TV의 데이터를 획득하는 방법으로 칩 오프(Chip-Off), 디버그포트 혹은 JTAG을 통한 접속, 권한상승을 통한 제어권 획득 방법 등이 있다.

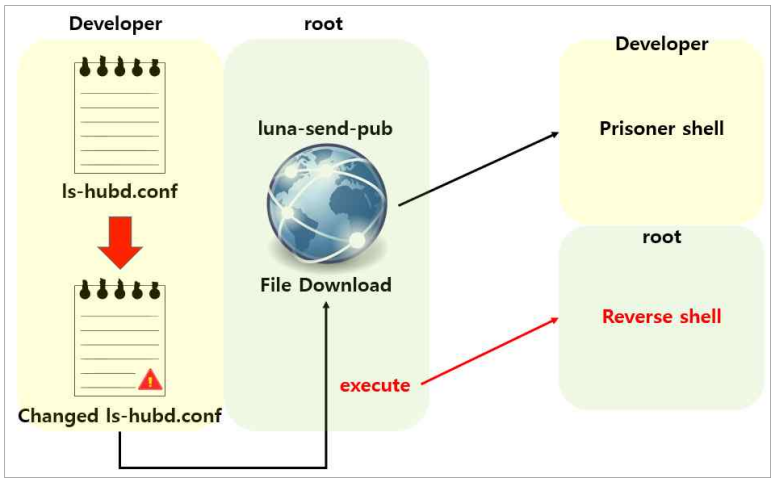
T.Nemayire et al.[13]은 타이젠 기반의 스마트 TV 포렌식 과정에서 칩 오프 방식을 사용하여 펌웨어를 획득하였다. 이는 성공 시 온전한 데이터를 얻을 수 있다는 장점이 있으나, 칩 오프 과정에서 칩 손상으로 인한 데이터 손상, 기기 손상의 위험성을 수반한다. 공식적으로 연구된 적은 없으나, 디버그포트 혹은 JTAG을 통한 접속 방법의 경우 역시 온전한 데이터를 얻을 수 있다는 장점이 있으나, 대부분의 기기들이 보안상의 이유로 디버그 포트나 JTAG 핀을 숨겨두거나 출시 단계에서 이를 제거하기 때문에 해당 방법을 채용하기 힘들다. 권한상승 취약점을 사용할 경우 최고 관리자 권한(ROOT) 으로의 권한 상승이 가능한 취약점이 존재해야 하고 공개된 취약점이 없다면 제로데이(0-DAY) 공격이 가능한 지점을 찾아야 한다. 성공 시 온전한 데이터를 얻을 수 있다. 스마트 TV의 데이터 획득 방법들에 대한 장단점은 아래와 같다.

〈Table 3〉 Pros and cons of data extract methods

데이터 획득 방법	Advantage	Weakness
칩 오프(Chip-Off)	온전한 데이터 추출 가능	칩손상으로 인한 데이터 손상, 기기 손상 가능성 존재
디버그포트, JTAG을 통한 접속	비교적 안전한 데이터 추출 가능	디버그 포트, JTAG 핀 등이 숨겨져 있어 분석이 어려움
권한상승 취약점 사용	데이터를 안전하게 추출 가능	1-DAY 공격이 불가능할 경우 0-Day 공격을 시도해야 함

본 논문에서 분석한 webOS는 공개된 권한상승 취약점이 존재하므로 이를 이용하여 데이터를 획득한다. 해당 취약점은 webOS에서 사용되는 API에서 발생되는 취약점으로 webOS가 탑재된 스마트 TV라면 벤더사와 상관없이 사용이 가능하다. 다만 취약점을 사용할 경우 별도의 포트포워딩 없이 ssh에 접속이 가능하므로 스마트 TV 취급에 주의해야 한다.

해당 취약점은 관리자(root) 권한으로 실행되는 파일에 대한 권한분리가 정상적으로 이루어지지 않아 발생하는 취약점이다. 권한 상승 과정은 아래의 그림과 같다.

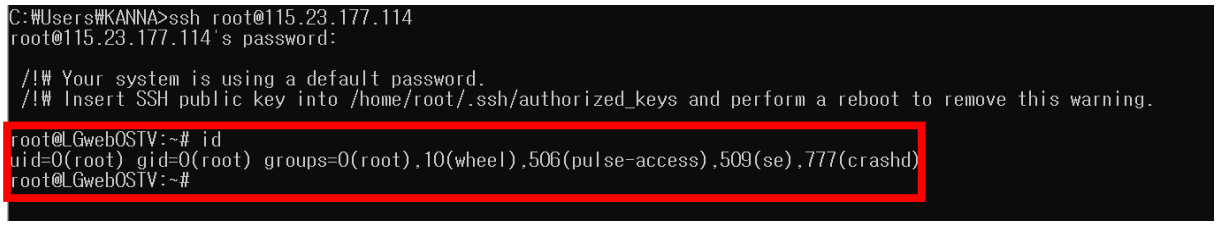


〈Figure 4〉 luna-send-pub vulnerability

webOS에서 사용하는 luna API 중 luna-send-pub 함수는 특정 파일을 다운로드 할 때 사용하는 함수이다. 해당 함수가 root 권한으로 실행되지만, 접근 권한에 대한 분리가 되어있지 않다. 따라서 개발자용 쉘에서 root 쉘로의 권한 상승이 가능하다.

〈Table 4〉 Exploit payload

```
luna-send-pub -n 1 -f luna://com.webos.service.downloadmanager/download '{"target":"http://192.168.1.107:8000/ls-hubd.conf","targetDir":"/etc/luna-service2","targetFilename":"ls-hubd.conf"}'
```



〈Figure 5〉 Obtain the root shell of the webOS smart TV

관리자 권한을 획득하였으므로 TV 내에 존재하는 모든 데이터에 대한 획득이 가능하다.

3.3 webOS 스마트TV 데이터 추출

관리자 권한이 존재하므로 Linux의 'scp' 명령어를 사용하여 데이터를 수집할 수 있다. 분석 대상의 저장용량이 많지 않으므로 디렉터리 별로 추출하거나 개별 추출한다. 예를들어 브라우저 히스토리 파일을 scp를 사용하여 가져올 때 아래와 같이 입력한다.

〈Table 5〉 Example Command of extract file using scp command

$ scp -r root@115.23.177.114:/mnt/lg/cmn_data/webbrowser/chrome/Default/Hostory /home/secretpack/Desktop/

Ⅳ. webOS 기반 스마트 TV 포렌식 수행

4.1 webOS 기반 스마트 TV 포렌식을 위한 시나리오

webOS 스마트 TV 포렌식을 수행하기 위해 해당 기기를 네트워크에 연결하고 기기를 등록하는 과정이 필요하다. 기기등록을 마치면 webOS의 다양한 기능과 어플리케이션 설치 및 실행이 가능하다. 따라서 webOS 스마트 TV 포렌식을 위한 데이터 수집을 위해 기기의 기능 및 특성을 고려하여 시나리오를 작성하였다. 시나리오는 〔Table. 5〕와 같다. 시나리오 1은 webOS 스마트 TV 의 인터넷 브라우저를 사용하여 인터넷 검색 및 특정 웹 페이지에 접속하는 것이며, 실제 스마트 TV에서 많이 사용되는 기능 중 하나이다. 시나리오 2는 스마트 TV를 이용하여 파일을 다운로드하거나 어플리케이션 설치 및 실행 등 스마트 TV에서 제공하는 서비스를 수행한다.

〈Table 6〉 Scenario list of using webOS smart TV that apply to the scenario

Scenario	Contents
Scenario 1	Internet Search and visit random web site.
Scenario 2	Download File and Application install & execute.

4.1.1 시나리오 1

시나리오 1은 webOS 기반 스마트 TV에서 기본적으로 제공하는 웹 브라우저를 사용하는 것이고, 해당 시나리오를 수행하기 위해 LG SMART TV LG-43UJ6260을 사용한다. 해당 기기는 지상파 공중파 방송 중계뿐만 아니라 webOS 라는 막강한 스마트 TV OS를 사용하여 사용자에게 웹 기반의 어플리케이션을 지원하여 다양한 서비스를 제공한다. 기본 브라우저로 Chrome 브라우저를 탑재하고 있다. 시나리오 1은 webOS 에 내장된 Chrome 브라우저를 사용하여 '아주대학교'를 검색하고 아주대학교 블랙보드 홈페이지에 접속하는 것이다. Linux 기반의 OS이므로 PC에서 수집 가능한 검색 기록, 웹 페이지 방문 기록, 사용자 정보, 위치 정보 등의 데이터를 획득할 수 있을 것으로 예상된다.

4.1.2 시나리오 2

시나리오 2는 webOS 기반 스마트 TV에서 특정 파일 다운로드 및 특정 어플리케이션 설치·실행을 하는 것

이며 해당 시나리오 수행을 위해 시나리오 1과 동일한 LG SMART TV LG-43UJ6260을 사용한다. 스마트 TV를 통해 웹 브라우저에 접속하거나 앱스토어 등에 접속하여 특정 파일 혹은 어플리케이션을 다운로드 받을 수 있다. webOS에서 특정 파일에 대한 다운로드를 진행할 때 luna API를 사용한다. 이 역시 Linux 기반의 OS 이므로 PC에서 수집 가능한 다운로드 파일 경로, 다운로드 url, 어플리케이션 다운로드 기록, 실행 기록, 실행 위치 정보, 사용자 정보 등의 데이터를 획득할 수 있을 것으로 예상된다.

4.2 시나리오 별 webOS 기반 스마트 TV 포렌식 수행 결과

webOS 기반 스마트 TV 포렌식을 수행하여 수집한 데이터에서 검색 기록, 사용자 위치정보, 기기연결 정보, 썸네일 등과 같은 기본 아티팩트 및 크리덴셜 아티팩트를 도출하였다. 획득한 주요 아티팩트는 아래의 〔Table. 6〕과 같다. 획득한 전체 아티팩트는 Appendix에 명시하였다.

4.2.1 시나리오 1

시나리오 1은 webOS 기반의 스마트 TV를 사용하여 인터넷 검색 및 특정 웹 사이트에 방문하는 것이다. 스마트 TV에서 시나리오 1을 수행한 결과 웹 브라우저에서 수집하는 데이터가 저장되는 db 파일을 획득하였고 해당 db 내에서 주요 아티팩트를 획득하였다. 〔Fig. 6〕은 webOS 기반 스마트 TV 내에 내장된 크롬 브라우저에서 수집된 아티팩트 중 사용자 검색 기록과 관련된 그림이다. 〔Fig. 7〕은 webOS 기반 스마트 TV의 브라우저 쿠키가 저장된 데이터베이스 파일이다. 일반적인 웹 브라우저에서 수집될 수 있는 포렌식 아티팩트들과 동일한 정보가 마찬가지로 수집되었으며 해당 아티팩트들을 통해서 사용자가 어느 웹 사이트를 이용하고 어떤 행위를 하였는지에 대한 정보를 수집할 수 있다.

	id	url	title	visit_count	typed_count	last_visit_time	hidden	favicon_id
		필터	필터	필터	필터	필터	필터	필터
1	1	https://rootmy.tv/	RootMyTV - Stage 1	1	1	13283077676650131	0	0
2	2	data:text/…		1	0	13283077677376654	0	0
3	3	http://ipconfig.com/		1	1	13283078060541962	0	0
4	4	http://ifconfig.kr/	ipconfig.kr,ipconfig.co.kr,ifconfig.kr	2	2	13283078641465461	0	0
5	5	http://youtube.com/	YouTube	1	1	13283105649227577	0	0
6	6	https://youtube.com/	YouTube	1	0	13283105649227577	0	0
7	7	https://www.youtube.com/	YouTube	1	0	13283105649227577	0	0
8	8	http://portal.ajou.ac.kr/		1	1	13283105701034630	0	0
9	9	https://mportal.ajou.ac.kr/		1	0	13283105722486035	0	0
10	10	https://mportal.ajou.ac.kr/index.do	아주대학교 포탈	1	0	13283105724865996	0	0
11	11	https://mportal.ajou.ac.kr/main.do	아주대학교 포탈	1	0	13283105724865996	0	0
12	12	http://eclass2.ajou.ac.kr/	Blackboard Learn	1	1	13283105811500992	0	0
13	13	https://eclass2.ajou.ac.kr/	Blackboard Learn	2	0	13283106402072852	0	0
14	14	https://www.daum.net/	Daum	1	1	13287588358945454	0	0
15	15	https://www.daum.net/	Daum	1	0	13287588358945454	0	0

〈Figure 6〉 webOS smart TV web Browser search history

	creation_utc	host_key	name	value	path	expires_utc	secure	httponly
	필터	필터	필터	필터	필터	필터	필터	필터
46	13298484749647475	mportal.ajou.ac.kr	JSESSIONID		/	0	0	0
47	13298484759983356	www.ajou.ac.kr	PHAROSVISITOR		/_attach/ajou/image/2022/04	0	0	1
48	13298484760552103	www.ajou.ac.kr	PHAROSVISITOR		/_attach/ajou/image/2022/05	0	0	1
49	13298484770040675	sso.ajou.ac.kr	JSESSIONID		/	0	0	0
50	13298484805282773	mportal.ajou.ac.kr	mportal		/	0	0	0
51	13298484805282979	.ajou.ac.kr	ssotoken		/	0	0	0
52	13298484854429945	gsl.ajou.ac.kr	JSESSIONID		/SmartSSO	0	0	1
53	13298484856603883	gsl.ajou.ac.kr	JSESSIONID		/	0	0	1

〈Figure 7〉 webOS smart TV web Browser cookie

4.2.2 시나리오 2

시나리오 2는 webOS 기반 스마트 TV에서 특정 파일 다운로드 및 특정 어플리케이션 설치·실행을 하는 것이다. 실행한 어플리케이션은 OTT 서비스를 제공하는 'netflix'와 'pooq', 그리고 동영상 공유 플랫폼인 'youtube'를 실행하였다. 스마트 TV에서 시나리오 2를 수행한 결과 파일 다운로드 기록 및 파일 다운로드 경

로, 어플리케이션 다운로드 경로 및 시간, 실행 시간, 구체적으로 어떤 행위를 수행했는지에 대한 아티팩트를 획득하였다. 〔Fig. 8〕은 특정 파일이나 어플리케이션을 다운로드 했을 때 이에 대한 정보를 저장하는 다운로드 히스토리 데이터베이스 파일이다. 이를 통해 다운로드 상태, 다운로드 경로 등을 추적할 수 있다. 〔Table. 9〕는 특정 어플리케이션을 실행했을 때 각 Manager나 Controller에서 App을 관리하면서 App에서 보낸 요청 정보에 대한 로그 기록을 남긴 결과물이다. 'netflix'나 'youtube.leanback.v4', 'com.webos.app.membership' 등 실제로 실행이 되었던 어플리케이션들에 대한 구체적인 실행 로그를 획득할 수 있으며, 이를 통해 사용자의 행위 분석이 가능하다. 또한 〔Table. 9〕는 해당 기기에 대한 부팅 시점을 확인할 수 있기 때문에, 해당 기기가 언제부터 사용되었고 언제 사용종료가 되었는지 그 시간 대역 또한 추정할 수 있는 포렌식 관점에서 유의미한 아티팩트로 활용될 수 있다.

	ticket	owner	interface	state	history
	필터	필터	필터	필터	필터
1	0	system-2	init	null	null
2	1	com.webos.appInstallService	wired	completed	{"destFile":"netflix.ipk","sourceUrl":"http://…
3	2	com.webos.appInstallService	wired	completed	{"destFile":"pooq.ipk","sourceUrl":"http://…
4	3	com.webos.appInstallService	wired	completed	{"destFile":"amazon.ipk","sourceUrl":"http://…
5	4	com.webos.appInstallService	wired	completed	{"destFile":"cj.eandm.ipk","sourceUrl":"http://…
6	5	com.webos.appInstallService	wired	completed	{"destFile":"channelplus.ipk","sourceUrl":"http…
7	6	com.webos.appInstallService	wired	completed	{"destFile":"com.frograms.watchaplay.webos…
8	7	com.webos.appInstallService	wired	completed	{"destFile":"com.disney.disneyplus-…
9	8	com.webos.appInstallService	wired	completed	{"destFile":"youtube.leanback.v4.ipk","source…
10	9	com.webos.app.facebooklogin	wired	completed	{"destFile":"start-…
11	10	com.webos.app.facebooklogin	wired	completed	{"destFile":"hbchannel.ipk","sourceUrl":"https:…

〈Figure 8〉 webOS smart TV download history database

〈Table 7〉 webOS Application boot log

DEBUG(12781.677149634) : Controller) 'com.webos.app.livetv' is foreground
DEBUG(12828.199562197) : Controller) 'org.webosbrew.hbchannel' is foreground
DEBUG(14577.096209323) : Controller) 'com.webos.app.browser' is foreground
DEBUG(14614.357653091) : Controller) 'com.webos.app.livetv' is foreground
DEBUG(14881.408166260) : Controller) 'com.webos.app.discovery' is foreground
DEBUG(14907.287135606) : Service) Handle-getBootStatus:Sender(netflix)/Subscribed(true)
DEBUG(14908.373719106) : Controller) 'netflix' is foreground
DEBUG(15304.055877628) : Controller) 'com.webos.app.browser' is foreground
DEBUG(15922.953138882) : Controller) 'com.webos.app.customersupport' is foreground
DEBUG(15929.269498426) : Controller) 'com.webos.app.browser' is foreground
DEBUG(15947.152114393) : Controller) 'com.webos.app.miracast' is foreground
DEBUG(16072.113650203) : Controller) 'com.webos.app.browser' is foreground
DEBUG(16216.704534105) : Service) Handle-getBootStatus:Sender(netflix)/Subscribed(true)
DEBUG(16217.912714105) : Controller) 'netflix' is foreground
DEBUG(19005.393947060) : Controller) 'com.webos.app.discovery' is foreground
DEBUG(19031.903784906) : Controller) 'youtube.leanback.v4' is foreground
DEBUG(19305.812473828) : Controller) 'netflix' is foreground
DEBUG(22519.068546985) : Controller) 'com.webos.app.membership' is foreground
DEBUG(22882.997776825) : Controller) 'netflix' is foreground

VI. 논 의

5.1 종합 결과 분석

이번 실험에서 webOS가 탑재된 스마트 TV에서 데이터를 수집하여 시나리오를 기반으로, 포렌식적으로 유효한 아티팩트들을 선별하였다. 스마트 TV로부터 데이터를 추출하하는 방법으로, 칩 오프, 디버그포트 혹은 JTAG을 이용한 방법, 권한상승 취약점을 이용한 방법 등이 존재하는데, webOS에서 사용되는 API에서 권한 상승이 가능한 취약점[17] 이 존재하고, 이를 이용하여 관리자 권한을 획득 한 뒤 'scp' 명령어를 사용하여 데이터 추출이 가능하였다. 두 개의 시나리오를 기반으로 하여 데이터를 수집하였으며. 시나리오 1은 스마트 TV의 브라우저를 사용하여 인터넷 검색을 수행하고, '아주대학교 Blackboard' 웹 사이트에 접속하는 것이다. 수집한 데이터를 분석한 결과 검색 기록, 세션 정보 등을 수집할 수 있었다. 시나리오 2는 webOS 기반의 스마트 TV를 이용하여 특정 파일을 다운로드하고 어플리케이션 다운로드 및 실행을 하는 것이다. 실행한 어플리케이션은 OTT 서비스를 제공하는 'netflix', 'pooq'과 동영상 공유 플랫폼인 'youtube' 이다. 분석 결과 파일 다운로드 기록 및 경로, 어플리케이션 다운로드 경로, 실행 일시, 어플리케이션이 어떤 행동을 수행하였는지에 대한 아티팩트를 수집할 수 있었다. 또한 해당 기록을 통해 TV가 언제 켜고 꺼졌는지에 대한 정보 또한 확인할 수 있었다.

5.2 데이터 획득 방법에 대한 한계와 의의 및 추후연구방향

권한상승 취약점을 이용한 데이터 획득 방법의 경우 스마트 TV에서 사용되는 컴포넌트, 혹은 모듈에 대하여 권한 상승 취약점이 선행으로 연구되어야 한다. 그리고 이러한 취약점을 방지하기 위해 안티 리버스 엔지니어링(Anti Reverse Engineering) 코드를 탑재하거나, 난독화를 이용하여 프로그램 코드를 분석하기 어렵게 하는 등 취약점을 찾기 어려워지고 있다. 따라서 스마트 TV의 데이터를 획득할 수 있는 방법에 대한 연구가 필요하다.

첫 번째로 J.Kim et al.[15]의 연구와 같이 네트워크 패킷을 통한 데이터 수집 방법이 있다. 스마트 TV와 앱, 서버 간 네트워크 패킷을 수집하여 이를 분석하고 포렌식 적으로 의미 있는 데이터를 추출할 수 있을 것으로 생각된다. 두 번째로 메모리에 저장되는 아티팩드 등을 수집하는 방법이 있다. 이는 실제 TV에서 특정 서비스가 실행될 때 메모리에 저장되는 정보를 분석하여 포렌식적으로 유효한 데이터를 추출할 수 있을 것으로 생각된다. 세 번째로 부채널 공격을 이용한 방법이 있다. 칩 오프를 사용하는 방법이 아닌 규격에 맞는 핀을 개발하여 이를 바탕으로 내부의 바이너리정보를 읽어 데이터를 획득할 수 있을 것으로 생각된다.

결과적으로 권한상승 취약점을 이용한 데이터 획득은 취약저이 존재해야만 사용 가능하므로 매우 한정적이지만 공개된 1-Day 취약점이 존재할 경우 가장 빠르게 시도할 수 있으며 가장 안정적으로 데이터를 획득할 수 있다. 다만 위에서 언급했던 바와 같이 스마트 TV에서 침해사고가 발생할 경우 데이터를 수집할 수 있는 다양한 획득 방법에 대한 연구가 필요하다.

VII. 결 론

본 논문에서는 webOS 기반의 스마트 TV에서 수집 가능한 아티팩트 들을 분석하였다. 스마트TV에서 제공하는 기능이 다양하므로 두 가지 시나리오를 작성하여 데이터를 수집하였다. 데이터 수집 방법으로 권한상승 취약점을 사용하여 관리자 권한을 획득하여 파일에 접근하는 방법을 사용하였다. 수집된 아티팩트를 분석하여 브라우저 검색 기록, 방문 페이지, 파일 다운로드 흔적 및 경로, 어플리케이션 설치 및 실행시간, TV 부팅 정보 등의 아티팩트를 수집하였다. 부가적으로 시스템 아티팩트와 사용자의 상호작용으로 발생할 수 있는 흔적이 기록된 아티팩트로 나누어 webOS 스마트 TV에서 수집 가능한 아티팩트들을 도출하였다. 향후 네트워크 및 메모리에 저장된 민감 정보 및 중요한 증거 자료로 활용될 수 있는 아티팩트들에 대한 존재 여부에 대한 연구가 필요하다.

Appendix

〈Table 8〉 webOS based SMART TV System Artifact

Artifact	File Type	Path	Description
Bash history	Text	/home/root/.bash_history	Bash history
Host Name	Text	/etc/hostname	TV Network host name
Access log	Text	/mnt/lg/cmn_data/var/log/wtmp	Access log

〈Table 9〉 webOS based SMART TV Location Artifact

Artifact	File Type	Path	Description
Country	json	/mnt/lg/cache/sdp/sdx/eula.json	Location Artifact (Country)
	Text	/mnt/lg/cmn_data/acr/data/service_country	Location Artifact (Country)
	Text	/mnt/lg/cmn_data/admanager/tmpData/baseInfo.tmp	Location Artifact (Server)
	Text	/mnt/lg/cmn_data/dmostCountry	Location Artifact (Country)
	Text	/mnt/lg/cmn_data/irdbmanager/country.conf	Location Artifact (Country)
	Text	/mnt/lg/cmn_data/var/btsvc/locale.conf	Location Artifact (Bluetooth)
	Text	/mnt/lg/cmn_data/var/log/tvconfig-gen.log	Location Artifact (TV Setup)
	Text	/mnt/lg/cmn_data/var/luna/preferences/localeInfo	Location Artifact (Country)
User Address	Database	/mnt/lg/cmn_data/epg/db/PBS_DB_0_4.db	User Location Artifact (Address)
Location Time	Text	/mnt/lg/cmn_data/var/luna/preferences/localtime	Location Artifact (Time)

〈Table 10〉 webOS based SMART TV User Artifact

Artifact	File Type	Path	Description
Cookie	Text	/mnt/lg/cache/webbrowser/chrome/SafeBrowsingCookies	Safe Browser Cookie
Bluetooth	Text	/mnt/lg/cmn_data/btsvc/pairing_history	Bluetooth pairing device information
	Text	/mnt/lg/cmn_data/var/btsvc/bleRemoteDb	Remote Bluetooth pairing device information
Application	Text	/mnt/lg/cmn_data/var/log/bootd.log	Application log
Download	Database	/mnt/lg/cmn_data/var/luna/data/downloadhistory.db	File download log with url
Download	File	/media/internal/downloads	Download file path
Bookmark	Text	/mnt/lg/cmn_data/webbrowser/chrome/Default/Bookmarks	Web browser Bookmark
	Text	/mnt/lg/cmn_data/webbrowser/chrome/Default/Cookies	Browser Cookie
Favicons	Text	/mnt/lg/cmn_data/webbrowser/chrome/Default/Favicons	Favicons
Web Access	Text	/mnt/lg/cmn_data/webbrowser/chrome/Default/History	Web page access log
Web Data	Text	/mnt/lg/cmn_data/webbrowser/chrome_Default/web Data	Web data
Event	Text	/mnt/lg/cmn_data/var/log/messages	Event log

참 고 문 헌 (References)

[1] KISA, "Smart TV Market Trend Analysis." Jan. 2013.

[2] Strategy Analysis, "Global Smart TV Household Ownership to Exceed 50% by 2026", Available: https://news.strategyanalytics.com/press-releases/press-release-details/2021/Strategy-Analytics-Global-Smart-TV-Household-Ownership-to-Exceed-50-by-2026/default.aspx, 2022.04.15. confirmed

[3] The JoonAng, " LG전자 TV 플랫폼 시장 출사표 "'스마트 TV계의 MS'가 되겠다는 시도" ", 2022-05-10. confirmed

[4] I.K. Oh et al. "Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling", Journal of The Korea Institute of Information Security & Cryptology, VOL 30, No.2, pp. 213-229, 2020

[5] webOS TV Developer, "webOS TV Under the Hood" Available: https://webostv.developer.lge.com/discover/overview/discover-webos-tv, 2022.04.15. confirmed

[6] webOS Open Source Edition, "Architeture Overview", Available: https://www.webososе.org/docs/guides/core-topics/architecture/architecture-overview, 2022.05.10. confirmed

[7] Y.K. Jeon, "An Applicability Study on Parallel Computing for webOS-based Smart TV", Proceedings of the Korea Information Processing Society Conference, 2014.11a, Issue 101, pp.336-339, 2014

[8] B.J. Lim et al, "A Study on the Difference between Software Design and Implementation through webOS Analysis", Proceedings of Korea Software Congress 2018, pp.459-461, 2018

[9] J.Y. Park, "Automated Analysis of Malicious Application in WebOS", Proceedings of Korea Institutes of Information Security and Cryptology Conference, Vol.27, No.2, pp.226-229, 2017

[10] Y.K. Wi, "Analysis of Smart TV Trends and Security Vulnerabilities to Use in the Smartwork", Journal of Korea Multimedia Society Vol 15, Issue 1, pp.76-79, 2012

[11] J.H. Kim et al, "Smart TV structure & vulnerability trend analysis", Proceedings of the Korea Information Processing Society Conference Vol.21, Issue 1, pp.426-428, 2014

[12] S.H. Hong "Hacking and Countermeasure on Smart TV", Journal of Digital Convergence Volume 12 Issue 1, pp.313-317, 2013.

[13] Terrence Nemayire et al, "A 2018 Samsung Smart TV Data Acquisition Method Analysis", Journal of Digital Forensics Vol 13, No.3, pp.205-218, 2018

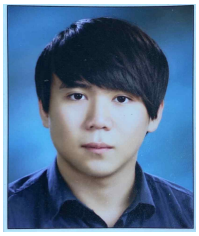
[14] H.S. Kang, "Study on Smart TV Forensics", Journal of the Korea Institute of Information Security & Cryptology Vol. 24, Issue 5, pp.851-860, 2014

[15] M.J. Kim, "Research on Network-based Smart Home Device Forensic Technology", Journal of Digital Forensics Vol. 15, Issue 4, pp.84-94, 2021

[16] H.S. Ryu "A Study on Data Classification for Digital Forensic in IoT", Proceedings of the Korea Information Processing Society Conference Vol. 22, No. 2, pp.705-707, 2015

[17] kapodamy, "RootMyTV", Available: https://github.com/RootMyTV/RootMyTV.github.io, 2022.05.10. confirmed

저 자 소 개



송 경 식 (Gyeongsik Song)
준회원

2019년 ~ 현재 : 아주대학교 소프트웨어융합대학 사이버보안학과 학사과정
2019년 ~ 현재 : 아주대학교 정보통신대학 전자공학과 학사과정
관심분야 : ICS/SCADA Security, IoT Security, Side-Channel Security

임 재 혁 (Jaehyuk Lim)
준회원

2017년 ~ 현재 : 아주대학교 소프트웨어융합대학 사이버보안학과 학사과정
관심분야 : Reverse Engineering, Malware Analysis, Artificial Intelligence

전 민 재 (Minjae Jeon)
준회원

2017년 ~ 현재 : 아주대학교 소프트웨어융합대학 사이버보안학과 학사과정
관심분야 : Fuzzing, Reverse Engineering, Financial Security

손 태 식 (Taeshik Shon)
평생회원

2000년 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 : 고려대학교 정보보호대학원 졸업(박사)
2004년 ~2005년 : University of Minnesota 방문연구원
2005년 ~2011년 : 삼성전자 통신· DMC 연구소 책임연구원
2017년 ~2018년 : Illinois Institute of Technology 방문교수
2011년 ~ 현재 : 아주대학교 정보통신대학 사이버보안학과 교수
관심분야 : Digital Forensics, ICS/Automotive Security