http://dx.doi.org/10.14400/JDPM.2014.12.1.313

스마트 TV 해킹 위협 및 대응방안 분석

홍성혁*
백석대학교, 정보통신학부

Hacking and Countermeasure on Smart TV

Sunghyuck Hong*
Baekseok University, Division of Information and Communication

요 약 스마트폰, PC나 태블릿과 같은 스마트 단말 플랫폼들이 대중들에게 확산되면서, 스마트 TV역시 이 추세에 편승하려고 한다. 시장 규모도 신속히 커지고 있다. 대한민국 스마트 TV 시장은 전 세계적으로 높은 보급률을 가지고 있는 반면, 그 만큼 보안요소와 해킹 위험 요소가 따르고 있다. 본 논문은 여러 가지 스마트 TV의 해킹 사례와 공격 가능성을 제시하여 취약점 분석 및 대응 방안에 대해 분석하였다. 삼성전자나, LG등 대부분 스마트 TV의 운영체제가 리눅스 기반으로 최근 해킹 사례도 리눅스 해킹 기법과 유사하다. 대부분 리눅스 OS를 기반으로 샌드박스를 탑재해 보안을 강화 했지만 프록시를 이용해 우회기법을 사용하거나 APT 공격이나 역공학으로 완성된 앱을 소스코드로 변환해 악성코드를 삽입 후 앱 스토어에 등록하는 등 현재 해킹 사례는 늘어가고 있다. 그리고 앞으로 새로운 해킹 기법과 다양한 방법들이 생길 것이다. 본 논문으로 발전해나가는 스마트 TV의 보안 위협을 인지하고 앞으로 새로운 해킹으로 인한 대비책을 세우고 준비하는 효과를 기대한다.

주제어 : 스마트 TV, 해킹, 분석, ATP 공격, 센드-박스, 프록시, 리패키징

Abstract Smart-phone, PC or tablet platforms, such as smart terminals spread to the masses trying to capitalize. Smart TV also is increasing. In Korea, market size of TV is growing fast with growth of risk of hacking. In this paper, several kinds of Smart TV hacking cases are presented with the possibility of attacks against the vulnerability analysis and countermeasures. Most of the Linux operating system is open. Thus, it is vulnerable for latest hacking techniques. Most are based on the Linux OS to enhance security mount Sand-Box. However, bypass procedure using the technique, or APT attacks can avoid San-Box technique. New hacking techniques and a variety of ways will occur in the future. Therefore, this paper will develop Smart TV, and it analysis of a security threat and establishes better prepared in the future because new hacking attacks are expected to prepare more.

Key Words : Smart TV, Hacking, Analysis, ATP Attack, Send-Box, proxy, Repackaging

1. 서론

현재 사용 중인 스마트 TV 앱은 수신기에 전달되고 실행된다. 위성, IPTV, 지상파, 케이블 등등 다양한 방송 매체에서 방송 사 업자는 특정한 앱의 실행을 명령하는 시그널을 방송 신호와 함께 송출할 수 있으며, 이를 전달받은 수신기는 해당 앱이다. 스마트TV도 해킹 대책 마련이 시급하다는 지적을 받고 있다. 스마트TV 역시 스마트폰과 마찬가지로 해킹 사고가 발생할 수도 있는 만큼 보안 필요하다.

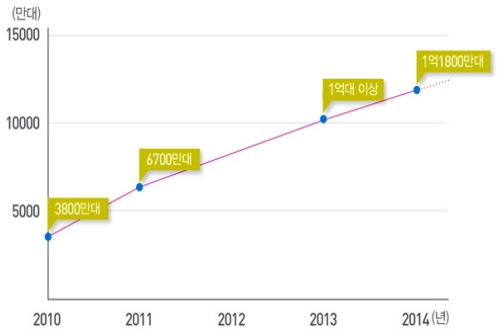
Received 15 October 2013, Revised 17 December 2013
Accepted 20 January 2014
Corresponding Author: Sunghyuck Hong(Baekseok University)
Email: shong@bu.ac.kr

ISSN: 1738-1916

스마트TV는 아직까지는 스마트폰에 비해 보급율이나 성능이 낮은 것으로 평가돼 실질적인 보안 위협은 그리 높지 않은 것으로 생각하고 있으나 TV 보급이 확산되는 만큼 앞으로의 위협은 안심하기 어렵다는 설명이다.

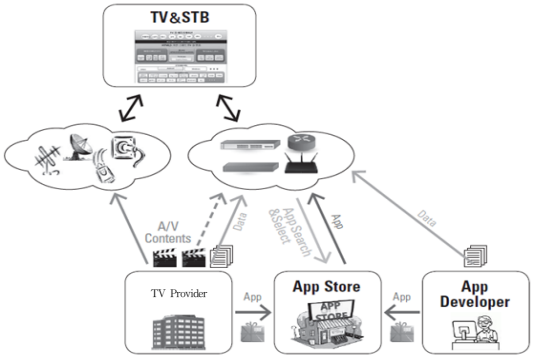
시장조사업체 가트너·디스플레이서치에 따르면 스마트TV는 지난해 세계 시장에서 6천 900만대가 팔렸고 올해 1억 800만대 판매가 예상된다. 2016년에는 그 두 배에 육박하는 1억 9천 800만대가 팔릴 것으로 점쳐지고 있다.

스마트TV도 스마트폰 만큼 해킹 위협에서 자유롭지 못하다는 근거는 밝혀지는 상태이다 [1]. Fig. 1 참조.



[Fig. 1] 스마트TV sales forecast worldwide

지난 3월 캐나다에서 열린 해킹 콘퍼런스 '캔섹웨스트(CanSecWest)'에서 고려대학교 사이버 국방학과 소속 이승진(29)씨는 스마트 TV를 해킹해 시청자의 사생활을 몰래 촬영한 뒤 이를 인터넷으로 생중계했다. 이론상으로 가능하다고 여겨진 스마트 가전기기의 해킹이 현실로 드러난 것이다. 심지어 전원이 꺼진 상태에서도 도촬이 가능했다 [1].



[Fig. 2] Overview of 스마트TV services

한 걸음 더 나아가 스마트TV로 인한 '티비싱(Tvishing)'은큰 위협이 되고 있다. 티비싱은 텔레비전(TV)와 피싱(Phishing)의 합성어다. 해커가 스마트TV가 원하는 해적방송을 내보낼 수 있고 이것을 통해 홈쇼핑 등 녹화된 화면을 띄운 다음 자동주문번호를 자신의 번호로 바꿔치기 해서 피해를 일으킬 수 있다[1].

스마트TV 해킹이 위험한 이유는 기본적으로 스마트TV도 스마트폰과 동일하게 PC에서 발생할 수 있는 해킹은 거의 다 가능하다. 우선 스마트TV의 경우 위치상 도청과 도촬에 더 유리하다. 스마트폰 역시 같은 위협이 존재하지만 스마트폰이 주로 주머니나 가방 속에 있거나 꺼내져 있을 때도 카메라의 위치가 천장을 향할 가능성이 커 상대적으로 위협이 작을 수 있다[1]. 따라서 본 연구에서는 스마트 TV의 취약점을 분석하고 이에 대한 대응책을 제시함으로써 보안에 대한 인식 제고를 위하여 연구하였다.

본 논문에서는 스마트TV의 구조 설계도를 분석하였고, 2장에서는 그에 따른 취약점 분석 및 원리로 모바일에서 해킹 관련된 공격 사례를 제시하였다. 3장에서는 피해 완화와 여러 가지 방법에 대한 대안을 제시를 하였다.

2. 스마트TV 구조 및 취약점

2.1 표준 개요

Fig. 1 은 스마트TV 오버비유이다. URL로 인터넷 망에서 접속하여 앱을 다운을 받고 실행하게 된다. 또한, 일반 개발자는 자신이 개발한 앱을 앱 스토어에 배포하여 유통할 수 있으며, 사용자는 앱 스토어에서 원하는 앱을 선택하고 설치하 여 실행할 수 있다. 수신기는 브라우저 기반의 실행 환경을 통해서 운영체제에 독립적으로 스마트 TV 플랫폼을 구동시킬 수 있다. 그리고 표준에 의해 웹 코어의 기능을 확장하고 TV디바이스와 애플리케이션을 관리하는 모듈을 제공해 HTML5 기반으로 개발된 다양한 스마트 TV 앱을 수신기 측에서 실행할 수 있는 환경을 구현하게 된다[2].

2.2 기업별 OS 비고 및 취약점 분석

Table 1의 표와 같이 LG전자 스마트TV는 리눅스 기반의 'NetCast 플랫폼'을 제공한다. NetCast 플랫폼은 임

베디드 환경에서 풀 브라우징을 가능하게 해주는 웹킷(WebKit) 기반의 'LG 브라우저'를 웹브라우저 엔진으로 사용한다. 앞서 말한 대로 LG전자 스마트TV SDK는 HTML5를 지원하는데 A/V, Canvas, Offline Storage DB, Document Editing, 드래그 앤 드롭 기능을 지원하고 있다. 또한 스마트TV '운영체제' 3강구도로 가나 삼성전자와・LG에서, 운영체제 신경전이 치열해진 가운데 기초는 리눅스 기반으로 공통점으로 시장방향을 지었다. 구글 안드로이드・애플 iOS로 TV시장은 본격 진출하였고, 스마트 TV에서의 운영체제는 보안성이 연계되는 리눅스를 선택하였다고 한다.

하지만 완벽한 운영체제가 존재 하지 않는 듯이, 실제 그에 따른 시연도 이루어졌다. 공격자가 공격자 서버에 미리 공격 웹페이지를 생성한 후, A씨의 스마트TV에 공격 웹페이지 URL이 전달되고 웹페이지를 클릭하는 순간, A씨의 스마트TV는 공격자가 장악하게 된다. 공격자는 탈옥이나 루팅을 통해 관리자 권한을 획득하고 커널에 악성코드를 설치하게 된다[4].

이렇게 되면 심각한 문제가 발생한다. 커널에 악성코드가 설치되면, 원격 공격자는 접속하고 싶을 때 문자를 보내 공격 사이트에 접속하게 만들 수도 있고 사용자 내장 메모리 카드를 원격에서 가져올 수도 있다. 폰 내부의 모든 개인정보를 훔쳐올 수 있는 것이다. 물론 음성 도청도 가능하고 커널에서 실행되기 때문에 공격을 분석할 방법이 없다. 누가 공격하고 있는지를 모르게 되는 것이다.

〈Table 1〉 Compare 스마트TV OS platforms

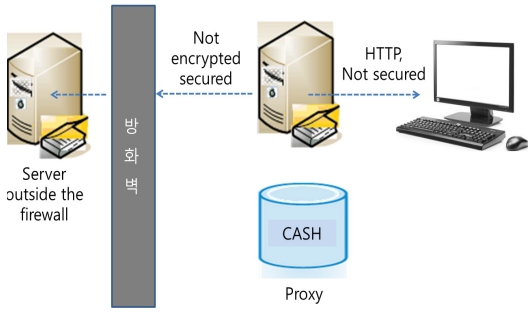
Compare specifications	Samsung TV	LG TV	Google TV	Apple TV	Tizen
Manufacturer	Samsung Electronics	LG Electronics	Samsung&LG under-developing	Apple	Linux, Intel, Samsung etc..
OS & S/W	Self-OS Macle Rash Player	Self-OS Netcast 2.0	Android Google crome	IOS(Undecided) ITunes I-Cloud Sri	Multi-platform Linux-based(under-developing)
Release Date	February 2010	January 2011	October 2010	2013 undefined	2012 undefined
Use Product	스마트TV	스마트TV	스마트TV Smart Phone Tablet PC	Apple TV iphone ipad	스마트TV Smart phone Tablet PC

더 나아가 현재의 스마트폰 백신들로는 전혀 탐지가 안되며 네트워크 상태 정보도 숨김이 가능하다. 또 그런 방식으로 수많은 스마트 좀비 TV를 만든 후 DDoS 공격을 감행할 수도 있고 이럴 경우 CNC 커넥션도 숨기고 공격 트래픽도 숨길 수 있다고 한다. 그 결과 피해자 스마트TV는 디도스 공격을 받게 되고 받은 사이트는 어디서 공격을 받은 지도 모른 채 다운된다는 것이다[5].

이 취약점은 안드로이드만의 문제가 아니다. 안드로이드는 기본적으로 리눅스 OS를 탑재하고 있기 때문에 기존 리눅스에 존재하는 잠재적인 보안 취약점을 그대로 내포하고 있다. 지난해 안드로이드 커널에서 보안상 문제점을 일으킬 수 있는 88개의 심각한 취약점들이 해외에서 발표됐다. 그리고 아이폰에 탑재된 IOS 역시 안드로이드와 비슷한 종류의 취약점을 내포하여, 특정 스마트TV 플랫폼의 문제라고 볼 수는 없는 상황이다 [5].

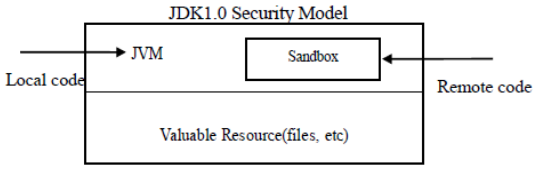
3. 제안하는 스마트 TV 공격 해결책

스마트 TV공격을 막기 위해 샌드박스를 통한 보안대책을 제안한다. 프록시 서버는 사용자가 자신을 통해 간접적으로 다른 네트워크 서비스(사이트접속) 를 사용할 수 있게 해주는 컴퓨터나 소프트웨어를 말한다. 프록시 서버와는 개념이 다른 프록시에 어떠한 데이터를 가지고 올 때 그 데이터가 저장되어있는 사이트에 들르지 않고 임시저장소애 들러서 가지고 오는 것. 이와 같은 방식으로 샌드박스를 우회하는 방법은 자신이 서버를 php를 이용해 proxy 서버로 셋팅하여 요청하는 것이다. 그러나 가상 proxy 스크립트를 짜놓고 돌리면 도메인을 자기 도메인으로 먹기에 보안에러를 속일 수 있는 것이다. 즉, 지름길을 놔두고 먼길로 돌아가는 (우회하는)방법이다. 직접 타 서버에 있는 것을 엑세스하는 것이 아니라 php를 통해 그 페이지를 요청하고, 이것이 통째로 자신의 서버로 불러진 다음 그것을 읽는 방식이므로 2배의 트래픽이 발생한다는 단점이 있다. 이렇게 하면 응답속도가 약간 늦더라도 모든 보안제약에서 해방될 수 있다. 이를 막기 위한 해결책은 포트 번호를 막아 접근 자체를 막는 대안이 있다. 그러므로 우회 공격을 막을 수 있다 [6].



[Fig. 3] The principle of a proxy structure

샌드박스는 놀이터와 같다고 해서 붙여진 이름인데, 앱서핑이나 P2P에서 다운로드한 프로그램 등 신뢰할 수 없는 어플리케이션을 가상머신 내에서 실행하게 된다. 그래서 바깥에 존재하는 중요한 문서 및 OS를 보호하는 역할을 한다. 샌드박스(Send-Box)에서는 악성행위를 하지 못하도록 하는 안티디버깅(Anti-Debugging) 등의 기능이 포함된 더비다 패커(themida packer)라는 팩킹 기술을 활용해 분석과 악성 코드 탐지를 하면 스마트TV위험에서 보호가 가능하며, 샌드박스 기본 구조는 아래 Fig. 4에 나타나 있다. 샌드박스(sandbox)는 외부로부터 들어온 프로그램이 보호된 영역에서 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태이며, 자바(Java)가 지원하는 기본 보안 소프트웨어로 JDK(Java development kit:자바개발도구)1.0부터 제공되고 있다. 외부에서 받은 프로그램을 JVM(Java Virtual Machine)이라는 보호된 영역 안에 가둔 뒤 작동시키는 방법으로 프로그램이 폭주하거나 악성 바이러스의 침투를 막는다. JAVA가 제공하는 샌드박스는 네트워크를 통해 전송받은 애플릿의 시스템 자원에 대한 접근을 제한한다. 샌드박스에서 접근을 허용한 애플릿은 작업이 가능하지만 그렇지 않은 경우는 로컬파일을 읽거나 바꿀 수 없게 하는 방법으로 시스템의 피해를 방지한다. 그리고 샌드박스는 클래스 로더(class loader), 바이트코드 검사기(bytecode verifier), 보안관리자(security manager)의 콤포넌트로 구성된다. 각 콤포넌트는 시스템의 신뢰성을 유지하는 역할을 하기 때문에 스마트 TV에 적용하면 지금까지 드러난 취약점을 막을 수 있을 것으로 기대한다.



[Fig. 4] The principle of the sandbox structure

4. 결론

스마트 TV도 네트워킹을 통해서 데이터를 주고 받고 pay-per-view를 통한 결재도 이루어지고 있어서 해킹으로부터 노출되어 있으며, PC나 스마트 폰에 비하여 안전에 대한 인식자체가 부족하여 통신 시 샌드박스를 이용하여 안전한 스마트 TV를 제안하였다.

본 논문에서는 스마트 TV의 구조와 OS에 대해 알아보고 시장성의 수요성이 급증함에 따라 그 만큼 보안문제에 적색 신호가 되었다. 아직 알려지지 않는 탐지기법이나 새로운 해킹 기법과 툴들이 무궁무진하다.

대부분 리눅스의 기반을 둔 OS에도 스마트폰 해킹사례와 비슷하며, 샌드박스를 탑제하여도, 완전히 안전치 않다는 점을 제시하였다. 프록시를 사용하여 php를 이용해 서버자체에 서비스를 요청하여 우회하는 기법도 있으며, 웹 어플리케이션의 취약점에 대해 다루었다.

또한 리패키징으로 어플리케이션을 역공학으로 디컴파일을 하여 악성코드를 심어 다시 앱 스토어에 등록을 하는 방법, 피싱 등 여러 가지 제시된 사례가 있었다. 앞으로 스마트 TV의 수요가 급증함에 따라 다양하고 신종 바이러스가 생길지도 모르며, 그에 따른 대비와 솔루션들을 개발해야 하는 단계에 서있다. 그리고 스마트 TV도 향후 발전도 무궁무진하다. 본 논문에서 다루었던 해킹 기술과 사례를 근거로 같은 공격을 당하지 않고 공격 여부를 판단하여 탐지하는 솔루션이 나오며, 신속한 대응을 하여 스마트 TV의 시장이 더욱 증진되길 기대한다.

REFERENCES

[1] Boyd, J., "Samsung's plasma displays barred from Japanese market," Spectrum, IEEE, vol. 41, no. 6, pp. 20-22, 2004

[2] Lee Dong-hoon, "HTML5 Standards-Based 스마트 TV Platform", TTA Exam certification Just Senior Researcher Shows

[3] Hwang Jung-Yeon, "Visited By App Users' Personal Information Infringement Analysis System", Korea Information Security Agency, 2008

[4] Se-Ho Park; Yong-Suk Park; Saet-Byeol Yu; Jun-rim Choi, "Implementation of ATSC mobile DTV broadcasting for N-screen smart devices," Consumer Electronics (ICCE), 2012 IEEE International Conference on , vol., no., pp. 331-332, 2012

[5] Albano, P.; Castiglione, A.; Cattaneo, G.; De Santis, A., "A Novel Anti-forensics Technique for the Android OS," Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on, vol., no., pp. 380-385, 2011

[6] Lin Sun; ShuTao Huang; YunWu Wang; Meimei Huo, "Application Policy Security Mechanisms of Android System," High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on, vol., no., pp. 1722-1725, 2012

[7] Zhi-Yong Li; Ran Tao; Zhen-He Cai; Hao Zhang, "A Web Page Malicious Code Detect Approach Based on Script Execution," Natural Computation, 2009. ICNC '09. Fifth International Conference on , vol. 6, no., pp. 308-312, 2009

[8] Mustafa, T., "Malicious Data Leak Prevention and Purposeful Evasion Attacks: An approach to Advanced Persistent Threat (APT) management," Electronics, Communications and Photonics Conference (SIECPC), 2013 Saudi International, vol., no., pp. 1-5, 2013

[9] Lee Hyun-Woo Sim Sung Jae, Learn Hacking Incident Analysis And Response To Cases, Unix, 2004

[10] Yun-Juho, Im Hyeon Suk, Kim, Yong Ho, Security Guide - Web Hacking Incident Analysis, 2009

[11] Mike Shema, Hacking For Beginners Web Attack And Defense, 2011

[12] Bak Yun-Su, Heo Gi-Taek, Jeong Seung-Mun, "스마트TV-based Smart Home Network Service Model", Dongshin University Industry-Academic Cooperation Foundation

홍 성 혁 (Hong, Sunghyuck)

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 네트워크 보안, 해킹, 센서네트워크 보안
- E-Mail : shong@bu.ac.kr