스마트TV 보안을 위한 확장 API 수정에 관한 연구

문정경[1*], 김진묵[1]
[1]선문대학교 IT교육학부

Modify of extended API for Smart-TV security

Jeong-Kyung Moon[*], Jin-Mook Kim[*]
[1]Division of IT Education, Sunmoon University

요 약 최근 스마트TV의 보급이 급속하게 증가하고 있다. 스마트TV는 표준화된 플랫폼을 기반으로 예약, 교육, 그리고 게임 서비스를 제공할 수 있다. 스마트TV에서 사용자가 요청한 앱을 실행하려면 표준 API를 실행해야 한다. 이때, 스마트TV 플랫폼의 취약점을 분석해서 악성 앱을 실행하거나 사용자가 요청한 컨텐츠를 위조하는 문제가 발생할 수 있다. 그러므로 우리는 확장 API를 수정해서 스마트TV 해킹을 막을 수 있는 방법에 대해 연구하였다. 우리가 제안한 연구 방법을 사용하면, 불법 장치가 스마트TV 장치에 불법적인 접근을 막을 수 있다.

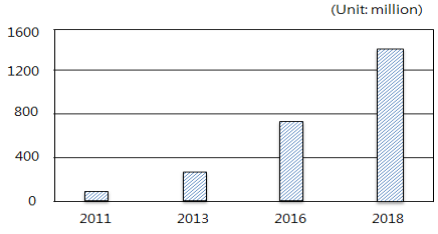
주제어 : 스마트TV, 에피아이, 확장 에이피아이, 정보보안

Abstract Latest Smart TV is rapidly increasing in prevalence. Smart-TV can provide reserve-service, training-service, and game service to user. Smart-TV need standard API for user requested app to run it. In this case, the cracker can run Malicious apps or user-request contents to modify it by analysis of the vulnerability of the smart-TV platform. Therefore, we modify the extension API on Smart-TV to prevent hacking. Our proposed research method can support that device is illegal in Smart-TV device can prevent unauthorized access.

• **Key Words** : Smart-TV, API, Extended API, Information Security

1. 서론

스마트TV는 스마트폰에 비해 보급률이나 성능이 낮은 것으로 평가되고 있지만, 스마트TV의 보급이 날로 확산되고 있어 보안의 위협이 증가하고 있다.



[Fig. 1] Smart TV world view

한국전자통신연구원 창의미래연구소의 보고서(2013)에 따르면 2018년 스마트TV 이용가구는 1,420만 가구에 이를 것이라 전망하고 있다. [그림 1]은 스마트 TV 시장 전망을 보여준다[1]. 스마트TV는 제조사별로 플랫폼이 서로 상이하고 표준화되어있지 않기 때문에 콘텐츠 시장의 단편화를 초래하고 스마트TV 발전에 장애요인이 되고 있다. 이에 한국정보통신기술협회(TTA)에서는 "HTML5 기반 스마트TV 플랫폼 표준"을 제정하여 독립·연동형 앱을 실현하는 기술을 정의하였다. 이 표준은 다양한 TV수신기 사이에서 앱이 동작할 수 있도록 지원하며, 스마트TV용 확장 API(Application Programming

*교신저자 : 김진묵(calf0425@sunmoon.ac.kr)
접수일 : 2014년 2월 11일, 수정일 2014년 4월 27일, 게재확정일 : 2014년 5월 6일

Interface)를 정의하여 앱이 TV 기능을 활용할 수 있는 인터페이스를 제공한다[2,3].

스마트TV의 증가는 스마트TV용 API사용의 증가로 이어지며, 이 과정에서 플랫폼의 취약점을 찾아 악성 앱을 실행하거나 컨텐츠를 위·변조하는 일이 가능한 일로 밝혀지고 있다[4]. 그러므로 본 논문은 스마트TV 플랫폼에서 확장API를 수정하여 스마트TV에 접근하는 장치 중 인증되지 않은 장치의 접근을 차단하고, 불법적으로 실행되는 앱을 차단하는 시스템을 제안하고자 한다. 2장에서는 관련연구에 대해 기술한다. 3장에서는 본 논문의 제안 시스템과 동작절차에 대해 기술한다. 4장과 5장에서는 시스템 고찰과 결론을 기술한다.

2. 관련연구

2.1 스마트TV의 위협 예

2.1.1 스마트TV 카메라 앱 실행

2013년 3월 캐나다 해킹 컨퍼런스 '캔섹웨스트(CanSecWest)'에서 고려대학교 사이버 국방학과 소속 이승진(20)씨가 스마트TV를 해킹해 내장된 카메라를 실행시켜 시청자의 사생활을 촬영하고 이를 인터넷으로 생중계 하였다. 심지어 전원이 꺼진 상태에서도 도촬이 가능했다[5].

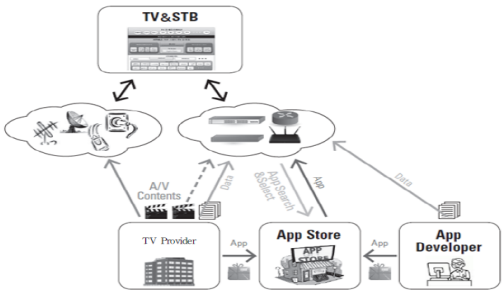
2.1.2 티비싱TV(Tvishing)

티비싱은 TV+ Phishing의 합성어이다. 티비싱은 해커가 사용자에게 홈쇼핑 방송을 내보내면서 원래의 자막을 변경시켜 자신의 계좌번호로 바꿔치기 하는 수법을 말한다[6].

2.2 스마트TV 구성

스마트TV 플랫폼은 리눅스나 윈도우즈와 같은 운영체제에 독립적이다. 플랫폼은 한국정보통신기술협회에서 발표한 표준에 따라 웹코어의 기능을 확장 할 수 있다.

그리고 애플리케이션과 TV 장치를 관리하는 모듈을 가지고 있다. HTML5를 기반으로 다양한 스마트TV용 앱을 실행시킬 수 있는 환경을 구현한다. 스마트TV 서비스의 개요는 [그림 2]와 같다[7, 8].



[Fig. 2] Overview of smart TV services

2.3 스마트TV용 확장 API

확장 API란 한국정보통신기술협회에서 정의한 W3C 기술 규격에 포함되지는 않았으나 스마트TV 앱에서 반드시 필요한 기술을 새롭게 정의한 API의 집합을 의미한다. 확장 API는 Web IDL을 통해 기술되며, 애플리케이션, 방송, 수신기 3가지 모듈로 정의된다. 표 1은 스마트TV의 확장API와 기능을 보여준다[4].

[Table 1] Smart-TV standard extended API

확장API	기능
애플리케이션	실행중인 앱 제어, 리모컨과 TV자원에대한 권한 제어, 앱 상세정보 제공
방송	방송 채널명, 채널번호 및 URI정보와 방송중인 프로그램 설명 자막 등 제공
수신기	네트워크 상태 및 설정 정보와 제조사 및 모델명 등 수신기 상태정보 제공

2.4 보안 요구사항

2.3.1 개발자 전자서명 기법

개발자 전자서명 기법은 마켓에 업로드 할 애플리케이션에 개발자의 전자서명을 요구하여 등록하는 방식이다. 현재 주도하고 있는 구글의 안드로이드 마켓에서는 이 방법을 시행하고 있다. 하지만, 개발자 인증의 신뢰도는 부족하며 애플리케이션 등록시 정당한 검증 과정이 없기 때문에 악의적인 애플리케이션 등록도 가능한 상태이다[2].

2.3.2 장치 인증

스마트TV는 스마트폰, PC, 테블릿, 모션리모컨, 음성인식 장치 등 다양한 장치로부터 명령을 입력받게 된다. 이때, 인증 받지 못한 장치의 접근을 제한하기 위해서 사전에 사용 중인 장치를 등록해야 한다. MAC주소와 ID,

PW를 사용하여 공개키 인증 방식을 사용하여 암호화한다. 서비스를 제공받기 위해 토큰을 발급받아 세션이 종료될 때가지 지속적으로 사용할 수 있도록 한다.

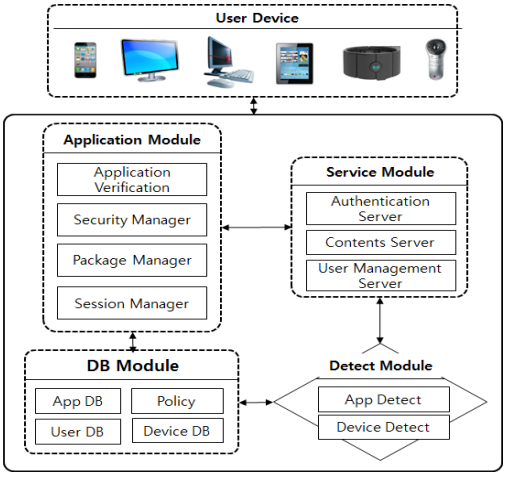
3. 제안시스템

본 논문은 스마트TV의 표준 API발표 이후 추가된 확장API를 수정하여 설계하였다. 이 시스템은 스마트TV에 접근하는 인증되지 않은 장치를 차단한다. 또한 서명되지 않은 불법적인 앱이 실행될 경우 차단한다. 본 논문의 제약사항은 다음과 같다.

1) 스마트TV에 카메라를 설치되어 있다.
2) 스마트TV의 전원이 켜져 있다.
3) 사전에 상대방의 공개키를 공유하고 있다.

3.1 제안시스템 구조

제안 시스템은 응용프로그램 모듈, 서비스 모듈, 탐지 모듈 그리고 DB 모듈로 구성되어있다. 제안 시스템의 이름은 ASDD로 한다. [그림 3]은 제안 시스템의 구조이다.



[Fig. 3] The structure of the proposed system

응용프로그램 모듈은 응용프로그램 검증과 보안 관리자, 패키지 관리자 그리고 세션관리자로 구성되어있다.

서비스 모듈은 인증서버와 컨텐츠 서버 그리고 사용자 관리 서버로 구성되어있다. 인증을 수행하고 컨텐츠 관리자로부터 자료를 전달받아 원활한 서비스를 제공할 수 있도록 중간 관리자 역할을 수행한다.

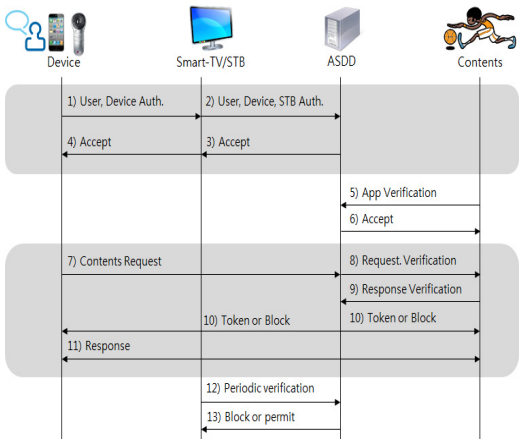
탐지 모듈은 App 탐지와 장치 탐지로 구분하여 장치의 인증 여부와 App의 서명 여부를 판별하여 DB에 등록한다.

DB 모듈에서는 정책, App DB, 사용자 DB, 장치 DB를 두어 각각 수집된 자료들을 저장한다. 탐지모듈에서는 DB를 검색하여 빠른 검출을 돕는다.

3.2 제안시스템 동작절차

본 논문에서 제안하는 스마트TV 인증 시스템의 동작절차는 크게 4단계로 나눈다. 첫 번째 단계는 사용자와 장치 인증 절차이다. 두 번째 단계는 App 또는 컨텐츠 제공자 인증 단계이다. 세 번째 단계는 서비스 인증 절차이다. 네 번째 단계는 주기적 검증 절차이다.

[그림 4]는 제안 시스템의 동작 절차를 나타내었다.



[Fig. 4] Operating procedures

첫 번째 단계는 사용자와 장치 인증하는 단계이다. 이 단계에서는 사용자 인증과 장치들을 등록하는 절차이다. 사용자와 장치는 다수 개일 수 있다.

1) User_n_ID= Enc_TS{User_n | PW | E-mail | TS}
Device_n_ID= Enc_TS{Device_n | MAC | TS}

사용자정보는 User_n, Password, 이메일 주소와 TS 정보를 연결한 값을 TS를 이용하여 대칭키 IDEA로 암호화한다.

장치 정보는 Device_n과 MAC 주소 그리고 TS를 연결한 값을 TS를 이용하여 대칭키로 암호화한다.

2) List_n= h{User_1_ID | User_n_ID | Device_1_ID | Device_n_ID | STB_ID}

스마트TV를 사용하는 사용자 n개와 장치 n개 그리고 내장된 STB의 정보를 새로 생성하여 연결한다. 이것을 해쉬함수 연산한다. 이렇게 생성된 List_n의 자료를 ASDD으로 전송한다. ASDD는 전송받은 정보를 검증하고 DB에 등록한다.

3) h{User_1_VID | User_n_VID | Device_1_VID | Device_n_VID | STB_VID}

4) h{User_1_VID | User_n_VID | Device_1_VID | Device_n_VID}

장치와 사용자 인증 값을 해쉬함수로 연산하여 STB로 전송한다.

두 번째 단계는 App개발자 또는 컨텐츠 제공자가 App또는 컨텐츠 제공 서버를 인증하는 단계이다.

5) App_n_ID= E_Sig{App_n | PW | E-mail | TS}

App의 등록번호, Password, App개발자 이메일 그리고 TS로 연결한 값을 전자서명하여 전송한다.

6) h{App_1_VID}

App의 인증값을 저장하여 해쉬함수로 연산하여 컨텐츠 서버로 전송한다. 이때, 컨텐츠 서버는 사전에 인증한 것으로 간주한다.

세 번째 단계는 서비스 인증 절차이다. 사용하고자 하는 컨텐츠가 인증 받지 못한 것이라면 실행하지 못하도록 하는 단계이다. 이때 사용하는 장치도 다시 검증하여 사용을 중단할 수 있다.

7) Contents_ID= Enc_RND{Contents# | User_n_VID | Device_n_VID | STB_VID}

사용자의 컨텐츠를 요청번호와 인증 받은 사용자 정보 그리고 장치 정보를 연결하여 난수값을 이용하여 암호화하여 전송한다.

8) Req_Signature=Enc_RND{Contents# | ASDD_ID}

컨텐츠 요청이 유효한지 확인하기 위해 ASDD의 DB를 검색한다. 인증 자료가 없는 경우에는 컨텐츠에 대한 인증을 요청한다.

9) Rsp_Signature=E_Sig{Contents#}

컨텐츠 인증은 전자서명으로 이루어진다. 인증요청에 응답하지 않으면 세션을 종료한다. 9)에 응답이 없으면 종료한다.

10) Enc_RND{Token}

ASDD는 전자서명된 Contents#를 복호화하고 DB에 저장한다. 그리고 STB와 컨텐츠 사이에 사용할 Token을 생성하여 암호화한 후 전달한다.

11) Rsp_Contents=Enc_Token{Contents | h}

이로서 요청한 자료에 대한 컨텐츠에 대해 접속이 이루어지고 자료를 송수신 할 수 있다. 컨텐츠 전송시 해쉬함수 연산을 한 후 전달함으로서 자료가 위·변조 되는 것을 방지할 수 있다.

네 번째 단계는 주기적 검증을 실행하는 단계이다. 사용중인 앱이나 장치를 주기적으로 점검한다.

12) EXEC_Contents{App_List || User_List || Device_List}

Enc_Token{Contents | h}

EXEC_Contents는 실행중인 App의 종류, 실행시킨 User 정보, 실행을 담당한 장치의 정보를 가지고 있다. 탐지 모듈은 이 정보에 대해 계속적인 탐지를 실시한다. 서비스 모듈과 DB 모듈과의 주기적인 확인을 통해 인증되지 않은 앱과 장치를 검색한다. 또한, 컨텐츠와 함께 전송된 해쉬값을 비교하여 위·변조된 자료 여부를 확인한다.

13) Connect() or finish()

탐색 결과 인증 받지 않은 장치의 접근은 즉시 차단한다. 컨텐츠의 경우 해쉬값과 다른 경우 위·변조된 것으로 간주하여 실행을 종료하고 DB에 등록한다.

4. 시스템 고찰

본 장에서는 제안 시스템의 보안 요구사항에 대한 적합성을 분석한다.

첫째, 장치와 인증서버 그리고 컨텐츠 사이에서 장치의 정보가 유출될 수 있다. 이를 방지하고자 장치의 번호와 MAC주소 그리고 TS를 조합하여 대칭키(IEDA)를 이용하여 암호화하였다. 그리고 인증서버에는 DB를 구성하여 인증되지 않은 장치의 접근을 차단하였다. 이로서 기밀성과 사용자인증을 보장한다[9,10].

둘째, 네트워크를 통해 전송하는 컨텐츠의 위·변조를 막기 위해 컨텐츠 사용시 전자서명을 실시한다. 또한, 컨텐츠 전송시 해쉬함수 연산을 실시하였다. 이로서 무결성 및 부인방지를 보장한다.

셋째, 주기적으로 앱 모니터링을 실시하여 실행 중인 앱과 장치를 체크한다. 인증된 애플리케이션인가? 애플리케이션 전송과정에서 위·변조가 있었는가? 애플리케

이션이 허가된 장치에서 실행되었는가? 사용되지 않는 앱이 실행되고 있는가? 에 대해 체크한다. 이때 DB 모듈을 참고하여 빠른 처리를 돕도록 한다.

5. 결론

스마트TV의 사용이 점차 늘어나고 있다. 스마트TV는 개방성과 양방향성 서비스를 제공할 수 있다는 장점을 갖는다. 하지만 이로 인한 해킹의 취약점이 예견되고 있다. 이를 보완하고자 본 논문에서는 확장API를 수정하여 안전한 스마트TV 환경을 만들고자 하였다. 제안 시스템은 보안요구사항인 인증, 기밀성, 무결성, 부인방지, 가로채기 등이 보장된다.

스마트TV의 수요가 급증하면서 새로운 바이러스나 해킹기법이 발생할 것이다. 신뢰성과 편의성을 갖춘 스마트TV 생태계를 만들기 위해서는 표준화된 플랫폼 구축이 필수적이다. 이것은 보안기술 연구를 집중화할 수 있고 사용자 접근 편의성을 제공하여 스마트TV 발전을 가속화할 것이다.

REFERENCES

[1] Sang Hoon Lee, Su-Yeon Kim, Design and Implementation of an Intelligent System for Personalized Contents Recommendation on Smart-TVs, JKSIIS, Vol. 18, No. 4, 2013.

[2] Dae-Sik Park, Jin Kwak, Pre-qualification based Application Contents Management Method for Smartphone, Journal of Korea Multimedia Society Vol. 13, No. 11, pp. 1677-1686, 2010.

[3] Yukyeong Wi, Jin Kwak, A Study on USIM Card Based User and Device Authentication Scheme in the Smartwork, Jounal of Korea Multimedia Society, Vol. 16, No. 3, pp. 309-317, 2013.

[4] KIM, SoonChoul, et al. An architecture of augmented broadcasting service for next generation smart-TV. In: Broadband Multimedia Systems and Broadcasting (BMSB), 2012 IEEE International Symposium on. IEEE, pp. 1-4, 2012.

[5] Sunghyuck Hong, Hacking and Countermeasure on Smart TV, Journal of Digital Convergence, Vol. 12, No.1, pp. 313-317, 2014.

[6] Dong Rye Kim, Ki Chang Shim, Moon Suk Jeon, A Study of privacy system against privacy laws, Journal of The Korea Institute of Information Security & Cryptology, Vol. 21, No. 6, pp. 15-22, 2011.

[7] Dong-Hoon Lee, Ho-Youn Kim, Dong-Young Park, Eun-Hyang Lee, Extended API Design and Implementation for HTML5 based Smart-TV Platform, KSBES, pp. 185-188, 2013.

[8] Kwihoon Kim, Chunghyun Ahn, Chunghyun Ahn, Research of Social TV service technology based on smart TV platform in next generation infrastructure, ICCIT, 2010.

[9] Hyungjun Yoo, Junggil Park, Jaeyoung Koh, Kyeoungju Ha, An Authentication Scheme to Guarnatee Reliability of Device Wireless Network Environments, Journal of Computing Science and Engineering.

[10] Junghwan Lee, Yudong Hwang, Donggue Park, Jongyook Han, A New Device Authentication Protocols for Secure Services in Home Network Environments, Journal of Korean Institute of Information Technology, Vol. 3, No. 6, pp. 57-65, 2005.

저자소개

문 정 경(Jeong-Kyung Moon) **[정회원]**

- 1993년 2월 : 배재대학교 원예학과(학사)
- 2006년 2월 : 단국대학교 인터넷정보학과(공학석사)
- 2013년 2월 : 공주대학교 컴퓨터공학과(공학박사)
- 2012년 3월 ~ 현재 : 선문대학교 IT교육학부 계약교수

<관심분야> : 클라우드 컴퓨팅, N-스크린, 네트워크, 정보보안

김 진 묵(Jin-Mook Kim) [정회원]

· 1998년 2월 : 배재대학교 전자계산학과(공학사)
· 2000년 2월 : 배재대학교 컴퓨터공학과(공학석사)
· 2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
· 2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
· 2008년 3월 ~ 현재 : 선문대학교 IT교육학부 부교수
<관심분야> : 유·무선 네트워크, 센서네트워크, 정보보안, N-스크린