Approach of Secure Smart-TV authentication using extended API

Jeong-Kyung Moon[1], Jin-Mook Kim [1], Bong-Hwa Hong [2]

[1.] Division of IT Education, Sunmoon University
[2.] Department of Information & Telecommunication, Kyunghee Cyber University
{moonjk, calf0425}@sunmoon.ac.kr, bhhong@khcu.ac.kr

Abstract: Smart-TV is rapidly spreading. Smart-TV is received to run apps such as scheduled, games education and a variety of services. In this case, the behavior of the app is running for the many smart-TV API. During this process, to find vulnerabilities in the Smart-TV platform to run a malicious app or content issues, and be a forged. For this reason, the management and security of the Smart-TV API has emerged as an important issue. Therefore, in this paper, in order to prevent hacking of smart-TV extension API has been fixed. This system is block illegal access of device. Also, the content is prevent from being forged and can prevent the execution of illegal Apps.
[Kharkwal G, Mehrotra P, Rawat YS. **Taxonomic Diversity of Understorey Vegetation in Kumaun Himalayan Forests**. *Life Sci J* 2014;11(7s):150-154] (ISSN:1097-8135). http://www.lifesciencesite.com. 28

Keywords: Smart-TV; Platform; Authentication; Extended API; Security service

1. Introduction

Smart-TV means to platform over a network connection that provided a variety of additional services such as broadcast, VOD, games, education and apps [1, 2]. Smart-TV is not only means that two-way service is possible. It should be a variety apps are able to install and run on TV. Also, it should be shared variety of information connect to social networks [3]. Manufacturer-specific non-standardized of Smart-TV platform has caused in fragmentation and failure in developing of contents market. Thus, the Korea Information and Communications Technology Association (TTA), the "HTML5-based Smart-TV platform standard" to establish an independent linked was defined as a technique for realizing Apps[4]. This standard supports to operate apps between the various TV receivers. And support interface for apps can take advantage Smart-TV by defined of extended API.

According to Gartner's research, Smart-TV units sold over 69 million in 2012. And it will sold 188 million in the world market at 2013. Figure 1 shows the status of the increase in Smart-TV.

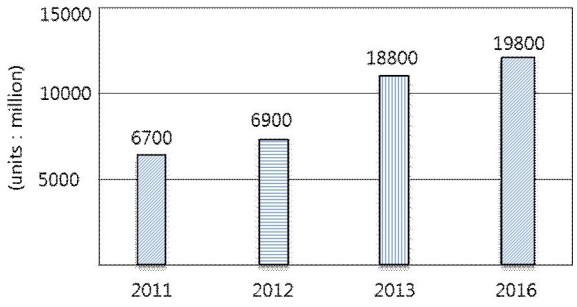

Figure 1. Smart-TV sales forecast worldwide

Smart-TV sales growth been followed by an increase in the execution of the API, Smart-TV hacking is becoming increasingly likely. For example, hacking conference in CanSecWest, at March 2013 in Canada that belongs to the Department of Defense Cyber hacking. Lee Seung – Jin in Korea University (20) who is Smart-TV hacked and views to run the built-in camera with internet and shoot the privacy of picture on another smart-TV. Also, Tvishing have a major security threat. Tvshing is a portmanteau of the TV + Phishing. Tvishing means phishing technique that hackers are exported to the user while the original home shopping broadcasting change the subtitle switched their account number [5, 6].

Smart-TV's hacking is higher than PC and smart phones the security threat. Many people are using the Smart-TV do not know about security because old people don't understand about characters of smart-TV. And replacement cycle on home appliances is long than electronics products [7].

Therefore, we will propose that blocked illegal running apps by modify extended API in the Smart-TV platform and denied not registered device to access system in this paper. Chapter 2 describes the structure and procedure of Smart-TV, and extended API of Smart-TV. Chapter 3 describes the proposed system and procedures for the operation. Chapter 4 and Chapter 5 describe Discussion and conclusions of the system.

2. Related research

2.1 Smart-TV Platform

Smart-TV platforms are independent from Linux or Windows operating system. Platform can extend the functionality of the Web core by the standards published to Korea Association of Information and Communication Technology. It has

apps and management module of TV device. In addition, Implement environment that can run apps for various Smart-TV in HTML5-based. Figure 2 is Smart-TV platform architecture [8].

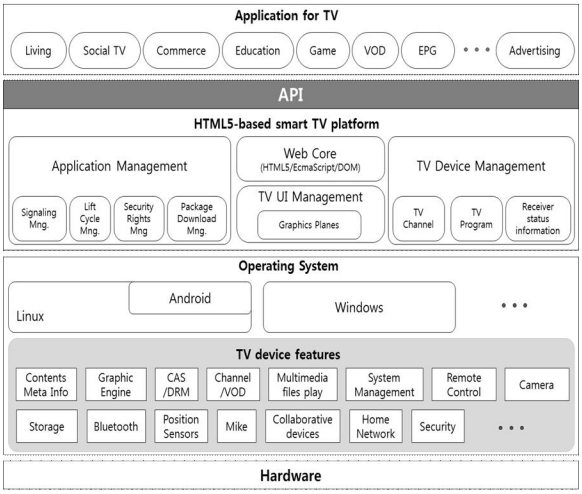

Figure 2. Smart-TV receiver platform architecture

2.2 Extended API for Smart-TV

Extended API is defined in the Korea Association of Information and Communication Technology has not been included in the W3C technical specifications. But it new defined set of API to new technology required in Smart-TV apps. Extended API is described through the Web IDL and defined three modules as application, broadcast, and the receiver. Table 1 shows the extended API and functionality of Smart-TV.

Table 1. Extended API of Smart-TV standard

Extended API	Function
Application	Running apps control Rights control of Remote Control and TV resource Provides detailed information of app
Broadcasting	Broadcast Channel Name & Channel Number URI information and description of the program being broadcast, Subtitling
Receivers	Network status and configuration information Manufacturer and Model Receiver status information

2.2 Security Requirements

2.2.1 Device authentication

Smart-TV receives a command from a variety of device such as smart phone, PC, tablet, motion remote control and voice recognition. In order to block the access of an unauthorized device should be registered your device. At this time, authentication scheme using public key encryption includes MAC addresses, ID and Password. To provide the service generate a token and until the session ends can be used.

2.2.2 Confidentiality

Server authentication values should be guaranteed by confidentiality. So a hacker to intercept server authentication value should be encrypted it that it cannot be read to hacker [9]. Such as data source address, destination address, data length, and counter.

Therefore, smart-TV authentication system must support to confidentiality service to user and device by encryption algorithms such as IDEA, RSA, and so on. Our proposal system use IEDA because symmetric encryption algorithm that is lighter and easy.

2.2.3 Integrity

Smart-TV terminals must be ensuring integrity for user can use the smart-TV services. Therefore, device-ID must be ensuring integrity because it affects the terminal_id creation. And when the content is sent through a network that is forged subtitles stemmed. If server doesn't blocking it, as well as Tvsing is happen and another-attack can lead to social chaos.

So, we support Hash function and digital signature method such as SHA-2, and MD-5 that can guaranty to data integrity services. This is very popular digital signature service algorithms and it can use to easy.

3. The proposed system

We design to modify extended API for smart-TV authentication and security service support to user in this paper. This system blocked illegally apps when app is running on Smart-TV by hacker. In addition, unauthorized access to the device is blocked. If Smart-TV is turned on, we controls unauthorized devices, apps and contents periodically detecting. The following is a limitation of this paper.

1) Smart-TV has built-in camera or installing the depended-camera.
2) Smart-TV's state is assumed that the power is on always.
3) They share the other's public key

3.1 The structure of the proposed system

In this study, we propose a system modifying the extended API. Proposed system consists of Application Interface, Service Manager, Detection Module and Database Manager. Our proposed system's name is ASDD (Application interface, Service manager, Detection module and Database manger's initial make it).

First, Application Interface consists of Application Verification, Security Manager, Package Manager and Session Manager. Second, Service Management consists of and the Authentication Server, User Management Server and Contents Server. This module performs authentication. Role as the intermediate manager receives data from the content manager to be able to provide seamless service.

Third, Detection module is divided Application detect and device detect. This module is detected the run apps and device periodically. And fourth, DB Management Module consists of Policy DB, Application DB, User DB and Device DB. Save the data to the DB details. Searching by DB helps faster processing if generated unauthorized User, Device and Apps. Figure 3 is structure of the proposed system.

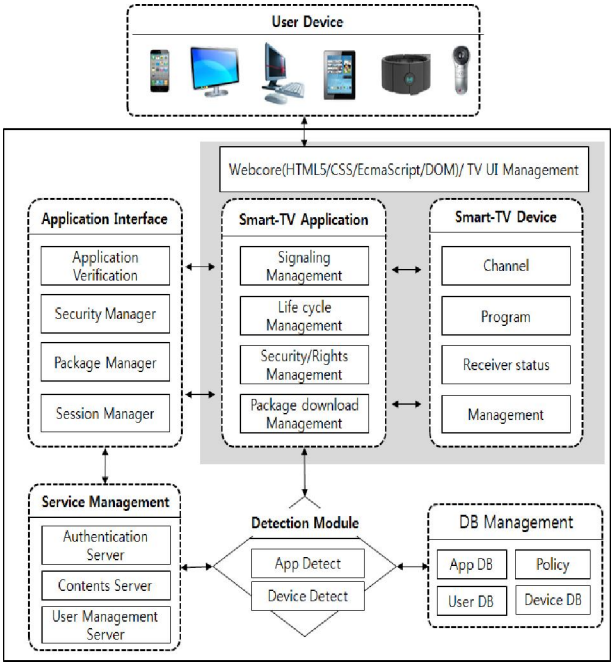

Figure 3. Structure of proposed system

3.2 The proposed system operating procedures

The proposed systems have procedures with 11 steps for the operation of the Smart-TV authentication that is divided into three phases. The first step is to the user and device authentication procedure. The second step is to service authentication procedure. The third step is the procedure is verified periodically.

The terms used in this paper are summarized in the table.

Table 2. Term table

Abbreviation	Explnation
Enc/Dec	Symmetric key encryption / decryption
E_Sig/D_Sig	Electronic signature public key encryption / decryption
User_id	Smart-TV user id
Device_id	User device id such as MAC
H(data)	Hash function operation
RND	Random value
VID	Certified by the result
TS	Timestamp
Req/Rsp	Request / Response
List	DB stored value

Figure 4 shows operation procedure of the proposed system. It has three procedures that have 11 steps more detail.

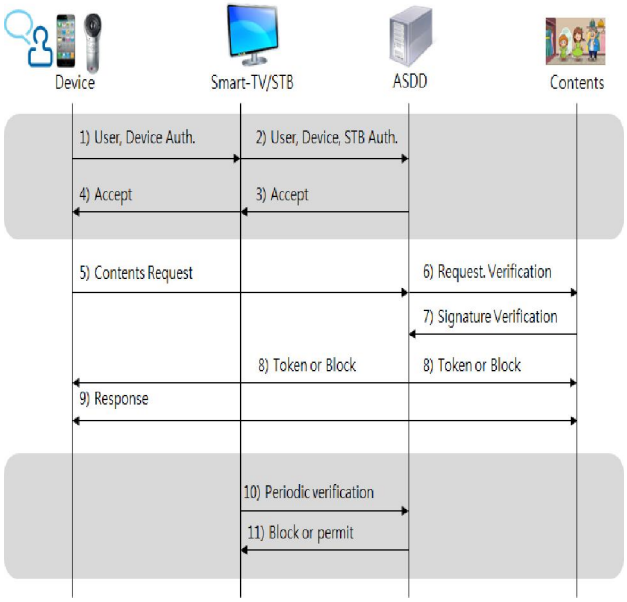

Figure 4. Operating procedures

The first step is to authenticate the user and the device. At this step, user and device authentication process then registration in the DB.

1) User_id= Enc_TS{User_id | PW | E-mail | TS}
Device_id= Enc_TS{Device_id | MAC | TS}

User information connects to User_id, Password, e-mail address and TS information. And this value is encrypted using TS (Time-stamp) and the symmetric key algorithm such as IDEA.

Device information connects Device_ID, MAC address and TS and this value is encrypted using TS and the symmetric key IDEA.

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

Smart-TV server connects N number of user information and N number of user Device. And they connect new generated information by the STB. This is compute by hash function. STB Generated List_n transmits to ASDD. ASDD verify transmitted information and register in the DB.

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}

Value of device and user authentication results by hash function operation transmits to the STB.

The service authentication procedure is second step. If you want to run the unauthorized contents it will be blocked. At this time, the device is used to verify again. And can be stop if it unauthorized.

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

In this step, It is connected that user requesting number, user information, device information and set-top box information. And Encrypted using a random number then transmits.

6) Req_Signature=Enc_RND{Contents# | ASDD_ID}

Search DB management of ASDD to validate possibility about request the content. If there is no authentication information is requests for contents authentication.

7) Rsp_Signature=E_Sig{Contents#}

Contests authentication is performed electronic signature authentication. If it do not respond to a request for authentication, the session is terminated.

8) Enc_RND{Token}

The ASDD decode Contents# by electronic signed then store in DB. ASDD passes the token generate and encrypt to use between the STB and contents.

9) Rsp_Contents=Enc_Token{Contents | h}

This allows the requested data can be used for the Contents. We can prevent forgery as a hash functions are used.

The third step is to run a verification step periodically. Being checked the app or device periodically. Running without authentication value by the app or the device is blocking it as an illegal.

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

Enc_Token{Contents | h}

EXEC_Contents has a running app information, user Information and device information. Detection Module is performed the continuous detection of the information. It through the check for the service manager and DB manager is searched unauthorized app and device. Futher, it determines whether to forgery as being compares content transmitted with a hash value.

11) Finish ( )

Unauthorized access of the device is immediately shut down. All resulting values are registered in the DB.

4. Discussions

This chapter is analyzing for the security requirements of the proposed system. It can be leaked information between the device, authentication server and between device and contents. To prevent steal and modify to authenticated information, It was encrypt using symmetric key algorithm such as IDEA that connect device number, MAC address and TS. Authentication server stores the device information and blocks the access of unauthorized device. This allows assure the confidentiality and user authentication [10, 11].

The proposed system is transmitted through a network a digital signature to prevent falsification of the content technologies. And a content server for transferring content to a user, using the hash function, integrity and non-repudiation services provided.

And our proposed system monitors app periodically for running apps and devices authentications services. IT can provide data integrity and device integrity service to them. Only authenticated app can run on our proposed system.

And while app running, data can't modify and forge between user and content's server. Only app can run authenticated device on our system. So, our system can support integrity and prevent of man-in-the-middle attack [12].

We will study about future work that proposed system can support user access control by privilege and various data encryption algorithms for more secure service to user and devices.

5. Conclusion

The increasing number of the use of the Smart-TV, the Smart-TV can provide openness and Interactive. However, predicted to be variety of hacked as vulnerability of openness. In this paper, we want to create a safe environment for Smart-TV by modify the extended API.

First, the user was registered to the authentication server and the device. The symmetric key using IEDA and TS were to maintain confidentiality. Be blocking an unauthorized access to device using the configured DB in the authentication server.

Secondly, to block the unauthorized execution of apps used the electronic signature. Also, we used hash function during transmission of the content to prevent forgery. This allows ensuring integrity could.

Third, this system inspect device execution and the illegally apps running periodically. Also block unauthorized device access and illegally apps.

While increasing the demand for Smart-TV will occurs new viruses or hacking techniques. In order to make the Smart-TV ecosystem with reliability and ease of use is essential to establish a standardized platform. This is so that we can centralize security technology research and to provide ease of user access will accelerate the development of the Smart-TV.

Corresponding Author:
Prof. Jin-Mook Kim
Division of IT Education
Sunmoon University
Asan-si, ChungNam, 336-708, Korea.
E-mail: calf0425@sunmoon.ac.kr

References

1. 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, 2012. p. 1-4.
2. Hyun-Jeong Kim, A Study on Defining User-centered contents and features of Smart-TV, KODDCO, 2014, 14.1: 321-332
3. Sang Hoon Lee, Su-Yeon Kim, Design and Implementation of an Intelligent System for Personalized Contents Recommendation on Smart-TVs, jksiis, 2013.18.4.073.
4. Dong-Hoon Lee, Ho-Youn Kim, Dong-Young Park, Eun-Hyang Lee, Extended API Design and Implementation for HTML5 based Smart-TV Platform, 2013.06.
5. KIM, MoonKoo; PARK, JongHyun. Demand forecasting and strategies for the successfully deployment of the smart TV in Korea. In: Advanced Communication Technology (ICACT), 2011 13th International Conference on. IEEE, 2011. p. 1475-1478..
6. Sunghyuck Hong, Hacking and Countermeasure on Smart TV, Journal of Digital Convergence, Vol. 12, No.1, 2014.01.313-317.
7. 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, 2011, 21.6: 15-22
8. KIM, Kwihoon; HONG, Jinwoo; AHN, Chunghyun. Research of Social TV service technology based on smart TV platform in next generation infrastructure. In: 5th International Conference on Computer Sciences and Convergence Information Technology. 2010. p. 556-559.
9. Yukyeong Wi, Jin Kwak, A Study on USIM Card Based User and Device Authentication Scheme in the Smartwork, Jounal of Korea Multimedia Society 2013; Vol. 16, No.3:309-317.
10. 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, Vol. 39, No.3, 2012. 06.
11. 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, 2005, 3.6: 57-65
12. Dae-Sik Park, Jin Kwak, Pre-qualification based Application Contents Management Method for Smartphone, Journal of Korea Multimedia Society Vol.13, No.11, 2010.11, 1677-1686.

4/28/2014