The Security Model of Broadcast Intelligent Terminal Application and Technology Realization on TVOS

Xin Wang [1 4], Delin Chen [2], Yue Sun [3], Xu Wang [1] , Suying Yao [1]
[1]School of Electronic Information Engineering, Tianjin University, Tianjin 300072, China
[2]National Academy of Broadcasting Science
[3]Department of Electronic Engineering, Tsinghua University
[4]Tianjin Broadcast and Television Network Co., Ltd.

***Abstract*—With the trends of intelligent terminal and broadband network, all kinds of intelligent terminal application based on internet emerge in an endless stream. How to ensure the security of the various applications running on the next generation operating system TVOS is a key technical problem to be solved urgently. In this paper, we analyse the security mechanism of broadcast intelligent terminal application environment, put forward the security model and technology on TVOS, developed a safe and reliable application environment of broadcast intelligent terminal.**

Keywords- Application ;NGB TVOS ;OTT ;DVB ;Android

I. INTRODUCTION

[1]According to the development of three network convergence, the constitute of the intelligent terminal product line has suffered a great change. The operation system supplier which stay on the upstream, develop basic rule of security mechanism, and relative application store policy, on basis of this rule, terminal manufacturer custom make terminal software, establish their own application store.

[2]The main task of next generation broadcasting network is terminal intelligentialization and standardization.Analysing from the technique, the security problem of broadcasting intelligent terminal exist in three levels, they are application level, terminal operation system level and terminal hardware level. To solve these problems, apart from the technical step such as security evaluation from the supervision department, also relates to the communication channel of the terminal application software (application store) and configuration security management of the third party server which provide the application services, that is to say , based on intelligent terminal operation system, establish safe and trustable application environment for broadcasting intelligent terminal.

[3]This article analyse and discuss the security mechanism of terminal application environment and security system structure, this is from the view of technology and security. Proposed a security model of broadcasting network terminal, and this model is based on TVOS operation system which developed by our own country.

II. THE SECURITY TARGET OF BROADCASTING NETWORK INTELLIGENT TERMINAL APPLICATION ENVIRONMENT

The security target of broadcasting network intelligent terminal application environment is to only allow download software from unified application store, not allow copy and distribution from the media, through the third party application program developing, verification and distribution, installation and update, loading and running , realize identity authorization , security evaluation, trust declaration and autography verification, integrity check for loading, running resource access control, security management for the whole life period.

A. Application developing

[4]Developer apply for the developer account, fill in personal profile of company information, and application type, read relative developer protocol , only verified developer can upload application. Mainly refer to security management of the developing process, require the developer to register trust certificate. Acquire the developer identity certificate issued by the system platform(X509 V3 digital certificate) use for platform to verify the application, which uploaded by developer, and trust declaration .

B. Verification and distribution

TVOS system need to ensure the trust and credibility of the download resources, this will be ensure by verification and trust declaration signature, before the application distribution by the developer and platform dealer.

C. Installation and update

In order to make sure the downloading process legal and liable. After the application downloading from the store and before the installation, digital signature verification has to be done to the trust declaration and permission to install the application, this will ensure the legal application to be installed in TVOS system

D. Loading and running

After the application's installation, before loading integrity check has to be done to prevent the application being changed maliciously. the checking process can be carried out by checking the local signature on customer's set top box during the installation, or checking the signature before loading.

During the running , the compliance check should be done according to the accessing rule in the trust declaration , kernel of TVOS will execute security access rule library based on mechanism of DAC and MAC.

III. SECURITY MODEL OF BROADCASTING NETWORK INTELLIGENT TERMINAL BASED ON TVOS APPLICATION ENVIROMENT

[5]Security model of broadcasting network intelligent terminal based on TVOS application environment , the model is consist of several aspects as below, security support for terminal hardware, integrity protection for application and data, safe distribution of software, access control and sandbox isolation, secret protection, security policy control.

Integrity protection of system software has been installed in safe boot, OS system software and inner system application , next step to offer integrity protection for downloading and installation of the application, the integrity protection of this process can not be support stably by LINUS for the time being. Need to be developed extendly, through digital signature technique to realize. Digital signature use popular HASH abstract and encryption technique of public key system. Use digital signature to distribute and manage the public key in general industry。

Abstract of execution plan for security model is as below：

(1) use the OS level security style supplied by LINUX

(2)mandatory to keep the application running within its own sandbox

(3)use file system encryption function

(4) key protection：prohibit using clear text to save the key, the length should be over 8 character, save as SHA-1 abstract style

(5) application to be downloaded and installed need to be certified by digital signature of the developer or platform dealer.

(6) use hardware security mechanism, such as TPM/CA-DRM security hardware model

IV. APPLICATION SECURITY MODEL TECHNIQUE REALIZATION PLAN

A. application authorization control

As a security mechanism , authorization will allow or restrict the application to access the restricted API and resources.

In default, application has not been granted authorization, this not allow they access the restricted API and resources on the equipment ,this ensure the security of the system, during the installation, authorization requested by application via manifest file, this is granted by the user.

System define a series of authorization ,to protect every aspects of system or other application program, via application authorization interface. Manufacture can extend his authorization outside the one defined by the system, to protect the new-added hardware and software resources, application can also define its own authorization to protect its resource, if other program want to access the resource protected by another application, must ask proper authorization via their manifest file.

Authorization declaration

If a application try to acquire an authorization, it must declare this authorization in its manifest file, the format of authorization declaration is as below

<uses - permission

tvos:name="tvos.permission.WRITE_EXTERNAL_STORAGE"/>

(1) Authorization grant

During the application ‘s installation, install package assembly will analyze the authorization declaration in manifest file of the application, through checking the signature in application packet and user interactive confirmation to decide whether or not grant the application of this authorization. All authorization declaration in the manifest file of application will display to the user through a dialogue box , user need to choose whether to confirm the grant or exit the installation.

(2) Authorization check

While an running application try to access restricted API and resource of the system, system will check the authorization of the application, see if the application has the authorization to prevent the malicious application to access the restricted resource, without authorization declaration in manifest file. Authorization checking will be running in authorization manage service of resource accessing, if authorization check fail, return error or throw an exception.

(3) Cancel of authorization

While application is uninstalled ,the granted authorization will be cancel.

B. Defined interface of application ‘s authorization

Taking expansibility into account, except for a series of authorization provided by the system, system also leave some interface for application authorization to define, this will let manufacturer and developer to define their own authorization

In order to their new added resource(hardware equipment or software resource) from being accessed by other application, the manufacturer can define their own application authorization, application program try to access the restricted resource, it’s need to declare its authorization in the manifest file.

Application can define their own authorization to protect their resource from being accessed, if other application want to access the resource, they must acquire proper authorization from their manifest file.

Define a format for an authorization as below

<permission tvos:description="*string resource*"
tvos:icon="*drawable resource*"
tvos:label="*string resource*"
tvos:name="*string*"
tvos:permissionGroup="*string*"
tvos:protectionLevel=["normal" | "dangerous" |
"signature" | "signatureOrSystem"] />

There is 4 value in property “protectionLevel”： normal，dangerous, signature, signaureOrSystem。

Normal is default value, has the lowest potential harm, it indicate that the operation of this authorization do the

lowest harm to the system and the user. System will grant this authorization to the request automatically .

[5]Dangerous mean that the operation related to this authorization has higher potential harm, system will not grant this authorization to the request automatically, it will display the authorization request to the user, and the user will confirm whether to grant the authorization or not.

V. CONCLUSION

In this paper, we analysed security mechanism, on radio and television intelligent terminal application environment from the point of view of technology and security architecture and put forward the security model and intelligent terminal application scheme and technology in smart TVOS terminal operating system which developed independently by China. At present, the security model and the technical implementation scheme has been used in broadcasting and television based on the TVOS1.0 operating system.

REFERENCES

[1] Bernhard J. Berger, Michaela Bunke, and Karsten Sohr. An Android Security Case Study with Bauhaus // 2011 18th Working Conference on Reverse Engineering.

[2] Felix Rohrer, Nebiyu Feleke, Yuting Zhang, Kenneth Nimley ,Lou Chitkushev, Tanya Zlateva1. Android Security Analysis and Protection in Finance and Healthcare. //Boston University MET

[3] Chen Delin ,Li Zheng ,Wang Ying, Zhao Liangfu, Zhang Dingjing.<<The main technical characteristics and software architecture of NGB TVOS>>, 《Radio and television information》 2013-10National Academy of Broadcasting Science

[4] NGB TVOS1.0 Version of cooperation and development. The next generation of radio and television (NGB) Intelligent Technology TV operating system v1.0.0, the State Press and Publication Administration

[5] GY/T267-2012.NGB Technical specification of terminal middleware, the State Press and Publication Administration

[6] Wang Mingmin、Zhu Yunbin. 《To explore the implementation model and techniques of intelligent television terminal security under NGB environment》, 《Radio and TV Technology》2012-10

[7] Ning Hua、Li Wei、Wang Kun、Lei Mingyu《Research on intelligent terminal security system》, 《Modern telecommunication technology》, 2012- 5