Research on the Network Security System of Intelligent TV Terminal

Du Jiang, Li Cheng

Chongqing University of Posts and Telecommunications, Chongqing400065

28361523@163.com

Keywords: TVOS, intelligent terminal set-top boxes, terminal security system

Abstract. In this paper, the author designed the TVOS intelligent terminal network security scheme. The scheme takes hardware security as the underlying support layer, and it connects the kernel layer of TVOS operating system, component layer, and the execution environment layer and application framework. Thus the design scheme can ensure organic coordination among function levels of TVOS, and form safety protection of mutual support and coordination. The design of the terminal security could provide environment for the TVOS intelligent terminal to carry out business. Besides, it could provide security to the users to effectively cope with external potential threats.

Introduction

TVOS as the first intelligent terminal operating system in China's radio and television industry, it is the first time that China's radio and television industry independently researched and developed this system. Therefore, it plays an important role in perfecting our country's radio and television network security. On security, TVOS, according to “controllable, safety broadcast” overall request, must adopt independently controlled safety kernel and safety control system, thus from the bottom to set technical limitations to achieve the result that there is no Root in products. Therefore, TVOS has put an end to the possibility of illegal program installed from the external. For the audit and installation of the application program, there must be strict procedures. And we should build a trustful foundation around the terminal hardware and a complete trustful chain system of the digital certificate, thus to make sure that the TVOS terminal system is unbreakable.

Through analyzing the hardware system and software platform of TVOS intelligent terminal and making reference security methods of other intelligent operating system, we put forward the security control scheme suitable for TVOS intelligent terminal box of Shaanxi radio and television networks. Besides, we introduced the above scheme in detail. In the scheme, the front security platform bearing the generation of the key security, safety management and safety circulation will be the key part to be discussed in this article.

Layered Structure of TVOS Intelligent Terminal

Intelligent, or non- intelligent set-top box can be divided into the software layer and hardware layer. And in the software layer, the intelligent set-top box can be divided into the application layer and operating-system layer. Therefore, the intelligent set-top box can be roughly divided into three layers: hardware layer, operating-system layer and application layer.

Hardware layer: support TVOS’s DVB + OTT chip scheme (3716 c or Hi Ms6A801, etc.);

Operating-system layer, support TVOS optimization scheme of DVB functions;

Application layer: business applications developed based on TVOS interface (DVB broadcast, VOD on demand and other Internet applications, etc.).

In the construction of intelligent terminal's three layers, the interfaces should be docked with an open unified standard. Besides, the interfaces are independent of each other, and the change in any layer couldn't affect other layers. In the designing process, the designer should fully consider the scalability and portability to provide flexible choices for the later participated manufacturers to replace or change the products.

Hardware System of TVOS Intelligent Terminal

At present stage, TVOS intelligent terminal set-top box adopts Hi3716C V200OTP Gao'an dual-core chips, which is the DVB + OTT scheme of Huawei Hisilicon. Hi3716C chips should be docked with the peripheral of TVOS.

Hi3716C V200 OTP Gao'an chip integrates dual-core processor of high-performance Cortex A9. The processing performance of the above mentioned chip can satisfy the business needs with different kinds of differentiations. It supports high-definition videos of different formats, such as MPEG2 / h. 264 / AVS + / RealVideo8 / AP / 9/10 / VC - 1 VP6 / VP8. Besides, it supports high-performance H.264 HD encoding. Therefore, it can also meet the requirements of growing multimedia playback, visual communication and trans-coding among multi-screens. The chip integrates high performance 2 d / 3 d acceleration engine, thus it can provide customers with friendly human-computer interaction interface and rich game experience. Besides, in the above mentioned chip, there are kilo mega internet access in road 2 and internet access PHY in road 1, USB2.0 in road 3, independent SDIO3.0 in road 1 and various peripheral interfaces, which could provide people a flexible connection scheme. Gao'an's chip design of Hi3716C V200 OTP meets the demands of mainstream senior security applications.

Software Platform of TVOS Intelligent Terminal

NGB TVOS supports the standards of NGB's middleware, and it could download API that is standardized by CA (DCAS). Therefore, it is safe and can be controlled, and it could load the Java and HTML applications. The software architecture of NGB TVOS, according to the functional hierarchy from top to bottom, can be divided into five layers: application framework layer, the environment execution layer, functional components, Hardware Abstract Layer (HAL) and the Linux kernel layer.

First of all, NGB TVOS software architecture has proposed a resource management framework from the top to the bottom to realize the global efficient management of scarce resources in the system. Second, NGB TVOS software architecture has presented a security framework from top to bottom to solve the safety problems to realize the global prevention and control.

(1) Application framework layer

Combine and encapsulate the exposed ability of the underlying function components and simplify the invocation of application program to the underlying function components, thus to provide convenience for the application development.

(2) Execution environment layer

Software code is used to interpret real-time operation environment in execution process. NGB TVOS has provided both Java and Web applications to execute environment.

(3) Functional components layer

Software modules with relatively independent function exist in the form of background service system or static libraries. Functional components is the one to achieve the core function of NGB TVOS, and all the functional components are realized by C/C + + code to achieve higher efficiency

than Java, which is especially important for terminal boxes. Through the combination and encapsulation of the application framework, we could provide the exposed ability of functional components to the application program.

（4）Hardware Abstract Layer

Hardware Abstract Layer (HAL) means abstractly encapsulate the parts related to hardware platform, in this way to provide a unified API for the upper layer. And the lower layer could adjust the specific hardware and software platform, in this way to make it easy for TVOS to conduct cross-platform transplantation. And the encapsulation is mainly conducted on the following Hardware components: WiFi, camera, USB, audio decoder, video decoder, tuning demodulator, power manager and etc.

(5) Linux kernel layer

Linux is an open source operating system. Taking advantage of Linux kernel is the foundation of opening the smart TV terminal operating system.

Network security

In this scheme, we use the IP tables and Linux firewall strategy to realize the black and white filtering of IP list, and the concrete implementation method is as following: establish a black list form and white list in the system respectively, as long as the IP address existed in the white list, we should admit the access request, and any IP will not be dropped because of the increase of traffic. If there is an IP address is in the blacklist, then we should set the rules of the IP tables that this IP should DROP directly. In this condition, the IP access request will be rejected. In addition, if the connection times of certain IP address are too frequent, then we can temporarily add it to the list in the black-list table, and if there is need in future, we could restore its access to the IP service later.

Main process lies in establishing filter, NAT Rules and structure for the IP tables: IP tables - > tables - > Chains - > Rules. In a few words, tables are composed of chains, and Chains are composed of rules. The structure of the IP table as shown in figure 1:

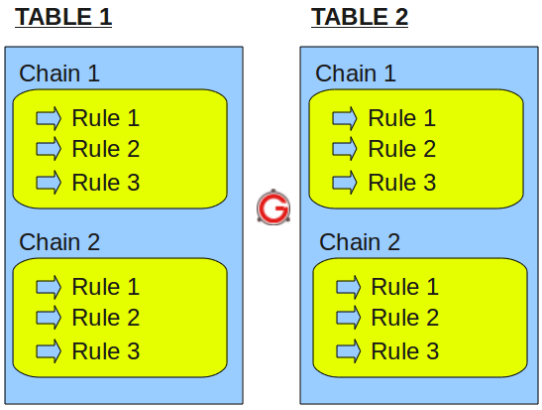

Figure 1 structure of IP tables

The key of the IP tables rules:

Rules include a condition and a target

If the rules meet the requirements, we should execute the rules or specific value of the target.

If the rules don’t meet the requirements, we should take the next rules into consideration。

Target Values:

ACCEPT – allow firewall receive packets

DROP – allow firewall receive packets

QUEUE – firewall transfer the packages to the user’s space

RETURN –firewall stop executing the current chain of the later rules, and return to the calling chain.

Some services in the system need to open ports to normal business visits, which would provide entrances to some programs with bad intentions, and lead to the insecurity of the system safety. To control and limit the service ports can, to a certain extent, reduce possibility of being attacked by the programs with bad intentions. Therefore, we could use the following method to achieve port control of the service interfaces.

①Use the minimum service sets and close all the services having nothing to do with business. In this way, we could narrow the port number of monitors. In the system, the best way to attack prevention is to run the software as few as possible. Besides, TVOS system could start the minimum service sets, and ban the services that are not needed in the system. In this way, we could, to the greatest extent, secure the safety of the system. And the default minimum service sets as shown in table 1:

service name
Service manager
Netd
Vold
Rild
Surfaceflinger
Drmserver
Mediaserver
Zygote

Table 1 The default minimum service sets in

②Control the ports of IP address segment. For ports that provide services, we should set IP address segment to allow accesses of viewers. If the IP address that has issued a request is in the illegal network segment, we should discard this request. Main method lies in establishing filter and NAT rules for iptables, and the method is just like establishing “black and white lists for IP address”.

（4）Network traffic monitoring

we should manage，count and conduct rights management towards network flow. And the scheme and detailed process are as follows:

① The system records the flow volume of each kind of application software and the time periods when people use the net work. Besides, the flow volume should be classified in accordance with the network connection type. We should add the statistical function in the protocol stack where the message is received, and use this function when we receive message. Based on the message sources, we can distinguish the network connection types, and the cumulated data packet length can be used to calculate out the traffic volume. We can separate message of each applications a part from the other by using the port number in the massage and the mapping the key of application of message. And while receiving message, we can accumulate the message respectively in accordance with the timestamp. In this way, we can count out the flow volume of each app of different time periods.

②Controlling based on the application of the networking modes

Providing the upper level interfaces, the user can freely choose applications access to the network according to use demand. In the protocol stack, we should add port and network equipment

binding function to the message sender. When the user is set as the network application mode that others have the access rights, and all ports in the applications should be bound with network equipment, and the message sent to the protocol stack, after being judged, should be sent from the network equipment link. If not, the processing procedures should be the same to each other.

③Record the used flow volume and the copy conditions of USB since the equipment was launched.

File copy records of USB device is achieved when we add filter function in the file-system-read and write functions. We should provide the upper interfaces and read traffic statistical file.

Conclusion

In the background that the traditional radio and television media and the new media accelerate the integration and fusion process, the demands of users on the integrated media of radio and film and requirements of new business are becoming more and more strict. And the rapid development of the new generation of information communication technology also would accelerate the development of intelligent terminal and television business. Therefore, only through constant evolution and optimization, could TVOS meet the demand of media integration development and the increasing users. At the same time, the continuous upgrading of TVOS technology is also the requirement and security of maintaining the core competitiveness of TVOS, promoting TVOS industry, promoting the ecological construction and speeding up the popularization of TVOS intelligent terminal TV and TVOS intelligent set-top boxes.

References

[1] Broustis I, Krishnamurthy S.A Multiband MAC Protocol for Impulse-based UWB Ad Hoc Networks.2nd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks(SENON): Academic Press,2008:231-236.

[2] Sun Tianze, Yuan Wenju. Embedded design and Linux driver development guide. Beijing: Publishing House of electronics industry, 2007

[3] Erwin, Li Yafeng Sheng. ARM embedded -Linux system development from entry to master. Beijing: Tsinghua University press, 2007

[4] Xue Hongquan, Yang Lin. Research and implementation of embedded smart home system with Internet. Modern electronic technology, 2007,03 (2): 26-31.

[5] M.Ghavami,L.B. Michael and R.Kohno, Ultra wideband Signals and Systems in Communication Engineering: Academic Press, 2007:175-179.