The Content Security Mechanism of Smart TV Broadcasting Operating System

Xin Wang

School of Electronic Information Engineering, Tianjin University, Tianjin, China
Email: pyhiloveyou@126.com

Received 5 November 2015; accepted 20 November 2015; published 25 November 2015

Abstract

Smart TV broadcasting system is an extensively deployed application which charges users based on their subscription. In Smart TV broadcasting service environments, services providers charge subscription fee by scrambling the programs in CAS. This technique abstain unauthorized televiewers to watch and receive the program. Smart TV malware presents significant threat to Homeland Security. Security for contents running on smart TV terminals is important. As a new smart TV operating system, SMART TV OS offers great flexibility not only for users but also for application developers. However, this flexibility exposes users to additional security threats. This is particularly dangerous for finance and healthcare applications which require high security for sensitive information and transactions. In this paper, we present the security mechanism of DCAS and the technology realization in SMART TV OS, a complete content protection system from head-end to terminal. It has all managements and authorization control functions of traditional CA, supporting DCAS terminal and traditional CA simultaneously.

Keywords

Security Model, NGB SMART TV OS, DCAS, DVB, Android

Subject Areas: **Information and Communication: Security, Privacy, and Trust**

1. Introduction

The NGB (Next Generation of Broadcast) Smart TV is a next generation television capable of transmitting, receiving and displaying a video stream. It provides access to on-demand gaming, home security, data services and digital music [1].

In Smart TV broadcasting, service providers charge subscribing fee by scrambling the program with a CAS (Conditional Access System) as well as controlling the illegal reception of the charged program [2]. Digital TV CAS has the history nearly 30 years. Most of the CA adopts the smart card way to decrypt and at the same time

How to cite this paper: Wang, X. (2015) The Content Security Mechanism of Smart TV Broadcasting Operating System. *Open Access Library Journal*, **2**: e2030. http://dx.doi.org/10.4236/oalib.1102030

carries out the binding of machine and card [3]. CAS protects not only on live TV but also on VoD, data broadcast TV, TV value-added services such as mail wallet etc [4].

With the rapid development of technology in the field of DTV, more and more service provides deliver different types of multimedia content ranging from free access programs to services such as Pay-TV, to satisfy the ever-increasing demands of the users [5].

At present, the integration of CAS has been covered to all aspects of STB chip, loader, middleware, applications; the extent of binding machine card has been growing [6].

This tightly bound meet the demand of the early development of content protection in digital TV, but, its limitation is more and more big, more and more prominent [7].

Terminal technology is closed and come to a standstill, can not form a horizontal market, and it is bad for the development of the industry [8]. Cable TV terminal morphology cannot expand to other terminals, limit died in set-top box [9].

It is particularly important to ensure the content security of NGB interconnection platform [10]. The content security model of traditional CA plus middleware is far from the demand of open smart TV platform [11].

In this background a longing with the mature of the security chip, the DCAS scheme which is based on software and hardware separation begins to attract the world's attention.

In this paper, we analyzed the DCAS security mechanism, security key model, security data management mechanism of smart TV, putting forward a DCAS security model and technology realization of smart TV terminal.

2. System Overview

The Cable broadcasting system consists of a headend transmitting content and the related information, Hybrid Fiber Coaxial (HFC) plant, and the user terminals receiving them [12]. In the headend, there are various systems including video encoders, CMTS, CAS and DCAS servers for providing broadcasting services through HFC plant [13]. In this paper, we analyzed the DCAS security mechanism, security key model, security data management mechanism of smart TV, putting forward a DCAS security model and technology realization of smart TV terminal.

DCAS is a complete content protection system from headend to terminal [4]. It has all managements and authorization control functions of traditional CA, supporting DCAS terminal and traditional CA simultaneously [14]. It can authorize the terminal by two-way channel and broadcast channel. The efficiency of authorization is high and the security of system is good [15]. The receiving terminal can download the client software through the DCAS, DCAS security mechanism using DCAS key mechanism, hardware and software security technology and security management, ensure the security of the whole broadcasting system. The DCAS key mechanism is consist of root key derivation, hierarchical key, security data management. The DCAS root key derivation make different DCAS system derive personalized root key based on the same terminal security chip, then the DCAS terminal can according to the DCAS client software which download from front end to realize decryption of the encrypted content of DCAS front end. The DCAS hierarchical key mechanism realize the authorization and trust among the DCAS terminal security chip, DCAS client software and DCAS front end through the handshake authentication function, ensure the security of transmission of hierarchical key. DCAS security data management mechanism ensure the security and neutrality of DCAS system by using the method of data distributed security management.

The DCAS system includes DCAS headend and the client terminals. The DCAS system consists of the DCAS headend, DCAS client software; security certification system; terminal security chip; DCAS application program interface terminal software platform; security chip production key management and separated security equipment.

3. The Security Design of DCAS System

The security design of DCAS uses DCAS key mechanism, software and hardware security technology to protect the DCAS headend and terminal and guarantee the whole security of DCAS from end to end.

The Smart TV OS have network interface, DCAS management module, the interface for memory access, filter interface, the interface of application communication, the interface of separated security device and the interface of hierarchical key.

The DCAS module is map to the Smart TV OS. The security chip of DCAS is map to the hardware level of Smart TV OS. The drivers of security chip of DCAS is map to the Linux cornel of Smart TV OS. The CA components and PKI of DCAS is map to the functional components layer of Smart TV OS. The API of DCAS is map to the execute environment layer of Smart TV OS. The DCAS manager is map to the application frame layer. The client of DCAS is map to the application layer of Smart TV OS.

The key model of smart TV terminal is consist of the root key derivation mechanism, hierarchical key mechanism, security data management of scrambling and descrambling mechanism.

The Root key derivation mechanism consists of the headend root key derivation and the terminal root key derivation. The head end of DCAS is adopted the security data and algorithms which provided by the manufacturer of terminal security chip and security data management platform, after deriving the root key from certain security chip of each terminal, it can work properly.

The terminal of DCAS adopts the software of client which provide necessary information for security chip.

The Hierarchical key mechanism include the function of multilayer key and handshake authentication function.

Multi key function refers to the control word layer by layer encryption in a hierarchical way, ensure the control word in use and transfer security. Generating key DCAS head-end system to control word layer encryption, terminal security chip receives the key layer decoding reduction control word, terminal security chip should support the three layer key mechanism.

Three key mechanisms is to ensure the control word transmitted in the terminal securely [5]. Three layer key mechanism by the root key K3 from the root key derivation module, followed by EK3 (K2) EK2 decryption, (K1), EK1 (CW) to obtain the control word descrambling necessary; at the same time, with the front end K2 send handshake information (nonce) and complete response is handshake authentication.

The Handshake authentication function is the validation of terminal security chip in the two-way system. Terminal security chip for authentication data received by hierarchical key in the key processing and return the results, DCAS headend to the terminal security chip results returned by the certification.

The Security data management mechanism is the central part of the DCAS key mechanism. The security information of decentralized management, the required headend and terminal root key derivation of information by the conditions of security data management platform.

The business of scrambling and descrambling mechanism is to realize the business data from the headend to the security terminal.

4. The Security Mechanism of DCAS Terminal Software

The Security Mechanism of Terminal Software

1) Bottom-up trusted chain

The DCAS client software security mechanism is based on a bottom-up trusted chain, software from the terminal security chip to start loading terminal software, software platform and the DCAS user end, build trusting chain using digital signature technology, only in the chain of trust to each link by signature verification, after a chain of trust links can start. DCAS client software in addition to the signature verification, in the operation should also be data security guarantee mechanism.

2) Start loading software certification

Start loading software before the operation by the security chip for the data source to verify the reliability and data integrity verification. Safety data management platform is responsible for the management of boot loader software signature.

3) Terminal software platform authentication

4) The DCAS client software verification.

Before the terminal software download and run by the boot loader software locally on the sources of data reliability and data integrity verification.

The DCAS client software needs to be sources of data reliability and data integrity verification by the terminal software before downloading and running. The DCAS client software to download according to application operators under the file access permissions to access terminal resources.

5) The data security of DCAS client software

The data of DCAS client software in the terminal, to guarantee the security of data storage, avoid because of abnormal power failure caused by factors such as loss of data.

Important data encryption storage, encryption handshake authentication mechanism can be used to encrypt the data.

5. The Security Mechanism of DCAS Terminal Hardware

The Security Mechanism of Terminal Hardware

The DCAS terminal hardware security mechanism is ensured by the terminal security chip.

1) The function of terminal security chip

Terminal security chip includes: OTP, root key derivation, hierarchical key descrambling and decoding module.

2) Terminal security chip work flow

Terminal security chip work flow: power on chip, OTP through ESCK and SCK built-in reduction function to generate SCK, and provide the root key derivation module, for generating the root key K3. Hierarchical key module receives the root key for decryption of K3 process and related key handshake authentication. Hierarchical key module consists of two functions: to enter the encryption key to realize hierarchical decryption; handle the handshaking information (nonce), and to generate the authentication response (DA (nonce)). The final decryption of CW obtained was sent to descramble and decoding module for business descrambling and decoding.

3) The work flow of decryption of security chip

Terminal security chip should follow the following procedure decryption scrambler business:

a) should receive encrypted EK3 (K2), the use of K3 to decrypt the ciphertext, and generate K2;

b) should receive encrypted EK2 (K1), the use of K2 to decrypt the ciphertext, and generate K1;

c) CW used to decrypt the scrambling operation.

EK3 (K2) said encrypted with the key K3 data K2.

EK2 (K1) said encrypted with the key K2 data K1.

EK2 (K1) said encrypted with the key K2 data K1.

EK1 (CW/Key) said encrypted with the key K1 data CW.

K3 is sent root key, length of 16 bytes.

K2 is used to decrypt K1 key, the length is 16 byte

K1 is used to decrypt CW key, the length is 16 bytes.

CW is for descrambling operation key, the length is 8 or 16 bytes.

4) Hierarchical key algorithm:

a) in the use of TDES algorithm, the key for every 7 bit after adding 1 bit redundant bits, 112 bit key up to 128 bits (16 bytes).

b) level key in AES refers to the FIPS defined in PUB 197 standard AES-128 algorithm, calculated using the 128 bit, model for the ECB.

6. The Technology Implementation of DCAS in SMART TV OS

6.1. The Interface of DCAS in SMART TV OS

The DCAS module is correspondence with the level of SMART TV OS.

The hardware of SMART TV OS is correspondence with the security chip of DCAS.

The Linux kernel of SMART TV OS is correspondence with the all kinds of drivers about security chip of DCAS.

The Functional components layer of SMART TV OS is correspondence with the PKI component and CA component of DCAS.

The Execute environment layer of SMART TV OS is responsible for abstract API from DCAS.

The Application framework layer of SMART TV OS is correspondence with the Conditional Access Manager of DCAS.

The Application layer of SMART TV OS is correspondence with the Client of DCAS.

6.2. The Management of DCAS

DCAS management is the core of the DCAS implementation of SMART TV OS [6].

CAS Module Manager is responsible for receiving program player events and accessing information related to current CA scrambling program, CAS Module Manger is selected according to the CA application of CA information; application management client for CA application for registration, so that CAS Module Manager is used in selecting the CA; each CA application client management service is responsible for the management of registration; the Chip Controller is responsible for local authentication. Descramber Context is responsible for the CA after descrambling data delivery to the security chip.

7. The Test Scheme of DCAS Security Chip

This program focuses on the functionality testing related to DCAS security chip, including the root key derivation, descrambling, handshake authentication.

7.1. Test Preparation

1) Prepared by the Chip manufacturers

The hardware platform which has installed the security chip need to be tested;

The software environment which is used to test the security chip;

The actual ChipID list used for test security chip;

The corresponding ESCK used for test security chip;

The corresponding Seedv used for test security chip (use Vendor_SysID = 0 to generate);

The reduction function of SCK;

The preliminary processing function of SCK;

The root key derivation function;

The corresponding tools for burning test platform for Bootloader;

The corresponding signature tool for Security chip;

The Bootloader file for test;

2) Prepared by the TA (Trust Authority)

The test stream contains at least 3 program streams. They are transparent program streams , the scrambling program stream which has 8 bytes control word contains 4 CW cycle, the scrambling program stream which has 16 bytes control word contains 4 CW cycle respectively.

The KeyLadder data which is generated using the AES algorithm, including EK3 (K2), EK2 (K1), EK1 (CW).

The KeyLadder data which is generated using the TDES algorithm, including EK3 (K2), EK2 (K1), EK1 (CW).

7.2. Test Content

1) Reading the chip ID

This test will verify the unique identifier (ChipID) reading function of security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the actual chip ID used to test the security chip provided by the chip manufacture.

The test step: starting the test platform; execute the operation of reading serial number of the security chip;

Compared the operation result whether consistent with the ID information provided by the chip manufacturers. Shutdown the test platform.

The expectation of the test is the chip ID reading from the test program is consistent with the known chip ID.

2) The program broadcast function when the CW is not encrypted

This test will verify the function of playing a transparent and scrambling streams by security chip. At the same time this test will verify the support ability to 8 byte and 16 byte control word by the security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively.

The test step: starting the test platform; Tuning to transparent program stream, tuning to the scrambling program stream, set 8 bytes control word, Tuning to the scrambling program stream 2, set 16 bytes control word and play. Shutdown the test platform.

The expectation of the test is the programs can be played normally.

3) Using the correct Vendor_SysID to play the scrambling program which the CW is encrypted by the AES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. Using the AES algorithm to encrypt the data, the security chip should be able to decrypt the scrambling program correctly. This test uses the Vendor_SysID which is used by the chip test specially, the value is 0.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and the AES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1 (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Shutdown the test platform.

4) Using the correct Vendor_SysID to play the program which the CW is encrypted by the TDES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. Using the TDES algorithm to encrypt the data, the security chip should be able to decrypt the scrambling program correctly. This test uses the Vendor_SysID which is used by the chip test specially, the value is 0.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and the AES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1 (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Shutdown the test platform.

5) Using the error Vendor_SysID to play the scrambling program which the CW is encrypted by the AES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. When input the error Vendor_SysID and the correct KeyLadder data, and the data is encrypted using the AES algorithm, the security chip should not be able to descrambling the encrypt program. This test uses the Vendor_SysID which is used by the chip test specially, the value is 0.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and the AES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1 (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Shutdown the test platform.

6) Using the error Vendor_SysID to play the scrambling program which the CW is encrypted by the TDES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. When input the error Vendor_SysID and the correct KeyLadder data, and the data is encrypted using the TDES algorithm, the security chip should not be able to descrambling the encrypt program. This test uses the Vendor_SysID which is used by the chip test specially, the value is 0.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and the TDES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1 (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program .Shutdown the test platform.

7) Using the correct Vendor_SysID and error KeyLadder data to play the scrambling program which the CW is encrypted by the AES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. When input the correct Vendor_SysID and error KeyLadder data, and the data is encrypted using the AES algorithm, the security chip should not be able to descrambling the encrypt program.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and the AES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1 (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the error Vendor_SysID and KeyLadder data, including EK3 (K2), EK2 (K1), EK1 (CW), playing the scrambling program .Shutdown the test platform.

8) Using the correct Vendor_SysID and error KeyLadder data to play the scrambling program which the CW is encrypted by the TDES algorithm.

This test will verify whether the security chip meet the keyladder function defined by the DCAS through broadcast by the scrambling program. When input the correct Vendor_SysID and error KeyLadder data, and the data is encrypted using the TDES algorithm, the security chip should not be able to descrambling the encrypt program.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; the Trust Authority provides the test stream, the stream contains at least 3 program stream, transparent program stream, the program stream which has 8 bytes control word contains 4 CW cycle scrambling, the program stream which has 16 bytes control word contains 4 CW cycle scrambling respectively. The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. Trust Authority according to the data provided by the chip manufacturers, using the correct Vendor_SysID (0) and error K1' and the TDES algorithm for generating KeyLadder test data, including EK3 (K2), EK2 (K1), EK1' (CW).

The test step: starting the test platform; Tuning to the scrambling program stream 1, set the correct Vendor_SysID and error KeyLadder data, including EK3 (K2), EK2 (K1), EK1' (CW), playing the scrambling program. Tuning to the scrambling program stream 2, set the correct Vendor_SysID and error KeyLadder data, including EK3 (K2), EK2 (K1), EK1' (CW), playing the scrambling program .Shutdown the test platform.

9) Using the correct Vendor_SysID and the AES algorithm to verify the handshake authentication.

This test will verify under the protection of AES algorithm the handshake authentication function of the security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. TA uses the correct Vendor_SysID (0) according to the data provided by the chip manufacturers and function, providing the handshake authentication of Nonce, and uses AES algorithm to check the return of the DA chip (Nonce).

The test step: starting the test platform; Set the correct Vendor_SysID (0), set the Nonce data used for handshake authentication. Check the DA (Nonce) data returned by the security chip. Shutdown the test platform.

10) Using the correct Vendor_SysID and the TDES algorithm to verify the handshake authentication.

This test will verify under the protection of TDES algorithm the handshake authentication function of the security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. TA uses the correct Vendor_SysID (0) according to the data provided by the chip manufacturers and function, providing the handshake authentication of Nonce, and uses TDES algorithm to check the return of the DA chip (Nonce).

The test step: starting the test platform; Set the correct Vendor_SysID (0), set the Nonce data used for handshake authentication. Check the DA (Nonce) data returned by the security chip. Shutdown the test platform.

11) Using the error Vendor_SysID and the AES algorithm to verify the handshake authentication.

This test will verify under the protection of AES algorithm the handshake authentication function of the security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. TA uses the error Vendor_SysID (0) according to the data provided by the chip manufacturers and function, providing the handshake authentication of Nonce, and uses AES algorithm to check the return of the DA chip (Nonce).

The test step: starting the test platform; Set the error Vendor_SysID (0), set the Nonce data used for handshake authentication. Check the DA (Nonce) data returned by the security chip. Shutdown the test platform.

12) Using the error Vendor_SysID and the TDES algorithm to verify the handshake authentication.

This test will verify under the protection of TDES algorithm the handshake authentication function of the security chip.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide the ESCK, Seedv, and SCK reduction function, SCK preliminary processing function and the root key derivation function corresponding for the security chip test. TA uses the error Vendor_SysID (0) according to the data provided by the chip manufacturers and function, providing the handshake authentication of Nonce, and uses TDES algorithm to check the return of the DA chip (Nonce).

The test step: starting the test platform; Set the error Vendor_SysID (0), set the Nonce data used for handshake authentication. Check the DA (Nonce) data returned by the security chip. Shutdown the test platform.

13) Right Bootloader signature data, starting security verification.

This test will verify the security starting function of the security chip under the right signature of bootloader.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide relevant tools for burning Bootloader of the test platform; The chip manufacturers provide the corresponding signature tool of the security chip for testing and the Bootloader file. The chip manufacture should ensure the OTP area has been configured to enable security startup function state. TA uses the BLK1 which is signed by BLK0 to sign the Bootloader.

The test step: using the BLK1 which is signed by BLK0 to sign the Bootloader. Burning the bootloader which has been signed to the test platform. Starting the test platform; Shutdown the test platform.

The platform should be able to start properly.

14) Error Bootloader signature data, starting security verification.

This test will verify the security starting function of the security chip under the right signature of bootloader.

The test environment: the hardware platform which has been installed the chip to be tested provided by the chip manufacture; the software environment which has been used to test the chip provided by the chip manufacture; The Chip manufacturer provide relevant tools for burning Bootloader of the test platform; The chip manufacturers provide the corresponding signature tool of the security chip for testing and the Bootloader file. The chip manufacture should ensure the OTP area has been configured to enable security startup function state. TA uses the BLK1 which is signed by BLK0 to sign the Bootloader.

The test step: using the BLK1 which is signed by BLK0 to sign the Bootloader. Burning the bootloader which has been signed to the test platform. Starting the test platform; Shutdown the test platform.

The platform should not be able to start properly.

8. Conclusion

In this paper, we present DCAS, a complete content protection system from headend to terminal. It has all managements and authorization control functions of traditional CA, supporting DCAS terminal and traditional CA simultaneously. DCAS security mechanism using DCAS key mechanism, hardware, software security technology and security management ensures the content security of the whole broadcast system.

References

[1] Berger, B.J., Bunke, M. and Sohr, K. (2011) An Android Security Case Study with Bauhaus. 2011 18*th Working Conference on Reverse Engineering*, Limerick, 17-20 October 2011, 179-183. http://dx.doi.org/10.1109/wcre.2011.29

[2] Rohrer, F., Feleke, N., Zhang, Y.T., Nimley, K., Chitkushev, L. and Zlateva, T. Android Security Analysis and Protection in Finance and Healthcare. Boston University MET.

[3] Chen, D.L., Li, Z., Wang, Y., Zhao, L.F. and Zhang, D.J. (2013) The Main Technical Characteristics and Software Architecture of NGB SMART TV OS. *Radio and Television Information*, National Academy of Broadcasting Science, 2013-10.

[4] NGB SMART TV OS1.0 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, M.M. and Zhu, Y.B. (2012) To Explore the Implementation Model and Techniques of Intelligent Television Terminal Security under NGB Environment. *Radio and TV Technology*, 10.

[7] Ning, H., Li, W., Wang, K. and Lei, M.Y. (2012) Research on Intelligent Terminal Security System. *Modern Telecommunication Technology*, 5.

[8] Mai, H.H., Pek, E., Xue, H., King, S.T. and Madhusudan, P. Verifying Security Invariants in Express OS. University of Illinois at Urbana-Champaign.

[9] National Academy of Broadcasting Science. The Security Framework of NGB SMART TV OS1.0 V1.2.20131224.

[10] Wang, X., Chen, D.L., Sun, Y., Wang, X. and Yao, S.Y. (2014) Security Control for SMART TV OS. 2014 2*nd Asian Pacific Conference on Mechatronics and Control Engineering*.

[11] Wang, X., Yao, S.Y., Wang, X., Chen, D.L., Sun, J., Hua, Z. and Wang, D.F. (2014) SMART TV OS Content Security Analysis and Protection in Smart TV. 2014 2*nd International Conference on Mechatronics and Control Engineering*.

[12] Wang, X., Chen, D.L., Sun, Y., Wang, X. and Yao, S.Y. (2014) The Security Model of Broadcast Illtelligent Terminal Application and Technology Realization on SMART TV OS. 2014 2*nd International Conference on Mechatronics and Control Engineering*.

[13] Yoon, E.-J. and Yoo, K.-Y. (2011) ECC-Based Key Exchange Protocol for IPTV Service. 2011 *International Conference on ICT Convergence* (*ICTC*), Seoul, 28-30 September 2011, 547-552. http://dx.doi.org/10.1109/ictc.2011.6082658

[14] Liu, B.F., Zhang, W.J. and Jiang, T.P. (2004) A Scalable Key Distribution Scheme for Conditional Access System in Digital Pay-TV System. *IEEE Transactions on Consumer Electronics MAY*, **50**, 632-637.

[15] You, W., Lee, J., Cho, Y. S., Kwon, O.-H. and Lee, S. I. (2004) Design and Implementation of DCAS User Terminal. *IEEE Transactions on Consumer Electronics MAY*.