International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.1204

(08/2020)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Smart TV operating system

The security framework of a smart TV operating system

Recommendation ITU-T J.1204

Recommendation ITU-T J.1204

The security framework of a smart TV operating system

Summary

Recommendation ITU-T J.1204 defines the security framework of a smart television operating system (TVOS) to enable integrated broadcast and broadband (IBB)-capable cable set-top box (STB) and TV to apply to broadcasting services and IP-based interactive services provided by cable television operators and third-party providers. By running the smart TV operating system, the IBB capable STB and TV will be able to provide subscribers with advanced and personalized services by downloading and installing advanced and personalized apps from cable operators' platforms and third-party platforms, which are interconnected with the related cable operators' platforms.

Recommendation ITU-T J.1204 intends to specify the smart TV operating system security framework, which exploits the popular hardware based trusted execution environment (TEE) technology and has multiple security defence capabilities.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T J.1204	2020-08-13	9	11.1002/1000/14357

Keywords

Security framework, smart TV operating system, smart TVOS.

[*] To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T J.1204

The security framework of a smart TV operating system

1 Scope

As described in the smart TV operating system requirement [ITU-T J.1201], the smart TV operating system can support both traditional TV services and IP-based TV services such as over the top (OTT) services. As such, the security of the smart TV operating system is very important.

This Recommendation intends to specify the smart TV operating system security framework, which exploits the popular hardware based trusted execution environment (TEE) technology and has multiple security defence capabilities.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T J.205] Recommendation ITU-T J.205 (2012), *Requirements for an application control framework using integrated broadcast and broadband digital television*.

[ITU-T J.1201] Recommendation ITU-T J.1201 (2019), *Functional requirements of a smart TV operating system*.

[ITU-T J.1202] Recommendation ITU-T J.1202 (2019), *The architecture of a smart TV operating system*.

[ITU-T X.509] Recommendation ITU-T X.509 (2019) | ISO/IEC 9594-8 (2020), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 integrated broadcast and broadband (IBB) DTV service [ITU-T J.205]: A service that simultaneously provides an integrated experience of broadcasting and interactivity relating to media content, data and applications from multiple sources, where the interactivity is sometimes associated with broadcasting programmes.

3.1.2 television operating system (TVOS) [ITU-T J.1201]: A system software running on IBB-capable cable STB and TV which is capable of managing hardware, software and data resources of the IBB-capable cable STB and TV, supporting and controlling the application software execution.

3.1.3 rich execution environment (REE) [ITU-T J.1201]: A hugely extensible and versatile operating environment which brings flexibility and capability.

3.1.4 trusted execution environment (TEE) [ITU-T J.1201]: A secure area of the main processor in an IBB-capable cable STB and TV to ensure that sensitive data is stored, processed and protected in an isolated and trusted environment. It offers isolated safe execution of authorized security software providing end-to-end security by enforcement of protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.

3.1.5 secure OS [ITU-T J.1202]: An operating system running in trusted execution environment (TEE) which is used to trigger secure execution of applications within the TEE.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 security chip: A chipset with security functions such as secure key storage, secure key deriving and key ladder processing, etc.

3.2.2 SETVOS: A mandatory access control model based on the television operating system (TVOS) kernel, which implements sandbox isolation, access control and other security mechanisms to improve the overall security of TVOS.

3.2.3 BootRom: A small read-only memory or write protected flash memory embedded in the chip. It contains the first boot code that the chip executes when powered on or reset.

3.2.4 sandbox: A security technology which confines a software process to run in an environment restricted by an operating system.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DTV	Digital Television
ECC	Elliptic Curves Cryptography
ESCK	Encrypted Security Chipset Key
IBB	Integrated Broadcast and Broadband
IPC	Inter Process Communications
NVM	Non-Volatile Memory
OS	Operating System
OTP	One-Time Programmable
OTT	Over The Top
REE	Rich Execution Environment
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman

SHA	Secure Hash Algorithm
SMC	Secure Monitor Call
SVP	Secure Video Path
TEE	Trusted Execution Environment
TVOS	Television Operating System
UI	User Interface

5 Conventions

In this Recommendation:

The phrase "**is required to**" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformity with this document is to be claimed.

The phrase "**is recommended**" indicates a requirement which is recommended but which is not absolutely required. Thus this requirement needs not be present to claim conformity.

The phrase "**is prohibited from**" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformity with this document is to be claimed.

The phrase "**can optionally**" indicates an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformity with this Recommendation.

In the body of this Recommendation and its annexes, the words *shall*, *shall not*, *should*, and *may* sometimes appear, in which case they are to be interpreted, respectively, as *is required to*, *is prohibited from*, *is recommended*, and *can optionally*. The appearance of such phrases or keywords in an appendix or in material explicitly marked as *informative* are to be interpreted as having no normative intent.

6 Overview

This Recommendation defines the television operating system (TVOS) security framework, which is a security hierarchy made of three security environments of rich execution environment (REE), trusted execution environment (TEE) and hardware based on the TVOS security architecture and mechanism. The TVOS security architecture defines the attribution of basic security capabilities to each security environment and how each security environment leverages the basic security capabilities that it has as well as the composition of each basic security capability of hardware, software, network, data and application within each security environment. The TVOS security mechanism defines how different security environments with various basic security capabilities work together jointly to build up the overall TVOS security and functionalities.

REE is the first security line of defence for TVOS, which directly faces to various Apps such as device user interface (UI) and security breaches through user interactions, etc. It is most vulnerable in terms of security among these three environments. It has to rely on the security computing and processing done within TEE and the hardware security as the security root provided by the hardware environment through TEE to guarantee that its security level is strong enough. As it requires the least security resources, it is most flexible in terms of expanding security capabilities and providing security services to different applications running on top of TVOS. It is also most adaptable to the hardware platform on which TVOS is running.

TEE is the middle security defence line and can make use of the hardware security as the security root by using its secure OS, which is separate and different from the operating system kernel within REE, through the security HAL between TEE and secure hardware environment. TEE directly works with and supports REE by implementing all the core security computing and processing relevant to any security computing and processing of the basic security capabilities within REE through the security communication interface between REE and TEE. As it requires more security software and hardware resources than REE, it is less flexible in providing a security service than REE, but it still has limited ability to expand its support for highly secured service by adding support for more trusted applications. Comparing to REE, it is also less adaptable to the hardware platform on which TVOS is running.

The security hardware environment is the last security line of defence and is the security root of TVOS. It is the strongest among the three security defence lines in terms of the security level, and makes TVOS security unbreakable unless the security hardware is compromised in terms of security. But it is also the least flexible in providing the security support, as once the hardware platform of a secure chip is made and used by TVOS, its security cannot be expanded. All the critical keys and cipher algorithm engines are embedded in the hardware environment. REE and TEE rely on the security resources provided by the hardware security within this environment according to the security requirement of related services and when necessary.

7 Security architecture

The TVOS security architecture, as shown in Figure 1, describes how basic capabilities form the REE, TEE and hardware security.

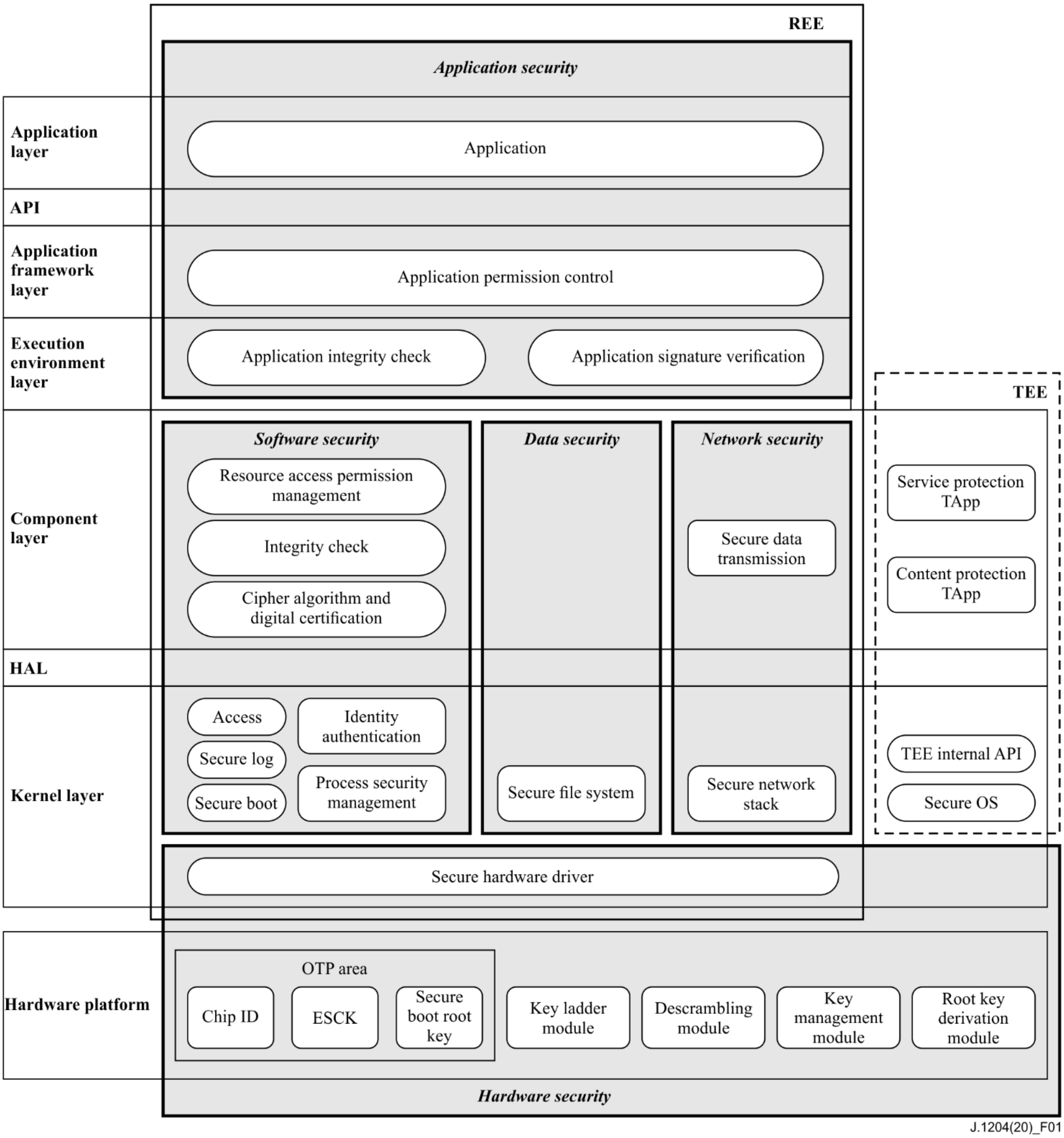

Figure 1 – Basic security architecture

The TVOS basic security architecture should integrate and collaborate with TVOS hardware security, software security, network security, data security and application security capabilities based on the TVOS software architecture and security mechanism to form defence-in-depth TVOS security functions.

The TVOS hardware security capabilities provide support for the building of basic security capabilities such as software security, network security, data security, and application security. The basic security capabilities such as software security, network security, and data security should be built based on the hardware basic security capabilities and provide support for the building of application basic security capabilities. The application basic security capabilities should be built based on the basic security capabilities such as software security, network security, and data security.

7.1 REE security

The TVOS REE security should provide software security, network security, data security and application security capabilities based on the hardware security. REE communicates with TEE through the security mechanism to complete service protection and content protection.

7.2 TEE security

The TVOS TEE as defined in [ITU-T J.1202] is a trusted and secure computing environment including trusted and secure hardware and software.

The TVOS trusted and secure hardware supports the security chip, secure memory access control, secure bus connection, secure interruption, secure clock, secure random number, secure encryption and decryption engine, and secure video path (SVP).

The TVOS trusted and secure software includes the secure OS and TEE HAL. The secure OS provides the memory management, secure time, task scheduling, interruption, task communication, and encryption and decryption functions, and supports memory isolation, version anti-rollback, secure storage, and dynamic TApp loading. The TEE HAL is a hardware abstract layer API to support various trusted applications such as DRM TApp and DCAS TApp.

7.3 Hardware security

The TVOS should provide hardware security capabilities for the implementation of the TVOS software security, network security, data security, and application security based on the security chip. These hardware security capabilities should include secure a storage area, security trust root, and a hardware cipher algorithm engine.

8 Basic security capabilities

TVOS overall security is based on various basic security capabilities. These basic capabilities cooperate to secure the software and hardware environments, and to secure the device functionalities.

Hardware security, which includes the storage, booting and cipher security, is the capabilities built inside hardware. It is the foundation of software security.

Software security manages the resource access and verification.

Network security, data security and application security are the capabilities at an upper layer, to secure the application functionalities.

8.1 Hardware security

8.1.1 Secure storage area

The secure storage area should support one-time programmable (OTP) storage for important secure information such as chip ID and secure boot root key.

8.1.2 Secure boot root trust

As the security information is in the non-writable secure storage area of the security chip, the hardware security trust root is used as the trust root of the security trust chain check mechanism for secure system boot, secure system software upgrade, and secure application software downloading and installation.

8.1.3 Hardware cipher algorithm engine

The hardware cipher algorithm engine implements various cipher algorithms in the hardware level to ensure key security. It should support following cipher algorithms:

- Symmetric cryptographic algorithm such as DES as defined in [b-NIST-FIPS-46-3] and AES as defined in [b-NIST-FIPS-197]
- Asymmetric cryptographic algorithm such as RSA as defined in [b-IETF RFC 8017] and ECC as defined in [b-IETF RFC 6090]
- Hash algorithm such as SHA-256 as defined in [b-NIST-FIPS-180-4].

8.2 Software security

The TVOS software security should guarantee the security of system resources (including hardware, calculation, and data) controlled by TVOS when TVOS is running.

The TVOS software security includes resource access permission management, cipher algorithm and digital certification, access control, identity authentication, secure log, process security management, and secure boot.

8.2.1 Resource access permission management

The security framework of TVOS should control and manage resource access permissions as well as save and query information about the application of resource access permissions. The security framework of TVOS should require that all the subjects' accessing to the resource objects must be clearly permitted based on the SETVOS permission control mechanism. The subjects refer to specific processes when TVOS is running. The resource objects include the inter process communications (IPC) channels, files and network hosts, etc. The subject's permission to access the resource object should be determined by the security context defined by the security policies. A subject is associated with an object by a unique security context. During running, the access control relationship between the access subjects and the resource objects must not be modified.

8.2.2 Cipher algorithm and digital certification

The cipher algorithm in the security framework of TVOS should be implemented by calling the hardware cipher algorithm engine.

The digital certification is a kind of cipher algorithm, which can encrypt and decrypt information, digital signature and signature verification, and ensure the security and integrity of information.

Based on the digital certification, the security framework of TVOS should check the authentication and authorization of applications when applications are being installed and run.

8.2.3 Access control

The security framework of TVOS should have an access control mechanism for TVOS software modules and applications to access data files, operate on device resources and invoke certain software modules. The access control mechanism allows TVOS software modules and applications to access data files, operate on device resources and invoke software modules only when the software modules and applications have respective right to access permissions for the corresponding data files, device resources and software modules. With this mechanism, TVOS can also prevent the software modules and applications from obtaining sensitive security data, performing unauthorized operations, invoking unauthorized software modules, and executing unauthorized intrusion code. The security framework of TVOS should support the SETVOS secure access control mechanism.

8.2.4 Identity authentication

The TVOS identity authentication capability should provide a user authentication function and prohibit illegal users from entering the system.

The TVOS identity authentication capability should implement the following functions:

- Provide user operating APIs such as creating user, deleting user in the TVOS system.
- Check password complexity when creating user or changing password.
- Storing password in irreversible encrypted format.

8.2.5 Secure log

The TVOS secure log should save the system information when system faults and/or important system events are happening.

The TVOS secure log capability should implement the following functions:

- Register system faults callback in the TVOS system.
- Provide APIs for other module to write log and read log.
- Save the log to non-volatile memory (NVM).

The TVOS secure log function should be automatically invoked when system faults are detected and processed. Every TVOS module can also write important events to secure log by calling secure log APIs.

8.2.6 Process security management

The TVOS is a multi-process system. The process security management capability should manage the system processes to prevent abnormal processes consuming resources or illegal processes attacking the system.

The TVOS process security management capability should implement the following functions:

- Detect and kill abnormal process in the TVOS system.
- Trace the root privilege process in the TVOS system.
- Reset the TVOS system if the system cannot recover.

The TVOS process security management function should be invoked automatically when the TVOS system is started up.

8.2.7 Secure boot

The TVOS should implement secure boot from the chip, bootloader to the TVOS software based on the hardware security and security mechanism, ensure the safe running of the TVOS software, and protect the system software from being tampered with.

Secure boot is implemented based on the secure chip. The secure boot trust chain starts with the secure chip, passes through the terminal bootloader, TVOS secure OS, TVOS kernel, other TVOS software and finally arrives at the TVOS applications. Each link of the trust chain can be started only after the digital signature verification is passed.

The secure boot process is as follows:

1. After the system is powered on, the BootROM loads the bootloader.
2. The bootloader loads the TVOS TEE and creates the secure memory.
3. The bootloader loads the TVOS REE.

The software loading and boot at each level should pass the validity and integrity security check of the digital certificate trust mechanism. A link can be started only after it passes the security check, and then the next link can enter the check status. The system can be started only after all the links pass the security check. Check failure of any link causes system start failure.

8.3 Network security

The TVOS network security should include secure network stack and secure data transmission.

8.3.1 Secure network stack

The TVOS secure network stack should support functions including anti-DDOS attack, anti-ARP spoofing, IP address blacklist and whitelist, service port access control list (ACL), network traffic management and statistics.

8.3.2 Secure data transmission

The TVOS should be able to guarantee the network communication security including data security through network transmission and network intrusion prevention.

8.4 Data security

The TVOS should be able to guarantee the security of data generated when the system software and application software are running.

The TVOS should be able to safely store data using the secure file system and support the file handle random allocation, file system security management, file system kernel module check, file integrity check, data encryption and decryption algorithms, and anti-rollback mechanism of key data, ensuring that the user data is not maliciously leaked and tampered with and protecting the security-sensitive information.

8.5 Application security

The TVOS application security should include application signature verification, application integrity check and application permission control.

8.5.1 Application verification

The applications running on TVOS should be verified before installation, upgrading and loading.

The application signature verification should verify the application by using the security trust chain check mechanism during installation or upgrading the application to prevent illegal applications being installed into the TVOS system.

The TVOS application signature verification capability should implement the following functions:

- Preinstall application verification certification in the TVOS system.
- Include the signature files in the application installation package.
- Provide signature verification function in the TVOS component layer.
- Provide application installation API in the application framework layer.

The signature verification function should be invoked with the application installation API when installing or upgrading applications.

The application integrity check should verify the application software before loading and running to prevent illegal applications running in the TVOS system.

The TVOS application integrity check capability should implement the following functions:

- Preinstall application integrity checking certification in the TVOS system.
- Include the integrity checking signature files in the application installation package.
- Provide integrity check function in the TVOS component layer.

The integrity check function should be invoked by the application management component when it starts loading and running applications.

8.5.2 Application permission control

The TVOS application permission control should configure the application permissions during application installation and control the permissions based on the permission configuration when the application running in the TVOS system.

The TVOS application permission control capability should implement the following functions:

- Include the permission configuration file in the application installation package.
- Provide permission management component based on access control mechanism in the TVOS component layer.

The application permission control function should be invoked by the application which calls the application installation API when it starts installing or upgrading applications. When TVOS application is running, the permission management component should manage and control the application permissions according to the permission configuration.

9 Security mechanism

The basic security capabilities use the TVOS security mechanism, which includes digital certificate security trust mechanism, security trust chain check mechanism, security storage mechanism and REE/TEE communication mechanism.

9.1 Digital certificate security trust mechanism

The digital certificate security trust mechanism should support hierarchical security trust verification based on the ITU-T X.509 specification as defined in [ITU-T X.509]. The security trust verification at each level should use the digital certificate of the corresponding level.

9.2 Security trust chain check mechanism

The security trust chain check mechanism should use the digital certificate security trust mechanism to check the validity and integrity of software at each level of the trust chain. The trust chain starts from the security chip and contains the bootloader, OS, and application software.

In the trust chain, software at each level should be cryptography signed. The software at a certain level should use the key pre-configured in the software at the previous level of the trust chain to step-by-step implement security verification. The bootloader should use the key embedded in the security chip.

9.3 Security storage mechanism

Security storage mechanism is to verify and protect the stored data from being accessed or modified illegally. The read or write access must be authorized, and the data must be verified before it is used.

9.4 REE/TEE communication

There are some mechanisms to communicate between REE and TEE such as:

1. SMC

   When the processor executes the secure monitor call (SMC), the core enters secure monitor mode to execute the secure monitor code.

2. GP TEE client APIs

   It provides the open session, invoke command, and close session API which sends a SMC to communicate between REE and TEE. The TEE interfaces accessed by the client APIs from the REE must go through the predefined commands by the invoke command API.

   TVOS applications such as DRM App and DCAS App can use Java or Web application programming interfaces which encapsulates the GP TEE client APIs to communicate with the trusted applications such as DRM TApp and DCAS TApp.

3. RPC

   The remote procedure call (RPC) command is used to communicate between TEE and TEE supplicant. The TEE supplication would help TEE to perform the file system access and the TApp loading.

9.5 Sandbox isolation security

An application sandbox should be built for each TVOS application based on the TVOS software architecture and basic security architecture. Each TVOS application sandbox should be built by the corresponding TVOS application process. The application process is defined by the corresponding TVOS application, application execution environment, as well as the functional interface unit instances at the TVOS application framework layer and client instances of functional components invoked by the TVOS application. The security of the TVOS application sandbox can be reinforced as required by using the TVOS basic security capabilities and security mechanism.

A component sandbox should be built for each TVOS functional component based on the TVOS software architecture and basic security architecture. Each TVOS component sandbox should be built by the corresponding TVOS component process. The component process is defined by the corresponding server of the TVOS functional component, client instances of other functional components invoked by the server, and instances of the HAL functional interface units. The security of the TVOS component sandbox can be reinforced as required by using the TVOS basic security capabilities and security mechanism.

The TVOS applications and functional component modules should comply with the TVOS sandbox isolation security architecture, as shown in Figure 2.

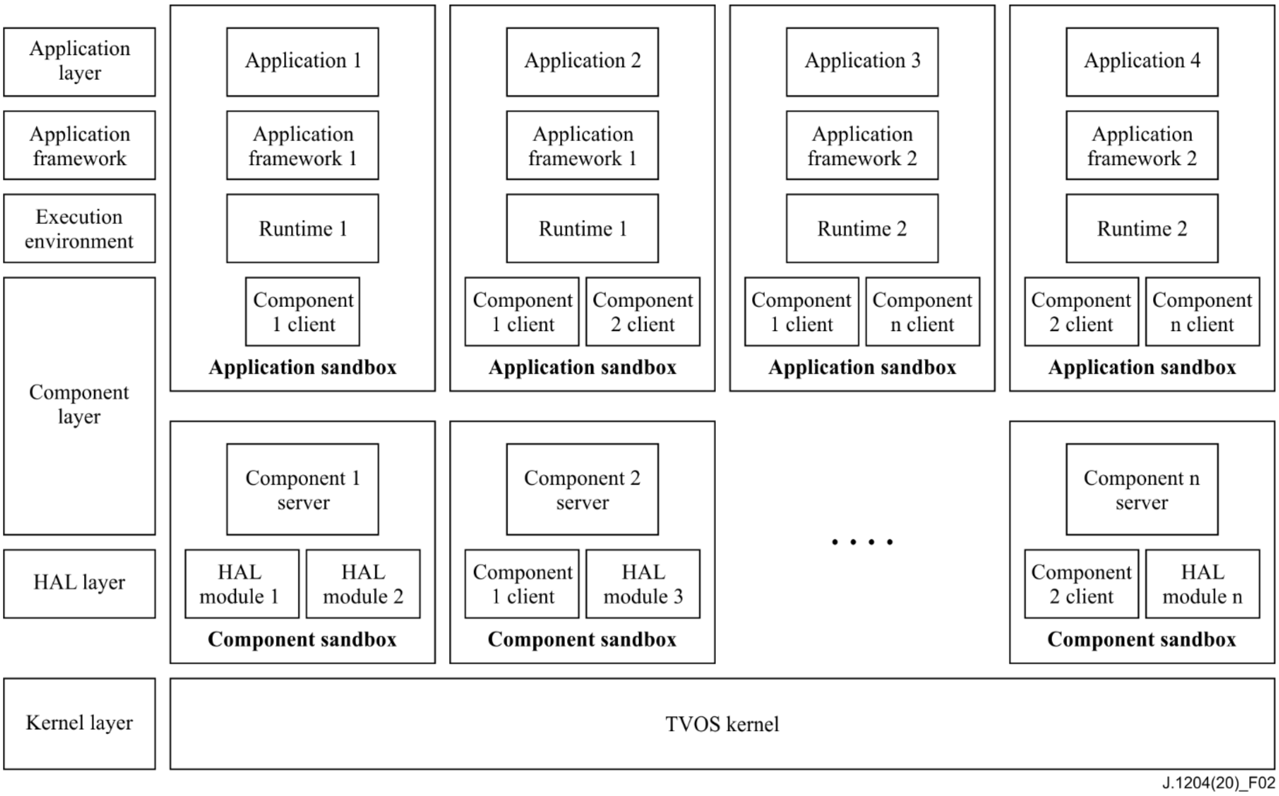

Figure 2 – Sandbox isolation security architecture

10 Security functions

10.1 Content security

The TVOS should guarantee the security of media content based on the basic security capabilities and security mechanism and ensure that the media content is safely played according to the license of the media content.

The TVOS content security should provide the DRM security trust chain based on the TVOS security mechanism and hardware trust root. The hardware based secure authorization of the media content, secure decryption, secure decoding, and secure playing and output are implemented by using the secure storage and management mechanism of the keys, secure decryption and security storage mechanism of the authorization information, and SVP protection methods.

10.2 Service security

The TVOS should guarantee the security of media content flow based on the basic security capabilities and security mechanism and ensure that the media content flow is safely played according to CA authorization of the media content flow.

The TVOS service security should provide the DCAS security trust chain based on the TVOS security mechanism and hardware trust root. The hardware based secure authorization of the CA service, secure decryption and descrambling, secure decoding, and secure playing are implemented by using the DCAS root key derivation, secure key storage and management, data decryption and secure storage, and SVP protection methods.

10.3 Secure upgrade

The TVOS should ensure the validity and integrity of the upgrade software package based on the hardware security and security mechanism and ensures the security of the remote upgrade and local upgrade of the system software.

The secure upgrade of the TVOS system should perform a security check based on the security trust chain check mechanism. Only the TVOS system packages that pass the security check are allowed to be upgraded. Rollback is forbidden for TVOS system upgrade.

10.4 Miscellaneous security functions

Some of the TVOS basic security capabilities can also work as TVOS security functions such as data security, network security, application security, and secure boot.

10.4.1 Data confidentiality

The TVOS should guarantee the confidentiality of data based on the basic security capabilities and security mechanism and ensure the data during transmission, storage and use.

TVOS provides a secure computing environment, secure key storage and management, data decryption and secure storage based on REE security, TEE security and hardware security.

10.4.2 Resource protection

TVOS supports full life cycle of resource protection when a subject accesses an object, a particular resource, with four steps including identification, authentication, authorization and accountability.

In order for any subject to access an object, TVOS defines and establishes the identifications for the subjects to access resources. The identification is used for identifying the identity of a subject to access an object.

The first step for any subject to access an object is the authentication, which requires the subject prove to the system that it is the permitted subject. After successful authentication, the system must decide whether the subject is authorized to access the particular resource and what actions it is permitted to perform on the respective resource.

The TVOS identity authentication capability should provide user authentication function and prohibit illegal users from entering the system.

The second step for a subject to access an object is the authorization which uses the identity of the subject together with other criteria to make a determination of operations that a subject can carry out on objects.

The security framework of TVOS should require that all the subjects' accesses to the resource objects must be clearly permitted based on the SETVOS access control mechanism.

The third step for a subject to access an object is the accountability which audits logs and monitoring information to track subject activities with objects.

The TVOS secure log should save the system information when system faults and/or important system events happen.

Bibliography

[b-GP-TEE] GlobalPlatform Device Technology TEE Client API Specification (V1.0), GlobalPlatform Device Technology (GP); *API specification between applications running in a rich operating environment and the applications residing in the Trusted Execution Environment (TEE)*.

[b-IETF RFC 6090] IETF RFC 6090 (2011), *Fundamental Elliptic Curve Cryptography Algorithms*.

[b-IETF RFC 8017] IETF RFC 8017 (2016), PKCS #1: *RSA cryptography specifications version 2.2*.

[b-NIST-FIPS-46-3] NIST FIPS PUB 46-3 (1999), *Data Encryption Standard (DES)*.

[b-NIST-FIPS-180-4] NIST FIPS PUB 180-4 (2015), *Secure Hash Standard (SHS)*.

[b-NIST-FIPS-197] NIST FIPS PUB 197 (2001), *Specification for the Advanced Encryption Standard (AES)*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020