symmetry

MDPI

Article

How to Obtain Common Criteria Certification of Smart TV for Home IoT Security and Reliability

Sooyoung Kang and Seungjoo Kim *

CIST (Center for Information Security Technologies), Korea University, Seoul 02841, Korea; bbang814@gmail.com

* Correspondence: skim71@korea.ac.kr; Tel.: +82-2-3290-4897

Received: 31 July 2017; Accepted: 25 September 2017; Published: 17 October 2017

Abstract: In the new era of IoT (Internet of Things), numerous gadgets and services include innovative IoT technologies that provide customers with convenience and improve their quality of life. Smart TVs are typical IoT devices that offer broadcasting services. However, they are susceptible to security intrusions via e-mail, media players, cameras, and internet connectivity. The frequency of hacking through malicious applications installed in Smart TV has rapidly increased. Therefore, appropriate countermeasures should be developed immediately. In April 2017, we (with LG electronics) received the 'world-first' Common Criteria EAL2 (Evaluation Assurance Level 2) certification for Smart TVs. As far as we know, no Smart TV has received a Common Criteria EAL2 security certification until now. This article describes our experience with the certification process and examines several security and reliability aspects of Smart TVs.

Keywords: IoT (Internet of Things); Smart TV; Common Criteria; security; reliability

1. Introduction

Smart TVs are typical products used in a home IoT environment that allow installing and running applications, connecting to internet, playing games, connecting to video calls, and enjoying broadcast services. However, since Smart TVs are connected to the Internet and public networks, they can be easily exposed to cyberattacks. If Smart TVs are hacked, a user's private information can be compromised, and the reputation of the company that manufactures the product can be negatively impacted [1,2].

In March of 2017, WikiLeaks (a global exposure site) announced that the US CIA (Central Intelligence Agency) and UK MI5 (Military Intelligence Section 5) intercepted general users' information by installing malware on Smart TVs and smartphones manufactured by global companies. Since Smart TVs contain data closely related to end-users, private information can be potentially exposed through security intrusions. As a countermeasure against hacking and to ensure security and reliability, Smart TVs may be certified under the Common Criteria, an international standard (International Organization for Standardization/International Electrotechnical Commission 15408) to evaluate information technology security [3].

Common Criteria consists of Part 1, Part 2, and Part 3, which respectively present the Common Criteria outline, Security Functionality Requirements (SFRs), and Security Assurance Requirements (SARs). Part 2 consists of 11 classes that define the SFRs, and Part 3 consists of 8 classes that define the SARs. Part 3 contains the Evaluation Assurance Level (EAL) classification from EAL1 to EAL7 [4]. A higher EAL widens the assurance scope of the evaluation target, thus further ensuring security and reliability.

In April 2017, we (with LG electronics) received the 'world-first' Common Criteria EAL2 certification for Smart TVs. As far as we know, no Smart TV has received a Common Criteria EAL2 security certification. Although only one Smart TV product has been previously evaluated under EAL1, EAL1

only provides the most basic security and reliability assurance. This article describes our experience with the EAL2 certification process and examines several security and reliability aspects of Smart TVs.

1.1. Acronyms

Common Criteria (CC) use acronyms and terms that are not commonly used. Acronyms used in CC [4] are listed in Table 1.

Table 1. Table of acronyms.

Acronyms	Description
ADV	Assurance DeVelopment Class
AGD	Assurance Guidance Documents Class
ALC	Assurance Life-Cycle Support Class
ARC	Security ARChitecture
ASE	Assurance Security Target Class
ATE	Assurance Teste Class
AVA	Assurance Vulnerability Analysis Class
CC	Common Criteria
CCDB	Common Criteria Development Board
cPP	Collaborative Protection Profiles
CCRA	Common Criteria Recognition Arrangement
CMC	Configuration Management Capabilities Component
CMS	Configuration Management Scope Component
DEL	Delivery Component
EAL	Evaluation Assurance Level
FAU	Security AUdit Function Component
FCS	Cryptographic Support Function Component
FDP	User Data Protection Function Component
FMT	Security ManagemenT Function Component
FPT	Protection of the TSF Function Component
FTP	Trusted Path/channels Function Component
FSP	Functional SPecification Component
iTC	International Technical Community
OPE	OPErational User Guidance Component
OR	Observation Report
PRE	PREparative Procedures Component
SAR	Security Assurance Requirement
SD	Supporting Document
SFR	Security Function Requirement
ST	Security Target
TDS	TOE DeSign
TOE	Target Of Evaluation
TSFI	TOE Security Function Interfaces
PP	Protection Profile

1.2. Related Works

The size of the Smart TV and total TV markets is gradually increasing, and Display Search, a market researcher, indicated that sales of Smart TVs will increase to 121.1 million units in 2017 and 118.1 million units in 2018 [5]. However, Smart TVs that are commonly used in homes are not usually armed with security threat defense systems. Therefore, they can be vulnerable to security intrusions, and actually several hacking incidents have been reported [6–8].

In August 2013 at one of the most famous hacking conference Black Hat USA, SeungJin (Beist) Lee and Seungjoo Kim announced a vulnerability in a Smart TV application store and network interface. The authors debugged many messages through the Smart TV's UART (Universal Asynchronous Receiver/Transmitter) port and analyzed ARM code using an IDA (Interactive DisAssembler) tool. The analyzed messages included booting logs, exception messages, segmentation messages with register values, and so on. After hacking the device, the authors were able to secretly record using the on-board camera and then posted the recorded videos live on the Internet. The hacked Smart TV platform used a Linux-based operating system, and therefore, vulnerabilities found in the Linux or

Android kernel could also be detected in the Smart TV platform. This is a good demonstration of an actual occurrence of hacking [9,10].

In October 2013 at the RSA (Rivest, Shamir, Adleman) Conference Europe, security threats and the various attack scenarios for Smart TVs were announced from a hacker's perspective. After the paper was released, more security vulnerabilities were found, and security patches were expedited. This resulted in an improvement in the security of Smart TVs [11].

Research on Smart TV forensics began in 2013. A paper published in DIPECC (Digital Information Processing, E-Business and Cloud Computing) 2013 described digital forensics to scientifically recover digital evidence. The author presented various problems and technical challenges facing Smart TV forensics [12].

This has become a foundation for research on Smart TV forensics and also contributed to the development of appropriate security measures to protect users' privacy, information, and assets [13,14]. In October 2014 at the Journal of the KIISC, Heesoo Kang, Minsu Park, and Seungjoo Kim announced the first experimental case study on Smart TV forensic [15].

In September 2014 at the ICCC (International Common Criteria Conferences), Minsu Park et al. proposed a security evaluation criteria (called as Protection Profile) to define the common security requirements for Smart TVs. Based on the general structure of Smart TVs, the authors developed the PP by deriving security threats and SFRs for the SDK (Software Development Kit), operating system, and hardware. Their paper included 23 security requirements for FAU, FCS, FDP, FMT, FPT, and FTP. Although it did not attempt to acquire PP certification officially, it became a good example evaluation for Smart TVs and similar products [16].

In August 2016, Samsung Electronics, one of Korea's leading companies, acquired Common Criteria EAL1 certification for their Smart TV. Samsung Smart TV's System Integrity Monitoring, Web App Protection, Data Encryption/Decryption, Phishing Site Blocking, and Update Server Communication functions were designated according to Target Of Evaluation (TOE). Their EAL1 certification was acquired in compliance with 15 security functional requirements among the components of protection class for password, data protection, and security management and TOE security function. The evaluation was carried out through the basic level functional tests with ST, development related function specification, manual, configuration management submission, and test books including all contents. This first Smart TV Common Criteria certification has become a good case study [17].

As I said in the above, the paper published in September 2014 [15] attempted to develop PP, but failed to obtain Common Criteria certification. Therefore, till now, there is no official Smart TV PP.

We have derived four PPs similar to smart TVs: PP [18] for General Purpose Operating Systems which have similar structures and features of Smart TV kernels; PP for Mobile Device Fundamentals [19] which have similar characteristics for downloading and installing applications on mobile devices; Application Software PP [20] which have similar characteristics for DRM function; and PP for Application Software [21] which have similar characteristics for general application.

2. Our Certification Process

The Common Criteria is an international standard (ISO/IEC 15408) to evaluate and certify products' IT security. Common Criteria evaluation and certification are based on both documentation and products. The documents include a PP that defines the common requirements for each product group and the ST that defines the requirements for a specific product.

CC is divided into different levels (from EAL1 to EAL7) depending on the scope of assurance. A higher level of assurance indicates higher security and reliability. Current Smart TVs only have CC certification for the lowest level (EAL1), which requires manual and general functional testing only.

Since the 2015 revision of the CCRA agreement, the mutual recognition scheme has changed from being based on EAL to base on a joint Protection Profile cPP. The mutual recognition level also changed from EAL4 to EAL2, and the highest level of international mutual recognition was EAL2. Therefore, our level of assurance was determined to be EAL2 to certify a Smart TV.

EAL1 consists of general functional testing while EAL2 consists of structured testing with the developer. Therefore, EAL2 has a higher assurance scope and higher assurance level. EAL2 provides an understanding of the TOE and assurance based on documents such as the interface specification, manual, and TOE design description that outlines the security function. If a PP exists, conformance can match the PP assurance level.

2.1. EAL2 Analysis and Requirements

EAL2 assurance requirements fall into six categories. During the submission development phase, the ARC describes the security of the TOE. To describe the secure initialization process, we explained the secure booting process for the Smart TV and sand boxing for an application installed on Smart TV to indicate that the security architecture is separate. A countermeasure against vulnerabilities is described through static analysis during TOE development. The developer removes a vulnerable function, code, or logic and also proves that there is no bypass path through the application.

The FSP describes the purpose, method of use, parameters, and parameter descriptions for all TSFIs. Additionally, for SFR-enforcing TSFIs, the developer has to describe SFR-enforcing actions and direct error messages. The TOE design submission describes the interaction in a subsystem view to describe the completeness and accuracy of the subsystem.

PRE and OPE describe that the deployment target changes to a developer team by targeting part of the Smart TV to the TOE. The TOE is delivered securely to the development team to describe all installation, management, and use. The configuration management submission describes the correct delivery, installation, and management of the configured version when it is distributed to the development team in the same way as a manual submission. The delivery submission describes the process and method through which the TOE is securely transferred to the development team.

Security Target describes TOE by threats, security objectives, SFRs, SARs, and TOE security functions that occur in TOE [22–25].

The test submission contains the tests conducted based on all TSFIs in TOE. The test results describe whether APIs constituting the TOE operated as designed.

The vulnerability analysis submission explores all the known vulnerabilities on Smart TVs and describes the results of fuzzing tests to determine potential vulnerabilities.

The security assurance requirements and submission s to satisfy EAL2 are shown in the Table 2.

Table 2. EAL2 Assurance Requirements and Submissions.

Class	Component	Description	Submissions
ADV	ADV_ARC.1	Security architecture description	Security architecture submission
	ADV_FSP.2	Security-enforcing functional Specification	Functional specification submission
	ADV_TDS.1	Basic design	TOE design submission
AGD	AGD_OPE.1	Operational user guidance	Manual submission
	AGD_PRE.1	Preparative procedures	
ALC	ALC_CMC.2	Use of a CM system	Configuration management submission
	ALC_CMS.2	Parts of the TOE CM coverage	
	ALC_DEL.1	Delivery procedures	Delivery submission
ASE	ASE_CCL.1	Conformance claims	Security Target
	ASE_ECD.1	Extended components definition	
	ASE_INT.1	ST introduction	
	ASE_OBJ.2	Security objectives	
	ASE_REQ.2	Derived security requirements	
	ASE_SPD.1	Security problem definition	
	ASE_TSS.1	TOE summary specification	
ATE	ATE_COV.1	Evidence of coverage	Test submission
	ATE_FUN.1	Functional testing	
	ATE_IND.2	Independent testing—sample	
AVA	AVA_VAN.2	Vulnerability analysis	Vulnerability analysis submission

2.2. Security Target

In Common Criteria, PP defines common requirements for each product group while the ST document defines the requirements for specific production. A Smart TV does not have official PP. Therefore, we created a Security Target [22] based on similar PPs [18–21]. Threats and Security Objectives defined by each PP mapped to the roles of Kernel, Mobile Device, DRM (Digital Rights Management), and Application of Smart TV are shown in Table 3.

In order to provide security and reliability for the Smart TV, we selected three assets to be protected [26]. Since Asset 3 is a particularly important asset in the TOE, it was added at the request of the evaluator.

Asset 1. Smart TV assets

Smart TV assets are service executable binary files, libraries, configuration files, device files, and so on that are provided by the smart TV. An application was installed on the smart TV to access these assets if necessary.

Asset 2. Applications

Applications are stored in the application execution path (read-write file system), including execution files, source files, and contents files of each application.

Asset 3. TOE execution files and configuration files

TOE execution files and configuration files are included in Smart TV asset.

Security functions to protect assets are as follows.

- DRM Verification

DRM verification for applications installed on Smart TVs is a very important feature. An application installed on a Smart TV provide DRM functionality. When it is executed, it confirms it is a normal application and is executed normally through DRM. To protect the content, encrypted audio and video streams are decrypted and executed only when released by DRM. The DRM verification function is a good way to improve the reliability of the Smart TV through one more verification at runtime, even if a malicious application is installed on a Smart TV.

To perform the DRM function, it is necessary to communicate with an external IT entity (DRM verification server) and provide confidentiality and integrity in the communication channel. Besides, for Common Criteria certification, we also made and submitted a document including the security key generation function, cryptographic key exchange function, and cryptographic key destruction function used in DRM.

To provide the DRM verification function, the protocol between the components is shown in Figure 1.

(1) The Web App requests DRM Service to create DRM Client with load () method. The load () method requires DRM type and App ID.
(2) The DRM Service creates DRM Client instance and returns its ID to Web App with a callback function.
(3) The DRM Service sends to Return DRM Client ID to Web App.
(4) The Web App uses sendDrmMessage () method to give DRM message to a DRM client. DRM message holds credential information in DRM message format.
(5) The DRM Service sends Credential Information to DRM Client.
(6) The DRM Client verifies DRM message and returns the result to Web App with a callback function.
(7) The Web App gives a content target, DRM Client ID, and playback options to Media Pipeline with video element and mediaOption Parameter.
(8) The Media Pipeline gets the credential information from DRM Client.

(9) The Media Pipeline sends Request Key to License Server.
(10) The License Server sends Return Key to Media Pipeline.
(11) The Media Pipeline gets the License Key from the License Server. Media Pipeline requests it with credential information.
(12) The Content Server sends encrypted stream to Media Pipeline.
(13) The Media Pipeline decrypts DRM content stream with License Key and plays decrypted content stream.
(14) The DRM Client must be removed with unload () method before unloading the App.
(15) The DRM Service removes DRM Client.

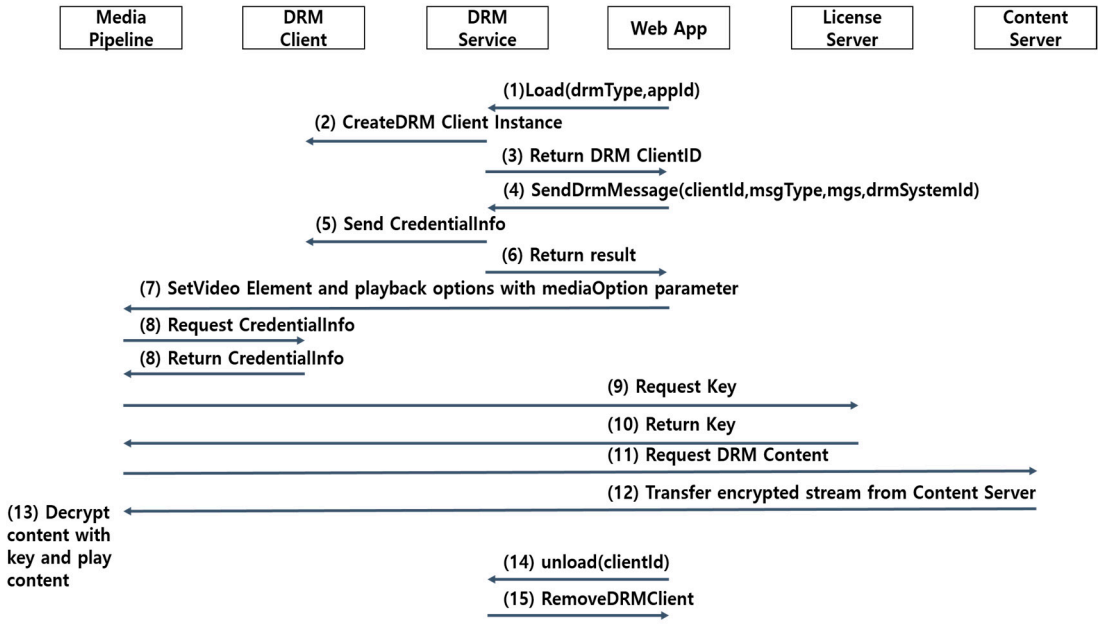

Figure 1. DRM verification protocol.

- Sandboxing

Various applications are installed in Smart TVs by users, and a malicious application with a virus may infect other applications, resulting in user information leaks or invasion of privacy. Sandboxing is used for each application to protect directory and file access by restricting file system access through chroot to allow the application to run only within a limited file system. This results in a more secure environment by controlling the access path of the application thorough a symbolic link to a specific device link. It also provides a copy of the library with limited functionality due to partial use of the original libraries, thus preventing malicious code from infecting the application. This structure was described in the ARC. The vulnerability was tested for security, and this structure can be utilized not only in Smart TVs, but also in other products where applications are installed and used.

- Backdoor detection

Products with kernels are often built and installed using firmware, and Smart TV software is also developed using the Linux kernel. We looked for ways to maintain and update the firmware. If an error occurs in a Smart TV or in the distributed firmware, a developer can access the Smart TV and update the firmware or correct the error. This process requires a path for the engineer to access the firmware. Previously, the firmware could be accessed via a dongle, but a dongle could be pointed out as a backdoor. So we removed the approaching path with dongle and enhanced the access path. When evaluating products with similar structures in the future, the backdoor should be removed.

Table 3. Comparing PP of Similar Products.

PP Name	Protection Profile for General Purpose Operating Systems [18]	Protection Profile for Mobile Device Fundamentals [19]	Application Software Protection Profile (ASPP) [20]	Protection Profile for Application Software [21]	Smart TV Security Target [22]
Date	9 March 2016	17 September 2014	10 November 2014	22 April 2016	19 April 2017
EAL	EAL1	EAL1	EAL1	EAL1	EAL2
Function	Kernel	Mobile Device	DRM	Application	Smart TV
Threat	T.NETWORK_ATTACK	T.NETWORK Network Attack	T.PLAINTEXT_DATA_SPOOFING	T.NETWORK_ATTACK	T.Modifying App Package File
	T.NETWORK_EAVESDROP	T.EAVESDROP Network Eavesdropping	T.PLAINTEXT_DATA_SPOOFING	T.NETWORK_EAVESDROP	T.Modifying App Package File
	T.LOCAL_ATTACK	—	T.KEYING_MATERIAL_COMPROMISE T.KEYSPACE_EXHAUST T.PLAINTEXT_COMPROMISE T.TSF_FAILURE T.UNSAFE_AUTHFACTOR_VERIFICATION	T.LOCAL_ATTACK	T.Unauthorized Access To Other App's Execution Domain
	T.LIMITED_PHYSICAL_ ACCESS	T.PHYSICAL Physical Access	T.UNAUTHORIZED_DATA_ACCESS	T.PHYSICAL_ACCESS	T.Unauthorized Access To Smart TV Assets
	—	T.FLAWAPP Malicious or Flawed Application	—	—	T.Unauthorized App Installation T.Modifying App Package File
	—	T.PERSISTENT Persistent Presence	—	—	T.Unauthorized Access To Smart TV Assets
	—	—	—	—	T.App Copyright Infringement
Security Objectives	O.ACCOUNTABILITY	O.AUTH Authorization and Authenticatio	O.AUTHORIZATION, O.DATA_AUTHENTICATION	—	O.App Package File Verification O.App Contents Protection
	O.INTEGRITY	O.INTEGRITY Mobile Device Integrit	—	O.INTEGRITY	O.App Contents Protection
	O.MANAGEMENT	O.CONFIG Mobile Device Configuration	O.WIPE_MEMORY O.SAFE_AUTHFACTOR_VERIFICATION	O.MANAGEMENT	O.App Access Control
	O.PROTECTED_STORAGE	O.STORAGE Protected Storage	O.KEY_MATERIAL_PROTECTION O.FEK_SECURITY O.PROTECT_DATA	O.PROTECTED_STORAGE	P.Secure Key Operation Management
	O.PROTECTED_COMMS	O.COMMS Protected Communication	—	O.PROTECTED_COMMS	O.App Contents Protection O.App Access Control P.Secure Smart TV Update
	—	—	—	O.QUALITY	P.Secure Key Operation Management P.Secure Smart TV Update

- Open source

Open source software is available for free to download, modify, and distribute. Since this freely share up-to-date technology, as well as problems and solutions, it has the advantage in its fast development, and in the initial development cost being lower than new development cost. Since open source mainly uses open formats or protocols, it is essential to have for an IoT environment or ubiquitous environment where various devices can be connected to each other through a network. Open source development is relatively stable because direct development and debugging is done by excellent developers around the world. Many bug fixes can be used to provide reliability and stability in the source code [10].

In Smart TVs, open source is used for communication with trusted entities, encryption/decryption of data stored internally, generation and exchange of encryption keys, and configuration of the TOE. We thought that open source was sufficient to acquire EAL2 assurance, and this was proven at the time of evaluation. However, due to a lack of documentation in open source design, it took a long time to produce a systematic description.

2.3. Test and Analysis

A lack of experience in evaluating existing Smart TVs made it difficult to acquire reference materials, tools, and evaluation methods. In particular, there was very little information about testing methods and tools. We surveyed the test methods to test Smart TVs. Practical security testing involves four methods, as shown in Figure 2 [27]. Functional testing checks whether the function works well, works according to the specification, and properly responds to errors during execution. This test was performed during the ATE evaluation. The vulnerability test checks whether the target product is safe from all the known vulnerabilities. This test was performed during the AVA evaluation. Penetration tests involve a mock hack against the target product, and this depends upon the analyst's experience. This test was performed during AVA evaluation.

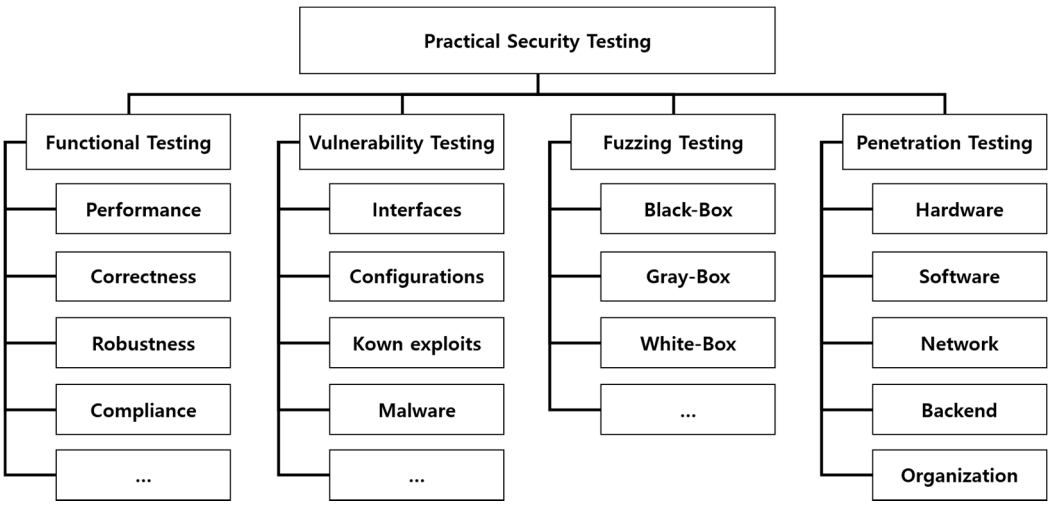

Figure 2. Classification of Practical Security Testing Methods.

Because there were no known tools for testing Smart TVs, the evaluator selected the fuzzing test to detect potential vulnerabilities and the evaluator requested us to develop a fuzzing tool for Smart TV. A fuzzing testing is a test that randomly generates and inputs arbitrary values to detect residual vulnerabilities. The fuzzing test is suitable to detect potential vulnerabilities not found during normal QA (Quality Assurance) testing or developer testing to verify undefined areas.

Our Smart TV consists of web OS-based firmware with a mobile operating system running the linux kernel, ans its source code calls many APIs. Therefore, our fuzzing test was mainly performed for the APIs. A fuzzing test tool was directly developed and verified by the evaluator.

3. Lessons Learned

3.1. Lack of Previous Evaluations

Our Smart TV evaluation started in December 2016 and lasted until April 2017 to obtain certification. If the evaluation is the first for a product group, the certification authority must verify the capability of the evaluators through the Certification Capability Verification process. During the Certification Capability Verification period, the evaluator should investigate and review issues that can be arose in using the target product. The evaluator then obtains a certification indicating sufficient capability to evaluate the target product. The evaluator should describe the systematic assessment methods used to evaluate the product, including known vulnerabilities, hacking case studies, countermeasures, evaluation techniques, and evaluation methods. Since this evaluation was the first attempt for Smart TVs with EAL2, it took about 1.5 months to obtain the Certification Capability Verification before commencing the actual evaluation. Therefore, the evaluation period can take about 1.5 to 2 months longer than expected due to the capability certification. So an evaluation plan for new product should consider the period needed for Certification Capability Verification. If the complexity of the evaluation suite increases or if there are many security threats, the Certification Capability Verification period may be even longer.

Furthermore, said before, the lack of experience in evaluating Smart TV has also made it very difficult to acquire reference materials, tools, and evaluation methods. Thus the evaluator requested us to develop something new to test a Smart TV.

3.2. Evaluation Assurance Level Decision

All of the topics on CC is discussed and defined by the Common Criteria Recognition Arrangement (CCRA) with the ISO/IEC international standards. The PP includes SFRs and SARs for each product family. It is developed to reflect the characteristics of each country's products. A total of 175 PPs are listed in the Common Criteria portal site. Efforts from each country have contributed to the development of a methodology to verify the security of IT products. However, the organization does not respond quickly to changes in new technologies, and this has raised issues to develop different security requirements for each country. Accordingly, CCRA's Common Criteria Development Board (CCDB) has formed the International Technical Community (iTC). Through participation with experts from each country, we are developing Supporting Document (SD) to support collaboration PP and cPP.

Since the CCRA agreement was revised in 2015, the EAL-based mutual recognition scheme also changed to a cPP-based mutual recognition scheme. The mutual recognition level changed from EAL4 to EAL2. The highest possible rating for mutual recognition is EAL2, which is the highest rating recognized internationally.

We had many discussions internally to determine the appropriate evaluation assurance level when planning and commencing Smart TV CC certification acquisition. And finally we decided that EAL2, the highest level of mutual recognition, is the most suitable for our case, because LG Smart TVs are distributed globally.

In addition, digital signatures, DRM verification, and sandbox technology are used to provide protection for the Smart TV assets, so it is necessary to perform structural testing for each subsystem. For this structural test, the EAL2 package conformance was considered to be appropriate. Therefore, our submissions were mapped to components according to the EAL2 package.

3.3. Simple design of security module

A Smart TV consists of modules that perform general functions and modules to provide security functions. TOE components consist of SAM, WAM, Security Manager, Jailer, and OpenSSL. Several modules are built into one firmware and are mounted on the Smart TV. If there are many modules, the complexity may be high. Therefore, for modules that perform security functions, the complexity should be minimized because a simple design can reduce the possibility of including faults that result in vulnerabilities [28]. Simple design is to develop modules separately for each security function. To enhance security with a simple design, the inside of the TOE should have a well-structured design. When the internal TOE is well-structured, general function changes will not affect security functions so that the product can be maintained without introducing faults.

3.4. Life Cycle—Configuration management and Delivery

Unlike general security software products, Smart TVs have very different production, development, and delivery processes. In particular, large development companies with high market share are outsourcing to a very large number of global suppliers in order to develop their products such as Smart TV. Thus the large development companies should manage all the outsourcing companies involved in development and prove that all the delivery is secure. To securely deliver software or firmware, the communication channel must be encrypted to provide confidentiality and integrity. A securely delivered recipient must verify the software or firmware version and verify that the version is correct.

Also Smart TVs are produced in domestic and overseas factories after conducting all development processes, including receiving requirements, development, and quality assurance. The source code is built as firmware and is delivered to the factory for mass production when QA passes. It is then loaded into Smart TVs and distributed to the customers. These complex processes should be described in the configuration management documentation to be submitted for evaluation. However, it is very difficult to describe each role because there are many teams in charge that are physically separated from overseas workshops and local factories. Also, when Common Criteria evaluation is performed for the first time, it is necessary to conduct a security check for the development environment. It takes time and money to interview and check all of the organizations involved in the configuration management and delivery.

Furthermore, in the usual case, the manuals (PRE, OPE) and the configuration management submissions (CMC, CMS, DEL) should describe the delivery process to the consumer. However, since our TOE was not a whole product but some parts only related to the security of Smart TV, TOE was delivered not to the customer but to the development team in the company, and so we had to rewrite the whole PRE, OPE, and ALC-related submissions.

3.5. Certification Process Resources

When the evaluator starts an evaluation, the evaluator grasps the TOE based on the ST and ADV class submissions. They understand the TOE scope and security functions through ST and the TOE design and structure through TDS and ARC. They then derive the TSFI through FSP and describe the interaction of each subsystem and interface. AGD classes PRE and OPE are used to install and operate the TOE. The tests are conducted based on a submission of the ATE class. The vulnerability is then checked by submitting the AVA class.

During this process, we reviewed the consistency of the submissions. If traceability and completeness were unsatisfactory or if the description is incorrect, OR was created and sent to the developer. Developers must modify their submissions simultaneously to provide traceability and completeness of the documentation. Since the OR should be revised until the 5th working day, there was a lack of resources to cope with the development of TOE at the same time due to a modification of all submissions and OR.

In general, a household appliance development company lacks a security engineer who performs CC or security as compared to a security production development company. For the company which prepares CC certification for the first time, the security engineer is much more lacking, and this can result in the certification delay. Therefore, it is recommended to revise submissions and prepare the TOE development resources sufficiently to have a smooth evaluation process before starting the evaluation.

4. Conclusions

In a home IoT environment, Smart TVs that are close to users increasingly require security and reliability. When a Smart TV is hacked, a user's sensitive information may be leaked and the invasion of privacy may occur because Smart TVs are connected to the Internet and have cameras. In addition, when user's payment information stored in Smart TV for shopping and contents purchasing is hacked, financial damage may occur. Therefore, the security and reliability of Smart TVs should be improved.

One of the best method to improve security and reliability is to obtain CC certification following ISO/IEC 15408. The existing CC certification is EAL1 passing only the basic functional tests. However, security threats continue to increase, so we have acquired the world's first EAL2 CC certification through structural testing for security and reliability.

Here, we have shared our case of a LG Smart TV obtaining EAL2 certification. The world's first EAL2 certification process presented in this study is novel and will add great value to the field of Smart TV security. This study can also be used as a good reference for future security and reliability studies of home appliances. We will study a single modularity of security platforms that can be applied to various home appliances in the future.

Acknowledgments: This research was supported by the Korea University Grant (K1711171).

Author Contributions: Sooyoung Kang: Research for related works, Smart TV analysis, write evaluation submissions, CC certification acquisition, and drafting of the article. Seungjoo Kim: Total supervision of paperwork, review, comments, assessment, etc.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mustafa, A.; Jacob, J. Adapting the Cloud-COVER threat modelling tool to cover threats for the Internet of Things. In Proceedings of the Eighth York Doctoral Symposium on Computer Science and Electronics, York, UK, 28 October 2015.
2. Ding, G.; Birgitta, L.; Gunnar, M.; Andler, S.F. Towards threat modeling for CPS-based critical infrastructure protection. In Proceedings of the 22nd International Emergency Management Society (TIEMS) Annual Conference, Rome, Italy, 30 September–2 October 2015; Volume 22.
3. Wikileaks. Available online: https://wikileaks.org/ (accessed on 20 September 2017).
4. *Common Criteria Recognition Arrangement, Common Criteria for Information Technology Security Evaluation*; Version 3.1; Revision 4; Centre for Cellular & Molecular Biology (CCMB): Telangana, India, 2012.
5. All Things Apple. Available online: https://technology.ihs.com/ (accessed on 20 September 2017).
6. Seigneur, J.M.; Jensen, C.D.; Farrell, S.; Gray, E.; Chen, Y. Towards security auto-configuration for smart appliances. In Proceedings of the Smart Objects Conference, Grenoble, France, 15–17 May 2003; Volume 2003.
7. Bachy, Y.; Frédéric, B.; Vincent, N.; Eric, A.; Mohamed, K.; Jean-Christophe, C.; Pierre, L. Smart-TV security analysis: Practical experiments. In Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Rio de Janeiro, Brazil, 22–25 June 2015.
8. Benjamin, M.; Karpow, A. Watch and be watched: compromising all Smart TV generations. In Proceedings of the IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2014.
9. Lee, S.; Seungjoo, K. Hacking, surveilling and deceiving victims on Smart TV. In *Blackhat*; Legendary Entertainment: Burbank, CA, USA, 2013.
10. Shankar, K.S.D.; Helmut, K. Certifying open source-the Linux experience. *IEEE Secur. priv.* **2004**, *2*, 28–33. [CrossRef]

11. Raimund, G. How hackers are outsmarting Smart TV's and why it matters to you. In Proceedings of the Rsa Conference Europe, Amsterdam, The Netherlands, 29–31 October 2013.
12. Al Falayleh, M. A review of Smart TV forensics: Present state & future challenges. In Proceedings of the International Conference on Digital Information Processing, E-Business and Cloud Computing (DIPECC), Dubai, UAE, 9–11 April 2013.
13. Sutherland, I.; Huw, R.; Konstantinos, X. Forensic analysis of Smart TV: A current issue and call to arms. *Digit. Investig.* **2014**, *11*, 175–178. [CrossRef]
14. Sutherland, I.; Xynos, K.; Read, H.; Jones, A.; Drange, T. A forensic overview of the LG Smart TV. In Proceedings of the 12th Australian Digital Forensics Conference, Perth, Australia, 1–3 December 2014.
15. Heesoo, K.; Minsu, P.; Seungjoo, K. (The First Experimental) Study on Smart TV forensics. *Korea Inst. Inf. Secur. Cryptol.* **2014**, *24*, 851–860.
16. Minsu, P.; Heesoo, K.; Jaeki, K.; Seungjin, L.; Seungjoo, K. Developing a protection profile for Smart TV. In Proceedings of the 14th International Common Criteria Conference, New Delhi, India, 9–11 September 2014.
17. *Samsung Smart TV Security Solution V1.0 Security Target V1.5*; Version 1.5; International Transplant Skin Cancer Collaborative (ITSCC): Milwaukee, WI, USA, 2016.
18. *Protection Profile for General Purpose Operating Systems*; Version 4.1; Significant Revision; National Information Assurance Partnership (NIAP): Columbia, SC, USA, 2016.
19. *Protection Profile for Mobile Device Fundamentals*; Version 2.0; National Information Assurance Partnership (NIAP): Columbia, SC, USA, 2014.
20. *Application Software Protection Profile (ASPP)*; Version 1.0; National Information Assurance Partnership (NIAP): Columbia, SC, USA, 2014.
21. *Protection Profile for Application Software*; Version 1.2; National Information Assurance Partnership (NIAP): Columbia, SC, USA, 2016.
22. *Application Security Solution V1.0 for LG webOS TV Security Target V1.5*; Version 1.5; National Information Assurance Partnership (NIAP): Columbia, SC, USA, 2017.
23. Amini, A.; Jamil, N.; Ahmad, A.R.; Zaba, M.R. Threat modeling approaches for securing cloud computing. *J. Appl. Sci.* **2015**, *15*, 953–967.
24. Di, J.; Scott, S. A hardware threat modeling concept for trustable integrated circuits. In Proceedings of the 2007 IEEE Region 5 Technical Conference, Fayetteville, AR, USA, 20–22 April 2007.
25. Kornecki, A.J.; Janusz, Z. Threat Modeling for Aviation Computer Security. Available online: http://m.crosstalkonline.org/issues/22/200/ (accessed on 20 September 2017).
26. Löhr, H.; Reza Sadeghi, A.; Stüble, C.; Weber, M.; Winandy, M. Modeling trusted computing support in a protection profile for high assurance security kernels. In Proceedings of the 2nd International Conference on Trusted Computing, Oxford, UK, 6–8 April 2009.
27. ETAS K.K. Security Crash Test—Practical Security Evaluations of Automotive Onboard IT Components. Available online: https://www.semanticscholar.org/paper/Security-Crash-Test-Practical-Security-Evaluations-Bayer-Enderle/7e564242772ad55f3151f331024638e0c94675b1 (accessed on 20 September 2017).
28. Michéle, B. Security & Privacy Implications. In *Smart TV Security*; Springer Briefs in Computer Science: Zürich, Switzerland, 2015; pp. 81–92.