KECS-CR-21-66

Smart TV Security Solution V6.0 for Samsung Knox
인증보고서

인증번호 : KECS-CISS-1136-2021

2021년 11월

IT보안인증사무국

1. 제품 개요

Smart TV Security Solution V6.0 for Samsung Knox(이하 'TOE')는 삼성 스마트 TV에 탑재되어 보안기능을 라이브러리 형태로 제공하는 스마트 TV 보안 솔루션이다.

TOE는 삼성 스마트 TV의 안전한 운영을 위해 시스템(Tizen 운영체제의 커널) 무결성 점검 및 비인가 웹앱 실행차단, 피싱 사이트 접속 차단 기능, 웹앱 데이터의 안전을 위해 데이터 암·복호화 기능을 제공한다.

TOE는 다음과 같이 식별된다.

구 분	내 용	배포형태
TOE	Smart TV Security Solution V6.0 for Samsung Knox	
버전	V6.0	
구성요소	Samsung_Smart_TV_Security_Solution_SYSTEM_001_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SYSTEM_001_V6.0_Release_1-1-1.armv7l.rpm)	소프트웨어 (CD)
	Samsung_Smart_TV_Security_Solution_PLATFORM_001_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_001_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_PLATFORM_003_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_003_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_PLATFORM_002_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_PLATFORM_002_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_SERVICE_001_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_001_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_SERVICE_002_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_002_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_SERVICE_003_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_003_V6.0_Release_1-1-1.armv7l.rpm)	
	Samsung_Smart_TV_Security_Solution_SERVICE_004_V6.0_Release_1-1-1.armv7l (Samsung_Smart_TV_Security_Solution_SERVICE_004_V6.0_Release_1-1-1.armv7l.rpm)	
가이드	Smart TV Security Solution V6.0 for Samsung Knox 개발자 가이드 V1.1 (Smart TV Security Solution V6.0 for Samsung Knox 개발자 가이드 V1.1.pdf)	문서파일 (CD)

TOE는 상기와 같은 rpm 패키지 형태로 개발자에게 배포되며 스마트 TV에 설치되어 운영될 때는 소프트웨어인 라이브러리 형태로 설치되어 동작한다.

평가대상 · 범위에 관한 고지: TOE는 스마트 TV 제품이 아닌 개발자에게 배포되는 라이브러리로(개발자 가이드 포함) 한정되며, 그 외 구성요소 및 기능은 평가 범위 및 대상에서 제외된다. Samsung Knox는 삼성전자에서 출시한 제품에 탑재되는 보안 플랫폼과 솔루션에 부여되는 브랜드이다.

TOE는 라이브러리 형태로 제공되는 소프트웨어 및 개발자 가이드로 구성된다. TOE는 삼성 스마트 TV 개발자에게 배포되며, 설치 후 운영 시에는 라이브러리 형태로 운영된다. TOE의 범위는 삼성 스마트 TV 전체를 구성하는 요소 중 보안기능을 담당하는 일부 라이브러리만 포함된다. 즉 배포되는 라이브러리와 라이브러리가 제공하는 API 사용방법 및 지침이 기술된 개발자 가이드가 TOE의 물리적 범위에 포함된다. TOE는 CD(지침포함)로 개발자에게 직접 배포된다.

TOE가 제공하는 보안기능은 아래와 같다.

- 시스템 무결성 모니터링 기능: Tizen 운영체제의 커널에 대한 무결성 점검 기능 및 점검 결과를 업데이트 서버 통신 기능으로 전달하는 기능
- 웹앱 보호 기능: 스마트 TV에서 실행되는 웹앱 중 인가되지 않은 웹앱이 실행되는 것을 차단하는 기능
- 데이터 암 · 복호화 기능: 웹앱에서 사용되는 데이터 중 개발자가 지정한 보호가 필요한 데이터에 대하여 저장 시 암호화 및 사용시 복호화하는 기능
- 피싱 사이트 차단 기능: 스마트 TV 사용자가 웹 브라우저를 이용하여 임의의 웹 사이트에 접속 시 접속대상 사이트가 피싱 사이트인지 검사하는 기능(Google Safe Browsing 연동)

TOE는 삼성 스마트 TV의 펌웨어에 보안성을 제공하기 위해 사용되는 라이브러리이며, 삼성 스마트 TV의 보안기능을 담당하는 역할을 수행한다. TOE는 삼성 스마트 TV 사용자가 웹 브라우저를 이용하여 임의의 웹 사이트에 접속하는 경우 피싱 사이트 차단 기능을 통해 사용자가 안전하게 웹 서핑을 할 수 있도록 한다. 또한, 비인가된 웹앱의 실행을 차단하여 비인가된 웹앱의 삼성 스마트 TV 내부 자원에 접근하는 것을 차단한다. 웹앱에서 사용되는 중요 데이터는 암호화를 통해 안전하게 저장한다. 삼성 스마트 TV의 안전한 운영을 위하여 내부적으로 시스템 무결성 모니터링 기능을 통해 시스템(Tizen 운영체제의 커널)에 대한 무결성 점검을 수행하여 안전하게 운영되는지 확인한다. 업데이트 매니저는 업데이트 서버와 통신하여 업데이트 파일을 스마트 TV로 다운로드 받고 업데이트 파일에 대한 무결성(전자서명) 검증을 수행한다. TOE는 스마트 TV로 다운로드 된 업데이트 파일을 이용하여, 업데이트 서버와 통신하여 수행하는 기능(무결성 점검 결과 리포팅 및 피싱 사이트 DB 목록 업데이트)에 대한 업데이트를 수행한다. TOE는 외부 IT 실체와의 통신을 수행한다. 외부 IT 실체와의

통신은 이더넷을 이용한 유선통신, Wi-Fi를 이용한 무선통신을 할 수 있으며, 통신 상대가 되는 외부 IT 실체는 시스템 무결성 모니터링 기능과 피싱 사이트 차단 기능과 통신하는 업데이트 서버와 피싱 사이트 차단 기능과 통신하는 Google Safe Browsing 서버가 존재한다. 단, 특정 지역에서는 삼성 스마트 TV와 업데이트 서버가 연동되지 않는다. 외부 IT 실체와의 통신은 운영 환경에서 제공하는 OpenSSL을 통해 기밀성과 무결성을 지원하는 안전한 통신채널을 제공한다. 개발자는 TOE를 이용하여 스마트 TV의 어플리케이션을 개발할 때 Serial Port를 이용하여 스마트 TV와 통신한다. Serial Port 통신은 개발자가 아닌 일반 스마트 TV 사용자에게는 제공되지 않는다.

TOE 운영을 위해 필요한 외부 IT 실체는 다음과 같다. TOE는 아래의 외부 IT 실체와 통신 시 운영환경에서 제공하는 TLS V1.2 프로토콜(OpenSSL 1.1.1l)을 이용하여 전송데이터에 대한 보호를 지원한다.

- Google Safe Browsing Server:
  - 피싱 사이트 URL 리스트를 제공하여 해당 URL이 피싱 사이트인지 여부를 알려주는 구글에서 제공하는 서버
- 업데이트 서버:
  - 삼성 스마트 TV의 시스템 무결성 모니터링 기능에 의해 탐지된 결과를 전달받고, 피싱 사이트 DB 목록을 스마트 TV로 전송한다.
  - 삼성 스마트 TV가 업데이트 서버와 통신하여 수행하는 기능(무결성 점검 결과 리포팅 및 피싱 사이트 DB 목록 업데이트)에 대한 업데이트 파일을 스마트 TV로 전송한다.

TOE는 삼성 스마트 TV에서 수행되는 라이브러리 형태의 보안솔루션으로 다음과 같은 하드웨어 및 소프트웨어가 요구된다. TOE 운영에 필요한 하드웨어 및 소프트웨어 사양은 [표 1]과 같다.

구분		내용
H/W	CPU	ARM architecture (Cortex A53 Quad) 이상
	DDR Memory	1.0GB 이상
	Flash Memory	eMMC 4GB 이상
	NIC	10/100 MB Ethernet*1
	Wi-Fi	802.11a/b/g/n
	Serial Port	RS-232C
S/W	Web Brower	Tizen Browser 4.1.9200
	OpenSSL	V1.1.1l(외부 IT 실체와의 통신 시 사용)
	SQLite	V3.33.0
	REE OS	Tizen 6.0 (kernel 4.1.10)
	TEE OS	TrustWare V3.1.0

인증 효력에 관한 고지: 상기 제품의 인증서는 IT보안인증사무국 또는 인증서를 인정하는 기관이 상기 제품에 대해 포괄적인 책임이 있음을 의미하지는 않는다.

2. 주요기능

TOE가 제공하는 보안기능은 다음과 같다.

■ 시스템 무결성 모니터링 기능

TOE는 삼성 스마트 TV의 기능이 안전하게 수행될 수 있도록 시스템 무결성 모니터링 기능을 통해 정규 운영 중 Tizen 운영체제의 커널에 대한 무결성 검증을 수행한다. 무결성 검증이 실패할 경우 업데이트 서버로 단말정보, 변조 검출 영역을 포함한 결과 리포트를 전송한다.

시스템 무결성 모니터링 기능은 크게 세 부분으로 구분된다. Tizen 운영체제의 application 영역에서 동작하면서 모니터링 기능의 시작 및 무결성 변조탐지 시 업데이트 서버로 리포팅하는 부분, Tizen 운영체제의 커널모듈 영역에서 동작하면서 TOE 동작 시 동적 영역의 시스템 모니터링을 수행하는 부분, Trustware의 application영역에서 동작하면서 정적 영역의 시스템 무결성 모니터링을 수행하는 부분으로 구성된다.

Tizen 운영체제의 Application에서 동작하는 시스템 무결성 모니터링 기능은 Tizen 운영체제의 Application 영역에 설치된 이후, 모니터링 프로세스를 시작하며, Tizen 운영체제의 커널 영역에서 모니터링 기능이 동작할 수 있도록 LKM(Loadable Kernel Module)형태의 커널 모듈로 삽입한다. 또한 Trustware의 application에서 동작하는 시스템 무결성 모니터링 기능으로부터 변조결과를 확인하고 이를 업데이트 서버로 리포팅한다. 앞서 언급한 바와 같이, Tizen 운영체제의 커널모듈 영역에서 동작하는 시스템 무결성 모니터링 기능은 TOE의 일부 기능으로써, TOE 동작 시, Tizen 운영체제의 application에서 동작하는 시스템 무결성 모니터링 기능에 의해 LKM(Loadable Kernel Module)형태의 커널 모듈로 삽입되어 동작한다. 모니터링 기능 시작 시, 커널 동적 메모리 영역에 대한 시스템 무결성 모니터링을 수행한다.

Trustware의 application 영역에서 동작하는 시스템 무결성 모니터링 기능은 주기적으로 커널 정적 메모리 영역에 해당하는 심볼영역의 메모리 값과 원본 값을 비교하여 변조를 탐지하며, Tizen 운영체제의 커널모듈 영역에서 동작하는 시스템 무결성 모니터링 기능으로부터 변조탐지 결과를 전달받아서 정적 메모리 변조탐지 결과와 같이 Trustware의 메모리 영역에 저장한다.

■ 웹앱 보호 기능

TOE는 인가되지 않은 웹앱이 삼성 스마트 TV에서 실행되는 것을 방지하기 위하여 웹앱 보호 기능을 제공한다. 삼성 스마트 TV는 삼성전자가 제공하는 앱 스토어(이하 “앱 컨텐츠 서버”)에서 제공되는 웹앱만 다운로드하여 저장할 수 있다. 앱 컨텐츠 서버에 웹앱 등록 시 삼성전자가 미리 웹앱을 암호화하여 등록하여 놓았으며, 삼성 스마트 TV 사용자는 앱 컨텐츠 서버에서 필요한 웹앱을 다운로드하여 삼성 스마트 TV에 저장할 수 있다. 저장된 웹앱을 실행하기 위해서는 복호화하는 과정이 필요하다. 이때 웹앱을 복호화하는 과정에서 TOE는 정상적인 암호 키를 이용하여 복호화함에도 복호화가 수행되지 않는 경우 웹앱이 변조되었다고 판단하여 해당 웹앱의 실행을 차단하게 된다. 이때 사용되는 암호는 AES 블록암호알고리즘이 사용(CTR 모드)되며, 암호 키의 길이는 128 bits를 사용한다.

■ 데이터 암복호화 기능

TOE는 웹앱을 사용하는 사용자의 중요데이터를 보호하기 위해 웹앱에서 사용되는 중요데이터(ID/Password 등 웹앱 개발자가 중요데이터로 지정한 데이터)에 대한 암·복호화 기능을 제공한다. 데이터 암복호화는 개발자 선택에 따라 REE OS 혹은 TEE OS에서 수행할 수 있다. 이때 사용되는 암호는 AES 블록암호알고리즘이 사용(CBC 모드)되며, 암호 키의 길이는 256 bits를 사용한다. 암호 키 생성은 하드웨어로부터 유도(PBKDF2 알고리즘 이용)된 정보를 이용하여 암호 키를 생성한다. 암호 키는 생성 후 메모리에서 동작하다 암호화 연산/복호화 연산이 종료되면 암호 키를 파기하게 된다. 암호 키 파기는 Zeroization 기술을 이용하여 파기한다.

■ 피싱 사이트 차단 기능

TOE는 삼성 스마트 TV 사용자가 유해한 피싱 사이트에 접속하여 개인정보 유출 등의 위험에 노출되는 것을 방지하기 위하여 피싱 사이트 차단 기능을 제공한다. 피싱 사이트 차단 기능은 사용자가 삼성 스마트 TV의 웹 브라우저(Tizen Browser)를 통해 임의의 사이트 접속 시 내부 DB에 저장된 피싱 사이트 목록을 기반으로 검증 후 피싱 사이트로 의심되는 경우 Google Safe Browsing 서비스를 이용하여 해당 사이트가 피싱 사이트인지 확인한다. 해당 사이트가 피싱 사이트로 확인된 경우 사용자에게 해당 사이트가 피싱 사이트임을 알려준다. 사용자가 접속 차단을 선택한 경우 피싱 사이트 접속을 차단하여 사용자의 개인정보를 보호한다. TOE는 피싱 사이트 차단 기능에 대하여 중지, 개시하는 능력을 스마트 TV 사용자에게 제공한다. 사용자가 피싱 사이트 차단 기능을 중지하는 경우 피싱 사이트 차단 기능은 동작하지 않는다. 피싱 사이트 DB 목록은 업데이트 서버를 통해 주기적으로 업데이트를 수행한다. TOE와 Google Safe Browsing 서버와 통신 시에는 운영환경에서 제공하는 TLS V1.2 프로토콜(OpenSSL 1.1.1l)을 이용하여 전송 데이터에 대한 보호를 지원한다.

3. 평가결과 요약

TOE에 대한 평가는 한국아이티평가원에서 수행하였다. 평가는 제품이 공통평가기준 2부와 3부의 EAL1 평가보증등급을 만족하여, 공통평가기준 1부 305항에 따라 “적합”한 것으로 평가하였다.

[인증제품 식별정보]

평가지침	정보보호시스템 평가인증지침 (2017. 8. 24) 정보보호제품 평가인증 수행규정 (2021. 5. 17)
평가제품	Smart TV Security Solution V6.0 for Samsung Knox
보호프로파일	없음
보안요구사항	없음
보안목표명세서	Smart TV Security Solution V6.0 for Samsung Knox 보안목표명세서 V1.1 (2021.11.11.)
평가보고서	Smart TV Security Solution V6.0 for Samsung Knox 평가결과보고서 V1.00 (2021.11.15.)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 R5
평가방법론	정보보호시스템 공통평가방법론 V3.1 R5
검증필 암호모듈 (탑재 필수)	해당 없음
평가신청인	삼성전자주식회사
개발업체	삼성전자주식회사
평가기관	(주)한국아이티평가원