DBpia

Trusted Execution Environment의 구성 요소 및 응용 기술 조사

A Survey of Components and Application Technologies of the Trusted Execution Environment

저자 (Authors)
전상기, 최창준, 이종혁
Sanggi Jeon, Changjun Choi, Jong-Hyouk Lee

출처 (Source)
한국통신학회 학술대회논문집 , 2017.11, 65-66(2 pages)
Proceedings of Symposium of the Korean Institute of communications and Information Sciences , 2017.11, 65-66(2 pages)

발행처 (Publisher)
한국통신학회
Korea Institute Of Communication Sciences

URL
http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07284621

APA Style
전상기, 최창준, 이종혁 (2017). Trusted Execution Environment의 구성 요소 및 응용 기술 조사 . 한국통신학회 학술대회논문집, 65-66

이용정보 (Accessed)
성균관대학교
115.145.3.***
2021/03/19 05:26 (KST)

저작권 안내
DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다. 그리고 DBpia에서 제공되는 저작물은 DBpia와 구독계약을 체결한 기관소속 이용자 혹은 해당 저작물의 개별 구매자가 비영리적으로만 이용할 수 있습니다. 그러므로 이에 위반하여 DBpia에서 제공되는 저작물을 복제, 전송 등의 방법으로 무단 이용하는 경우 관련 법령에 따라 민, 형사상의 책임을 질 수 있습니다.

Copyright Information
Copyright of all literary works provided by DBpia belongs to the copyright holder(s)and Nurimedia does not guarantee contents of the literary work or assume responsibility for the same. In addition, the literary works provided by DBpia may only be used by the users affiliated to the institutions which executed a subscription agreement with DBpia or the individual purchasers of the literary work(s)for non-commercial purposes. Therefore, any person who illegally uses the literary works provided by DBpia by means of reproduction or transmission shall assume civil and criminal responsibility according to applicable laws and regulations.

Trusted Execution Environment의 구성 요소 및 응용 기술 조사

전상기, 최창준, 이종혁
상명대학교 프로토콜공학연구실
{sanggi, changjun, jonghyouk}@pel.smuc.ac.kr

A Survey of Components and Application Technologies of the Trusted Execution Environment

Sanggi Jeon, Changjun Choi, Jong-Hyouk Lee
Protocol Engineering Lab., Sangmyung University

요 약

TEE (Trusted Execution Environment)는 스마트폰 또는 모바일 장치의 메인 프로세서에 있는 보안 영역으로 중요한 데이터를 신뢰할 수 있는 환경에 저장, 처리 및 보호한다. 본 논문에서는 TEE의 정의 및 아키텍처와 통신에 필요한 API (Application Programming Interface)를 설명한다. 또한 TEE 활용 사례로 ARM TrustZone과 Intel SGX (Software Guard Extensions)를 이용한 응용 기술들을 살펴본다.

Ⅰ. 서론

최근 모바일 장치 사용이 증가하고 있고, 모바일 장치는 사람들의 실생활에 밀접하게 관련된다. 이러한 모바일 기기에는 민감한 개인 정보(메시지, 메일, 전자 지갑, 금융데이터 등)가 저장된다. 따라서 공격자들이 모바일 기기 내에 중요한 데이터를 탈취하는 사례들이 증가하고 있다. 이러한 공격 때문에 신뢰할 수 있는 격리 환경에서 민감한 데이터를 저장, 처리 및 보호하는 기술인 TEE가 등장했다. 본 논문에서는 신뢰할 수 있는 격리 환경에서 응용프로그램을 실행할 수 있도록 하는 기술인 TEE에 대해서 설명하고, TEE의 활용 사례와 응용 기술을 살펴본다.

본 논문의 2장 본론에서는 TEE를 정의하고, TEE를 이해하기 위해 필요한 배경지식을 설명한다. 또한 TEE의 아키텍처를 살펴보고, TEE 활용 사례 및 응용 기술들을 설명한다. 본 논문의 3장에서 결론을 맺는다.

Ⅱ. TEE

TEE [1]는 신뢰할 수 있는 격리 환경을 통해 응용프로그램의 무결성 및 기밀성을 제공하는 기술이다. 또한 실행된 코드의 신뢰성과 런타임 상태의 무결성 및 영구메모리에 저장된 코드, 데이터 및 런타임 상태의 기밀성을 보장한다. TEE에서 사용되는 관련 기술 간의 관계를 (그림 1)과 같이 나타낼 수 있다.

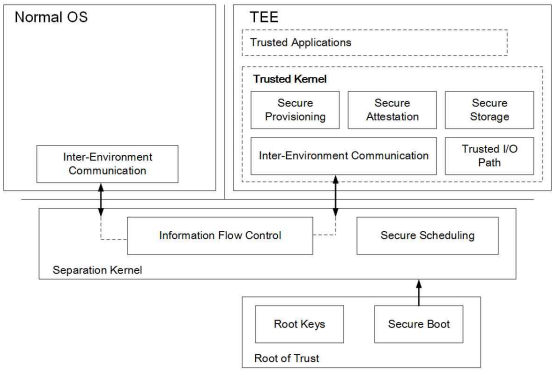
2.1. 관련 기술

2.1.1. Separation Kernel

Separation Kernel은 격리 환경을 제공하기 위한 TEE의 기초 구성 요소로써 분산 시스템을 시뮬레이션 하는 데 사용되는 보안 커널이다. 설계 목적은 동일한 플랫폼에서 여러 수준의 보안이 필요한 시스템들이 공존할 수 있게 하는 데 있다. 여러 개의 파티션으로 나뉘며 파티션 간 통신을 위해 제어되는 인터페이스를 사용하는 방법으로 격리를 보장한다. Separation Kernel에 대한 보안 요구사항은 SKPP [2] (Separation Kernel Protection Profile)에 정의된다.

2.1.2. Root of Trust

RoT (Root of Trust)는 시스템 상태와 관련하여 신뢰할 수 있는 증거를 제공하기 위한 엔티티이다. RoT는 변조 방지 하드웨어 모듈로써 신뢰도를 측정하고 신뢰 점수를 계산하는 역할을 한다. RoT는 Secure Boot과정을 통해 부팅될 때마다 로드된 TEE가 플랫폼 공급자가 인증한 TEE인지 확인한다.

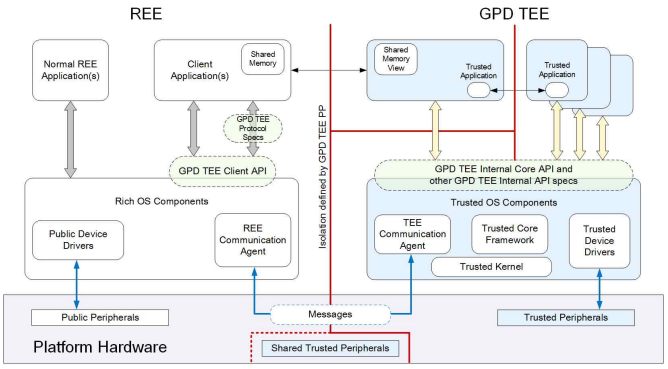


(그림 1) TEE Building Blocks [1]

2.2. 아키텍처

GlobalPlatform [3]에서는 (그림 2)와 같이 Rich OS를 실행하는 환경인 REE (Rich Execution Environment)와 Trusted OS를 실행하는 신뢰할 수 있는 격리 환경인 GPD (GlobalPlatform Device) TEE으로 분리하였다.

성균관대학교 | IP:115.145.3.*** | Accessed 2021/03/19 05:26(KST)



(그림 2) TEE Software Architecture [3]

REE 내에서 식별하는 세 가지 클래스 구성 요소는 다음과 같다.

- TEE Client Application
- TEE Client API 라이브러리 구현
- REE Communication Agent

GPD TEE 내에서 식별하는 세 가지 클래스 구성 요소는 다음과 같다.

- TEE Internal APIs를 사용하는 TAs (Trusted Applications)
- TEE Internal API 라이브러리 구현
- Trusted OS Components

일반적인 응용프로그램은 TEE Client API를 사용하여 TEE와 통신을 설정하고 TA와의 세션, 공유 메모리를 설정하며 TA 관련 명령을 보내 신뢰할 수 있는 서비스를 호출한 다음 통신을 종료한다. TEE 내에서 사용되는 TEE Internal APIs는 일반적으로 TA에서 필요로 하는 기능에 대한 공통 구현을 제공하는 API이며 종류는 (표 1)과 같다.

API	설명
TEE Internal Core API	TA에 기능을 제공하는 특정 API 집합
TEE Secure Element API	TEE가 구현되는 장치에 연결된 보안 요소에 대한 통신을 지원하는 활성화 레이어를 지정
TEE Sockets API	소켓 방식을 사용하여 네트워크 통신을 설정하고 활용하기 위해 TA가 사용하는 일반적인 C언어 인터페이스를 지정
TEE TA Debug API	TEE Internal API의 TA 개발 및 적합성 테스트를 지원하는 API 집합을 지정
TEE Trusted User Interface API	보안 표시, 보안 입력, 보안 표시기의 목적을 가지며 사용자에게 화면을 표시해주는 API

(표 1) TEE Internal APIs [3]

2.3. 활용 사례 및 응용 기술

TEE는 스마트폰과 같은 모바일 장치의 메인 프로세서에 있는 보안 영역으로 중요한 데이터를 신뢰할 수 있는 환경에 저장, 처리 및 보호한다. 그리고 Rich OS 환경에서 소프트웨어 공격에 대한 보호 수준을 제공하여 기업에서의 기밀 정보 및 독점 정보를 안전하게 처리할 수 있도록 접근 권한을 제어하며 모바일 서비스에서 안전하고 신뢰할 수 있는 User Interface를 이용하여 모바일 장치의 인증 기능을 강화할 수 있는 이상적인 환경을 제공한다. 또한 영화, 음악 및 전자 서적과 같은 프리미엄 컨텐츠를 무료로 공유할 수 없도록 Rich OS 환경에서 제공하는 보호 수준을 제공한다 [4].

TEE의 대표적인 기술로는 ARM TrustZone [5]과 Intel SGX [6]가 있다. ARM TrustZone을 응용한 기술로는 사용자 인증 정보 및 각종 암호화 키 정보를 하드웨어 칩셋 내부에 구현한 TrustZone을 통해 관리하는 Samsung의 Knox [7]가 있다. Intel SGX를 응용한 기술로는 기존의 블록체인 기술과 신뢰할 수 있는 응용프로그램 실행 환경인 Intel SGX 및 VSM (Windows Virtual Secure Mode)을 제공하는 Microsoft사의 Coco Framework [8]가 있다.

Ⅲ. 결론

본 논문에서는 중요한 데이터를 격리된 신뢰할 수 있는 환경에서 저장, 처리 및 보호하는 TEE 기술에 대해 설명하고 활용 사례 및 응용 기술들을 살펴보았다. TEE는 격리 환경을 제공하기 위한 기초 구성 요소인 Speration Kernel을 가지며 REE와 GPD TEE로 분리되고 RoT를 통해 시스템 상태의 신뢰도를 측정한다. 민감한 데이터를 안전하게 저장할 수 있는 기술인 TEE와 결합하여 새로운 응용 기술들을 만들어내는 연구가 활발히 진행되고 있다.

ACKNOWLEDGMENT

이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 '범부처 Giga KOREA 사업'의 지원을 받아 수행된 연구임 (No.GK17P0400, (초저지연-총괄/1세부)저지연 융합서비스를 위한 모바일 에지 컴퓨팅 플랫폼 기술 개발)

참 고 문 헌

[1] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: What it is, and what it is not." Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.

[2] Directorate, I. A. Protection profile for separation kernels in environments requiring high robustness. Technical report, US Government, 2007.

[3] Platform, Global. "Global Platform Device Technology TEE System Architecture." Public Review Draft, 2011.

[4] https://translate.google.com/translate?hl=ko&sl=en&tl=ko&u=https%3A%2F%2Fwww.globalplatform.org%2FmediaguideTEEUse.asp&anno=2&sandbox=1, last accessed 2017.10.24.

[5] Ngabonziza, Bernard, et al. "TrustZone Explained: Architectural Features and Use Cases." Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on. IEEE, 2016.

[6] Jain, Prerit, et al. "OpenSGX: An Open Platform for SGX Research." NDSS. 2016.

[7] Atamli-Reineh, Ahmad, et al. "Analysis of Trusted Execution Environment usage in Samsung KNOX." Proceedings of the 1st Workshop on System Software for Trusted Execution. ACM, 2016.

[8] https://azure.microsoft.com/ko-kr/blog/announcing-microsoft-s-coco-framework-for-enterprise-blockchain-networks, last accessed 2017.10.24

성균관대학교 | IP:115.145.3.*** | Accessed 2021/03/19 05:26(KST)