



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0095780
(43) 공개일자 2017년08월23일

(51) 국제특허분류(Int. Cl.)
H04M 1/725 (2006.01) G06F 21/51 (2013.01)
(52) CPC특허분류
H04M 1/72522 (2013.01)
G06F 21/51 (2013.01)
(21) 출원번호 10-2017-0098934
(22) 출원일자 2017년08월04일
심사청구일자 없음

(71) 출원인
안나영
서울특별시 동대문구 제기로6길 9-13(제기동)
(72) 발명자
안나영
서울특별시 동대문구 제기로6길 9-13(제기동)

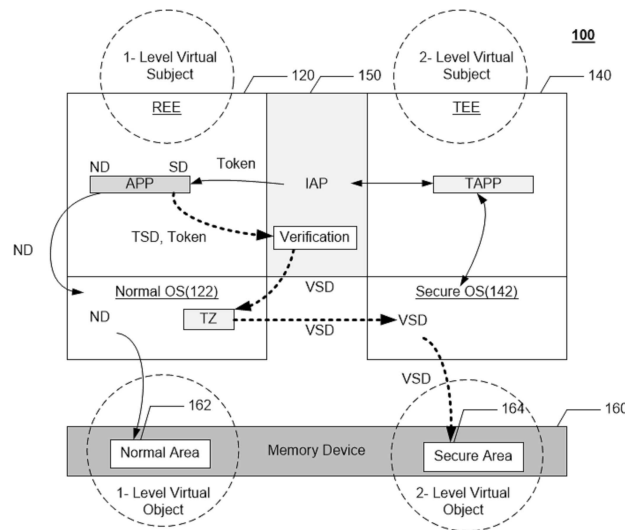
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 클락 원순 모델을 적용한 모바일 장치 및 그것의 동작 방법

(57) 요약

본 발명의 실시 예에 따른 모바일 장치의 동작 방법은, REE(rich execution environment)의 어플리케이션에서 제 1 데이터와 제 1 토큰에 대한 제 1 XOR 연산을 수행하는 단계, 상기 어플리케이션에서 상기 제 1 토큰과 제 2 토큰이 동일한 지를 판별하는 단계, 무결성 보장 프로그램에서 상기 제 1 XOR 연산의 결과값과 상기 제 2 토큰에 대한 제 2 XOR 연산을 수행하는 단계, 및 상기 제 2 XOR 연산의 결과값을 TEE(trusted execution environment)로 전송하는 단계를 포함할 수 있다.

대 표 도 - 도2



명세서

청구범위

청구항 1

모바일 장치의 동작 방법에 있어서:

REE(rich execution environment)의 어플리케이션에서 제 1 데이터와 제 1 토큰에 대한 제 1 XOR 연산을 수행하는 단계;

상기 어플리케이션에서 상기 제 1 토큰과 제 2 토큰이 동일한 지를 판별하는 단계;

무결성 보장 프로그램에서 상기 제 1 XOR 연산의 결과값과 상기 제 2 토큰에 대한 제 2 XOR 연산을 수행하는 단계; 및

상기 제 2 XOR 연산의 결과값을 TEE(trusted execution environment)로 전송하는 단계를 포함하는 방법.

발명의 설명

기술 분야

[0001] 본 발명은 클락 월슨 모델을 적용한 모바일 장치 및 그것의 동작 방법에 관한 것이다.

배경 기술

[0002] TEE (trusted execution environment)는 메인 프로세서의 보안 영역이다. TEE는 기밀 유지 및 무결성과 관련하여 내부에 로드된 코드 및 데이터를 보호한다. 격리된 실행 환경인 TEE는 신뢰할 수 있는 어플리케이션의 무결성 및 자산의 기밀성과 같은 보안 기능을 제공한다. 일반적으로 TEE는 REE(rich execution environment) 모바일 운영 체제 (모바일 OS) 보다 높은 보안 수준을 제공하고, SE(secure element)보다 많은 기능을 제공하는 실행 공간을 갖는다. TEE는 모바일 장치의 칩(SoC; system on chip)을 기반으로 한 일종의 가상화 공간이다.

선행기술문헌

특허문헌

[0003] (특허문헌 0001) 공개특허: 10-2016-0008012, 공개일자: 2016년01월21일, 제목: 휴대단말기에서의 사용자 인증 방법.

(특허문헌 0002) 미국공개특허: US 2017/0083882, 공개번호: 2017년 03월 23일, 제목: Secure Payment Method and Electronic Device Adapted Thereto.

(특허문헌 0003) 공개번호: 10-2016-0140159, 공개일자: 2016년12월07일, 제목: 전자 장치 및 커널 데이터 접근 방법.

비특허문헌

[0004] (비특허문헌 0001) Ning Zhang and Kun Sun and Deborah Shands and Wenjing Lou and Y. Thomas Hou, "TruSpy: Cache Side-Channel Information Leakage from the Secure World on ARM Devices", <http://eprint.iacr.org/2016/>

발명의 내용

해결하려는 과제

[0005] 본 발명의 목적은 데이터의 신뢰성을 향상시키는 모바일 장치 및 그것의 동작 방법을 제공하는데 있다.

과제의 해결 수단

[0006] 본 발명의 실시 예에 따른 모바일 장치의 동작 방법은: REE(rich execution environment)의 어플리케이션에서 제 1 데이터와 제 1 토큰에 대한 제 1 XOR 연산을 수행하는 단계; 상기 어플리케이션에서 상기 제 1 토큰과 제 2 토큰이 동일한 지를 판별하는 단계; 무결성 보장 프로그램에서 상기 제 1 XOR 연산의 결과값과 상기 제 2 토큰에 대한 제 2 XOR 연산을 수행하는 단계; 및 상기 제 2 XOR 연산의 결과값을 TEE(trusted execution environment)로 전송하는 단계를 포함할 수 있다.

발명의 효과

[0007] 본 발명의 실시 예에 따른 모바일 장치 및 그것의 동작 방법은 REE에서 발생된 데이터를 보안 영역에 직접 저장하지 않고, 무결성 보장 프로그램(IAP)에 의해 검증된 데이터를 보안 영역에 저장함으로써, 전송된 데이터의 무결성을 보장할 수 있다.

[0008] 또한, 본 발명의 모바일 장치 및 그것의 동작 방법은 상술된 방법에 따라 해커의 잠재적인 활동을 저지할 수 있으며, 보안을 극대화시킬 수 있다.

도면의 간단한 설명

[0009] 이하에 첨부되는 도면들은 본 실시 예에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 실시 예들을 제공한다. 다만, 본 실시예의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시 예로 구성될 수 있다.

도 1은 일반적인 클락 윌슨(clark wilson) 모델을 설명하기 위한 도면이다.

도 2는 본 발명의 실시 예에 따른 모바일 장치(100)를 예시적으로 보여주는 도면이다.

도 3은 본 발명의 실시 예에 따른 IAP(150)의 무결성 보장 동작을 예시적으로 보여주는 도면이다.

도 4는 본 발명의 실시 예에 따른 IAP(150)의 무결성 검증 과정(IVP)을 예시적으로 보여주는 도면이다.

도 5는 본 발명의 실시 예에 따른 무결성 보장 동작에서 토큰 발행 과정을 예시적으로 보여주는 래더 다이어그램이다.

도 6은 본 발명의 실시 예에 따른 모바일 장치에 클락 윌슨 모델을 적용을 개념적으로 설명하는 도면이다.

도 7은 본 발명의 실시 예에 따른 모바일 장치(100)의 동작 방법을 예시적으로 보여주는 도면이다.

도 8은 본 발명의 다른 실시 예에 따른 모바일 장치(100)의 동작 방법을 예시적으로 보여주는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0010] 아래에서는 도면들을 이용하여 본 발명의 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있을 정도로 본 발명의 내용을 명확하고 상세하게 기재할 것이다.

[0011] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시 예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 개시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 제 1, 제 2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다.

[0012] 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로 사용될 수 있다. 예를 들어, 본 발명의 권리 범위로부터 이탈되지 않은 채 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 혹은 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접

연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

- [0013] 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 혹은 "~에 이웃하는"과 "~에 직접 이웃하는" 등도 마찬가지로 해석되어야 한다. 본 출원에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.
- [0014] 본 출원에서, "포함하다" 혹은 "가지다" 등의 용어는 실시된 특징, 숫자, 단계, 동작, 구성요소, 부분품 혹은 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 혹은 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부분품 혹은 이들을 조합한 것들의 존재 혹은 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다. 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미이다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미인 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0015] 도 1은 일반적인 클락 윌슨(clark wilson) 모델을 설명하기 위한 도면이다.
- [0016] 클락 윌슨의 무결성 모델은 지정 및 컴퓨팅 시스템에 대한 무결성 정책을 분석하기 위한 기반을 제공한다. 이 모델은 주로 정보 무결성의 개념을 공식화하는 데 관심이 있다. 오류 또는 악의적인 의도로 인해 시스템의 데이터 항목이 손상되는 것을 방지하여 정보 무결성을 유지한다.
- [0017] 클락 윌슨 모델은 데이터 무결성을 강화하기 위해 각 데이터 항목을 정의하고 작은 프로그램 세트를 통해서만 수정할 수 있다. 이 모델은 트리플 또는 액세스 제어 트리플로 알려진 주체/프로그램/객체 (프로그램이 트랜잭션과 상호 교환 가능)의 세 부분으로된 관계를 사용한다. 이 관계 내에서 주체(subject)는 객체(object)에 직접 액세스할 수 없고, 프로그램을 통해서만 객체를 액세스할 수 있다.
- [0018] 이 모델에는 데이터 항목과 해당 데이터 항목에서 동작하는 프로세스를 모두 나타내는 기본 구성이 많이 포함되어 있다. 클락 윌슨 모델의 주요 데이터 유형은 CDI(constrained data item)이다. 무결성 검증 절차(integrity verification procedure; IVP)는 시스템의 모든 CDI가 특정 상태에서 유효함을 보장한다. 무결성 정책을 시행하는 트랜잭션은 변환 절차(transformation procedure; TP)로 표현된다. TP는 CDI 또는 UDI(unconstrained data item)를 입력 받아 CDI를 생성한다. TP는 시스템을 하나의 유효한 상태에서 다른 유효한 상태로 전환해야 한다. UDI는 시스템 입력을 나타낸다. TP는 UDI의 모든 가능한 값을 "안전한" CDI로 변환하도록 (인증을 통해) 보장해야 한다.
- [0019] 모델의 중심에는 일련의 데이터 항목 (예 : UDI 및 CDI)에서 작동하는 인증 된 사용자 (즉, 사용자)와 일련의 프로그램 (예 : TP) 간의 관계 개념이 있다. 그러한 관계의 구성 요소들은 함께 취해서 클락 윌슨 트리플 이라고 불린다. 모델은 또한 다른 주체가 주체, 트랜잭션 및 데이터 항목 간의 관계를 조작할 책임이 있음을 보장해야 한다. 간단한 예로서, 관계를 인증하거나 생성할 수 있는 사용자는 해당 관계에 지정된 프로그램을 실행할 수 없어야 한다.
- [0020] 모델은 인증 규칙 (C)과 시행 규칙 (E)의 두 가지 규칙으로 구성된다. 아래의 9 가지 규칙은 데이터 항목의 외부 및 내부 무결성을 보장한다.
- [0021] C1- IVP가 실행되면 CDI가 유효한지 확인해야 한다.
- [0022] C2- 연관된 CDI 세트의 경우, TP는 해당 CDI를 유효한 상태에서 다른 상태로 변환해야 한다. 이러한 TP는 특정 CDI에서 작동하도록 인증되어야 하므로 E1과 E2가 있어야 한다.
- [0023] E1- 시스템은 인증된 관계 목록을 유지하고 CDI를 실행하도록 인증 된 TP 만 해당 CDI를 변경하도록 보장해야 한다.
- [0024] E2 시스템은 사용자를 각 TP 및 CDI 세트와 연관시켜야 한다. TP는 "합법적"인 경우 사용자를 대신하여 CDI에 액세스할 수 있다. 이를 위해서는 "허용된 관계"라고 하는 트리플 (사용자, TP, {CDI})를 추적해야 한다.
- [0025] C3- 허용 관계는 "의무 분립"의 요구 사항을 충족해야 한다. 이를 추적하기 위해서는 인증이 필요하다.
- [0026] E3 시스템은 TP를 시도하는 모든 사용자를 인증해야 한다. 이는 TP 요청이 아니라 로그인이다. 보안을 위해 로

그를 보관해야 한다.

- [0027] C4 - 모든 TP는 작업을 재구성하기에 충분한 정보를 로그에 추가해야 한다. 정보가 시스템에 입력되면 신뢰할 수 있거나 제한될 필요가 없다 (즉, UDI 일 수 있음).
- [0028] C5 - UDI를 입력으로 사용하는 TP는 가능한 모든 UDI 값에 대해 유효한 트랜잭션만 수행할 수 있다. TP는 CDI로 수락하거나 UDI를 거부한다.
- [0029] 마지막으로, TP의 자격을 변경하여 사람들이 접근하지 못하도록 방지하기 위해: E4 - TP의 인증자는 해당 TP와 연관된 엔티티 목록을 변경할 수 있다.
- [0030] 한편, 트러스트 존(trust zone)을 갖는 모바일은 장치는 멀티 레벨 시큐리티 시스템(multi level security systme)으로 가정할 수 있다. 예를 들어, 제 1 레벨 시큐리티 시스템은 TEE(trusted execution environment)으로, 제 2 레벨 시큐리티 시스템은 REE(rich execution environment)으로 해석 가능하다.
- [0031] 본 발명의 실시 예에 따른 모바일 장치는 무결성 확보를 위해 이러한 멀티 레벨 시큐리티 시스템에 클락 월슨 모델을 적용하도록 구현될 수 있다. 이때 모바일 장치의 TEE 및 REE은 일반적인 개념으로써 객체(object)가 아니라 주체(subject)로 해석될 것이다. 아래에서는 REE는 제 1 레벨 가상 주체(1-Level Virtual Subject)라고 하고, TEE는 제 2 레벨 가상 주체(2-Level Virtual Subject)로 하겠다.
- [0032] 도 2는 본 발명의 실시 예에 따른 모바일 장치(100)를 예시적으로 보여주는 도면이다. 도 2를 참조하면, 모바일 장치(100)는 REE(120), TEE(140), 무결성 보장 프로그램(integrity assurance program; IAP, 150), 및 메모리 장치(160)를 포함할 수 있다. 모바일 장치(10)는, 예를 들어, 스마트폰(smartphone), 태블릿 PC(tablet personal computer), 웨어러블 장치(wearable device) 일 수 있다.
- [0033] 도 2에 도시된 REE(120), TEE(140), 및 IAP(150)는 적어도 하나의 프로세서로 구현될 수 있다.
- [0034] 프로세서는 모바일 장치(100)의 적어도 하나의 내부 구성들을 제어하거나 통신에 관한 연산/데이터를 처리를 실행하도록 구현될 수 있다. 실시 예에 있어서, 프로세서는 CPU(central processing unit), GPU(graphic processing unit), AP(application processor), CP(communication processor) 중 적어도 하나를 포함할 수 있다.
- [0035] REE(120)는, 하드웨어, 소프트웨어, 혹은 펌웨어적으로 구현되고, 일반적인 실행 환경을 제공하도록 구현될 수 있다. REE(120)는 적어도 하나의 어플리케이션(APP), 및 노멀 OS(operating system, 122)을 포함할 수 있다.
- [0036] 어플리케이션(APP)은 사용자에게 필요한 서비스를 제공하도록 구현될 수 있다. 본 발명의 어플리케이션(APP)은 메모리 장치(160)의 노멀 영역(162)에 저장될 노멀 데이터(ND) 및 메모리 장치(160)의 보안 영역(164)에 저장될 보안 데이터(SD)를 생성하도록 구현될 수 있다.
- [0037] 도시되지 않았지만, REE(120)는 사용자 인증 어플리케이션을 포함할 수 있다. 예를 들어, 사용자 인증 어플리케이션은 사용자에게 인증 동작을 수행하도록 REE(110)에서 구동될 수 있다. 여기서 인증 동작은 사용자의 선택 혹은 서비스 제공자의 선택의 의거하여 다양한 형태 혹은 다양한 조합으로 수행될 수 있다. 인증 동작은 사용자가 알고 있는 것 (예를 들어, 패스워드), 사용자가 갖고 있는 것 (예를 들어, 디지털 지문, 토큰, 공인인증서 등), 사용자의 특징(생리적, 심리적, 행동 등; 생체 인증으로 대표되는 지문, 얼굴, 홍채, 심박수 등) 중 어느 적어도 하나, 혹은 그것들 중 적어도 2 개의 조합으로 이루어질 수 있다. 즉, 사용자 인증 어플리케이션은 멀티 팩터 인증을 수행하도록 구현될 수 있다. 사용자 인증 어플리케이션은, 인증 동작을 TEE(140)의 적어도 하나의 보안 어플리케이션(TAPP) 통하여 안전하게 처리하도록 구현될 수 있다.
- [0038] 노멀 OS(122)은 REE(120)에서 사용자에게 서비스를 제공하는 적어도 하나의 어플리케이션을 실행하는 커널이다. 예를 들어, 노멀 OS(122)는, 안드로이드(Android), 안드로이드웨어(Android Wear), 심비안(Symbian) OS, 윈도우(Windows) OS 계열, 타이젠(Tizen), 유닉스, 리눅스, 등 일 수 있다. 실시 예에 있어서, 노멀 OS(122)은 모바일 장치(10)를 제조한 후에 써드 파티(third party)로부터 업데이트 될 수 있다. 실시 예에 있어서, 노멀 OS(122)은 복수의 운영 체제들을 동시에 구동할 수 있는 가상 플랫폼(예, hypervisor)을 포함할 수 있다.
- [0039] 또한, 노멀 OS(122)은 트러스트존 드라이버(TZ; trustzone driver)를 포함할 수 있다. TZ는 노멀 OS(122)에 로딩되는 커널 모듈으로써, REE(120)의 어플리케이션(APP)과 TEE(140)의 어플리케이션(TAPP) 사이의 통신을 중계할 수 있다. TZ는 REE(120)에 의해 TEE(140)의 안전한 접근을 하도록 구현될 수 있다. 여기서 안전한 접근은 기본적으로 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 등 조건들을 만족할 수 있다고 이

해되어야 할 것이다.

- [0040] TEE(140)는, 하드웨어, 소프트웨어, 혹은 펌웨어로 구성되고, REE(120)에서 생성되는 소프트웨어 공격으로부터 보호 수준을 제공하도록 구현될 수 있다. TEE(140)는 REE(120)로부터 격리될 필요가 있는 민감한 어플리케이션, 즉, 적어도 하나의 트러스티드 어플리케이션의 접근/실행을 제어할 수 있다. 트러스티드 어플리케이션은 TEE(140)에서 구동되는 보안을 필요로 하는 보안 어플리케이션(DRM(digital right management), bank, payment, corporate 등) 일 수 있다. 예를 들어, 보안 어플리케이션(TAPP)은, 프리로드 어플리케이션(preloaded application), 네이티브 어플리케이션(native application), 혹은 서드파티 어플리케이션(third party application)을 포함할 수 있다.
- [0041] 또한, TEE(140)는 적어도 하나의 보안 어플리케이션(TAPP), 및 보안 OS(142)을 포함할 수 있다. 보안 어플리케이션(TAPP)은 REE(120)의 인증 동작을 수행하는데 필요한 데이터를 안전하게 처리하도록 구현될 수 있다. 인증 동작에 필요한 인증 데이터의 비식별 처리 동작, 암호화 동작, 비교 동작 등이 보안 어플리케이션(TAPP)에서 수행될 수 있다. 한편, 보안 어플리케이션(TAPP)의 동작이 여기에 제한되지 않는다고 이해되어야 할 것이다.
- [0042] 또한, 보안 어플리케이션(TAPP)은 REE(120)에서 TEE(140)으로 전송된 데이터의 무결성을 보장하기 위하여 IAP(150)과 긴밀한 동작을 수행할 수 있다.
- [0043] 보안 OA(142)는 TEE(140)에서 보안 어플리케이션(TAPP)을 구동할 수 있다. 보안 OA(142)는 보안 커널을 포함하고, 보안 커널은 악의적인 사용자로부터 물리적/소프트웨어적으로 보호된 상태에서 구동되므로, 키 관리와 같이 보안이 요구되는 작업 등에 사용된다. 보안 커널은 가상 파일 시스템을 포함할 수 있다. 보안 어플리케이션(TAPP)에서 가상 파일 시스템의 파일 기능을 호출하는 경우, 가상 파일 시스템은 내부적으로 암호/복호화 등의 작업을 수행한 뒤, REE(120)의 파일시스템에 안전하게 저장/로딩/삭제할 수 있다.
- [0044] 무결성 보장 프로그램(IAP, 150)은 REE(120)에서 발생된 데이터가 TEE(140)으로 전송될 경우 데이터의 무결성을 보장하도록 구현될 수 있다. 예를 들어, IAP(150)은 도 1에 설명된 클락 월스 모델을 적용하도록 구현될 수 있다.
- [0045] IAP(150)은 TEE(140)에 의해 신뢰받은 프로그램일 수 있다. IAP(150)의 신뢰 보장은 TEE(140)의 보안 어플리케이션(TAPP)과의 통신에 의해 결정될 수 있다. 실시 예에 있어서, IAP(150)은 REE(120)의 노멀 OA(122) 상에서 구동될 수 있다. 다른 실시 예에 있어서, IAP(150)은 REE(120)의 노멀 OA(122)에 의해 구현된 가상화 OA 상에서 구동될 수 있다. 한편, IAP(150)의 구동이 이러한 OA에 제한되지 않는다고 이해되어야 할 것이다. IAP(150)을 구동하기 위한 별도의 OA가 구비될 수 있다.
- [0046] 실시 예에 있어서, IAP(150)은 TEE(140)의 TAPP와 연동하여 무결성 보장을 돕기 위한 토큰을 발행할 수 있다.
- [0047] 실시 예에 있어서, IAP(150)은 REE(120)의 APP로부터 전송된 변형된 보안 데이터(TSD)와 토큰을 수신하고, 보안 데이터(SD)를 검증하고, 검증된 보안 데이터(VSD)를 발생하도록 구현될 수 있다. 여기서 변형된 보안 데이터(TSD)는 REE(120)의 APP에서 토큰을 이용하여 보안 데이터(SD)를 변형시킨 것이다.
- [0048] 실시 예에 있어서, IAP(150)은 REE(120)의 APP에서 변형된 보안 데이터(TSD)와 토큰을 수신하고, 토큰을 이용하여 변형된 보안 데이터(TSD)에 포함된 보안 데이터(SD)의 무결성을 검증할 수 있다.
- [0049] 메모리 장치(160)는 휘발성/비휘발성 메모리 장치로 구현될 수 있다. 실시 예에 있어서, 메모리 장치(160)는 휘발성 메모리 장치일 수 있다. 예를 들어, 메모리 장치(160)는, DRAM(dynamic random access memory), SRAM(static random access memroy), DIMM(dual line memory module) 등 일 수 있다. 다른 실시 예에 있어서, 메모리 장치(160)는 비휘발성 메모리 장치일 수 있다. 예를 들어, 메모리 장치(160)는 낸드 플래시 메모리(NAND Flash Memory), 수직형 낸드 플래시 메모리(Vertical NAND; VNAND), 노아 플래시 메모리(NOR Flash Memory), 저항성 램(Resistive Random Access Memory: RRAM), 상변화 메모리(Phase-Change Memory: PRAM), 자기저항 메모리(Magnetoresistive Random Access Memory: MRAM), 강유전체 메모리(Ferroelectric Random Access Memory: FRAM), 스핀주입 자화반전 메모리(Spin Transfer Torque Random Access Memory: STT-RAM), 3D Xpoint 메모리 등이 될 수 있다. 또 다른 실시 예에 있어서, 메모리 장치(160)는 휘발성 메모리 장치와 비휘발성 메모리 장치로 구성된 하이브리드 메모리 장치일 수 있다. 예를 들어, 메모리 장치(160)는 NVDIMM(nonvolatile dual line memory module), HMC(hybrid memory cube) 등 일 수 있다.
- [0050] 또한, 메모리 장치(160)는 노멀 영역(162)과 보안 영역(164)을 포함할 수 있다. 노멀 영역(162)은 REE(120)에 의해 접근될 수 있는 영역이고, 보안 영역(164)은 TEE(140)에 의해 접근될 수 있는 영역이다. 또한, 보안 영역

(164)은 보안 데이터(secure data; SD)를 저장하거나, 암호화되어 데이터를 저장하기 위한 보안 영역을 포함할 수 있다.

[0051] 실시 있어서, 노멀 영역(162)에 REE(120)의 APP에서 발생된 노멀 데이터(ND)가 노멀 OS(122)을 경유하여 저장될 수 있다.

[0052] 실시 예에 있어서, 보안 영역(164)에 IAP(150)의 도움을 받아 REE(120)의 보안 데이터(SD)가 간접적으로 저장될 수 있다. 이때 저장되는 보안 데이터(SD)는 REE(120)에서 생성되는 오리지널 보안 데이터(SD)가 아니라, IAP(150)에 검증받은 검증된 보안 데이터(VSD)이다.

[0053] 한편, 보안 레벨 관점에서 모바일 장치(100)를 고려할 때, 도 2에 도시된 바와 같이, REE(120)는 제 1 레벨 가상화 주체이고, 노멀 영역(162)는 제 1 레벨 가상화 객체이고, TEE(140)는 제 2 레벨 가상화 주체이고, 보안 영역(164)는 제 2 레벨 가상화 객체이다. 제 1 레벨 가상화 주체(REE)는 IAP(무결성 보장 프로그램)를 이용하여 제 2 레벨 가상화 주체(TEE)로 무결성을 보장한 데이터(VSD)를 전송할 수 있다. 제 2 레벨 가상화 주체(TEE)는 이렇게 보장된 데이터(VSD)를 제 2 레벨 가상화 객체(보안 영역)에 저장할 수 있다.

[0054] 일반적인 모바일 장치는 REE 환경에서 TEE 환경에서 합법적 인증을 받기만 하면 자유롭게 보안 영역에 접근할 수 있었다. 예를 들어, 일반적인 모바일 장치는 노멀 OA 상의 트러스트존과 같은 모듈에서 접근 통제만 수행되고 있다. 그러나 합법적 인증이더라도 REE에 전송된 데이터에 악의적인 정보(바이러스, 스파이웨어, 악성코드 등)가 포함될 수 있다. 이 경우 TEE 환경이 해커에 의해 무력화될 수 있다.

[0055] 반면에, 본 발명의 실시 예에 따른 모바일 장치(100)는 REE(120)에서 발생된 데이터(SD)를 보안 영역(164)에 직접 저장하지 않고, IAP(150)에 의해 검증된 데이터(VSD)를 보안 영역(164)에 저장함으로써, 전송된 데이터의 무결성을 보장할 수 있다. 본 발명의 모바일 장치(100)는 그에 따른 해커의 잠재적인 활동을 저지할 수 있으며, 보안을 극대화시킬 수 있다.

[0056] 한편, 상술된 무결성 보장 동작은 XOR(exclusice or) 연산에 의해 구현될 수 있다.

[0057] 도 3은 본 발명의 실시 예에 따른 IAP(150)의 무결성 보장 동작을 예시적으로 보여주는 도면이다. 도 2 내지 도 3을 참조하면, 무결성 보장 동작은 다음과 같이 진행될 수 있다.

[0058] REE(120)의 APP는 보안 영역(164)에 저장할 오리지널 데이터(SD)를 생성할 수 있다. 이때 REE(120)의 APP는 IAP(150)로부터 무결성 보장을 위한 토큰 발행을 요청 및 발행된 토큰을 수신할 수 있다. REE(120)의 APP는 오리지널 데이터(SD)와 토큰을 제 1 XOR 연산함으로써 변형된 데이터(UDI: TSD)를 발생할 수 있다. 여기서 변형된 데이터(TSD)가 생성되는 과정이 변형 과정(TP)이라 하겠다.

[0059] 이후, REE(120)의 APP는 변형된 데이터(TSD)와 토큰을 IAP(150)에 전송할 수 있다. IAP(150)는 REE(120)의 APP로부터 변형된 데이터(TSD)와 토큰을 수신하고, 수신된 변형된 데이터(TSD)와 토큰을 제 2 XOR 연산함으로써 검증된 데이터(CDI: VSD)를 발생할 수 있다. 검증된 데이터(VSD)는 오리지널 데이터일 것이다. 검증된 데이터(VSD)가 보안 영역(164)에 저장될 수 있다.

[0060] 도 4는 본 발명의 실시 예에 따른 IAP(150)의 무결성 검증 과정(IVP)을 예시적으로 보여주는 도면이다. 도 4를 참조하면, IAP(150)는 REE(120)의 APP로부터 수신된 제 1 토큰과 내부에 존재하는 제 2 토큰을 비교함으로써, 수신된 데이터의 무결성 검증을 수행할 수 있다.

[0061] 도 5는 본 발명의 실시 예에 따른 무결성 보장 동작에서 토큰 발행 과정을 예시적으로 보여주는 래더 다이어그램이다. 도 2 내지 도 5를 참조하면, 무결성 보장 동작을 위한 토큰 발행과정은 다음과 같이 진행될 수 있다.

[0062] REE(120)의 APP는 IAP(150)에 보안 영역(164)에 접근을 요청할 수 있다. IAP(150)는 이러한 APP의 접근 요청을 수신하고, 인증 요청을 APP에 전송할 수 있다. APP는 이러한 인증 요청에 응답하여 사용자에게 의해 ID/패스워드 기입 혹은 생체 인식을 통한 생체 코드를 IAP(150)에 전송할 수 있다. IAP(150)는 수신된 ID/패스워드 혹은 생체 코드를 TEE(140)의 TAPP에 전송하면서 토큰 발행을 요청할 수 있다. TAPP는 이러한 요청에 응답하여 우선적으로 APP가 합법적인 사용자인지 인증을 수행하고, APP가 합법적인 사용자라면 토큰을 발행 및 저장할 수 있다. APP가 합법적인 사용자라는 것은 ID/패스워드 혹은 생체 코드의 확인 과정을 통해 수행될 수 있다. 이와 관련된 인증 관련 정보는 TEE(140)에 저장되어 있을 수 있다. 실시 예에 있어서, 발행된 토큰은 유효 시간 정보를 포함할 수 있다. TAPP에 의해 발행된 토큰은 IAP(150)에 전송될 수 있다. IAP(150)는 전송된 토큰을 REE(120)의 APP에 전송할 수 있다.

- [0063] 도 6은 본 발명의 실시 예에 따른 모바일 장치에 클락 윌슨 모델을 적용을 개념적으로 설명하는 도면이다. 도 6을 참조하면, 제 1 주체(S1)는 REE(120)이고, 제한되지 않은 데이터 항목(unconstrained data item, UDI; SD) 및 토큰을 가질 수 있다. IAP(150)에서 무결성 검증 절차를 수행함으로써, 제 1 주체(S1)의 제 1 제한된 데이터 항목(constrained data item, CDI1)이 발생 될 수 있다. 제 1 제한된 데이터 항목(CDI1)은 객체(0, 164)에 저장될 수 있다. 또한, 제 2 주체(S1)의 제 2 제한된 데이터 항목(CDI2)은 객체(0)에 저장될 수 있다.
- [0064] 한편, 상술 된 도 2에 도시된 IAP(150)의 기능은 TEE 내에서 수행될 수도 있다.
- [0065] 도 7은 본 발명의 실시 예에 따른 모바일 장치(100)의 동작 방법을 예시적으로 보여주는 도면이다. 도 2 내지 도 7을 참조하면, 모바일 장치(100)의 동작 방법을 다음과 같다.
- [0066] REE(120)의 APP로부터 보안 영역(164)에 대한 접근 요청에 응답하여 TEE(140)는 인증 동작을 수행할 수 있다(S110). TEE(140)는 대응하는 토큰을 수신할 수 있다(S120). REE(120)의 APP는 토큰을 이용하여 데이터를 변형할 수 있다(S130). REE(120)의 APP는 변형된 데이터 및 토큰을 TEE(140)으로 전송할 수 있다(S140).
- [0067] 도 8은 본 발명의 다른 실시 예에 따른 모바일 장치(100)의 동작 방법을 예시적으로 보여주는 도면이다. 도 2 내지 도 8을 참조하면, 모바일 장치(100)의 동작 방법은 다음과 같다.
- [0068] IAP(150)의 토큰 발행 요청에 응답하여 TEE(140)는 토큰을 발생할 수 있다(S210). 발생한 토큰은 REE(120)에 전송될 수 있다(S220). TEE(140)은 REE(120)로부터 변형된 데이터 및 토큰이 수신될 수 있다(S230). 수신된 토큰과 발생한 토큰이 동일한지 판별될 수 있다(S240). 만일 수신된 토큰과 발생한 토큰이 동일하다면, 토큰을 이용하여 변형된 데이터로부터 오리지널 데이터가 추출될 수 있다(S250).
- [0069] 본 발명에 따른 단계들 및/또는 동작들은 기술분야의 통상의 기술자에 의해 이해될 수 있는 것과 같이, 다른 순서로, 또는 병렬적으로, 또는 다른 에포크(epoch) 등을 위해 다른 실시 예들에서 동시에 일어날 수 있다.
- [0070] 실시 예에 따라서는, 단계들 및/또는 동작들의 일부 또는 전부는 하나 이상의 비-일시적 컴퓨터-판독가능 매체에 저장된 명령, 프로그램, 상호작용 데이터 구조(interactive data structure), 클라이언트 및/또는 서버를 구동하는 하나 이상의 프로세서들을 사용하여 적어도 일부가 구현되거나 또는 수행될 수 있다. 하나 이상의 비-일시적 컴퓨터-판독가능 매체는 예시적으로 소프트웨어, 펌웨어, 하드웨어, 및/또는 그것들의 어떠한 조합일 수 있다. 또한, 본 명세서에서 논의된 "모듈"의 기능은 소프트웨어, 펌웨어, 하드웨어, 및/또는 그것들의 어떠한 조합으로 구현될 수 있다.
- [0071] 본 발명의 실시 예들의 하나 이상의 동작들/단계들/모듈들을 구현/수행하기 위한 하나 이상의 비-일시적 컴퓨터-판독가능 매체 및/또는 수단들은 ASICs(application-specific integrated circuits), 표준 집적 회로들, 마이크로 컨트롤러를 포함하는, 적절한 명령들을 수행하는 컨트롤러, 및/또는 임베디드 컨트롤러, FPGAs(field-programmable gate arrays), CPLDs(complex programmable logic devices), 및 그와 같은 것들을 포함할 수 있지만, 여기에 한정되지는 않는다.
- [0072] 한편, 상술 된 본 발명의 내용은 발명을 실시하기 위한 구체적인 실시 예들에 불과하다. 본 발명은 구체적이고 실제로 이용할 수 있는 수단 자체뿐 아니라, 장치 기술로 활용할 수 있는 추상적이고 개념적인 아이디어인 기술적 사상을 포함할 것이다.

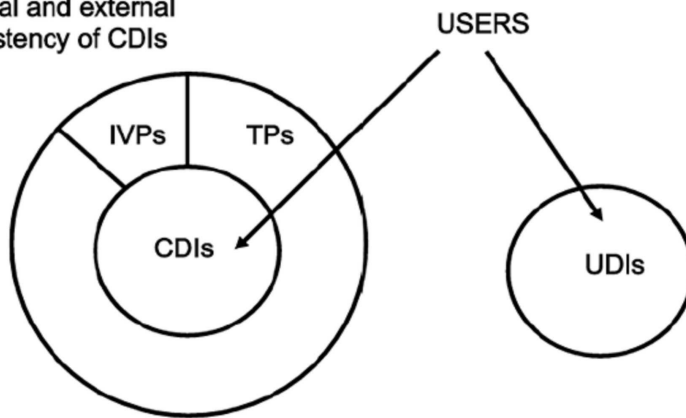
부호의 설명

- [0073] 100: 모바일 장치
- 120: REE
- 122: 노멀 OS
- 140: TEE
- 142: 보안 OS
- 150: IVP
- 160: 메모리 장치

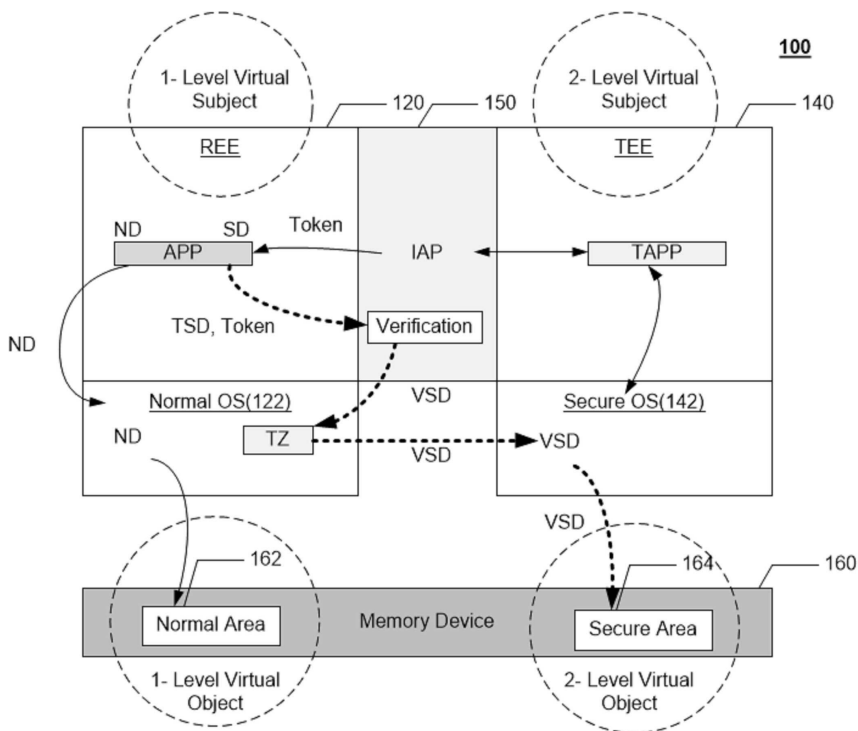
도면

도면1

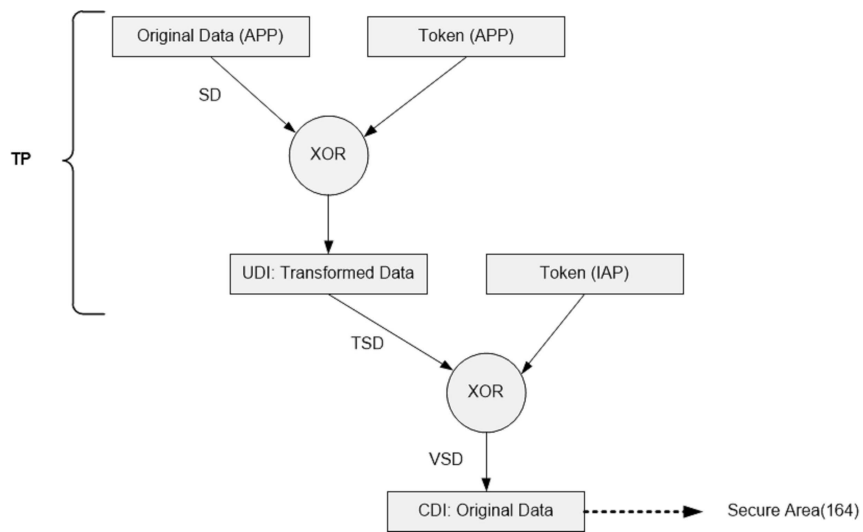
Internal and external consistency of CDIs



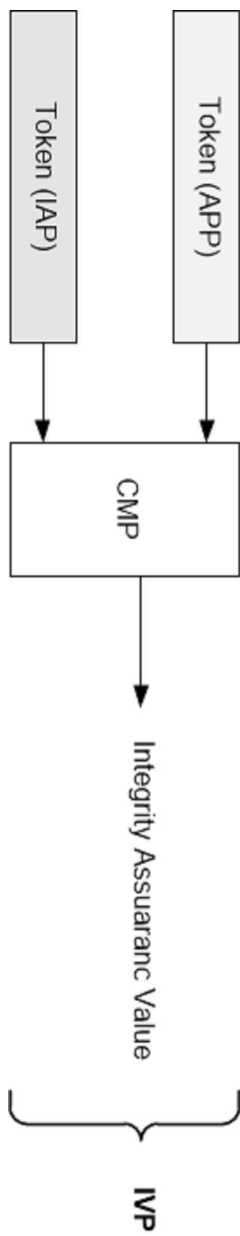
도면2



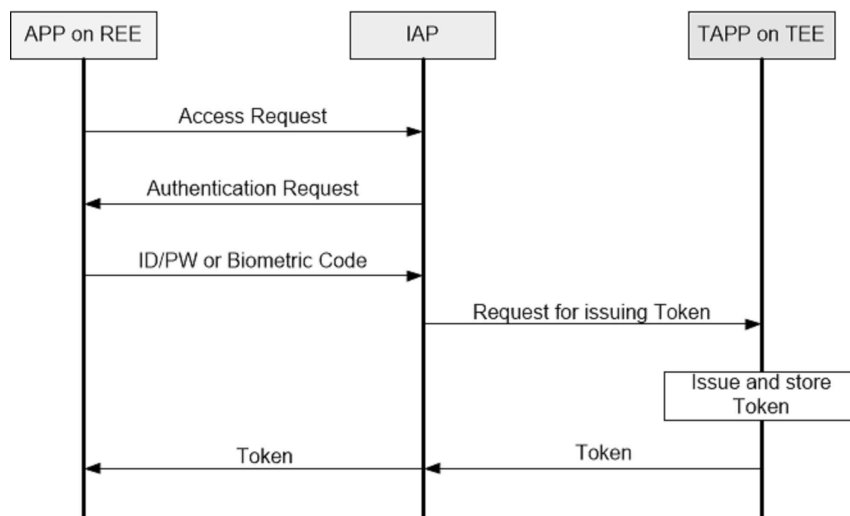
도면3



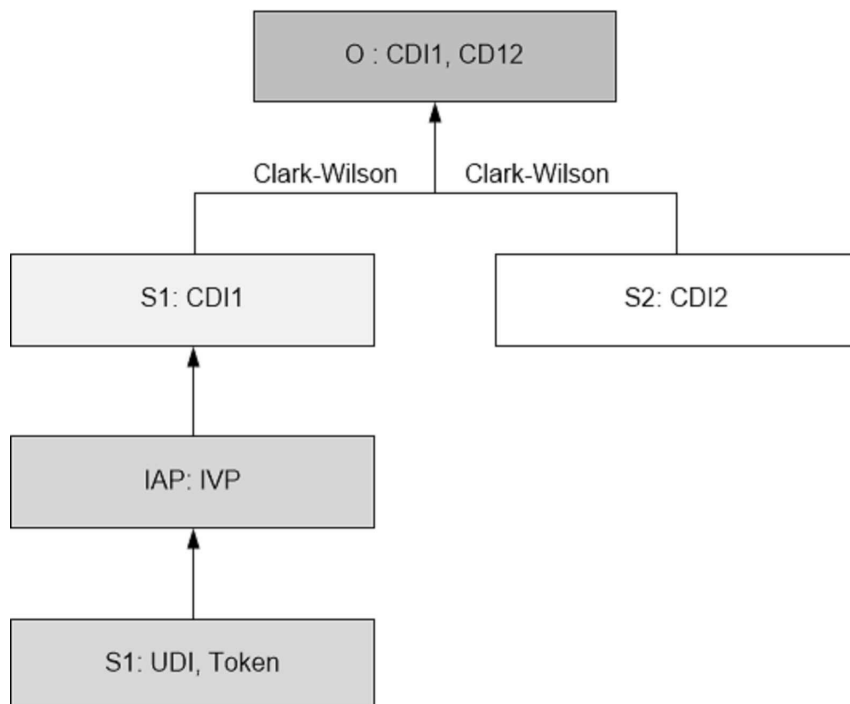
도면4



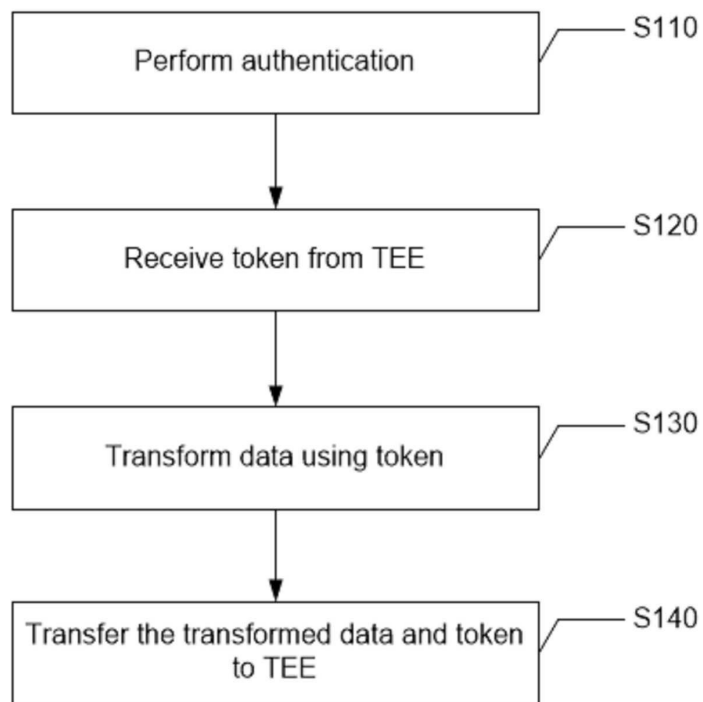
도면5



도면6



도면7



도면8

