

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2022-0140168
(43) 공개일자 2022년10월18일

- | | |
|--|---|
| (51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) G06F 21/64 (2013.01)
G06F 21/78 (2013.01)
(52) CPC특허분류
G06F 21/50 (2013.01)
G06F 21/64 (2013.01)
(21) 출원번호 10-2021-0046330
(22) 출원일자 2021년04월09일
심사청구일자 2021년04월09일 | (71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
장진수
대전광역시 유성구 대학로 99
류재철
대전광역시 유성구 대학로 99
박찬규
대전광역시 유성구 대학로 99
(74) 대리인
이은철, 김재문 |
|--|---|

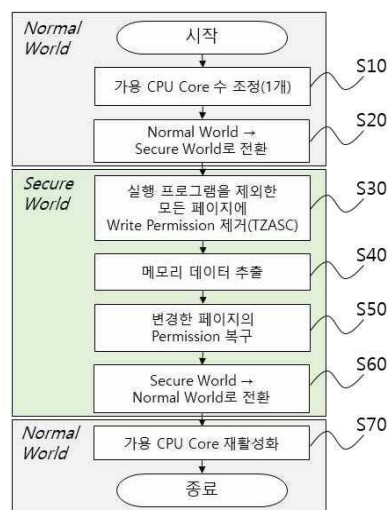
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법 및 시스템

(57) 요약

본 발명은 ARM 트러스트존(TrustZone)을 이용하여 모바일 디바이스 내 메모리 데이터가 변경될 수 있는 요소들을 최소화하고, 안정적으로 휘발성 메모리 데이터를 수집하는 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법 및 시스템에 관한 것이다. 본 발명의 실시 예에 따른 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법은 모바일 디바이스의 운영체제에서 사용중인 CPU 코어(Core)의 수를 한 개로 조정하는 단계(S10)와, ARM 프로세서의 실행환경을 일반영역(Normal World)에서 보안영역(Secure World)으로 전환하는 단계(S20)와, 상기 ARM 프로세서의 보안영역(Secure World)에서 일반영역의 모든 물리 메모리의 쓰기 권한(Write permission)을 제거하는 단계(S30) 및 쓰기 권한이 제거된 물리 메모리로부터 메모리 데이터를 추출하는 단계(S40)를 포함한다.

대표도 - 도3



(52) CPC특허분류

G06F 21/78 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711119385
과제번호	2020-0-01840
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발
연구과제명	스마트폰의 내부데이터 접근 및 보호 기술 분석
기 여 율	1/1
과제수행기관명	서울대학교 산학협력단
연구기간	2020.06.01 ~ 2027.12.03

명세서

청구범위

청구항 1

ARM 프로세서 기반 모바일 디바이스에서 휘발성 메모리 데이터를 추출하는 휘발성 데이터 획득 방법에 있어서,
모바일 디바이스의 운영체제에서 사용중인 CPU 코어(Core)의 수를 한 개로 조정하는 단계(S10);
ARM 프로세서의 실행환경을 일반영역(Normal World)에서 보안영역(Secure World)으로 전환하는 단계(S20);
상기 ARM 프로세서의 보안영역(Secure World)에서 일반영역의 모든 물리 메모리의 쓰기 권한(Write permission)을 제거하는 단계(S30); 및
쓰기 권한이 제거된 물리 메모리로부터 메모리 데이터를 추출하는 단계(S40)를 포함하는 휘발성 데이터 획득 방법.

청구항 2

제1항에 있어서,
상기 메모리 데이터를 추출하는 단계(S40) 이후에
쓰기 권한(Write permission)이 변경된 상기 물리 메모리의 퍼미션(Permission)을 이전 상태로 복구하는 단계(S50)와,
상기 ARM 프로세서의 실행환경을 보안영역(Secure World)에서 일반영역(Normal World)으로 전환하는 단계(S60) 및
상기 모바일 디바이스의 운영체제에서 비활성화된 CPU 코어(Core)를 재활성화하는 단계(S70)를 더 포함하는 휘발성 데이터 획득 방법.

청구항 3

제1항에 있어서,
상기 CPU 코어(Core)의 수를 한 개로 조정하는 단계(S10)는 ARM 프로세서의 일반영역(Normal World)에서 수행되는 것을 특징으로 하는 휘발성 데이터 획득 방법.

청구항 4

제1항에 있어서,
상기 물리 메모리의 쓰기 권한(Write permission)을 제거하는 단계(S30)는 보안영역에서 ARM 트러스트존(TrustZone)의 TZASC(TrustZone Address Space Controller)를 이용하여 물리 메모리의 퍼미션(Permission)을 변경하는 것을 특징으로 하는 휘발성 데이터 획득 방법.

청구항 5

ARM 프로세서 기반 모바일 디바이스에서 휘발성 메모리 데이터를 추출하는 휘발성 데이터 획득 시스템에 있어서,
모바일 디바이스의 운영체제에서 사용중인 CPU 코어(Core)의 동작을 비활성화 상태 또는 활성화 상태로 제어하

는 CPU 코어 제어부;

ARM 트러스트존(TrustZone)의 TZASC(Trustzone address space controller) 사용을 위해 ARM 프로세서의 실행환경을 일반영역(Normal World)에서 보안영역(Secure World)으로 전환하거나, 또는 실행환경을 보안영역(Secure World)에서 일반영역(Normal World)으로 전환하는 실행환경 변환부;

상기 ARM 프로세서의 보안영역(Secure World)에서 물리 메모리의 쓰기 권한(Write permission)을 변경하는 퍼미션 변환부; 및

상기 퍼미션 변환부를 통해 쓰기 권한이 제거된 물리 메모리로부터 메모리 데이터를 추출하는 데이터 추출부를 포함하는 휘발성 데이터 획득 시스템.

청구항 6

제5항에 있어서,

상기 퍼미션 변환부는 ARM 트러스트존(TrustZone)의 TZASC(TrustZone Address Space Controller)를 활용하여 특정 물리 메모리 영역에 대한 퍼미션(Permission)을 변경하며, 상기 TZASC에서 제공하는 레지스터를 이용하여 물리 메모리를 여러 구획으로 분할하고, 분할된 각 구획에 대한 메모리 접근 퍼미션을 설정하는 것을 특징으로 하는 휘발성 데이터 획득 시스템.

발명의 설명

기술 분야

- [0001] 본 발명은 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법 및 시스템에 관한 것으로서, 더욱 상세하게는 ARM 트러스트존(TrustZone)을 이용하여 모바일 디바이스(스마트폰, 태블릿 PC 등) 내 메모리 데이터가 변경될 수 있는 요소들을 최소화하고, 안정적으로 휘발성 메모리 데이터를 수집하는 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법 및 시스템에 관한 것이다.

배경 기술

- [0003] 일반적으로 디지털 포렌식(Digital Forensic)이란 컴퓨터나 스마트폰 내에 들어있는 데이터를 획득 및 분석하여 사건의 단서나 증거를 찾아내는 수사기법을 나타낸다. 또한, 메모리 포렌식(Memory Forensic)은 상기 디지털 포렌식에 포함되는 범주로서 RAM과 같은 휘발성 메모리를 대상으로 포렌식을 수행하는 기술을 나타낸다.
- [0004] 상기 휘발성 메모리에는 운영체제의 실행코드와 데이터를 비롯해 실행되는 모든 프로그램의 실행코드와 데이터가 메모리에 기록되었다가 삭제된다. 예를 들어, 데이터를 암호화하거나 암호화된 데이터를 처리할 때 평문은 메모리에 일시적으로 기록되는데, 평문 단계에서 메모리 데이터를 수집할 경우 복호화 과정 없이 데이터를 수집할 수 있다.
- [0005] 일반적인 모바일 디바이스에서는 여러 CPU 코어(Core)가 여러 프로그램의 실행코드를 동시에 처리하고 있어 메모리 기록과 삭제가 동시다발적으로 이루어지고 있다. 이로 인해, 메모리 데이터가 주기적으로 변경되어 안정적인 데이터 수집이 어려운 문제가 있다.
- [0006] 또한, 운영체제 수준의 악성코드(예, 루트킷)가 설치될 경우, 정상적인 메모리 수집을 방해할 수 있다. 따라서, 본 발명은 ARM 프로세서 기반 모바일 디바이스 기기에서 휘발성 메모리 데이터를 안정적으로 획득하는 방법 및 시스템을 제시하고자 한다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허 제10-2079124호(2020년 02월 19일 공고)

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적 과제는 종래의 단점을 해결한 것으로서, 모바일 디바이스의 메모리로부터 데이터를 획득할 수 있는 디지털 포렌식 방법을 제공하고자 하는데 그 목적이 있다. 또한, ARM 프로세서 기반의 모바일 디바이스에서 운영체제 수준의 악성코드가 설치된 상황에서도 휘발성 메모리 데이터를 안정적으로 수집하고자 하는데 그 목적이 있다.

과제의 해결 수단

[0011] 이러한 기술적 과제를 이루기 위한 본 발명의 일 측면에 따른 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법은 모바일 디바이스의 운영체제에서 사용중인 CPU 코어(Core)의 수를 한 개로 조정하는 단계(S10)와, ARM 프로세서의 실행환경을 일반영역(Normal World)에서 보안영역(Secure World)으로 전환하는 단계(S20)를 포함한다.

[0012] 또한, 본 발명은 상기 ARM 프로세서의 보안영역(Secure World)에서 일반영역의 모든 물리 메모리의 쓰기 권한(Write permission)을 제거하는 단계(S30) 및 쓰기 권한이 제거된 물리 메모리로부터 메모리 데이터를 추출하는 단계(S40)를 포함한다.

[0013] 또한, 본 발명은 쓰기 권한(Write permission)이 변경된 상기 물리 메모리의 퍼미션(Permission)을 이전 상태로 복구하는 단계(S50)와, 상기 ARM 프로세서의 실행환경을 보안영역(Secure World)에서 일반영역(Normal World)으로 전환하는 단계(S60) 및 상기 모바일 디바이스의 운영체제에서 비활성화된 CPU 코어(Core)를 재활성화하는 단계(S70)를 포함한다.

[0014] 바람직하게는, 상기 CPU 코어(Core)의 수를 한 개로 조정하는 단계(S10)는 ARM 프로세서의 일반영역(Normal World)에서 수행된다. 또한, 상기 물리 메모리의 쓰기 권한(Write permission)을 제거하는 단계(S30)는 보안영역에서 ARM 트러스트존(TrustZone)의 TZASC(TrustZone Address Space Controller)를 이용하여 물리 메모리의 퍼미션(Permission)을 변경한다.

[0015] 또한, 본 발명의 다른 측면에 따른 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 시스템은 모바일 디바이스의 운영체제에서 사용중인 CPU 코어(Core)의 동작을 비활성화 상태 또는 활성화 상태로 제어하는 CPU 코어 제어부와, ARM 트러스트존(TrustZone)의 TZASC(Trustzone address space controller) 사용을 위해 ARM 프로세서의 실행환경을 일반영역(Normal World)에서 보안영역(Secure World)으로 전환하거나, 또는 실행환경을 보안영역(Secure World)에서 일반영역(Normal World)으로 전환하는 실행환경 변환부를 포함한다.

[0016] 또한, 본 발명은 상기 ARM 프로세서의 보안영역(Secure World)에서 물리 메모리의 쓰기 권한(Write permission)을 변경하는 퍼미션 변환부와, 상기 퍼미션 변환부를 통해 쓰기 권한이 제거된 물리 메모리로부터 메모리 데이터를 추출하는 데이터 추출부를 포함한다.

[0017] 바람직하게는, 상기 퍼미션 변환부는 ARM 트러스트존(TrustZone)의 TZASC(TrustZone Address Space Controller)를 활용하여 특정 물리 메모리 영역에 대한 퍼미션(Permission)을 변경하며, 상기 TZASC에서 제공하는 레지스터를 이용하여 물리 메모리를 여러 구획으로 분할하고, 분할된 각 구획에 대한 메모리 접근 퍼미션을 설정한다.

발명의 효과

[0019] 이상에서 설명한 바와 같이, 본 발명에 따른 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 방법 및 시스템은 모바일 디바이스의 메모리로부터 의미 있는 데이터를 획득할 수 있는 효과가 있다. 또한, 모바일 디바이스 내의 메모리가 변경될 수 있는 요소들을 최소화하여 ARM 프로세서 기반의 모바일 디바이

스에서 안정적으로 휘발성 메모리 데이터를 수집할 수 있는 효과가 있다.

도면의 간단한 설명

도 1은 ARM 프로세서 트러스트존(TrustZone)을 나타내는 도면이다.

도 2는 본 발명의 실시 예에 따른 휘발성 데이터 획득 시스템을 나타내는 구성도이다.

도 3은 본 발명의 실시 예에 따른 휘발성 데이터 획득 방법을 나타내는 순서도이다.

발명을 실시하기 위한 구체적인 내용

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면부호를 붙였다.

명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "...모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어 또는 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예를 설명함으로써, 본 발명을 상세히 설명한다.

각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

도 1은 ARM 프로세서 트러스트존(TrustZone)(120)을 나타내는 도면이고, 도 2는 본 발명의 실시 예에 따른 휘발성 데이터 획득 시스템(20)을 나타내는 구성도이다.

최근 모바일 디바이스(예를 들어, 스마트폰, 태블릿 PC 등)(10)의 대부분은 ARM 프로세서(100)를 기반으로 생산된다. 또한, ARM 프로세서(100)에는 트러스트존(TrustZone)(120)이라는 신뢰 실행 환경(Trusted Execution Environment) 모듈을 제공한다.

이러한 ARM 트러스트존(120)을 활용하면 시스템을 일반영역(Normal World)(121)과 보안영역(Secure World)(122)으로 구분할 수 있다. 일반적인 운영체제 및 애플리케이션은 일반영역(Normal World)(121) 상에서 실행되고, 보안 OS나 검증된 모듈들은 보안영역(Secure World)(122) 상에서 실행된다.

본 발명은 트러스트존 모듈(120) 중 TZASC(TrustZone Address Space Controller)(123)에서 제공하는 기능을 이용하여 물리 메모리(210)의 시작 물리 주소와 끝 물리 주소를 설정하고, 해당 영역에 대한 메모리 접근 권한을 설정한다.

본 발명의 실시 예에 따른 ARM 프로세서 기반 모바일 디바이스에서 안정적인 휘발성 데이터 획득 시스템(20)은 CPU 코어 제어부(300), 실행환경 변환부(400), 퍼미션 변환부(500), 데이터 추출부(600) 및 데이터베이스(700)를 포함한다.

CPU 코어 제어부(300)는 모바일 디바이스(10)의 운영체제에서 사용중인 CPU 코어(Core)(110)의 동작을 제어한다. 즉, CPU 코어 제어부(300)는 모바일 디바이스(10)의 운영체제에서 사용중인 CPU 코어(Core)(110)의 동작을 비활성화하여 동작을 제한하거나, 동작이 비활성화된 CPU 코어(Core)(110)를 재활성화하여 다시 동작이 가능하게 조정할 수 있다.

예를 들어, CPU 코어 제어부(300)는 모바일 디바이스(10)의 운영체제에서 가용중인 CPU 코어(Core)(110)의 수가 하나가 되도록 미리 선택된 하나의 CPU 코어(110)를 제외한 다른 프로세서들의 동작을 비활성화할 수 있다.

또한, 실행환경 변환부(400)는 ARM 트러스트존(TrustZone) 모듈(120)의 TZASC(Trustzone address space controller)(123) 사용을 위해 ARM 프로세서(100)의 실행환경을 일반영역(Normal World)(121)에서 보안영역(Secure World)(122)으로 전환하거나, 또는 보안영역(Secure World)(122)에서 일반영역(Normal World)(121)으로 전환할 수 있다.

- [0034] 또한, 퍼미션 변환부(500)는 ARM 프로세서(100)의 보안영역(Secure World)(122)에서 물리 메모리(210)의 쓰기 권한(Write permission)을 변경할 수 있다. 예를 들어, 퍼미션 변환부(500)는 ARM 프로세서(100)의 보안영역(Secure World)(122)에서 실행 프로그램을 제외한 모든 물리 메모리(210)의 쓰기 권한(Write permission)을 제거하거나, 쓰기 권한(Write permission)이 변경된 상기 물리 메모리(210)의 퍼미션(Permission)을 이전 상태로 복구할 수 있다.
- [0035] 이때, 퍼미션 변환부(500)는 ARM 트러스트존(TrustZone)(120)의 TZASC(TrustZone Address Space Controller)(123)를 활용하여 특정 물리 메모리(210) 영역에 대한 퍼미션(Permission)을 변경한다.
- [0036] 또한, 퍼미션 변환부(500)는 TZASC(123) 기능 또는 TZASC(123)에서 제공하는 레지스터를 이용하여 물리 메모리(210)를 기준으로 구획을 여러 구획으로 분할하고, 분할된 각 구획에 대한 메모리 접근 퍼미션을 설정할 수 있다. 예를 들어, 퍼미션 변환부(500)는 안정적인 메모리(200) 획득을 위해 일반 실행 환경(121)에서 사용하는 모든 물리 영역에 대한 쓰기 권한을 제거할 수 있다.
- [0037] 일반적으로 컴퓨터 또는 모바일 디바이스(10)는 실제 메모리(Physical Memory)(210)를 추상화하여 가상 메모리(Virtual Memory)(220)로 적용하여 사용함으로써 프로세스들이 연속된 물리적 메모리(210) 공간처럼 인식하도록 만들 수 있을 뿐만 아니라 실제 메모리보다 많은 양의 메모리 운용이 가능하다.
- [0038] 또한, 본 발명의 데이터 추출부(600)는 퍼미션 변환부(500)를 통해 쓰기 권한이 제거된 물리 메모리(210)로부터 메모리 데이터를 추출한다. 또한, 데이터베이스(700)는 데이터 추출부(600)가 추출한 메모리 데이터를 저장한다.
- [0039] 도 3은 본 발명의 실시 예에 따른 휘발성 데이터 획득 방법을 나타내는 순서도이다.
- [0040] 본 발명의 실시 예에 따른 ARM 프로세서 기반 모바일 디바이스(10)에서 안정적인 휘발성 데이터 획득 방법은 CPU 코어 제어부(300)가 모바일 디바이스(10)의 운영체제에서 사용중인 CPU 코어(Core)(110)의 수를 한 개로 조정하는 단계(S10)와, 실행환경 변환부(400)가 ARM 프로세서(100)의 실행환경을 일반영역(Normal World)(121)에서 보안영역(Secure World)(122)으로 전환하는 단계(S20)를 포함한다.
- [0041] 즉, CPU 코어 제어부(300)가 모바일 디바이스(10)의 운영체제에서 가용중인 CPU 코어(Core)(110)의 수가 하나가 되도록 미리 선택된 하나의 CPU 코어(110)를 제외한 다른 프로세서들의 동작을 비활성화하여 다른 프로세서들의 동작을 제한한다(S10). 이때, 상기 CPU 코어(Core)(110)의 수를 한 개로 조정하는 단계(S10)는 ARM 프로세서(100)의 일반영역(Normal World)(121)에서 수행된다.
- [0042] 또한, 실행환경 변환부(400)는 ARM 트러스트존(TrustZone) 모듈(120)의 TZASC(Trustzone address space controller)(123) 사용을 위해 ARM 프로세서(100)의 실행환경을 일반영역(Normal World)(121)에서 보안영역(Secure World)(122)으로 전환한다(S20).
- [0043] 또한, 본 발명은 퍼미션 변환부(500)가 ARM 프로세서(100)의 보안영역(Secure World)(122)에서 일반영역(121)의 모든 물리 메모리(210)의 쓰기 권한(Write permission)을 제거하는 단계(S30)와, 데이터 추출부(600)가 쓰기 권한이 제거된 물리 메모리(210)로부터 메모리 데이터를 추출하는 단계(S40)를 포함한다. 즉, 퍼미션 변환부(500)는 일반영역(121)에서 사용하는 모든 물리 메모리(210)의 쓰기 권한을 제거할 수 있다(S30).
- [0044] 또한, 본 발명은 퍼미션 변환부(500)가 쓰기 권한(Write permission)이 변경된 물리 메모리(210)의 퍼미션(Permission)을 이전 상태로 복구하는 단계(S50)와, 실행환경 변환부(400)가 ARM 프로세서(100)의 실행환경을 보안영역(Secure World)(122)에서 일반영역(Normal World)(121)으로 전환하는 단계(S60)와, CPU 코어 제어부(300)가 모바일 디바이스(10)의 운영체제에서 비활성화된 CPU 코어(Core)(110)를 재활성화하는 단계(S70)를 포함한다.
- [0045] 즉, CPU 코어 제어부(300)는 상기 CPU 코어(Core)(110)의 수를 한 개로 조정하는 단계(S10)에서 동작이 비활성화된 가용 CPU 코어(Core)(110)를 재활성화하여 프로세서들의 동작이 다시 가능하도록 조정한다(S70).
- [0046] 이와 같이 본 발명의 실시 예에 따른 휘발성 데이터 획득 방법 및 시스템(20)은 ARM 트러스트존(120) 기능을 활용하여 모바일 디바이스(10) 내 휘발성 메모리 데이터를 안정적으로 획득할 수 있는 효과가 있다.
- [0047] 이상으로 본 발명에 관한 바람직한 실시예를 설명하였으나, 본 발명은 상기 실시예에 한정되지 아니하며, 본 발명의 실시예로부터 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의한 용이하게 변경되어 균등하다고 인정되는 범위의 모든 변경을 포함한다.

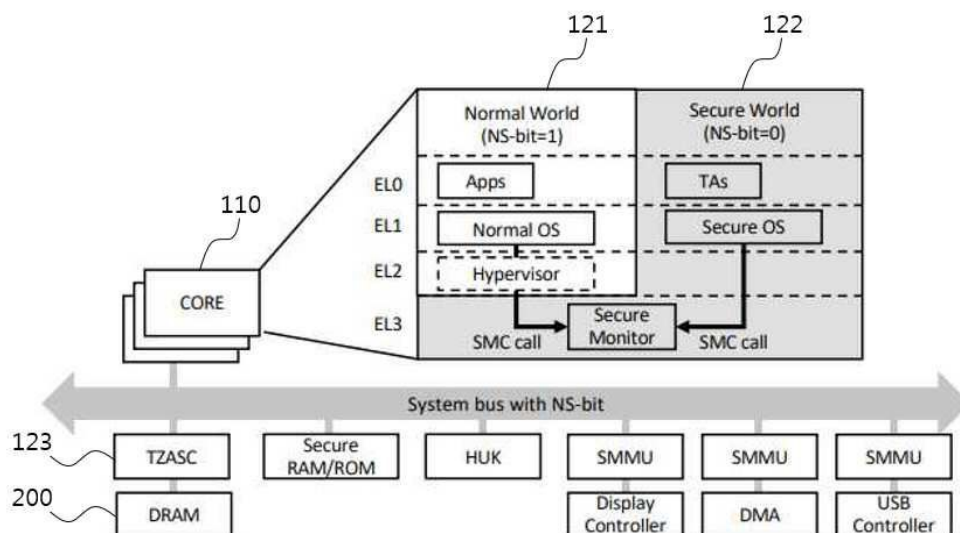
부호의 설명

[0049]

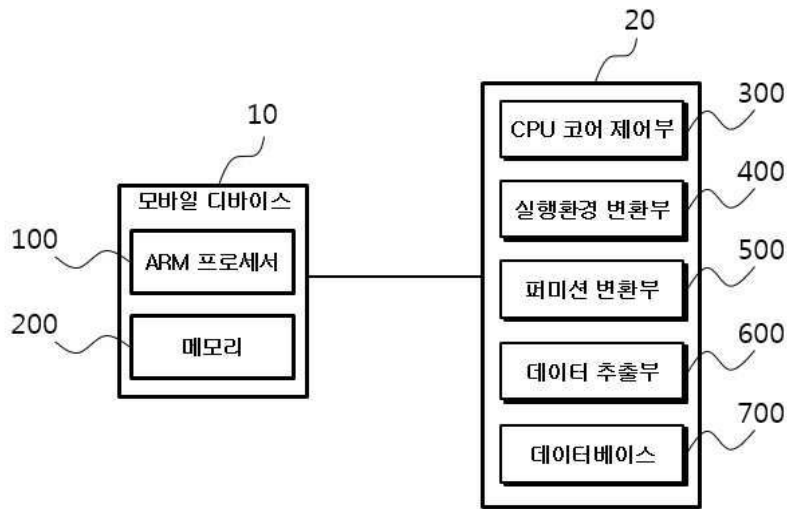
- 10 : 모바일 디바이스
- 20 : 휘발성 데이터 획득 시스템
- 100 : ARM 프로세서
- 110 : CPU 코어(Core)
- 120 : ARM 트러스트존(TrustZone)
- 121 : 일반영역(Normal World)
- 122 : 보안영역(Secure World)
- 123 : TZASC(TrustZone Address Space Controller)
- 200 : 메모리
- 210 : 물리 메모리(Physical Memory)
- 220 : 가상 메모리(Virtual Memory)
- 300 : CPU 코어 제어부
- 400 : 실행환경 변환부
- 500 : 퍼미션 변환부
- 600 : 데이터 추출부
- 700 : 데이터베이스

도면

도면1



도면2



도면3

