	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2013-0017762 (43) 공개일자 2013년02월20일
(51) 국제특허분류(Int. Cl.) G06F 21/22 (2006.01) G06F 21/20 (2006.01)		(71) 출원인 한국전자통신연구원
(21) 출원번호	10-2011-0080381	대전광역시 유성구 가정로 218 (가정동)
(22) 출원일자	2011년08월12일	(72) 발명자
심사청구일자	없음	김영호
기술이전 희망	기술양도, 실시권허여, 기술지도	
		서울특별시 성동구 행당로 82, 한진아파트 105동 2102호 (행당동)
		김정녀
		대전광역시 유성구 문지로 22, 101동 103호 (도룡동, 우성아파트)
		(뒷면에 계속)
		(74) 대리인
		제일특허법인

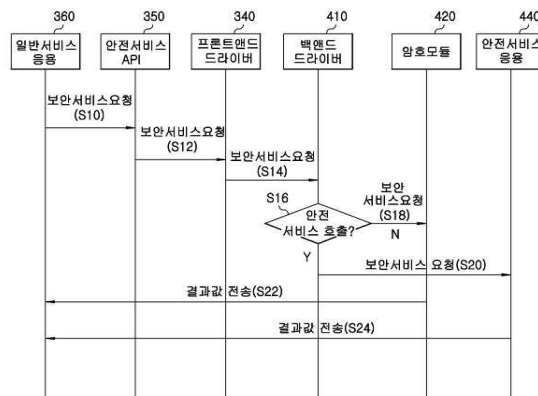
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 도메인 분리 기반 안전 실행 환경 제공 방법 및 장치

(57) 요약

본 발명은 모바일 단말에서 안전한 소프트웨어 실행 환경을 제공하기 위한 방법 및 장치에 있어서, 가상화 기반의 도메인 분리를 통해서 독립적인 두 개의 실행환경을 구성하고, 분리된 도메인 간 보안 서비스 채널을 통해 안전 서비스를 제공함으로써, 단말에서 실행되는 소프트웨어에 대한 보안성을 높이고 외부의 불법적인 접근으로부터 내부 정보를 보호할 수 있다.

대표도 - 도3



(72) 발명자

전용성

대전광역시 서구 월평전사로 11, 102동 1002호 (월평동, 무지개아파트)

주홍일

대전광역시 서구 월평동로 83, 102동 908호 (월평동, 다모아아파트)

이윤경

대전광역시 유성구 배울2로 19, 대덕테크노밸리 꿈에그린아파트 910동 1202호 (관평동)

이 발명을 지원한 국가연구개발사업

과제고유번호 11921-05001

부처명 방송통신위원회

연구사업명 방송통신기술개발사업(●한국전자통신연구원연구개발지원)

연구과제명 다자간 협업을 위한 몰입형 스마트워크 핵심기술 개발

주관기관 한국전자통신연구원

연구기간 2011.03.01 ~ 2015.02.28

특허청구의 범위

청구항 1

도메인 분리 기반 안전 실행 환경 제공 장치로서,
모바일 단말기에서 일반 서비스로 요청되는 동작을 수행하는 일반 서비스 도메인과,
상기 일반 서비스 도메인과 가상화 기반으로 분리되어 보안 서비스로 요청되는 동작을 수행하는 안전 서비스 도메인
을 포함하는 도메인 분리 기반 안전 실행 환경 제공 장치.

청구항 2

제 1 항에 있어서,
상기 일반 서비스 도메인은,
모바일 응용에서 제공되지 않는 보안 서비스를 연동시키는 일반 서비스 응용과,
상기 일반 서비스 응용에서 요청되는 상기 보안 서비스를 상기 안전 서비스 도메인으로 연동시키는 안전 서비스 API와,
상기 안전 서비스 API로부터 수신 받은 상기 보안 서비스를 상기 안전 서비스 도메인으로 전송하여 실행시키는
프론트 엔드 드라이버
를 포함하는 것을 특징으로 하는 도메인 분리 기반 안전 실행 환경 제공 장치.

청구항 3

제 1 항에 있어서,
상기 안전 서비스 도메인은,
상기 안전 서비스 도메인에서 호출된 보안 서비스를 수행하는 안전 서비스 응용과,
상기 안전 서비스 응용에서 수행되는 보안 서비스를 인터페이스하는 암호 API와,
상기 암호 API로부터 전송되는 상기 보안 서비스를 실행하는 암호 모듈
을 포함하는 것을 특징으로 하는 도메인 분리 기반 안전 실행 환경 제공 장치.

청구항 4

제 3 항에 있어서,
상기 안전 서비스 도메인은,
상기 일반 서비스 도메인으로부터 전송되는 보안 서비스의 수행 요청을 수신하여 상기 암호 모듈 또는 안전 서비스 응용으로 전송하고, 상기 보안 서비스를 수행한 결과를 제공하는 백엔드 드라이버
를 더 포함하는 것을 특징으로 하는 도메인 분리 기반 안전 실행 환경 제공 장치.

청구항 5

제 2 항에 있어서,
상기 프론트 엔드 드라이버는,

상기 보안 서비스에 대한 실행 요청을 하이퍼바이저에서 제공하는 도메인간 통신 방식을 이용하여 상기 안전 서비스 도메인으로 전송하는 것을 특징으로 하는 도메인 분리 기반 안전 실행 환경 제공 장치.

청구항 6

도메인 분리 기반 안전 서비스 실행 방법으로서,

모바일 단말에서 실행되는 응용 프로그램의 도메인을 가상화 기반으로 일반 서비스 도메인과 안전 서비스 도메인으로 분리시키는 단계와,

상기 일반 서비스 도메인에서 보안 서비스가 호출되는 경우 상기 보안 서비스의 요청을 상기 안전 서비스 도메인으로 전송하는 단계와,

상기 안전 서비스 도메인에서 상기 보안 서비스를 수행하고, 수행 결과를 상기 일반 서비스 도메인으로 전송하는 단계

를 포함하는 도메인 분리 기반 안전 서비스 실행 방법.

청구항 7

제 6 항에 있어서,

상기 안전 서비스 도메인으로 전송하는 단계는,

상기 일반 서비스 도메인에서 일반 서비스 응용으로 보안 서비스가 호출되는 단계와,

상기 보안 서비스가 안전 서비스 API를 통해 상기 일반 서비스 도메인의 프론트 엔드 드라이버로 전송되는 단계와,

상기 프론트 엔드 드라이버에서 상기 안전 서비스 도메인의 백엔드 드라이버로 상기 보안 서비스가 전송되는 단계와,

상기 안전 서비스 도메인의 안전 서비스 응용에서 상기 보안 서비스가 수행되는 단계

를 포함하는 도메인 분리 기반 안전 서비스 실행 방법.

청구항 8

제 6 항에 있어서,

상기 안전 서비스 도메인으로 전송하는 단계는,

상기 일반 서비스 도메인에서 일반 서비스 응용으로 보안 서비스가 호출되는 단계와,

상기 보안 서비스가 안전 서비스 API를 통해 상기 일반 서비스 도메인의 프론트 엔드 드라이버로 전송되는 단계와,

상기 프론트 엔드 드라이버에서 상기 안전 서비스 도메인의 백엔드 드라이버로 상기 보안 서비스가 전송되는 단계와,

상기 안전 서비스 도메인의 암호 모듈에서 상기 보안 서비스가 수행되는 단계

를 포함하는 도메인 분리 기반 안전 서비스 실행 방법.

청구항 9

제 7 항 또는 제 8 항에 있어서,

상기 보안 서비스는,

하이퍼바이저에서 제공하는 도메인간 통신 방식을 이용하여 상기 프론트 앤드 드라이버에서 상기 백엔드 드라이버로 전송되는 것을 특징으로 하는 도메인 분리 기반 안전 서비스 실행 방법.

청구항 10

도메인 분리 기반 안전 서비스 실행 방법으로서,

모바일 단말에서 실행되는 응용 프로그램의 도메인을 가상화 기반으로 일반 서비스 도메인과 안전 서비스 도메인으로 분리시키는 단계와,

상기 안전 서비스 도메인의 안전 서비스 응용에서 보안 서비스가 호출되는 단계와,

상기 안전 서비스 응용에서 상기 안전 서비스 도메인의 암호 모듈로 상기 보안 서비스를 전송하는 단계와,

상기 암호 모듈에서 상기 보안 서비스를 수행하는 단계

를 포함하는 도메인 분리 기반 안전 서비스 실행 방법.

명세서

기술분야

- [0001] 본 발명은 모바일 단말(mobile terminal)에서 안전한 소프트웨어 실행 환경을 제공하기 위한 방법 및 장치에 관한 것으로, 특히 모바일 단말 환경에서 소프트웨어(software) 실행 및 데이터 보호(data protection)를 위한 보안 분야에서 소프트웨어 공격으로 인한 침해 확산을 차단하고 안전한 서비스를 불법적인 공격으로부터 보호할 수 있도록 하는 도메인 분리 기반 안전 실행 환경 제공 방법 및 장치에 관한 것이다.

배경기술

- [0002] 일반적으로 종래의 모바일 단말 보호 기술은 전용 하드웨어(hardware)를 탑재한 방식과 악성코드 탐지 등 소프트웨어를 이용한 방식으로 분류된다. 특히 하드웨어를 이용한 방식은 암호 알고리즘 및 키 정보를 별도의 폐쇄된 물리적 장치 내부에서 관리하여 안전성은 높지만 물리적 장치의 자원 한계로 아주 제한적인 형태로만 적용되고 있다. 따라서 단말에서 동작되는 다양하고 복잡한 프로그램 또는 실행 환경을 보호하는 데에는 한계가 있다.
- [0003] 반면, 소프트웨어를 이용한 보안 기술은 물리적 자원에 대한 제한은 없지만, 단일 도메인으로 구성된 현재의 플랫폼 환경으로 인하여 해킹 및 불법 관리자 권한 획득(rooting) 공격에 의한 불법적인 정보 유출이 가능하다.
- [0004] 즉, 기존의 단말 소프트웨어 실행환경은 운영체제 및 응용 프로그램이 하나의 도메인을 구성하기 때문에 외부의 악의적인 공격 또는 내부 소프트웨어 결함으로 인하여 도메인 내에서 실행되는 모든 소프트웨어의 실행 정보 및 중요 데이터에 대한 불법 유출이 가능하다.

선행기술문헌

특허문헌

- [0005] (특허문헌 0001) 대한민국 공개특허공보 10-2008-0093359호 공개일자 2008년 10월 21일에는 가상화 환경에서 악성코드(malware) 등 악의적인 접근으로부터 시스템 자원을 보호하는 기술이 개시되어 있다.
- (특허문헌 0002) 대한민국 공개특허 10-2009-0044971호 공개일자 2010년 02월 17일에는 두 개 이상의 도메인 환경에서 하드웨어 디바이스를 포함하는 가상화 장치에 접근할 때 접근 제어 모듈을 이용하여 접근에 대한 동작을 제어하는 기술이 개시되어 있다.

발명의 내용

해결하려는 과제

- [0006] 한편, 현재 모바일 단말 환경에서의 보안 기술은 악성 코드 탐지 및 접근 제어 기술 등을 응용 프로그램 또는 운영체제 단계의 소프트웨어 방식으로 접근하고 있으며, 이러한 기술들은 해킹 또는 불법 관리자 권한 획득 (rooting) 등의 공격에 취약성을 보이고 있다. 따라서 모바일 오피스 또는 금융 서비스에서 반드시 요구되는 프로그램 실행에 관한 보안성 및 안전성을 제공하기 위해서 단말 보안 기술이 절실히 요구되고 있다.
- [0007] 따라서, 본 발명은 단일 도메인으로 구성된 실행 환경이 갖는 보안상 문제점을 해결하기 위하여, 모바일 단말 환경에서 소프트웨어 실행 및 데이터 보호를 위한 보안 분야에서 소프트웨어 공격으로 인한 침해 확산을 차단하고 안전한 서비스를 불법적인 공격으로부터 보호할 수 있도록 하는 도메인 분리 기반 안전 실행 환경 제공 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

- [0008] 상술한 본 발명은 도메인 분리 기반 안전 실행 환경 제공 장치로서, 모바일 단말기에서 일반 서비스로 요청되는 동작을 수행하는 일반 서비스 도메인과, 상기 일반 서비스 도메인과 가상화 기반으로 분리되어 보안 서비스로 요청되는 동작을 수행하는 안전 서비스 도메인을 포함한다.
- [0009] 또한, 상기 일반 서비스 도메인은, 모바일 응용에서 제공되지 않는 보안 서비스를 연동시키는 일반 서비스 응용과, 상기 일반 서비스 응용에서 요청되는 상기 보안 서비스를 상기 안전 서비스 도메인으로 연동시키는 안전 서비스 API와, 상기 안전 서비스 API로부터 수신 받은 상기 보안 서비스를 상기 안전 서비스 도메인으로 전송하여 실행시키는 프론트 엔드 드라이버를 포함하는 것을 특징으로 한다.
- [0010] 또한, 상기 안전 서비스 도메인은, 상기 안전 서비스 도메인에서 호출된 보안 서비스를 수행하는 안전 서비스 응용과, 상기 안전 서비스 응용에서 수행되는 보안 서비스를 인터페이스하는 암호 API와, 상기 암호 API로부터 전송되는 상기 보안 서비스를 실행하는 암호 모듈을 포함하는 것을 특징으로 한다.
- [0011] 또한, 상기 안전 서비스 도메인은, 상기 일반 서비스 도메인으로부터 전송되는 보안 서비스의 수행 요청을 수신하여 상기 암호 모듈 또는 안전 서비스 응용으로 전송하고, 상기 보안 서비스를 수행한 결과를 제공하는 백엔드 드라이버를 더 포함하는 것을 특징으로 한다.
- [0012] 또한, 상기 프론트 엔드 드라이버는, 상기 보안 서비스에 대한 실행 요청을 하이퍼바이저에서 제공하는 도메인 간 통신 방식을 이용하여 상기 안전 서비스 도메인으로 전송하는 것을 특징으로 한다.
- [0013] 또한, 본 발명은 도메인 분리 기반 안전 서비스 실행 방법으로서, 모바일 단말에서 실행되는 응용 프로그램의 도메인을 가상화 기반으로 일반 서비스 도메인과 안전 서비스 도메인으로 분리시키는 단계와, 상기 일반 서비스 도메인에서 보안 서비스가 호출되는 경우 상기 보안 서비스의 요청을 상기 안전 서비스 도메인으로 전송하는 단계와, 상기 안전 서비스 도메인에서 상기 보안 서비스를 수행하고, 수행 결과를 상기 일반 서비스 도메인으로 전송하는 단계를 포함한다.
- [0014] 또한, 상기 안전 서비스 도메인으로 전송하는 단계는, 상기 일반 서비스 도메인에서 일반 서비스 응용으로 보안 서비스가 호출되는 단계와, 상기 보안 서비스가 안전 서비스 API를 통해 상기 일반 서비스 도메인의 프론트 엔드 드라이버로 전송되는 단계와, 상기 프론트 엔드 드라이버에서 상기 안전 서비스 도메인의 백엔드 드라이버로 상기 보안 서비스가 전송되는 단계와, 상기 안전 서비스 도메인의 안전 서비스 응용에서 상기 보안 서비스가 수행되는 단계를 포함한다.
- [0015] 또한, 상기 안전 서비스 도메인으로 전송하는 단계는, 상기 일반 서비스 도메인에서 일반 서비스 응용으로 보안 서비스가 호출되는 단계와, 상기 보안 서비스가 안전 서비스 API를 통해 상기 일반 서비스 도메인의 프론트 엔드 드라이버로 전송되는 단계와, 상기 프론트 엔드 드라이버에서 상기 안전 서비스 도메인의 백엔드 드라이버로 상기 보안 서비스가 전송되는 단계와, 상기 안전 서비스 도메인의 암호 모듈에서 상기 보안 서비스가 수행되는 단계를 포함한다.
- [0016] 또한, 상기 보안 서비스는, 하이퍼바이저에서 제공하는 도메인간 통신 방식을 이용하여 상기 프론트 엔드 드라

이버에서 상기 백엔드 드라이버로 전송되는 것을 특징으로 한다.

[0017] 또한, 본 발명은 도메인 분리 기반 안전 서비스 실행 방법으로서, 모바일 단말에서 실행되는 응용 프로그램의 도메인을 가상화 기반으로 일반 서비스 도메인과 안전 서비스 도메인으로 분리시키는 단계와, 상기 안전 서비스 도메인의 안전 서비스 응용에서 보안 서비스가 호출되는 단계와, 상기 안전 서비스 응용에서 상기 안전 서비스 도메인의 암호 모듈로 상기 보안 서비스를 전송하는 단계와, 상기 암호 모듈에서 상기 보안 서비스를 수행하는 단계를 포함한다.

발명의 효과

[0018] 본 발명은 모바일 단말에서 안전한 소프트웨어 실행 환경을 제공하기 위한 방법 및 장치에 있어서, 가상화 기반의 도메인 분리를 통해서 독립적인 두 개의 실행환경을 구성하고, 분리된 도메인 간 보안 서비스 채널을 통해 안전 서비스를 제공함으로써, 단말에서 실행되는 소프트웨어에 대한 보안성을 높이고 외부의 불법적인 접근으로부터 내부 정보를 보호할 수 있는 이점이 있다.

[0019] 또한, 도메인 분리를 통해 소프트웨어 공격으로 인한 침해 확산을 차단하고, 안전한 서비스를 불법적인 공격으로부터 보호할 수 있는 이점이 있다.

[0020] 또한, 단일 도메인으로 구성된 실행 환경이 갖는 보안상 문제점을 해결하여 모바일 단말 환경에서 기업 정보 및 사용자 정보 유출을 방지하고, 지불, 결제 등의 서비스를 제한하는 소프트웨어 취약성을 보완할 수 있는 이점이 있다.

도면의 간단한 설명

[0021] 도 1은 본 발명의 실시예에 따른 도메인 분리 기반 안전 실행 환경 제공 장치의 구성도,
도 2는 본 발명의 실시예에 따른 안전 서비스 도메인을 이용한 보안 서비스 처리 개념도,
도 3은 본 발명의 실시예에 따른 일반 서비스 도메인과 안전 서비스 도메인간 보안 서비스 처리를 위한 신호 처리 흐름도.

발명을 실시하기 위한 구체적인 내용

[0022] 이하, 첨부된 도면을 참조하여 본 발명의 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0023] 도 1은 본 발명의 실시예에 따른 도메인 분리 기반 안전 실행 환경 제공 장치의 구성을 도시한 것이다.

[0024] 위 도 1을 참조하면, 본 발명에서 제안하는 도메인 분리 기반 안전 실행 환경은 물리적인 장치인 프로세서(processor)(100) 상에 실행되는 모니터(monitor) 또는 하이퍼바이저(hypervisor)(200)를 기준으로 두 개의 소프트웨어 도메인(software domain)인 일반 서비스 도메인(300) 및 안전 서비스 도메인(400)으로 크게 구성된다.

[0025] 본 발명에서는 도메인 분리 방법에 대해서 특정 기술을 제한하지 않으며 소프트웨어 및 하드웨어에 의하여 서로 독립적인 도메인을 생성하는 모든 방법을 포함할 수 있다.

[0026] 일반 서비스 도메인(300)은 일반적으로 단말 사용자가 새로운 드라이버 및 모바일 응용을 설치하고 변경할 수 있는 개방형 환경으로서 최하위 계층인 임베디드 운영체제(embedded operating system)(310)을 기반으로 라이브러리(library)(320), 그리고 모바일 응용(mobile application)(330)들이 상위 개체로 실행되는 구조를 갖는다.

[0027] 이와 같이, 개방형 구조의 실행 환경을 갖기 때문에 일반 서비스 도메인(300)에서 실행되는 모든 요소들은 외부의 보안 위협으로부터 잠재적으로 노출될 수 있다. 또한, 일반 서비스 도메인 내부에는 외부의 보안 위협으로부터 안전하게 실행될 부분들을 안전 서비스 도메인(400)으로부터 제공받을 수 있도록 프론트 앤드 드라이버(Front-end driver)(340) 및 안전 서비스 API(application programming interface)(350)를 제공하고 있으며,

이를 이용하여 구현된 일반 서비스 응용(360)는 모바일 응용(330)에서 제공되지 않는 보안 서비스(secure service)를 연동시킬 수 있다.

- [0028] 안전 서비스 도메인(400)은 일반 서비스 도메인(300)과 달리 폐쇄형 실행 구조를 가지며 도메인 내부 구성 요소에 대한 일반 사용자의 불법접근 및 변경이 불가능하다. 안전 서비스 도메인(400)을 구성하는 암호 모듈(420), 암호 API(430)는 안전 서비스 응용(440)을 실행하는데 필요한 암호 기능 및 프로그래밍 인터페이스를 제공한다. 또한 백엔드 드라이버(Back-end driver)(410)는 일반 서비스 도메인(300)으로부터 요청된 보안 서비스를 안전 서비스 도메인(400) 내부의 서비스로 요청하는 역할을 수행한다. 안전 서비스 도메인(400)을 구성하는 각 요소를 보다 자세히 살펴보면 다음과 같다.
- [0029] 안전 서비스 응용(440)은 안전 서비스 도메인(400) 내부에서 실행되는 보안 서비스의 수행 단위로서 독립된 실행 문맥을 갖는다. 특히 서비스 제공자의 에이전트 프로그램(agent program)과 같이 단말 내부에서 사용자가 설치 가능한 일반 프로그램과는 별도로 안전하게 실행되는 서비스를 구현하는데 이용될 수 있다. 그러므로, 안전 서비스 도메인(400) 내에서 실행되는 안전 서비스 응용의 실행 여부와 실행에 필요한 내부 정보는 일반 서비스 도메인(300)에서는 직접 접근할 수 없다.
- [0030] 암호 모듈(420)은 암호 키 생성, 난수 생성, 그리고 암호 및 서명 알고리즘 등을 포함한 모듈로서 암호학적 연산을 수행한다. 따라서 암호 모듈(420)이 특정 연산을 수행하는 동안에는 안전 서비스 도메인(400) 내부에서 실행되기 때문에 일반 서비스 도메인(300) 영역에서는 암호 연산 시 사용되는 중요 내부 정보에 대한 확인이 불가능하다.
- [0031] 암호 API(430)의 목적은 안전 서비스 응용(440)에게 암호 모듈(420) 사용에 대한 투명성을 제공하는데 있다. 따라서 암호 모듈(420)이 소프트웨어 혹은 전용 하드웨어 모듈을 이용하여 구현되는지 여부에 상관없이 암호 API(430)를 이용하여 안전 서비스 응용을 구현할 수 있는 구조이다.
- [0032] 백엔드(Back-end driver)(410)는 일반 서비스 도메인(300) 내부에서 안전 서비스 도메인(400) 내부의 안전 서비스 응용(440) 또는 암호 모듈(420)에게 보안 서비스를 요청할 때 이용된다. 백엔드 드라이버(410)는 일반 서비스 도메인(300)에서 요청한 보안 서비스에 대해 안전 서비스 도메인(400) 내에서의 실행 허용 여부를 판단하고 해당되는 보안 서비스 수행 주체에 전달한다.
- [0033] 도 2는 본 발명의 실시 예에 따른 안전 서비스 도메인을 이용한 보안 서비스 처리 개념을 도시한 것이다.
- [0034] 도 2를 참조하면, 본 발명에서 제안하는 도메인 분리 기반 안전 실행 엔진을 이용하여 보안 서비스를 제공하는 모델은 크게 두 가지 유형으로 분류된다.
- [0035] 첫 번째 방법은, 안전 서비스 도메인(400) 내부의 독립된 안전 서비스 응용(440) 방식으로 일반 서비스 도메인(300)과의 상호 작용 없이 단독으로 서비스를 수행한다. 이 경우, 안전 서비스 응용(440)은 암호 API(430)를 이용하여 암호 모듈(420)에 접근하거나 자체 실행 프로세스에 따라 보안 서비스를 수행한다.
- [0036] 안전 서비스 응용(440)은 안전 서비스 도메인(400)의 폐쇄적인 실행 환경에 의해서 외부로 노출될 수 있는 보안 취약성이 매우 낮고 실행되는 동안에도 보안 서비스 내부 정보가 유출되지 않는다. 안전 서비스 응용(440)에서 암호 모듈(420)에 접근하는 경우에는 도 2에서 보여 지는 바와 같이 암호 API(430)를 이용하여 암호 모듈(420) 내부의 기능을 호출하는 경로(540)를 따르게 된다.
- [0037] 본 발명에서 보안 서비스를 제공하는 두 번째 방법은, 일반 서비스 응용(360)에서 안전한 실행이 요구되는 부분을 안전 서비스 도메인(400)에게 요청하여 안전 서비스 도메인 내부에서 실행시키고 그 결과값을 되돌려 받는 구조이다.
- [0038] 도 3은 일반 서비스 응용(360)에서 안전한 실행이 요구되는 부분을 안전 서비스 도메인(400)에게 요청하여 안전 서비스 도메인 내부에서 실행시키고 그 결과값을 되돌려 받는 신호 처리 흐름을 도시한 것이다. 이하, 도 2 및 도 3을 참조하여 본 발명의 실시예에 따른 보안 서비스를 제공하는 두 번째 방법에 대해 상세히 설명하기로 한다.
- [0039] 일반적으로 일반 서비스 도메인(300)에서 실행되는 모바일 응용(330)의 경우 모든 실행이 일반 서비스 도메인 내에서 이루어지기 때문에 도메인 상에서 발생하는 보안 침해로 인하여 실행 중에 중요 연산 및 정보에 대한 불법유출이 가능하지만, 본 발명에서 제안하고 있는 서로 다른 도메인으로 분리된 형태의 서비스 모델에서는 보안 취약성으로 인한 위험성을 일반 서비스 도메인으로 제한시킬 수 있게 된다. 이때, 일반 서비스 응용(360)에서

안전 서비스 도메인(400)를 이용하여 보안 서비스를 연동시키는 구조는 다시 아래와 같이 세분화 된다.

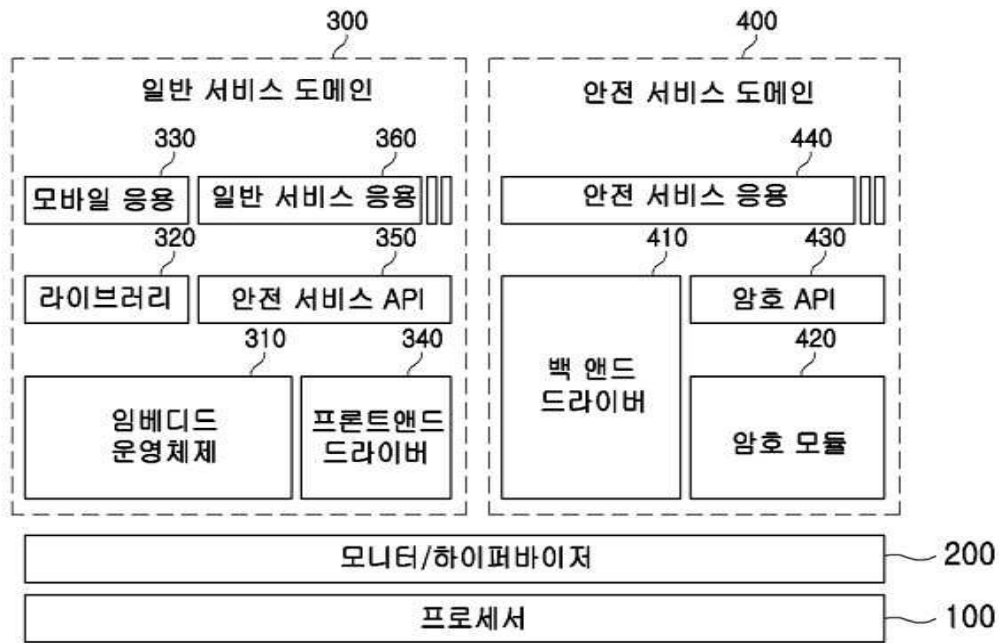
- [0040] 일반 서비스 도메인(300) 내부의 일반 서비스 응용(360)에서 안전 서비스 도메인(400) 내부의 암호 모듈(420) 또는 안전 서비스 응용(440)을 호출하기 위해서는, 먼저 안전 서비스 API(350)를 이용하여 서비스를 요청한다(S10). 안전 서비스 API(350)을 통해 시작된 안전 서비스 도메인(400)에 대한 보안 서비스 요청은 일반 서비스 도메인(300) 내부의 프론트 엔드 드라이버(340)로 전송되고(S12), 다시 안전 서비스 도메인(400)의 백엔드 드라이버(410)로 전달되는 호출 경로(510)를 따른다.
- [0041] 이때, 안전 서비스 도메인(400)의 프론트 엔드 드라이버(340)에서 보낸 보안 서비스 요청은 모니터 또는 하이퍼바이저(200)에서 제공하는 도메인 간 통신 방식을 이용하여 안전 서비스 도메인(400)의 백엔드 드라이버(410)로 전달된다(S14). 이에 따라, 안전 서비스 도메인(400)의 백엔드 드라이버(410)는 전달 받은 보안 서비스에 대한 메시지 디코딩(decoding) 및 역다중화(de-multiplexing) 기능을 다음과 같이 수행한다.
- [0042] 먼저, 백엔드 드라이버(410)는 일반 서비스 도메인(300)의 일반 서비스 응용(360)에서 요청한 보안 서비스가 별도의 독립적인 실행이 요구되는지 또는 안전 서비스 응용(440)과의 연동이 필요한지 여부를 검사한다(S16).
- [0043] 이때, 일반 서비스 도메인(300)의 일반 서비스 응용(360)에서 요청한 보안 서비스가 별도의 독립적인 실행이 요구되는 안전 서비스 응용(440)과 관련 없이 암호 기능인 경우, 호출 경로는 암호 모듈(420)로 연결되는 경로(530)를 따르게 되며, 백엔드 드라이버(410)는 보안 서비스 요청을 암호 모듈(420)로 전송한다(S18).
- [0044] 반면, 일반 서비스 응용(360)에서 요청한 보안 서비스가 안전 서비스 도메인(400) 내부의 안전 서비스 응용(440)과의 상호 작용이 필요한 경우, 안전 서비스 응용(440)으로 연결되는 호출 경로(520)를 따르게 되며, 백엔드 드라이버(410)는 보안 서비스 요청을 안전 서비스 응용(440)으로 전송한다(S20).
- [0045] 위와 같이, 서로 다른 경로를 통해 호출된 보안 서비스 요청에 대한 처리가 암호 모듈(420) 또는 안전 서비스 응용(440)에서 수행되어 완료되면 각각 해당 호출 경로의 역순으로 최초의 호출자인 일반 서비스 도메인(300)의 일반 서비스 응용(360)으로 결과값이 되돌려진다(S22, S24). 결과값은 오류 상황이 발생하는 경우를 대비하여, 오류 사실과 원인을 확인할 수 있는 코드가 일반 서비스 응용(360)에게 함께 전달되는 구조이며 이를 통해 최초의 일반 서비스 도메인(300)의 일반 서비스 응용(360)은 오류 사실을 인지할 수 있게 한다.
- [0046] 이상에서와 같이 도면과 명세서에서 최적 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

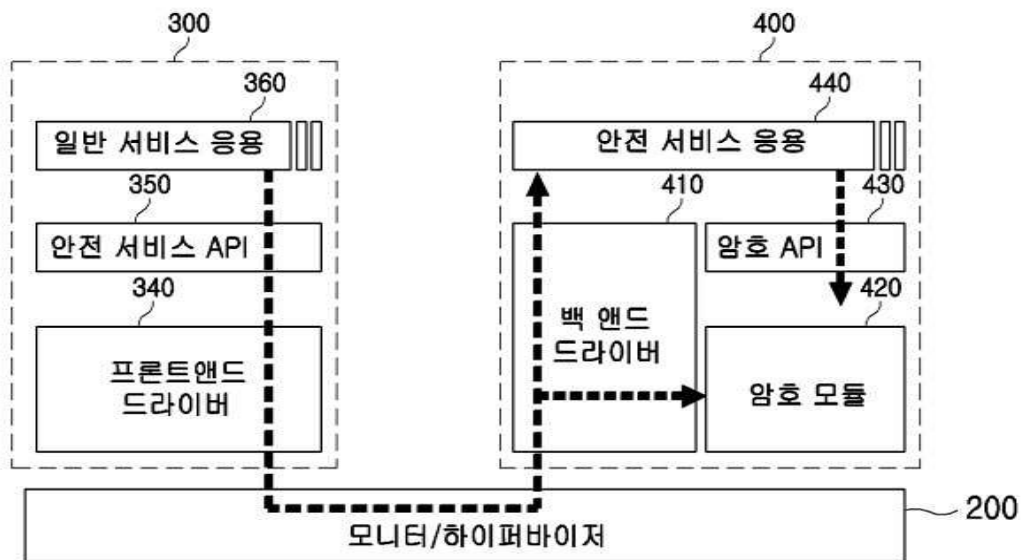
- [0047]
- | | |
|-------------------|------------------|
| 300 : 일반 서비스 도메인 | 310 : 임베디드 운영체제 |
| 320 : 라이브러리 | 330 : 모바일 응용 |
| 340 : 프론트 엔드 드라이버 | 350 : 안전 서비스 API |
| 360 : 일반 서비스 응용 | 400 : 안전 서비스 도메인 |
| 410 : 백엔드 드라이버 | 420 : 암호 모듈 |
| 430 : 암호 API | 440 : 안전 서비스 응용 |

도면

도면1



도면2



도면3

