(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년11월29일
(11) 등록번호 10-1802806
(24) 등록일자 2017년11월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/53* (2013.01)
(52) CPC특허분류
G06F 21/6218 (2013.01)
G06F 21/53 (2013.01)
(21) 출원번호 10-2016-7018988
(22) 출원일자(국제) 2013년12월17일
심사청구일자 2016년07월14일
(85) 번역문제출일자 2016년07월14일
(65) 공개번호 10-2016-0098430
(43) 공개일자 2016년08월18일
(86) 국제출원번호 PCT/US2013/075598
(87) 국제공개번호 WO 2015/094176
국제공개일자 2015년06월25일
(56) 선행기술조사문헌
US20120159184 A1*
US20030101322 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
싱 빈 세드릭
미국 미국 97124 힐스보로 노스이스트 오로라 드라이브 2756
랄 레쉬마
미국 오레곤주 97124 힐스보로 노스이스트 25번 애비뉴 2111 엠에스: 제이에프2-65
(74) 대리인
제일특허법인

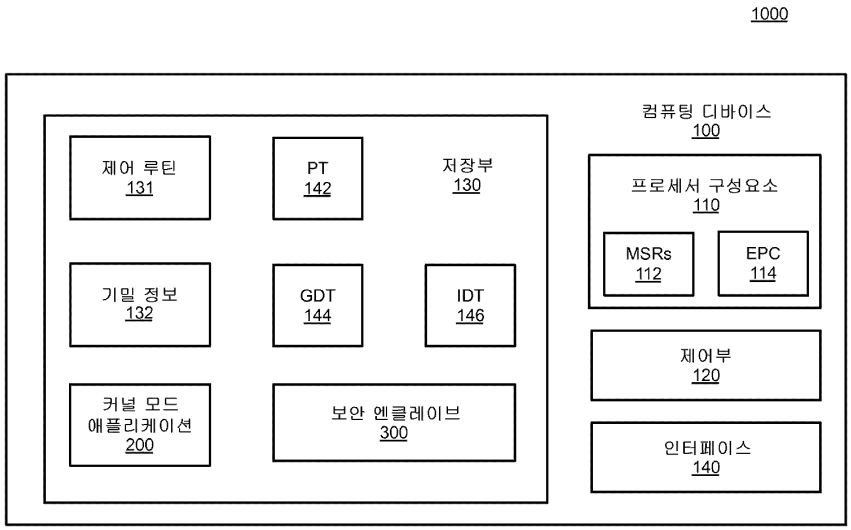
전체 청구항 수 : 총 25 항 심사관 : 구대성

(54) 발명의 명칭 **커널 모드 애플리케이션에 의한 사용을 위한 보안 엔클레이브**

(57) 요 약

다양한 실시예는 일반적으로 커널 모드 애플리케이션에 의한 사용을 위해 보안 엔클레이브를 로딩 및 실행하기 위한 기술에 관한 것이다. 보안 엔클레이브에 대한 커널 모드 액세스를 제공하는 장치는, 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하고 커널 모드 애플리케이션 대신에 보안 엔클레이브를 초기화하기 위한 커널 모드 보안 엔클레이브 드라이버, 및 커널 모드 애플리케이션으로부터 보안 엔클레이브로의 명령어를 프로세싱하기 위한 사용자 모드 보안 엔클레이브 관리기를 포함한다.

대 표 도



명 세 서

청구범위

청구항 1

보안 엔클레이브(secure enclave)에 대한 커널 모드 액세스(kernel mode access)를 제공하는 장치로서,

프로세서와,

상기 프로세서에 의해 실행 가능한 명령어들을 포함하는 메모리를 포함하고,

상기 명령어들은 상기 프로세서로 하여금

운영 시스템이 컴퓨팅 디바이스 상에 로딩되기 이전에 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하고,

상기 운영 시스템이 로딩되기 이전에 상기 커널 모드 애플리케이션 대신에 상기 컴퓨팅 디바이스의 저장 구성요소 상에서 보안 엔클레이브를 초기화하고,

상기 운영 시스템이 로딩되기 이전에 상기 커널 모드 애플리케이션으로부터의 명령어를 프로세싱하도록 하며,

상기 커널 모드 애플리케이션으로부터의 상기 명령어는 상기 컴퓨팅 디바이스의 적어도 일부에 인터페이스 기능을 제공하거나 초기화하기 위해 상기 보안 엔클레이브에서 기밀 정보를 프로세싱하는 것을 포함하는

커널 모드 액세스 제공 장치.

청구항 2

제 1 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 보안 엔클레이브로의 상기 커널 모드 애플리케이션에 대한 사용자 모드 액세스를 허용하기 위해 페이지 테이블 엔트리(page table entry)를 수정하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 3

제 2 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 커널 모드 애플리케이션이 커널 모드와 사용자 모드 사이에서 스위칭하는 것을 가능하게 하는 세그먼트 디스크립터를 글로벌 디스크립터 테이블 내에 포지셔닝하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 4

제 3 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 모델 특정 레지스터가 커널 모드와 사용자 모드 사이에서 스위칭을 제공하는 것을 가능하게 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 5

제 2 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 보안 엔클레이브를 생성하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 6

제 5 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 저장 구성요소로부터의 적어도 하나의 메모리 페이지를 보안 엔클레이브 페이지 캐시(secure enclave page cache)에 부가하도록 하는 명령어를 포함하고,

상기 적어도 하나의 메모리 페이지는 상기 보안 엔클레이브에 대응하는

커널 모드 액세스 제공 장치.

청구항 7

제 6 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 보안 엔클레이브 이미지를 상기 적어도 하나의 메모리 페이지로 확장시키도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 8

제 1 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 커널 모드 애플리케이션으로부터 상기 명령어를 수신하고, 상기 보안 엔클레이브로 하여금 상기 명령어를 프로세싱하게 하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 9

제 1 항에 있어서,

상기 명령어는 패스프레이즈(passphrase)를 검증하고,

상기 메모리는 상기 프로세서로 하여금 상기 패스프레이즈를 상기 보안 엔클레이브로 송신하고, 상기 보안 엔클레이브 내의 상기 패스프레이즈를 검증하도록 상기 보안 엔클레이브에 지시하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 10

제 1 항에 있어서,

상기 명령어는 암호화된 메모리 블록을 복호화하고,

상기 메모리는 상기 프로세서로 하여금 상기 암호화된 메모리 블록을 상기 보안 엔클레이브로 송신하고, 상기 암호화된 메모리 블록을 상기 보안 엔클레이브에서 복호화하도록 상기 보안 엔클레이브에 지시하도록 하는 명령

어를 포함하는

커널 모드 액세스 제공 장치.

청구항 11

제 1 항에 있어서,

상기 메모리는 상기 프로세서로 하여금 상기 운영 시스템이 로딩되면 상기 보안 엔클레이브를 상기 운영 시스템으로 전달하도록 하는 명령어를 포함하는

커널 모드 액세스 제공 장치.

청구항 12

커널 모드 애플리케이션을 통해 보안 엔클레이브에 액세스하기 위한 컴퓨팅-구현 방법으로서,

운영 시스템이 컴퓨팅 디바이스 상에 로딩되기 이전에 보안 엔클레이브에서 기밀 정보를 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하는 단계와,

상기 운영 시스템이 로딩되기 이전에 상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하는 단계와,

상기 운영 시스템이 로딩되기 이전에 상기 컴퓨팅 디바이스의 저장 구성요소 상에서 상기 보안 엔클레이브를 초기화하는 단계와,

상기 컴퓨팅 디바이스의 적어도 일부에 인터페이스 기능을 제공하거나 초기화하기 위해 상기 운영 시스템이 로딩되기 이전에 상기 기밀 정보를 프로세싱하기 위해 상기 보안 엔클레이브를 실행하는 단계를 포함하는

컴퓨팅-구현 방법.

청구항 13

제 12 항에 있어서,

상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하는 단계는 상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하기 위해 페이지 테이블 엔트리를 수정하는 단계를 포함하는

컴퓨팅-구현 방법.

청구항 14

제 13 항에 있어서,

커널 모드와 사용자 모드 사이에서 스위칭하기 위한 세그먼트 디스크립터를 글로벌 디스크립터 테이블 내에 포지셔닝하는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 15

제 13 항에 있어서,

상기 보안 엔클레이브를 초기화하는 단계는,

상기 보안 엔클레이브에 대해 상기 저장 구성요소로부터 적어도 하나의 메모리 페이지를 할당하는 단계와,

상기 적어도 하나의 메모리 페이지를 상기 보안 엔클레이브에 대응하는 엔클레이브 페이지 캐시에 부가하는 단계를 포함하는

컴퓨팅-구현 방법.

청구항 16

제 15 항에 있어서,

보안 엔클레이브 이미지의 콘텐츠를 상기 적어도 하나의 메모리 페이지로 확장시키는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 17

제 12 항에 있어서,

상기 명령어는 패스프레이즈를 검증하고,

상기 방법은 상기 패스프레이즈를 상기 보안 엔클레이브로 송신하고, 상기 보안 엔클레이브 내의 상기 패스프레이즈를 검증하도록 상기 보안 엔클레이브에 지시하는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 18

제 12 항에 있어서,

상기 명령어는 암호화된 메모리 블록을 복호화하고,

상기 방법은 상기 암호화된 메모리 블록을 상기 보안 엔클레이브로 송신하고, 상기 보안 엔클레이브 내의 상기 암호화된 메모리 블록을 복호화하도록 상기 보안 엔클레이브에 지시하는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 19

제 12 항에 있어서,

상기 운영 시스템이 로딩되면 상기 보안 엔클레이브를 상기 운영 시스템으로 전달하는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 20

제 19 항에 있어서,

상기 운영 시스템이 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 상기 보안 엔클레이브에 대해 상기 저장 구성요소로부터의 하나 이상의 부가적인 메모리 페이지를 할당할 수 있도록, 상기 운영 시스템이 로딩되면 상기 보안 엔클레이브 페이지 캐시 사용을 상기 운영 시스템으로 전달하는 단계와,

상기 보안 엔클레이브를 선택된 가상 메모리 위치로 맵핑하는 단계를 더 포함하는

컴퓨팅-구현 방법.

청구항 21

명령어를 포함하는 적어도 하나의 머신-판독 가능 저장 매체로서,

상기 명령어는, 컴퓨팅 디바이스에 의해 실행될 때, 상기 컴퓨팅 디바이스로 하여금,

운영 시스템이 컴퓨팅 디바이스에 로딩되기 이전에 보안 엔클레이브에서 기밀 정보를 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하게 하고,

상기 운영 시스템이 로딩되기 이전에 상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하고,

상기 운영 시스템이 로딩되기 이전에 상기 컴퓨팅 디바이스의 저장 구성요소 상에서 상기 보안 엔클레이브를 초기화하게 하고,

상기 컴퓨팅 디바이스의 적어도 일부에 인터페이스 기능을 제공하거나 초기화하기 위해 상기 운영 시스템이 로딩되기 이전에 상기 기밀 정보를 프로세싱하기 위해 상기 보안 엔클레이브를 실행하게 하는

머신-판독 가능 저장 매체.

청구항 22

제 21 항에 있어서,

실행될 때, 상기 컴퓨팅 디바이스로 하여금,

상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 허용하도록 페이지 테이블 엔트리를 수정하게 하고,

커널 모드와 사용자 모드 사이에서 스위칭하기 위한 세그먼트 디스크립터를 글로벌 디스크립터 테이블 내에 포지셔닝하게 하는 명령어를 더 포함하는

머신-판독 가능 저장 매체.

청구항 23

제 22 항에 있어서,

실행될 때, 상기 컴퓨팅 디바이스로 하여금,

상기 보안 엔클레이브에 대해 상기 저장 구성요소로부터 적어도 하나의 메모리 페이지를 할당하게 하고,

상기 적어도 하나의 메모리 페이지를 상기 보안 엔클레이브에 대응하는 엔클레이브 페이지 캐시에 부가하게 하는 명령어를 더 포함하는

머신-판독 가능 저장 매체.

청구항 24

커널 모드 애플리케이션을 통해 보안 엔클레이브를 액세스하기 위한 장치로서,

운영 시스템이 컴퓨팅 디바이스 상에 로딩되기 이전에 보안 엔클레이브에서 기밀 정보를 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하기 위한 수단과,

상기 운영 시스템이 로딩되기 이전에 상기 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하기 위한 수단과,

상기 운영 시스템이 로딩되기 이전에 상기 컴퓨팅 디바이스의 저장 구성요소 상에서 상기 보안 엔클레이브를 초기화하기 위한 수단과,

상기 컴퓨팅 디바이스의 적어도 일부에 인터페이스 기능을 제공하거나 초기화하기 위해 상기 운영 시스템이 로

딩되기 이전에 상기 기밀 정보를 프로세싱하기 위해 상기 보안 엔클레이브를 실행하기 위한 수단을 포함하는

보안 엔클레이브 액세스 장치.

청구항 25

제 24 항에 있어서,

상기 운영 시스템이 로딩되면 보안 엔클레이브 페이지 캐시 사용을 상기 운영 시스템으로 전달하기 위한 수단 - 상기 운영 시스템은 상기 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 상기 저장 구성 요소로부터의 하나 이상의 부가적인 메모리 페이지를 할당하도록 구성됨 - 과,

상기 보안 엔클레이브에 대응하는 메모리 어드레스를 상기 운영 시스템으로 전달하기 위한 수단 - 상기 운영 시스템은 상기 메모리 어드레스에 적어도 부분적으로 기초하여 상기 보안 엔클레이브를 가상 메모리 위치로 맵핑하도록 구성됨 - 을 더 포함하는

보안 엔클레이브 액세스 장치.

발명의 설명

기 술 분 야

[0001] 본원에 개시된 실시예는 일반적으로 보안 엔클레이브(secure enclave) 및 커널 모드 애플리케이션(kernel mode application)으로부터 보안 엔클레이브를 액세스하는 것에 관한 것이다.

배 경 기 술

[0002] 보안 엔클레이브는 메모리 애퍼처(memory aperture)이고, 애플리케이션은 메모리 애퍼처를 통해 기밀 정보를 프로세싱할 수 있다. 예를 들면, 일부 보안 엔클레이브는 컴퓨터 시스템 내의 물리적 메모리의 특수 범위 내의 메모리 위치이다. 메모리는 파워-온마다 컴퓨터 시스템의 프로세서에 의해 생성된 임시 키(ephemeral key) 하에서 암호화된다. 이와 같이, 메모리는, 프로세서 자체를 제외하면 컴퓨터 시스템 내의 임의의 하드웨어 디바이스에 대해 액세스 불가하다.

[0003] 보안 엔클레이브는 컴퓨터 시스템의 임의의 다른 구성요소 및/또는 프로세스에 의해 액세스 불가한 메모리 위치 내의 기밀 정보를 프로세싱하는데 사용될 수 있다. 예를 들면, 기밀 정보는 보안 엔클레이브 내에서 암호화될 수 있다. 암호화된 정보는 기밀 정보를 암호화하는데 사용된 보안 엔클레이브 내에서만 복호화될 수 있다. 이와 같이, 데이터는, 데이터를 암호화 및/또는 복호화하는데 사용된 키를 노출시키지 않고서, 암호화 및 복호화될 수 있다. 따라서, 애플리케이션은 다양한 함수를 사용하여 보안 엔클레이브를 호출하고 임의의 필요한 데이터를 보안 엔클레이브로 전달함으로써 보안 엔클레이브와 상호작용할 수 있다. 보안 엔클레이브의 성질 및 그의 특수하게 암호화된 메모리 위치의 사용으로 인해, 보안 엔클레이브와의 상호작용은 사용자 모드에서 동작하는 애플리케이션으로 제한된다. 커널 모드에서 동작하는 애플리케이션은 보안 엔클레이브와 상호작용하는 것이 방지된다.

[0004] 인식될 바와 같이, 컴퓨터 시스템을 초기화하는 것을 담당하는 애플리케이션은 커널 모드에서 동작한다. 예를 들면, 기본 입력/출력 시스템("BIOS") 및 통합형 확장 가능 펌웨어 인터페이스("UEFI")는 컴퓨터 시스템을 개시하기 위해 필요한 다양한 플랫폼 디바이스(특히, 운영 시스템이 상주하는 저장 디바이스)를 초기화하는 애플리케이션(또는 애플리케이션의 콜렉션)이다. 이들 애플리케이션은 커널 모드에서 동작하고, 컴퓨터 시스템에서 "사전-부트" 동작을 수행하는 것으로 지칭될 수 있다. 사전-부트 동안에 보안 엔클레이브에서 기밀 정보를 프로세싱하는 것이 바람직한 경우가 존재한다. 예를 들면, 도난 방지 기술(anti-theft technology) 및 풀 디스크 암호화 기술은 (예를 들면, 컴퓨팅 디바이스를 잠금해제(unlock)하거나, 디스크를 복호화하는 것 등을 위해) 키를 활용한다. 키는 전형적으로 사용자에 의해 선택된 패스프레이즈(passphrase)를 사용하여 암호화된다. 사전-부트 동안에, 사용자는 패스프레이즈를 공급하고, 키는 메모리에서 평문(plaintext)으로 복호화된다. 그러나, 메모리가 보호되지 않을 때, 키는 다른 애플리케이션에 의해 액세스 가능할 수 있다.

[0005] 따라서, 커널 모드에서 동작하는 애플리케이션에 의한 기밀 정보의 보안 프로세싱을 제공하기 위해, 특히 사전-부트 동안에, 커널 모드 애플리케이션에 의해 보안 엔클레이브를 액세스할 필요성이 존재한다.

도면의 간단한 설명

[0006] 도 1은 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 실시예를 도시한다.

도 2는 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 실시예의 일부를 도시한다.

도 3은 일 실시예에 따른 논리 흐름을 도시한다.

도 4는 저장 매체의 실시예를 도시한다.

도 5는 실시예에 따른 논리 흐름을 도시한다.

도 6은 저장 매체의 실시예를 도시한다.

도 7은 실시예에 따른 프로세싱 아키텍쳐를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0007] 본원에서 사용되는 기호 및 명명법을 일반적으로 참조하면, 후속하는 상세한 설명의 부분은 컴퓨터 상에서 또는 컴퓨터의 네트워크 상에서 실행되는 프로그램 프로시져의 관점에서 제시될 수 있다. 이들 프로시져의 설명 및 표현이 당업자에 의해 사용되어 다른 당업자에게 이들 연구의 핵심을 가장 효과적으로 전달한다. 프로시져는 여기에서, 그리고 일반적으로, 원하는 결과로 이어지는 동작의 자기 일관적 시퀀스(a self-consistent sequence)가 되는 것으로 간주된다. 이들 동작은 물리적 수량의 물리적 조작을 필요로 하는 것이다. 일반적으로, 반드시 그러한 것을 아니지만, 이들 수량은 저장, 전달, 통합, 비교, 또는 조작되는 것이 가능한 전기적, 자기적 또는 광학적 신호의 형태를 취한다. 이들 신호를 비트, 값, 요소, 심볼, 문자, 용어, 숫자, 또는 유사한 것으로서 지칭하는 것이 주로 일반적인 사용의 이유로 가끔 편리하다고 입증되었다. 그러나, 이들 및 유사한 용어의 모두는 적합한 물리적 수량과 연관되고 이들 수량에 적용되는 단지 편리한 라벨인 것에 유의해야 한다.

[0008] 또한, 이들 조작은 종종 사람 운영자에 의해 수행되는 정신적 동작과 일반적으로 연관되는, 추가 또는 비교와 같은, 용어로 지칭된다. 그러나, 사람 운영자의 이러한 능력은, 하나 이상의 실시예의 부분을 형성하는 본원에 설명된 임의의 동작에서, 대부분의 경우에, 필요하거나 바람직한 것은 아니다. 오히려, 이들 동작은 머신 동작이다. 다양한 실시예의 동작을 수행하기 위해 유용한 머신은 본원의 교시에 따라 기록된 내부에 저장된 컴퓨터 프로그램에 의해 선택적으로 활성화 또는 구성되는 것으로서 범용 디지털 컴퓨터를 포함하고/거나 필요한 목적에 대해 특별하게 구성되는 장치를 포함한다. 다양한 실시예는 또한 이들 동작을 수행하기 위한 장치 또는 시스템에 관한 것이다. 이들 장치는 필요한 목적에 대해 특별하게 구성될 수 있거나 범용 컴퓨터를 포함시킬 수 있다. 다양한 이들 머신에 대해 필요한 구조는 주어진 설명으로부터 명백해질 것이다.

[0009] 이제 도면에 대한 참조가 이루어지고, 동일한 참조부호는 전반적으로 동일한 요소를 지칭하도록 사용된다. 다음의 설명에서, 설명의 목적을 위해, 이들의 완전한 이해를 제공하도록 다양한 특정 상세가 제시된다. 그러나, 진보적인 실시예가 이들 특정 상세 없이 실시될 수 있다는 것이 명백할 수 있다. 다른 경우에, 잘 알려진 구조 및 디바이스는 이들의 설명을 용이하게 하도록 블록도로 도시된다. 청구항의 범위 내에서 모든 수정, 등가, 및 대안을 커버하도록 의도된다.

[0010] 도 1은 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템(1000)의 블록도이다. 시스템(1000)은 컴퓨팅 디바이스(100)를 통합한다. 컴퓨팅 디바이스(100)는, 제한 없이, 데스크톱 컴퓨터 시스템, 데이터 입력 단말, 랩톱 컴퓨터, 넷북 컴퓨터, 태블릿 컴퓨터, 핸드헬드 개인 정보 단말, 스마트폰, 디지털 카메라, 의류 또는 착용 가능한 액세서리(예를 들면, 안경, 시계 등)에 통합되는 신체-착용 컴퓨팅 디바이스, 운송수단(예를 들면, 자동차, 자전거, 휠체어 등)에 통합되는 컴퓨팅 디바이스, 서버, 서버의 클러스터, 서버 팜, 스테이션, 무선 스테이션, 사용자 장비 등을 포함하여 다양한 타입의 컴퓨팅 디바이스 중 임의의 것일 수 있다. 실시예는 이러한 문맥으로 제한되지 않는다.

[0011] 일반적으로, 시스템(1000)은 커널 모드 애플리케이션이 보안 엔클레이브와 상호작용하도록 허용하도록 구성된다. 상기와 달리, 시스템(1000)은 커널 모드에서 동작하는 애플리케이션에 의해 보안 엔클레이브를 로딩 및 실행하는 것을 허용하도록 구성된다. 커널 모드 애플리케이션에 의한 사용을 위해 보안 엔클레이브를 로딩 및 실행하는 단일의 컴퓨팅 디바이스(예를 들면, 컴퓨팅 디바이스(100))가 기재되지만, 컴퓨팅 디바이스의 특징

이 다수의 컴퓨팅 디바이스에 통합될 수 있다는 것이 유의되어야 한다.

[0012] 인식될 바와 같이, 많은 현대 프로세싱 구성요소(예를 들면, x86 등)는 "커널 모드" 및 "사용자 모드"로 지칭되는 상이한 동작 모드를 제공한다. 프로세싱 구성요소는, 프로세싱 구성요소가 명령어를 실행하는 특정 애플리케이션이 어떠한 특권을 갖는지에 의존하여 이들 2 개의 모드 사이에서 스위칭한다. 일반적으로, 인터페이스 기능을 초기화하고 이를 컴퓨팅 디바이스의 구성요소(예를 들면, 드라이버, 운영 시스템 구성요소, 사전-부트 애플리케이션 등)에 제공하는데 사용되는 애플리케이션은 커널 모드 특권을 갖고, 따라서 커널 모드에서 동작한다. 상기와 달리, 이러한 타입의 애플리케이션으로부터의 명령어를 실행할 때, 프로세싱 구성요소는 커널 모드에서 동작한다. 반대로, 대부분의 다른 애플리케이션은 사용자 모드 특권을 갖는다. 이와 같이, 이러한 타입의 애플리케이션으로부터의 명령어를 실행할 때, 프로세싱 구성요소는 사용자 모드에서 동작한다.

[0013] 따라서, 본 개시내용의 다양한 실시예는 보안 엔클레이브를 로딩 및 실행할 수 있는 커널 모드 애플리케이션을 제공한다. 예를 들면, 전형적으로 커널 모드에서 동작하는, "사전-부트" 동작을 수행하는 애플리케이션(예를 들면, BIOS, UEFI 등)은 보안 엔클레이브를 로딩 및 실행할 수 있다. 특정 예에서, 컴퓨터 시스템이 초기화하는 동안에 보안 민감 프로세싱을 수행하는 도난-방지 및/또는 풀 디스크 암호화 기술은 보안 정보(예를 들면, 검증 패스프레이즈, 복호화 필요 부트 드라이버 등)를 프로세싱하기 위해 보안 엔클레이브를 사용할 수 있다.

[0014] 다양한 실시예에서, 컴퓨팅 디바이스(100)는 프로세서 구성요소(110), 제어부(120), 저장 구성요소(130), 및 컴퓨팅 디바이스(100)를 네트워크에 연결하기 위한 인터페이스(140) 중 하나 이상을 통합한다. 프로세서 구성요소는 하나 이상의 MSR(model specific register)(112) 및 보안 EPC(enclave page cache)(114)를 포함할 수 있다. 일부 예에서, EPC(114)는 프로세서(110) 상의 메모리 캐시 위치에 저장될 수 있다. 다른 예에서, EPC(114)는 다른 메모리 위치(예를 들면, 로컬 메모리 등)에 저장될 수 있다. 특히 특정 예에서, EPC(114)는 플랫폼 로컬 메모리(예를 들면, DRAM 등)의 암호로 보호되는 (예를 들면, MEE 등) 영역에 저장될 수 있다. 저장 구성요소(130)는 제어 루틴(131), 기밀 정보(132), 커널 모드 애플리케이션(200), 보안 엔클레이브(300), 페이지 테이블(PT)(142), GDT(global descriptor table)(144) 및 IDT(interrupt descriptor table)(146) 중 하나 이상을 저장한다.

[0015] 컴퓨팅 디바이스(100)에서, 제어 루틴(131)은 다양한 기능을 수행하기 위한 로직을 구현하는 메인 프로세서 구성요소로서 역할을 하는 프로세서 구성요소(110) 상에서 동작하는 명령어의 시퀀스를 통합한다. 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 커널 모드 애플리케이션(200)에 대한 사용자 모드 지원을 제공하고, 그래서 커널 모드 애플리케이션(200)은 보안 엔클레이브(300)와 상호작용할 수 있다.

[0016] 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 커널 모드 애플리케이션(200)에 대한 사용자 모드 특권을 제공하기 위해 GDT(142) 및 IDT(144)를 수정할 수 있다. 부가적으로, 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 사용자 모드 및 커널 모드 동작 사이의 스위칭을 가능하게 하도록 하나 이상의 MSR(112)을 설정할 수 있다. 예를 들면, 하나 이상의 MSR(112)은 SYSCALL/SYSRET 명령어를 인에이블하도록 설정될 수 있고, SYSCALL/SYSRET 명령어는, 인식될 바와 같이, 사용자 모드 및 커널 모드 사이에서 프로세싱 구성요소(110)를 스위칭한다.

[0017] 또한, 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 다수의 메모리 페이지를 EPC(114)에 부가할 수 있다. 부가적으로, 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 보안 엔클레이브(300)를 생성할 수 있다. 보안 엔클레이브를 생성 및 관리하기 위한 다양한 상이한 기술이 이용 가능하다는 것이 인식된다. 특정 구현은 프로세싱 구성요소의 타입 및/또는 운영 시스템의 타입에 의존할 수 있다. 예를 들면, Intel® Security Guard Extension® 기술은 보안 엔클레이브(300)를 생성하고, 보안 엔클레이브(300)에서 기밀 정보(132)를 프로세싱하는데 사용될 수 있다. 그러나, 이것은 단지 하나의 예이고, 실시예는 이에 관련하여 제한되지 않는다.

[0018] 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는 부가적으로 사용자 모드 동작으로 스위칭하고, 커널 모드 애플리케이션(200)을 대신하여 보안 엔클레이브(300)에서 기밀 정보(132)를 프로세싱할 수 있다. 일부 예에서, 언급된 바와 같이, 커널 모드 애플리케이션(200)은 사전-부트 애플리케이션이다. 상기와 달리, 커널 모드 애플리케이션은 운영 시스템이 로딩되기 전에 명령어가 프로세싱 구성요소에 의해 실행되게 할 수 있다. 예를 들면, 커널 모드 애플리케이션(200)은 도난-방지 애플리케이션, 풀-디스크 암호화 애플리케이션 등일 수 있다. 일부 예에서, 제어 루틴(131)을 실행하는데 있어서, 프로세서 구성요소(110)는, 일단 운영 시스템이 로딩되면 보안 엔클레이브(300)를 운영 시스템으로 전달할 수 있다.

[0019] 다양한 예에서, PT(142), GDT(144), IDT(146) 및 EPC(114)는 시스템(1000) 및 특히 컴퓨팅 디바이스(100)에 관한 특성을 정의하는 다양한 데이터 구조일 수 있다. 데이터 구조를 구현하고 특히 페이지 테이블, 글로벌 디스크립터 테이블, 인터럽트 디스크립터 테이블 및 엔클레이브 페이지 캐시를 구현하기 위한 다양한 상이한 기술이 알려져 있다는 것이 인식된다. 특정 구현은 컴퓨팅 디바이스(100)의 타입, 프로세서(110)의 타입, 저장 구성요소(130)의 타입 및 컴퓨팅 디바이스(100) 상에서 실행되는 소프트웨어 및/또는 운영 시스템에 의존할 수 있다.

[0020] 다양한 실시예에서, 프로세서 구성요소(110)는, 예를 들면, 중앙 처리 장치, 그래픽 프로세싱 유닛, 또는 그렇지 않다면 임의 프로세싱 유닛과 같은 매우 다양한 상업적으로 이용 가능한 프로세서 구성요소 중 임의의 것을 포함할 수 있다. 또한, 이들 프로세서 구성요소 중 하나 이상은 다수의 프로세서, 다중-스레드 프로세서, 다중-코어 프로세서(다수의 코어가 동일하거나 별개의 다이 상에 공존하든지 간에) 및/또는 다수의 물리적으로 별개의 프로세서가 일부 방식으로 링크되는 몇몇의 다른 다양한 다중-프로세서 아키텍처를 포함할 수 있다.

[0021] 다양한 실시예에서, 저장 구성요소(130)는, 가능하게는, 전력의 중단되지 않는 제공을 요구하는 휘발성 기술을 포함하여, 그리고 가능하게는 제거 가능하거나 가능하지 않을 수 있는 머신-판독 가능 저장 매체의 사용을 수반하는 기술을 포함하여 매우 다양한 정보 저장 기술 중 임의의 것에 기초할 수 있다. 따라서, 이들 저장부 각각은 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 동적 RAM(DRAM), 더블-데이터-레이트 DRAM(DDR-DRAM), 동기화 DRAM(SDRAM), 정적 RAM(SRAM), 프로그래밍가능 ROM(PROM), 삭제 가능한 프로그래밍가능한 ROM(EPROM), 전기적으로 삭제가능한 프로그래밍 가능한 ROM(EERPOM), 플래쉬 메모리, 폴리머 메모리(예를 들면, 강유전성 폴리머 메모리), 오보닉 메모리, 상변화 또는 강자성체 메모리, SONOS(silicon-oxide-nitride-oxide-silicon) 메모리, 자기 또는 광학 카드, 하나 이상의 개별적인 강자성체 디스크 드라이브, 또는 하나 이상의 어레이로 조직화되는 복수의 저장 디바이스(예를 들면, 독립 디스크 어레이의 리던던트 어레이 또는 RAID 어레이로 조직화된 다수의 강자성체 디스크 드라이브)를 제한 없이 포함하는, 임의의 광범위한 타입(또는 타입의 조합)의 저장 디바이스를 포함할 수 있다. 비록 이들 저장부의 각각은 단일 블록으로서 도시되었지만, 이들 중 하나 이상은 상이한 저장 기술에 기초할 수 있는 다수의 저장 디바이스를 포함할 수 있다는 것이 유의되어야 한다. 따라서, 예를 들면, 이들 도시된 저장부의 각각 중 하나 이상은 프로그램 및/또는 데이터가 일부 형태의 머신 판독 가능 저장 매체 상에서 저장되고 전달될 수 있는 것에 의한 광학 드라이브 또는 플래쉬 메모리 카드 판독기의 조합, 상대적으로 연장된 기간에 대해 로컬적으로 프로그램 및/또는 데이터를 저장하는 강자성체 디스크 드라이브, 및 프로그램 및/또는 데이터에 대한 상대적으로 신속한 액세스를 가능하게 하는 하나 이상의 휘발성 솔리드 스테이트 메모리 디바이스(예를 들면, SRAM 또는 DRAM)를 나타낼 수 있다. 이들 저장부의 각각은 동일한 저장 기술에 기초한 다수의 저장 구성요소로 구성될 수 있지만, 이는 사용 중에 특화(예를 들면, 일부 DRAM 디바이스가 주요 저장부로서 이용되고 반면 다른 DRAM 디바이스는 그래픽 제어기의 구별 프레임 버퍼로서 이용됨)의 결과로서 개별적으로 유지될 수 있음에 또한 유의해야 한다.

[0022] 도시되지 않지만, 컴퓨팅 디바이스(100)는 기밀 정보를 전달하는 데이터를 네트워크(미도시)를 통해 다른 컴퓨팅 디바이스(미도시)와 교환할 수 있다. 부가적으로, 컴퓨팅 디바이스는 기밀 정보와 전체적으로 관련되지 않은 다른 데이터를 네트워크를 통해 다른 컴퓨팅 디바이스와 교환할 수 있다. 다양한 실시예에서, 네트워크는 단일 빌딩 또는 다른 상대적으로 제한된 영역 내에서 확장되는 것으로 가능하게는 제한된 단일 네트워크, 가능하게는 상당한 거리를 확장하는 접속된 네트워크의 조합일 수 있고 및/또는 인터넷을 포함할 수 있다. 따라서, 네트워크는, 제한 없이, 전기적으로 및/또는 광학적으로 전도성 케이블링을 채용하는 유선 기술, 및 적외선, 라디오 주파수 또는 다른 형태의 무선 송신을 채용하는 무선 기술을 포함하여, 신호가 교환될 수 있는 임의의 다양한 (또는 조합의) 통신 기술에 기초할 수 있다.

[0023] 다양한 실시예에서, 설명된 바와 같이 인터페이스(140)는 컴퓨팅 디바이스가 다른 디바이스에 연결되는 것을 가능하게 하는 임의의 광범위한 시그널링 기술을 이용할 수 있다. 이들 인터페이스 각각은 이러한 연결을 가능하게 하는 필수 기능 중 적어도 일부를 제공하는 회로를 포함한다. 그러나, 이들 인터페이스의 각각은 (예를 들면, 프로토콜 스택 또는 다른 특징을 구현하기 위해) 프로세서 구성요소 중 대응하는 것에 의해 실행되는 명령어의 시퀀스로 적어도 부분적으로 또한 구현될 수 있다. 전기적으로 및/또는 광학적으로 전도성 케이블링이 이용되는 경우에, 이들 인터페이스들은 RS-232C, RS-422, USB, 이더넷(IEEE-802.3) 또는 IEEE-1394를 제한 없이 포함하는, 임의의 다양한 산업 표준을 준수하는 시그널링 및/또는 프로토콜을 이용할 수 있다. 무선 신호 송신의 사용이 수반되는 경우에, 이들 인터페이스는, IEEE 802.11a, 802.11b, 802.11g, 802.16, 802.20(일반적으로 "모바일 브로드밴드 무선 액세스"로서 지칭됨), 블루투스, 지그비, 또는 일반 패킷 무선 서비스(GSM/GPRS)를 갖는 GSM과 같은 셀룰러 무선전화 서비스, CDMA/1xRTT, EDGE(Enhanced Data Rates for Global Evolution), EV-DO(Evolution Data Only/Optimized), EV-DV(Evolution For Data and Voice), HSDPA(High Speed Downlink

Packet Access), HSUPA(High Speed Uplink Packet Access), 4G LTE 등을 제한 없이 포함하는, 임의의 다양한 산업 표준을 준수하는 시그널링 및/또는 프로토콜을 이용할 수 있다.

[0024] 도 2는 제어 루틴(131)을 포함하는 도 1의 컴퓨팅 시스템(1000)의 실시예의 일부의 간략한 블록도이다. 특히, 도 2는 커널 모드 애플리케이션으로부터 보안 엔클레이브를 액세스하는 양태를 도시한다. 또한, 도 2는 커널 모드(1101)에서 발생하는 그러한 동작 및 사용자 모드(1102)에서 발생하는 그러한 동작을 도시한다.

[0025] 다양한 실시예에서, 제어 루틴(131)은 운영 시스템, 디바이스 드라이버 및/또는 애플리케이션-레벨 루틴(예를 들면, 소위 디스크 미디어 상으로 제공되는 "소프트웨어 스위트", 원격 서버로부터 획득되는 "애플릿" 등) 중 하나 이상을 포함할 수 있다. 운영 시스템이 포함되는 경우에, 운영 시스템은 컴퓨팅 디바이스(100) 및/또는 프로세서 구성요소(110)에 적합한 임의의 다양한 이용 가능한 운영 시스템일 수 있다. 하나 이상의 디바이스 드라이버가 포함되는 경우에, 그러한 디바이스 드라이버는 임의의 다양한 다른 구성요소, 컴퓨팅 디바이스(100)의 하드웨어 또는 소프트웨어 구성요소 중 어느 하나에 대한 지원을 제공할 수 있다.

[0026] 더 상세하게 도 2로 넘어가면, 제어 루틴은 커널 모드 보안 엔클레이브 드라이버(1311) 및 사용자 모드 보안 엔클레이브 관리기(1312)를 포함한다. 커널 모드 보안 엔클레이브 드라이버(1312)는 커널 모드 애플리케이션에 대한 사용자 모드 액세스를 허용하기 위해 페이지 테이블 엔트리를 수정할 수 있다. 일부 예에서, 커널 모드 보안 엔클레이브 드라이버(1312)는 PT(142) 내의 엔트리를 수정할 수 있다. 예를 들면, 사용자 모드 코드를 포함하는 그러한 페이지는 PT(142) 내의 그들 각각의 엔트리에서 사용자 페이지로서 구성될 수 있다. 일부 예에서, PT(142) 내의 모든 엔트리의 사용자/관리자 비트는, 엔트리에 대응하는 메모리 위치가 사용자 모드 애플리케이션에 대해 액세스 가능하다는 것을 표시하는 1로 설정될 수 있다.

[0027] 커널 모드 보안 엔클레이브 드라이버(1312)는 또한 커널 모드 애플리케이션이 커널 모드 및 사용자 모드 사이에서 스위칭하는 것을 가능하게 하기 위한 GDT(144) 내의 세그먼트 디스크립터를 포지셔닝(position)한다. 예를 들면, 커널 모드 및 사용자 모드 사이에서 스위칭하는 것을 가능하게 하기 위한 세그먼트 디스크립터가 GDT(144) 내에서 포지셔닝될 수 있다. 예를 들면, SYSCALL/SYSRET, SYSENTRY/SYSEXIT, INT/IRET 또는 다른 세그먼트 디스크립터는, 구현에 따라 GDT(144)에서 포지셔닝될 수 있다.

[0028] 커널 모드 보안 엔클레이브 드라이버(1312)는 또한 하나 이상의 MSR(112)을 인에이블할 수 있다. 예를 들면, SYSCALL/SYSRET 명령어는 IA32_STAR 및 IA32_LSTAR MSR이 적절히 설정되도록 요구할 수 있다. 커널 모드 보안 엔클레이브 드라이버(1312)는 또한, 사용자 모드 보안 엔클레이브 관리기(1312)가 사용자 모드에서 실행될 때를 제외하고 인터럽트를 캡처하기 위한 하나 이상의 인터럽트 루틴의 메모리 어드레스를 결정하기 위해 IDT(146)를 수정할 수 있다.

[0029] 커널 모드 보안 엔클레이브 드라이버(1311)는 또한 저장 구성요소(130) 상의 보안 엔클레이브(300)를 초기화한다. 상기와 달리, 커널 모드 보안 엔클레이브 드라이버(1311)는 보안 엔클레이브(300)를 생성한다. 예를 들면, 커널 모드 엔클레이브 드라이버(1311)는 저장 구성요소(130)로부터의 적어도 하나의 메모리 페이지를 EPC(114)에 부가할 수 있다. 일부 예에서, 커널 모드 보안 엔클레이브 드라이버(1311)는 다수의 보안 엔클레이브를 생성하는 것을 지원할 수 있다. 일부 예에서, 커널 모드 보안 엔클레이브 드라이버(1311)는, 예를 들면, EPC 범위의 하나의 단부로부터 시작하여 EPC(114)에서 페이지를 계속해서 할당함으로써, 한번에 단일의 보안 엔클레이브를 생성하는 것을 지원할 수 있다.

[0030] 커널 모드 보안 엔클레이브 드라이버(1311)는 또한 보안 엔클레이브 이미지를 보안 엔클레이브(300)와 연관된 메모리 페이지의 위치(예를 들면, EPC(114)에서 생성된 하나 이상의 메모리 페이지)로 확장할 수 있다.

[0031] 사용자 모드 보안 엔클레이브 관리기(1312)는 커널 모드(1101) 및 사용자 모드(1102) 사이에서 프로세싱 구성요소(110)의 동작을 스위칭한다. 예를 들면, 사용자 모드 보안 엔클레이브 관리기(1312)는 프로세싱 구성요소(110)로 하여금 GDT(144)에서 세그먼트 디스크립터를 실행하게 함으로써 모드 사이에서 스위칭할 수 있다.

[0032] 사용자 모드 보안 엔클레이브 관리기(1312)는 또한 명령어를 프로세싱하기 위해, 커널 모드 애플리케이션(200)으로부터 명령어를 수신하고 보안 엔클레이브(300)로 하여금 실행하게 한다. 상기와 달리, 사용자 모드 보안 엔클레이브 관리기는 커널 모드 애플리케이션으로부터 명령어를 수신하고, 명령어는 보안 엔클레이브에서 기밀 정보를 프로세싱하는 것을 포함한다. 그후, 사용자 모드 보안 엔클레이브 관리기는 커널 모드 애플리케이션 대신에 기밀 정보를 프로세싱하기 위해 보안 엔클레이브를 실행한다. 일반적으로, 사용자 모드 보안 엔클레이브 관리기(1312)는 보안 엔클레이브(300)와 기밀 정보(132)를 "프로세싱"하기 위한 명령어를 수신한다.

[0033] 예를 들면, 커널 모드 애플리케이션(200)은 사용자의 패스프레이즈가 사용자 식별을 검증하도록 유도하는 도난-

방지 애플리케이션일 수 있다. 명령어는 보안 엔클레이브(300) 내에서 기밀 정보(132)(예를 들면, 수신된 패스프레이즈 등)를 검증할 수 있다.

[0034] 일부 예에서, 커널 모드 애플리케이션(200)은, 운영 시스템을 계속해서 부팅 및 로딩하기 위해 필요한 구성요소를 포함하여, 사용자의 패스프레이즈가 디스크를 복호화하도록 유도하는 풀 디스크 암호화 애플리케이션일 수 있다. 명령어는 보안 엔클레이브(300) 내부에서 수신된 패스프레이즈를 사용하여 기밀 정보(132)(예를 들면, 운영 시스템 로더, 운영 시스템 커널 및/또는 운영 시스템 부트 드라이버 등을 저장하는 암호화된 메모리 블록)를 복호화할 수 있다.

[0035] 기밀 정보(132)를 보안 엔클레이브(300)로 전달하고 보안 엔클레이브(300)가 기밀 정보(132)를 프로세싱하게 하기 위한 프로세스가 구현에 따라 상이할 수 있다는 것이 인식된다.

[0036] 사용자 모드 보안 엔클레이브 관리기(1312)는 또한 보안 엔클레이브(300) 내의 기밀 정보(132)의 프로세싱의 표시를 커널 모드 애플리케이션(200)에 제공한다. 예를 들면, 사용자 모드 보안 엔클레이브 관리기(1312)는, 패스프레이즈의 검증이 성공하였다는 표시를 커널 모드 애플리케이션(200)에 제공할 수 있다. 일부 예에서, 사용자 모드 보안 엔클레이브 관리기(1312)는 복호화된 메모리 블록(또는 복호화된 메모리 블록의 위치)을 커널 모드 애플리케이션(200)에 제공할 수 있다.

[0037] 커널 모드 보안 엔클레이브 드라이버(1311)는 또한 보안 엔클레이브(300)를 운영 시스템(미도시)으로 전달할 수 있다. 본원에 사용된 바와 같이, 보안 엔클레이브(300)를 운영 시스템으로 "전달"하는 것은 보안 엔클레이브(300)가 실행시간 동안에 운영 시스템에 의해 (예를 들면, EPC(114)에서) 사용되게 남겨두도록 허용하는 것을 포함한다. 예를 들면, 커널 모드 애플리케이션(200)이 풀 디스크 암호화 애플리케이션이면, 운영 시스템은 실행시간 동안에 디스크를 복호화하기 위해 동일한 보안 엔클레이브(300)를 요구할 수 있다. 따라서, 다양한 실시예는, 보안 엔클레이브(300)가 운영 시스템으로 전달될 수 있는 것을 제공한다. 일부 예에서, 커널 모드 보안 엔클레이브 드라이버(1311)는 EPC(114)를 운영 시스템으로 전달할 수 있다. 부가적으로, 커널 모드 보안 엔클레이브 드라이버(1311)는 보안 엔클레이브(300)를 운영 시스템에 대한 동일한 가상 메모리 어드레스로 맵핑할 수 있다. 일부 예에서, EPC(114)는 ACPI 테이블들 등을 사용하여 운영 시스템으로 전달될 수 있다. 일부 예에서, 보안 엔클레이브(300)는 ACPI 테이블, UEFI 변수, 고정된 메모리 어드레스 등을 사용하여 사전-부트 환경으로부터 실행시간 환경(예를 들면, 운영 시스템 등)으로 전달될 수 있다.

[0038] 도 3은 논리 흐름(2000)의 일 실시예를 도시한다. 논리 흐름(2000)은 본원에 개시된 하나 이상의 실시예에 의해 실행되는 동작 중 일부 또는 전부를 나타낼 수 있다. 더 구체적으로, 논리 흐름(2000)은 적어도 제어 루틴(131)을 실행하는데 있어서 프로세서 구성요소(110)에 의해 수행되고 및/또는 컴퓨팅 디바이스(100)의 다른 구성요소(들)에 의해 수행되는 동작을 도시할 수 있다.

[0039] (2100)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 보안 엔클레이브에서 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하게 된다.

[0040] 예를 들면, 제어 루틴(131)의 커널 모드 보안 엔클레이브 드라이버(1311)는 커널 모드 애플리케이션(200)으로부터 명령어를 수신하고, 명령어를 사용자 모드 보안 엔클레이브 관리기(1312)로 송신할 수 있다. 일부 예에서, 사용자 모드 보안 엔클레이브 관리기(1312)는 커널 모드 애플리케이션(200)으로부터 직접적으로 명령어를 수신할 수 있다.

[0041] (2200)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하게 된다.

[0042] 예를 들면, 제어 루틴(131)의 커널 모드 보안 엔클레이브 드라이버(1311)는 커널 모드 애플리케이션(200)에 대한 사용자 모드 지원을 가능하게 할 수 있다. 일부 예에서, 커널 모드 보안 엔클레이브 드라이버는 커널 모드 애플리케이션(200)에 대한 사용자 모드 지원을 가능하게 하기 위해 PT(142), GDT(144), IDT(146), MSR(112)을 수정할 수 있다.

[0043] (2300)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소

(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 보안 엔클레이브를 초기화하게 된다.

[0044] 예를 들면, 제어 루틴(131)의 커널 모드 보안 엔클레이브 드라이버(1311)는 하나 이상의 페이지 엔트리를 EPC(114)에 부가하고, 하나 이상의 페이지 엔트리에 대응하는 메모리 위치에서 보안 엔클레이브(300)를 생성하고 및/또는 그 메모리 위치에서 보안 엔클레이브의 이미지를 확장시킬 수 있다.

[0045] (2400)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 기밀 정보를 프로세싱하기 위해 보안 엔클레이브를 실행하게 된다.

[0046] 예를 들면, 사용자 모드 보안 엔클레이브 관리기(1312)는 보안 엔클레이브로 하여금 기밀 정보(132)를 프로세싱하게 할 수 있다. 일부 예에서, 사용자 모드 보안 엔클레이브 관리기(1312)는 보안 엔클레이브에 대한 적절한 기능 호출을 사용하여 보안 엔클레이브(300)를 호출할 수 있다.

[0047] 도 4는 저장 매체의 실시예를 예시한다. 도 4에 도시된 바와 같이, 저장 매체는 저장 매체(3000)를 포함한다. 저장 매체(3000)는 제조 물품을 포함할 수 있다. 일부 예에서, 저장 매체(3000)는 광학, 자기 또는 반도체 저장부와 같은 임의의 비일시적인 컴퓨터 판독 가능 매체 또는 머신 판독 가능 매체를 포함할 수 있다. 저장 매체(3000)는 논리 흐름(2000)을 구현하기 위한 명령어와 같은 다양한 타입의 컴퓨터 실행 가능 명령어를 저장할 수 있다. 컴퓨터 판독 가능 또는 머신 판독 가능 저장 매체의 예는, 휘발성 메모리 또는 비휘발성 메모리, 제거 가능 또는 제거 불가능 메모리, 소거 가능 또는 소거 불가능 메모리, 기록 가능 또는 재기록 가능 메모리 등을 포함하여, 전자 데이터를 저장할 수 있는 임의의 유형의 매체를 포함할 수 있다. 컴퓨터 실행 가능 명령어의 예는 소스 코드, 컴파일링된 코드, 해석된 코드, 실행 가능 코드, 정적 코드, 동적 코드, 객체-지향형 코드, 비주얼 코드 등과 같은 임의의 적절한 타입을 포함할 수 있다. 예가 이러한 문맥으로 제한되지 않는다.

[0048] 도 5는 논리 흐름(4000)의 일 실시예를 예시한다. 논리 흐름(4000)은 본원에 개시된 하나 이상의 실시예에 의해 실행되는 동작 중 일부 또는 전부를 나타낼 수 있다. 더 구체적으로, 논리 흐름(4000)은 적어도 제어 루틴(131)을 실행하는데 있어서 프로세서 구성요소(110)에 의해 수행되고 및/또는 컴퓨팅 디바이스(100)의 다른 구성요소(들)에 의해 수행되는 동작을 도시할 수 있다.

[0049] (4100)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하게 된다. 예를 들면, 커널 모드 보안 엔클레이브 드라이버(1311)는 EPC(114) 사용을 운영 시스템으로 전달할 수 있다. 상기와 달리, 커널 모드 보안 엔클레이브 드라이버(1311)는 EPC(114)의 사용을 운영 시스템으로 전달하여, 운영 시스템은 온전한 보안 엔클레이브(300)를 남겨두고서 저장 구성요소(130)로부터 하나 이상의 부가적인 메모리 페이지를 할당할 수 있다.

[0050] (4200)에서, 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 가능하게 하기 위한 시스템의 컴퓨팅 디바이스의 프로세서 구성요소(예를 들면, 시스템(1000)의 컴퓨팅 디바이스(100)의 프로세서 구성요소(110))는 제어 루틴의 커널 모드 보안 엔클레이브 드라이버의 실행에 의해 보안 엔클레이브에 대응하는 메모리 어드레스를 운영 시스템으로 전달하게 되어, 운영 시스템이 보안 엔클레이브를 가상 메모리 위치로 맵핑할 수 있다. 예를 들면, 커널 모드 보안 엔클레이브 드라이버(1311)는 보안 엔클레이브(300)에 대응하는 가상 메모리 어드레스를 운영 시스템으로 전달할 수 있어서, 운영 시스템은 보안 엔클레이브(300)를 (예를 들면, 저장 구성요소(130) 등 내의) 동일한 가상 메모리 어드레스로 맵핑할 수 있다.

[0051] 도 6은 저장 매체의 실시예를 예시한다. 도 6에 도시된 바와 같이, 저장 매체는 저장 매체(5000)를 포함한다. 저장 매체(5000)는 제조 물품을 포함할 수 있다. 일부 예에서, 저장 매체(5000)는 광학, 자기 또는 반도체 저장부와 같은 임의의 비일시적인 컴퓨터 판독 가능 매체 또는 머신 판독 가능 매체를 포함할 수 있다. 저장 매체(5000)는 논리 흐름(4000)을 구현하기 위한 명령어와 같은 다양한 타입의 컴퓨터 실행 가능 명령어를 저장할 수 있다. 컴퓨터 판독 가능 또는 머신 판독 가능 저장 매체의 예는, 휘발성 메모리 또는 비휘발성 메모리, 제거 가능 또는 제거 불가능 메모리, 소거 가능 또는 소거 불가능 메모리, 기록 가능 또는 재기록 가능 메모리 등을 포함하여, 전자 데이터를 저장할 수 있는 임의의 유형의 매체를 포함할 수 있다. 컴퓨터 실행 가능 명령어의 예는 소스 코드, 컴파일링된 코드, 해석된 코드, 실행 가능 코드, 정적 코드, 동적 코드, 객체-지향형 코드, 비주얼 코드 등과 같은 임의의 적절한 타입을 포함할 수 있다. 예가 이러한 문맥으로 제한되지 않는다.

[0052] 도 7은 이전에 설명된 바와 같이 다양한 실시예를 구현하기에 적합한 예시의 프로세싱 아키텍처(6000)의 실시예를 도시한다. 더 구체적으로, 프로세싱 아키텍처(6000)(또는 이들의 변형)는 컴퓨팅 디바이스(100)의 부분으로서 구현될 수 있다.

[0053] 프로세싱 아키텍처(6000)는 하나 이상의 프로세서, 다중 코어 프로세서, 코프로세서, 메모리 유닛, 칩셋, 제어기, 주변장치, 인터페이스, 오실레이터, 타이밍 디바이스, 비디오 카드, 오디오 카드, 멀티미디어 입력/출력(I/O) 구성요소, 전원 공급기 등을 제한 없이 포함하는 디지털 프로세싱에서 일반적으로 이용되는 다양한 요소를 포함할 수 있다. 본 출원에서 사용되는 바와 같이, 용어 "시스템" 및 "구성요소"는 디지털 프로세싱이 수행되는 컴퓨팅 디바이스의 엔티티를 지칭하도록 의도되고, 엔티티는 하드웨어, 하드웨어 및 소프트웨어의 조합, 소프트웨어, 또는 실행 중인 소프트웨어이고, 이들의 예시는 이 도시된 예시적인 프로세싱 아키텍처에 의해 제공된다. 예를 들면, 구성요소는, 프로세서 구성요소 상에서 실행되는 프로세스, 프로세서 구성요소 자체, 저장 디바이스(예를 들면, 하드 디스크 드라이브, 어레이의 다수의 저장 드라이브 등)가 될 수 있지만, 이에 제한되지 않고, 이는 광학 및/또는 자기 저장 매체, 소프트웨어 객체, 실행가능한 명령어의 시퀀스, 실행의 쓰레드, 프로그램, 및/또는 전체 컴퓨팅 디바이스(예를 들면, 전체 컴퓨터)를 이용할 수 있다. 예시의 방식으로, 서버 상에서 실행되는 애플리케이션 및 서버 모두는 구성요소일 수 있다. 하나 이상의 구성요소는 프로세스 및/또는 실행의 쓰레드 내에 존재할 수 있고, 구성요소는 하나의 컴퓨팅 디바이스 상에 위치되고 및/또는 둘 이상의 컴퓨팅 디바이스들 사이에 분포될 수 있다. 또한, 구성요소는 동작을 조정하도록 다양한 타입의 통신 매체에 의해 서로 통신 가능하게 연결될 수 있다. 조정은 정보의 단방향 또는 양방향 교환을 포함할 수 있다. 예를 들면, 구성요소는 통신 매체를 통해 전달되는 신호의 형태로 정보를 전달할 수 있다. 정보는 하나 이상의 신호 라인에 할당되는 신호로서 구현될 수 있다. 메시지(커맨드, 상태, 어드레스 또는 데이터 메시지를 포함함)는 그러한 신호 중 하나일 수 있거나, 복수의 그러한 신호일 수 있고, 임의의 다양한 접속 및/또는 인터페이스를 통해 직렬 또는 실질적으로는 병렬로 전송될 수 있다.

[0054] 도시된 바와 같이, 프로세싱 아키텍처(3000)를 구현하는 것에 있어서, 컴퓨팅 디바이스는 적어도 프로세서 구성요소(950), 저장부(960), 다른 디바이스에 대한 인터페이스(990) 및 커플링(955)을 포함한다. 설명될 바와 같이, 프로세싱 아키텍처(3000)를 구현하는 컴퓨팅 디바이스의 다양한 양태에 따라 - 이의 의도된 사용 및/또는 사용 조건을 포함함 -, 이러한 컴퓨팅 디바이스는 제한 없이 디스플레이 인터페이스(985)와 같은 추가적인 구성요소를 더 포함할 수 있다.

[0055] 커플링(955)은 적어도 프로세서 구성요소(950)를 저장부(960)에 통신 가능하게 연결하는 하나 이상의 버스, 포인트 투 포인트 상호접속부, 송수신기, 버퍼, 크로스포인트 스위치, 및/또는 다른 컨덕터 및/또는 로직을 포함한다. 커플링(955)은 또한 (이들 및/또는 다른 구성요소 중 어느 것이 또한 존재하는지에 따라) 프로세서 구성요소(950)를 인터페이스(990), 오디오 서브시스템(970) 및 디스플레이 인터페이스(985) 중 하나 이상에 연결시킬 수 있다. 프로세서 구성요소(950)가 커플링(955)에 의해 이렇게 연결되면, 상술된 컴퓨팅 디바이스들 중 어느 컴퓨팅 디바이스(들)든지 프로세싱 아키텍처(3000)를 구현하므로, 프로세서 구성요소(950)는 위에서 상세히 설명된 태스크들 중 다양한 태스크를 수행할 수 있다. 커플링(955)은 임의의 다양한 기술 또는 기술의 조합으로 (이들에 의해 신호가 광학적으로 및/또는 전기적으로 전달됨) 구현될 수 있다. 또한, 커플링(955)의 적어도 일부는 AGP(Accelerated Graphics Port), CardBus, E-ISA(EIndustry Standard Architecture), MCA(Micro Channel Architecture), NuBus, PCI-X(Peripheral Component Interconnect(Extended)), PCI-E(PCI Express), PCMCIA(Personal Computer Memory Card International Association) 버스, HyperTransPort™, QuickPath, 등을 제한 없이 포함하는, 임의의 광범위한 산업 표준을 준수하는 타이밍 및/또는 프로토콜을 이용할 수 있다.

[0056] 이전에 논의된 바와 같이, 프로세서 구성요소(950)(가능하게는 프로세서 구성요소(110)에 대응함)는, 임의의 광범위한 기술을 이용하고 임의의 다수의 방식으로 물리적으로 통합되는 하나 이상의 코어로 구현되는, 임의의 광범위한 상업적으로 사용가능한 프로세서를 포함할 수 있다.

[0057] 이전에 논의된 바와 같이, 저장부(960)(가능하게는 저장 구성요소(130)에 대응함)는 임의의 광범위한 기술 또는 기술의 조합에 기초하는 하나 이상의 분리 저장 디바이스로 구성될 수 있다. 더 구체적으로, 도시된 바와 같이, 저장부(960)는 휘발성 저장부(961)(예를 들면, RAM 기술의 하나 이상의 형태에 기초한 솔리드 스테이트 저장부), 비휘발성 저장부(962)(예를 들면, 콘텐츠를 보존하기 위해 전력의 일정한 공급을 필요로 하지 않는 솔리드 스테이트, 강자성 또는 다른 저장부), 및 제거 가능한 매체 저장부(963)(예를 들면, 정보가 컴퓨팅 디바이스들 사이에서 전달될 수 있는 제거 가능한 디스크 또는 솔리드 스테이트 메모리 카드 저장부) 중 하나 이상을 포함할 수 있다. 가능하면 다수의 분리된 타입의 저장부를 포함하는 저장부(960)의 이러한 도시는 컴퓨팅 디바이스에서 저장 디바이스의 하나 보다 더 많은 타입의 일반적인 사용을 인지하고, 여기서 하나의 타입은 프로세서 구

성요소(950)에 의한 데이터의 더 신속한 조작을 가능하게 하는 상대적으로 신속한 판독 및 기록 능력을 제공하고(그러나 가능하면 전력을 일정하게 요구하는 "휘발성" 기술을 사용) 반면 다른 타입은 상대적으로 고밀도의 비휘발성 저장부를 제공한다(그러나 상대적으로 느린 판독 및 기록 능력을 제공할 것이다).

[0058] 상이한 기술을 이용하는 상이한 저장 디바이스의 종종 상이한 특성이 주어지면, 이러한 상이한 저장 디바이스가 상이한 인터페이스를 통해 상이한 저장 디바이스에 연결되는 상이한 저장 제어기를 통해 컴퓨팅 디바이스의 다른 부분에 연결되는 것이 또한 일반적이다. 예시의 방식으로, 휘발성 저장부(961)가 존재하고 RAM 기술에 기초하는 경우에, 휘발성 저장부(961)는 아마도 로우 및 컬럼 어드레싱을 이용하는 휘발성 저장부(961)에 적합한 인터페이스를 제공하는 저장부 제어기(965a)를 통해 커플링(955)에 통신 가능하게 연결될 수 있고, 여기서 저장부 제어기(965a)가 로우 리프레싱 및/또는 휘발성 저장부(961) 내부에 저장된 정보를 보존하는 것을 보조하는 다른 유지보수 태스크를 수행할 수 있다. 다른 예시의 방식으로, 비휘발성 저장부(962)가 존재하고 하나 이상의 강자성 및/또는 솔리드 스테이트 디스크 드라이브를 포함하는 경우에, 비휘발성 저장부(962)는 아마도 정보의 블록 및/또는 실린더 및 섹터의 어드레싱을 이용하는 비휘발성 저장부(962)에 적합한 인터페이스를 제공하는 저장부 제어기(965b)를 통해 커플링(955)에 통신 가능하게 연결될 수 있다. 또 다른 예시의 방식으로, 제거 가능한 매체 저장부(963)가 존재하고 하나 이상의 조각들의 제거 가능한 머신 판독 가능 저장 매체(969)를 이용하는 하나 이상의 광학 및/또는 솔리드 스테이트 디스크 드라이브를 포함하는 경우에, 제거 가능한 매체 저장부(963)는 아마도 정보 블록의 어드레싱을 이용하는 제거 가능한 매체 저장부(963)에 적합한 인터페이스를 제공하는 저장 제어기(965c)를 통해 커플링(955)에 통신 가능하게 연결될 수 있고, 여기서 저장부 제어기(965c)는 머신 판독 가능 저장 매체(969)의 수명을 연장하는데 특정한 방식으로 판독, 삭제 및 기록 동작을 조정할 수 있다.

[0059] 휘발성 저장부(961) 또는 비휘발성 저장부(962) 중 하나 또는 다른 하나는, 각각이 기초하는 기술에 따라, 다양한 실시예를 구현하기 위해 프로세서 구성요소(950)에 의해 실행가능한 명령어의 시퀀스를 포함하는 루틴이 저장될 수 있는 머신 판독 가능 저장 매체 형태의 제조 물품을 포함할 수 있다. 예시의 방식으로, 비휘발성 저장부(962)가 강자성 기반 디스크 드라이브(예를 들면, 소위 "하드 드라이브")를 포함하는 경우에, 각각의 이러한 디스크 드라이브는 자기적으로 응답하는 입자의 코팅이 명령어의 시퀀스와 같은 정보를 플로피 디스켓과 같은 저장 매체 유사한 방식으로 저장하는 다양한 패턴으로 증착되고 자기적으로 배향되는 하나 이상의 회전 플래터를 통상적으로 이용한다. 다른 예시로서, 비휘발성 저장부(962)는 컴팩트 플래쉬 카드와 유사한 방식으로, 명령어의 시퀀스와 같은 정보를 저장하는 솔리드 스테이트 저장 디바이스의 뱅크로 구성될 수 있다. 다시, 실행가능한 루틴 및/또는 데이터를 저장하도록 상이한 시간에 컴퓨팅 디바이스에서의 저장 디바이스의 상이한 타입을 이용하는 것이 일반적이다. 따라서, 다양한 실시예를 구현하기 위해 프로세서 구성요소(950)에 의해 실행될 명령어의 시퀀스를 포함하는 루틴은 머신 판독 가능 저장 매체(969) 상에서 초기에 저장될 수 있고, 머신 판독 가능 저장 매체(969) 및/또는 루틴이 실행됨에 따라 프로세서 구성요소(950)에 의한 더 신속한 액세스를 가능하게 하는 휘발성 저장부(961)의 계속적인 존재를 필요로 하지 않는 더 장기적인 저장부에 대한 비휘발성 저장부(962)에 대한 루틴을 복사하는 것에 있어서 제거 가능한 매체 저장부(963)가 후속하여 이용될 수 있다.

[0060] 이전에 논의된 바와 같이, 인터페이스(990)(가능하게는 인터페이스(140)에 대응함)는 컴퓨팅 디바이스를 하나 이상의 다른 디바이스에 통신 가능하게 연결시키도록 이용될 수 있는 임의의 다양한 통신 기술에 대응하는 임의의 다양한 시그널링 기술을 이용할 수 있다. 다시, 다양한 형태의 유선 또는 무선 시그널링 중 하나 또는 양자는 프로세서 구성요소(950)가 입력/출력 디바이스(예를 들면, 도시된 예시의 키보드(920) 또는 프린터(925)) 및/또는 다른 컴퓨팅 디바이스와 가능하게는 네트워크 또는 상호접속된 네트워크 세트를 통해 상호작용하는 것을 가능하게 하도록 이용될 수 있다. 임의의 하나의 컴퓨팅 디바이스에 의해 종종 지원되어야만 하는 다수의 타입의 시그널링 및/또는 프로토콜의 종종 매우 상이한 특성을 인지하면, 인터페이스(990)는 다수의 상이한 인터페이스 제어기(995a, 995b 및 995c)를 포함하는 것으로서 도시된다. 인터페이스 제어기(995a)는 도시된 키보드(920)와 같은, 사용자 입력 디바이스로부터 연속으로 전송된 메시지를 수신하도록 임의의 다양한 타입의 유선 디지털 직렬 인터페이스 또는 무선 주파수 무선 인터페이스를 이용할 수 있다. 인터페이스 제어기(995b)는 도시된 네트워크(999)(아마도 네트워크는 하나 이상의 링크, 더 소형 네트워크, 또는 아마도 인터넷으로 구성됨)를 통해 다른 컴퓨팅 디바이스에 액세스하는 임의의 다양한 케이블링 기반 또는 무선 시그널링, 타이밍 및/또는 프로토콜을 이용할 수 있다. 인터페이스(995c)는 도시된 프린터(925)에 데이터를 전달하는 직렬 또는 병렬 신호 전송 중 하나의 사용을 가능하게 하는 임의의 다양한 전기적으로 전도성 케이블링을 이용할 수 있다. 인터페이스(990)의 하나 이상의 인터페이스 제어기를 통해 통신 가능하게 연결될 수 있는 다른 예시의 디바이스는, 마이크로폰, 원격 제어, 스타일러스 펜, 카드 판독기, 지문 판독기, 가상 현실 상호작용 장갑, 그래픽 입력 태블릿, 조이스틱, 다른 키보드, 망막 스캐너, 터치 스크린의 터치 입력 구성요소, 트랙볼, 다양한 센서, 제스처들 및/또는 안면 표정을 통해 사람에 의해 시그널링되는 커맨드 및/또는 데이터를 수용하기 위해 그러한 사람의 움직

임을 모니터링하는 카메라 또는 카메라 어레이, 레이저 프린터, 잉크젯 프린터, 기계 로봇, 밀링 머신(milling machine) 등을 제한 없이 포함한다.

[0061] 컴퓨팅 디바이스가 디스플레이(예를 들면, 디스플레이(140 및/또는 240)에 대응하는 도시된 예시의 디스플레이(980))에 통신 가능하게 연결되는(또는 아마도 실제로 포함하는) 경우에, 프로세싱 아키텍처(3000)를 구현하는 이러한 컴퓨팅 디바이스는 디스플레이 인터페이스(985)를 또한 포함할 수 있다. 더 일반화된 타입의 인터페이스가 디스플레이에 통신 가능하게 연결하는데 이용될 수 있지만, 디스플레이 상에서 다양한 형식의 콘텐츠를 시각적으로 디스플레이하는데 종종 필요한 다소 특수화된 추가적인 프로세싱뿐만 아니라 사용되는 케이블링 기반 인터페이스의 다소 특수화된 특성은, 종종 분리된 디스플레이 인터페이스의 제공을 바람직하게 만든다. 디스플레이(980)의 통신 가능한 연결에서 디스플레이 인터페이스(985)에 의해 이용될 수 있는 유선 및/또는 무선 시그널링 기술은 임의의 다양한 아날로그 비디오 인터페이스, 디지털 비디오 인터페이스(DVI), 디스플레이포트 등을 제한 없이 포함하는 임의의 다양한 산업 표준을 준수하는 시그널링 및/또는 프로토콜을 이용할 수 있다.

[0062] 더 일반적으로, 본원에 개시 및 도시된 컴퓨팅 디바이스의 다양한 요소는 다양한 하드웨어 요소, 소프트웨어 요소, 또는 양자의 조합을 포함할 수 있다. 하드웨어 요소의 예시는 디바이스, 로직 디바이스, 구성요소, 프로세서, 마이크로프로세서, 회로, 프로세서 구성요소, 회로 요소(예를 들면, 트랜지스터, 레지스터, 커패시터, 인덕터 등), 집적 회로, 애플리케이션 특정 집적 회로(ASIC), 프로그래밍가능한 로직 디바이스(PLD), 디지털 신호 프로세서(DSP), 필드 프로그래밍가능한 게이트 어레이(FPGA), 메모리 유닛, 로직 게이트, 레지스터, 반도체 디바이스, 칩, 마이크로칩, 칩 셋 등을 포함할 수 있다. 소프트웨어 요소의 예시는 소프트웨어 구성요소, 프로그램, 애플리케이션, 컴퓨터 프로그램, 애플리케이션 프로그램, 시스템 프로그램, 소프트웨어 개발 프로그램, 머신 프로그램, 운영 시스템 소프트웨어, 미들웨어, 펌웨어, 소프트웨어 모듈, 루틴, 서브루틴, 함수, 방법, 프로시져, 소프트웨어 인터페이스, 애플리케이션 프로그램 인터페이스(API), 명령어 세트, 컴퓨팅 코드, 컴퓨터 코드, 코드 세그먼트, 컴퓨터 코드 세그먼트, 워드, 값, 심볼, 또는 이들의 임의의 조합을 포함할 수 있다. 그러나, 실시예가 하드웨어 요소 및/또는 소프트웨어 요소를 사용하여 구현되는지 여부를 판정하는 것은 주어진 구현예에 대해 바람직한 것으로서, 바람직한 계산 레이트, 전력 레벨, 열 허용치, 프로세싱 사이클 예산, 입력 데이터 레이트, 출력 데이터 레이트, 메모리 리소스, 데이터 버스 속도 및 다른 설계 또는 성능 제약과 같은, 임의의 수의 인자에 따라 변할 수 있다.

[0063] 일부 실시예는 "일 실시예" 또는 "실시예"와 같은 표현을 이들의 파생어와 함께 사용하여 설명될 수 있다. 이들 용어는 실시예와 연관되어 설명되는 특정 특징, 구조 또는 특성이 적어도 하나의 실시예에 포함된다는 것을 의미한다. 명세서에서 다양한 위치에서 "일 실시예"라는 구절의 출현은 반드시 모두가 동일한 실시예를 지칭하는 것이 아니다. 또한, 일부 실시예는 "연결된" 및 "접속된"이라는 표현을 이들의 파생어와 함께 사용하여 설명될 수 있다. 이들 용어는 반드시 서로에 대한 동의어로서 의도되는 것은 아니다. 예를 들면, 일부 실시예는 둘 이상의 요소가 서로 직접 물리적 또는 전기적 접촉 중인 것을 나타내도록 "접속된" 및/또는 "연결된"이라는 용어를 사용하여 설명될 수 있다. 그러나, 용어 "연결된"은 또한 둘 이상의 요소가 서로 직접 접촉 중은 아니지만, 여전히 서로 협업 또는 상호작용하는 것을 의미할 수 있다. 또한, 상이한 실시예로부터의 양태 또는 요소가 조합될 수 있다.

[0064] 요약서는 독자가 기술적인 개시의 특성을 신속하게 확인하는 것을 가능하게 하도록 제공됨이 강조된다. 이것이 청구항의 범위 또는 의미를 해석 또는 제한하도록 사용되지 않을 것이라는 이해가 함께 제출된다. 또한, 이전의 상세한 설명에서, 다양한 특징이 개시를 간소화하는 목적으로 단일 실시예에서 함께 그룹화된다는 것을 알 수 있다. 이 방법의 개시는 청구된 실시예가 각각의 청구항에서 명시적으로 언급되는 것 외에 더 많은 특징을 필요로 한다는 의도를 반영하는 것으로서 해석되지 않는다. 오히려, 다음의 청구항이 반영하는 바와 같이, 발명의 청구대상은 단일의 개시된 실시예의 모든 특징보다 적게 존재한다. 따라서 다음의 청구항은 여기에서 상세한 설명에 통합되고, 각각의 청구항은 분리된 실시예로서 자체에 기초한다. 첨부된 청구항에서, 용어 "포함하는(including)" 및 "여기서(in which)"는 개별적인 용어 "포함하는(comprising)" 및 "여기서(wherein)"의 평이한 영어 동의어로서 각각 사용된다. 또한, 용어 "제 1", "제 2", "제 3" 등은 단지 레이블로서 사용되고, 이들의 객체에 대한 숫자 필요조건을 부가하는 것으로 의도되지 않는다.

[0065] 위에서 설명된 것은 개시된 아키텍처의 예들을 포함한다. 물론, 구성요소 및/또는 방법의 모든 구상 가능한 조합을 설명하는 것이 불가능하지만, 당업자는 많은 추가 조합 및 순열이 가능하다는 것을 인식할 수 있다. 따라서, 새로운 아키텍처는 첨부된 청구항의 사상 및 범위 내에 속하는 모든 이러한 변경, 수정 및 변형을 포함하도록 의도된다. 상세한 개시는 이제 추가 실시예에 관련된 예를 제공하는 것으로 넘어간다. 이하에서 제공되는 예

들은 제한하는 것으로 의도되지 않는다.

[0066] 예 1: 보안 엔클레이브에 대한 커널 모드 액세스(kernel mode access)를 제공하는 장치. 상기 장치는 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하기 위한 커널 모드 보안 엔클레이브 드라이버 - 커널 모드 보안 엔클레이브 드라이버는 커널 모드 애플리케이션 대신에 컴퓨팅 디바이스의 저장 구성요소 상에서 보안 엔클레이브를 초기화함 - 와, 커널 모드 애플리케이션으로부터의 명령어를 프로세싱하기 위한 사용자 모드 보안 엔클레이브 관리기 - 명령어는 보안 엔클레이브에서 기밀 정보를 프로세싱하는 것을 포함함 - 를 포함한다.

[0067] 예 2: 예 1의 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브에 대한 커널 모드 애플리케이션에 대한 사용자 모드 액세스를 허용하기 위해 페이지 테이블 엔트리를 수정한다.

[0068] 예 3: 예 1 또는 2 중 어느 한 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 커널 모드 애플리케이션이 커널 모드 및 사용자 모드 사이에서 스위칭하는 것을 가능하게 하는 세그먼트 디스크립터를 글로벌 디스크립터 테이블에서 포지셔닝한다.

[0069] 예 4: 예 3의 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 모델 특정 레지스터가 커널 모드 및 사용자 모드 사이의 스위칭을 제공하는 것을 가능하게 한다.

[0070] 예 5: 예 1 내지 4 중 어느 한 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브를 생성한다.

[0071] 예 6: 예 5의 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 저장 구성요소로부터의 적어도 하나의 메모리 페이지를 보안 엔클레이브 페이지 캐시에 부가하고, 적어도 하나의 메모리 페이지는 보안 엔클레이브에 대응한다.

[0072] 예 7: 예 6의 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브 이미지를 적어도 하나의 메모리 페이지로 확장시킨다.

[0073] 예 8: 예 4 내지 7 중 어느 한 장치에 있어서, 사용자 모드 보안 엔클레이브 관리기는 모델 특정 레지스터 및/또는 글로벌 디스크립터 테이블 내의 세그먼트 디스크립터에 적어도 부분적으로 기초하여 커널 모드 및 사용자 모드 특권 사이에서 커널 모드 애플리케이션을 스위칭한다.

[0074] 예 9: 예 1 내지 8 중 어느 한 장치에 있어서, 사용자 모드 보안 엔클레이브 관리기는 커널 모드 애플리케이션으로부터 명령어를 수신하고, 보안 엔클레이브로 하여금 명령어를 프로세싱하게 한다.

[0075] 예 10: 예 1 내지 9 중 어느 한 장치에 있어서, 명령어는 패스프레이즈를 검증하고, 사용자 모드 보안 엔클레이브 관리기는 패스프레이즈를 보안 엔클레이브로 송신하고, 보안 엔클레이브에서 패스프레이즈를 검증하도록 보안 엔클레이브에 지시한다.

[0076] 예 11: 예 10의 장치에 있어서, 사용자 모드 보안 엔클레이브 관리기는 패스프레이즈의 검증에 대응하는 표시를 보안 엔클레이브로부터 수신한다.

[0077] 예 12: 예 1 내지 예 9 중 어느 한 장치에 있어서, 명령어는 암호화된 메모리 블록을 복호화하고, 사용자 모드 보안 엔클레이브 관리기는 암호화된 메모리 블록을 보안 엔클레이브로 송신하고, 암호화된 메모리 블록을 보안 엔클레이브에서 복호화하도록 보안 엔클레이브에 지시한다.

[0078] 예 13: 예 12의 장치에 있어서, 사용자 모드 보안 엔클레이브 관리기는 보안 엔클레이브로부터 암호화된 메모리 블록의 콘텐츠를 수신하고, 콘텐츠를 커널 모드 애플리케이션으로 송신한다.

[0079] 예 14: 예 1 내지 예 13 중 어느 한 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브를 운영 시스템으로 전달한다.

[0080] 예 15: 예 6의 장치에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하고, 운영 시스템은 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 저장 구성요소로부터 하나 이상의 부가적인 메모리 페이지를 할당하고, 보안 엔클레이브에 대응하는 메모리 어드레스를 운영 시스템으로 전달하도록 구성되고, 운영 시스템은 메모리 어드레스에 적어도 부분적으로 기초하여 보안 엔클레이브를 가상 메모리 위치로 맵핑하도록 구성된다.

[0081] 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하고, 운영 시스템은 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 보안 엔클레이브에 대해 저장 구성

요소로부터 하나 이상의 부가적인 메모리 페이지를 할당하고, 보안 엔클레이브를 선택된 가상 메모리 위치로 맵핑하도록 구성된다.

[0082] 예 16: 예 1 내지 15 중 어느 한 장치에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션 또는 도난-방지 애플리케이션 중 어느 하나이다.

[0083] 예 17: 예 13의 장치에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션이고, 암호화된 메모리 블록은 운영 시스템 로더, 운영 시스템 커널 및/또는 운영 시스템 부트 드라이버를 포함한다.

[0084] 예 18: 예 11의 장치에 있어서, 커널 모드 애플리케이션은 도난-방지 애플리케이션이고, 패스프레이즈는 사용자 검증 패스프레이즈에 대응한다.

[0085] 예 19: 예 1의 장치에 있어서, 보안 엔클레이브는 프로세서 구성요소에 의해 생성된 임시 키 하에서 암호화된다.

[0086] 예 20: 커널 모드 애플리케이션에 의한 보안 엔클레이브에 대한 액세스를 허용하는 컴퓨팅 시스템. 컴퓨팅 시스템은 프로세싱 구성요소와, 프로세싱 구성요소에 의한 실행을 위한 컴퓨팅 시스템 펌웨어 인터페이스 - 컴퓨팅 시스템 펌웨어 인터페이스는 커널 모드 애플리케이션을 시작하고, 커널 모드 애플리케이션은 컴퓨터 시스템의 일부를 초기화함 - 와, 프로세싱 구성요소에 의한 실행을 위한 커널 모드 보안 엔클레이브 드라이버 - 커널 모드 보안 엔클레이브 드라이버는 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하고, 커널 모드 애플리케이션 대신에 저장 구성요소 상에서 보안 엔클레이브를 초기화함 - 와, 및 프로세싱 구성요소에 의한 실행을 위한 사용자 모드 보안 엔클레이브 관리기를 포함하고, 사용자 모드 보안 엔클레이브 관리기는 커널 모드 애플리케이션으로부터 명령어를 프로세싱하고, 명령어는 보안 엔클레이브에서 기밀 정보를 프로세싱하는 것을 포함한다.

[0087] 예 21: 예 19의 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브에 대한 커널 모드 애플리케이션에 대한 사용자 모드 액세스를 허용하기 위해 페이지 테이블 엔트리를 수정한다.

[0088] 예 22: 예 19 또는 20 중 어느 한 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 커널 모드 애플리케이션이 커널 모드 및 사용자 모드 사이에서 스위칭하는 것을 가능하게 하는 세그먼트 디스크립터를 글로벌 디스크립터 테이블에서 포지셔닝한다.

[0089] 예 23: 예 21의 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 모델 특정 레지스터가 커널 모드 및 사용자 모드 사이의 스위칭을 제공하는 것을 가능하게 한다.

[0090] 예 24: 예 19 내지 22 중 어느 한 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브를 생성한다.

[0091] 예 25: 예 23의 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 저장 구성요소로부터의 적어도 하나의 메모리 페이지를 보안 엔클레이브 페이지 캐시에 부가하고, 적어도 하나의 메모리 페이지는 보안 엔클레이브에 대응한다.

[0092] 예 26: 예 24의 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브 이미지를 적어도 하나의 메모리 페이지로 확장시킨다.

[0093] 예 27: 예 22 내지 25 중 어느 한 컴퓨팅 시스템에 있어서, 사용자 모드 보안 엔클레이브 관리기는 모델 특정 레지스터 및/또는 글로벌 디스크립터 테이블 내의 세그먼트 디스크립터에 적어도 부분적으로 기초하여 커널 모드 및 사용자 모드 특권 사이에서 커널 모드 애플리케이션을 스위칭한다.

[0094] 예 28: 예 19 내지 26 중 어느 한 컴퓨팅 시스템에 있어서, 사용자 모드 보안 엔클레이브 관리기는 커널 모드 애플리케이션으로부터 명령어를 수신하고, 보안 엔클레이브로 하여금 명령어를 프로세싱하게 한다.

[0095] 예 29: 예 19 내지 27 중 어느 한 컴퓨팅 시스템에 있어서, 명령어는 패스프레이즈를 검증하고, 사용자 모드 보안 엔클레이브 관리기는 패스프레이즈를 보안 엔클레이브로 송신하고, 보안 엔클레이브에서 패스프레이즈를 검증하도록 보안 엔클레이브에 지시한다.

[0096] 예 30: 예 28의 컴퓨팅 시스템에 있어서, 사용자 모드 보안 엔클레이브 관리기는 패스프레이즈의 검증에 대응하는 표시를 보안 엔클레이브로부터 수신한다.

[0097] 예 31: 예 19 내지 예 27 중 어느 한 컴퓨팅 시스템에 있어서, 명령어는 암호화된 메모리 블록을 복호화하고,

사용자 모드 보안 엔클레이브 관리기는 암호화된 메모리 블록을 보안 엔클레이브로 송신하고, 암호화된 메모리 블록을 보안 엔클레이브에서 복호화하도록 보안 엔클레이브에 지시한다.

[0098] 예 32: 예 30의 컴퓨팅 시스템에 있어서, 사용자 모드 보안 엔클레이브 관리기는 보안 엔클레이브로부터 암호화된 메모리 블록의 콘텐츠를 수신하고, 콘텐츠를 커널 모드 애플리케이션으로 송신한다.

[0099] 예 33: 예 19 내지 예 31 중 어느 한 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브를 운영 시스템으로 전달한다.

[0100] 예 34: 예 24의 컴퓨팅 시스템에 있어서, 커널 모드 보안 엔클레이브 드라이버는 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하고, 운영 시스템은 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 저장 구성요소로부터 하나 이상의 부가적인 메모리 페이지를 할당하고, 보안 엔클레이브에 대응하는 메모리 어드레스를 운영 시스템으로 전달하도록 구성되고, 운영 시스템은 메모리 어드레스에 적어도 부분적으로 기초하여 보안 엔클레이브를 가상 메모리 위치로 맵핑하도록 구성된다.

[0101] 예 35: 예 19 내지 33 중 어느 한 컴퓨팅 시스템에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션 또는 도난-방지 애플리케이션 중 어느 하나이다.

[0102] 예 36: 예 31의 컴퓨팅 시스템에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션이고, 암호화된 메모리 블록은 운영 시스템 로더, 운영 시스템 커널 및/또는 운영 시스템 부트 드라이버를 포함한다.

[0103] 예 37: 예 29의 컴퓨팅 시스템에 있어서, 커널 모드 애플리케이션은 도난-방지 애플리케이션이고, 패스프레이즈는 사용자 검증 패스프레이즈에 대응한다.

[0104] 예 38: 예 20의 컴퓨팅 시스템에 있어서, 보안 엔클레이브는 프로세서 구성요소에 의해 생성된 임시 키 하에서 암호화된다.

[0105] 예 39: 커널 모드 애플리케이션을 통해 보안 엔클레이브를 액세스하기 위한 컴퓨팅-구현 방법. 상기 방법은 보안 엔클레이브에서 기밀 정보를 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하는 단계와, 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하는 단계와, 컴퓨팅 디바이스의 저장 구성요소 상에서 보안 엔클레이브를 초기화하는 단계와, 기밀 정보를 프로세싱하기 위해 보안 엔클레이브를 실행하는 단계를 포함한다.

[0106] 예 40: 예 39의 컴퓨팅-구현 방법에 있어서, 커널 모드 애플리케이션을 런칭하는 단계를 더 포함한다.

[0107] 예 41: 예 39 또는 40 중 어느 한 컴퓨팅-구현 방법에 있어서, 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하는 단계는 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하기 위해 페이지 테이블 엔트리를 수정하는 단계를 포함한다.

[0108] 예 42: 예 39 내지 41 중 어느 한 컴퓨팅-구현 방법에 있어서, 커널 모드 및 사용자 모드 사이에서 스위칭하기 위한 세그먼트 디스크립터를 글로벌 디스크립터 테이블에서 포지셔닝하는 단계를 더 포함한다.

[0109] 예 43: 예 39 내지 42 중 어느 한 컴퓨팅-구현 방법에 있어서, 보안 엔클레이브를 초기화하는 단계는 보안 엔클레이브에 대해 저장 구성요소로부터 적어도 하나의 메모리 페이지를 할당하는 단계와, 적어도 하나의 메모리 페이지를 보안 엔클레이브에 대응하는 엔클레이브 페이지 캐시에 부가하는 단계를 포함한다.

[0110] 예 44: 예 43의 컴퓨팅-구현 방법에 있어서, 적어도 하나의 메모리 페이지에서 보안 엔클레이브를 생성하는 단계를 더 포함한다.

[0111] 예 45: 예 43의 컴퓨팅-구현 방법에 있어서, 보안 엔클레이브 이미지의 콘텐츠를 적어도 하나의 메모리 페이지로 확장시키는 단계를 더 포함한다.

[0112] 예 46: 예 39 내지 45 중 어느 한 컴퓨팅-구현 방법에 있어서, 명령어는 패스프레이즈를 검증하고, 상기 방법은 패스프레이즈를 보안 엔클레이브로 송신하고, 패스프레이즈를 보안 엔클레이브에서 검증하도록 보안 엔클레이브에 지시하는 단계를 더 포함한다.

[0113] 예 47: 예 46의 컴퓨팅-구현 방법에 있어서, 패스프레이즈의 검증에 대응하는 표시를 보안 엔클레이브로부터 수신하는 단계를 더 포함한다.

[0114] 예 48: 예 39 내지 45의 컴퓨팅-구현 방법에 있어서, 명령어는 암호화된 메모리 블록을 복호화하고, 상기 방법은 암호화된 메모리 블록을 보안 엔클레이브로 송신하고, 암호화된 메모리 블록을 보안 엔클레이브에서 복호화

하도록 보안 엔클레이브에 지시하는 단계를 더 포함한다.

[0115] 예 49: 예 48의 컴퓨팅-구현 방법에 있어서, 암호화된 메모리 블록의 콘텐츠를 보안 엔클레이브로부터 수신하고, 콘텐츠를 커널 모드 애플리케이션으로 송신하는 단계를 더 포함한다.

[0116] 예 50: 예 39 내지 49 중 어느 한 컴퓨팅-구현 방법에 있어서, 보안 엔클레이브를 운영 시스템으로 전달하는 단계를 더 포함한다.

[0117] 예 51: 예 43의 컴퓨팅-구현 방법에 있어서, 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하는 단계 - 운영 시스템은 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 저장 구성요소로부터 하나 이상의 부가적인 메모리 페이지를 할당하도록 구성됨 - 과, 보안 엔클레이브에 대응하는 메모리 어드레스를 운영 시스템으로 전달하는 단계 - 운영 시스템은 메모리 어드레스에 적어도 부분적으로 기초하여 보안 엔클레이브를 가상 메모리 위치로 맵핑하도록 구성됨 - 을 더 포함한다.

[0118] 예 52: 예 39 내지 51 중 어느 한 컴퓨팅-구현 방법에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션 또는 도난-방지 애플리케이션 중 어느 하나이다.

[0119] 예 53: 예 49의 컴퓨팅-구현 방법에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션이고, 암호화된 메모리 블록은 운영 시스템 로더, 운영 시스템 커널 및/또는 운영 시스템 부트 드라이버를 포함한다.

[0120] 예 54: 예 47의 컴퓨팅-구현 방법에 있어서, 커널 모드 애플리케이션은 도난-방지 애플리케이션이고, 패스프레이즈는 사용자 검증 패스프레이즈에 대응한다.

[0121] 예 55: 커널 모드 애플리케이션을 통해 보안 엔클레이브를 액세스하기 위한 장치. 상기 장치는 보안 엔클레이브에서 기밀 정보를 프로세싱하기 위한 명령어를 커널 모드 애플리케이션으로부터 수신하기 위한 수단과, 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하기 위한 수단과, 컴퓨팅 디바이스의 저장 구성요소 상에서 보안 엔클레이브를 초기화하기 위한 수단과, 기밀 정보를 프로세싱하기 위해 보안 엔클레이브를 실행하기 위한 수단을 포함한다.

[0122] 예 56: 예 55의 장치에 있어서, 커널 모드 애플리케이션을 런칭하기 위한 수단을 더 포함한다.

[0123] 예 57: 예 55 또는 56 중 어느 한 장치에 있어서, 커널 모드 애플리케이션에 대한 사용자 모드 지원을 가능하게 하기 위한 수단은 커널 모드 애플리케이션에 대한 사용자 모드 지원을 제공하기 위해 페이지 테이블 엔트리를 수정하기 위한 수단을 포함한다.

[0124] 예 58: 예 55 내지 57 중 어느 한 장치에 있어서, 커널 모드 및 사용자 모드 사이에서 스위칭하기 위한 세그먼트 디스크립터를 글로벌 디스크립터 테이블에서 포지셔닝하기 위한 수단을 더 포함한다.

[0125] 예 59: 예 55 내지 58 중 어느 한 장치에 있어서, 보안 엔클레이브를 초기화하기 위한 수단은 보안 엔클레이브에 대해 저장 구성요소로부터 적어도 하나의 메모리 페이지를 할당하기 위한 수단과, 적어도 하나의 메모리 페이지를 보안 엔클레이브에 대응하는 엔클레이브 페이지 캐시에 부가하기 위한 수단을 포함한다.

[0126] 예 60: 예 59의 장치에 있어서, 적어도 하나의 메모리 페이지에서 보안 엔클레이브를 생성하기 위한 수단을 더 포함한다.

[0127] 예 61: 예 59의 장치에 있어서, 보안 엔클레이브 이미지의 콘텐츠를 적어도 하나의 메모리 페이지로 확장시키기 위한 수단을 더 포함한다.

[0128] 예 62: 예 55 내지 61 중 어느 한 장치에 있어서, 명령어는 패스프레이즈를 검증하고, 상기 장치는 패스프레이즈를 보안 엔클레이브로 송신하고, 패스프레이즈를 보안 엔클레이브에서 검증하도록 보안 엔클레이브에 지시하기 위한 수단을 더 포함한다.

[0129] 예 63: 예 62의 장치에 있어서, 패스프레이즈의 검증에 대응하는 표시를 보안 엔클레이브로부터 수신하기 위한 수단을 더 포함한다.

[0130] 예 64: 예 55 내지 61의 장치에 있어서, 명령어는 암호화된 메모리 블록을 복호화하고, 상기 장치는 암호화된 메모리 블록을 보안 엔클레이브로 송신하고, 암호화된 메모리 블록을 보안 엔클레이브에서 복호화하도록 보안 엔클레이브에 지시하기 위한 수단을 더 포함한다.

[0131] 예 65: 예 64의 장치에 있어서, 암호화된 메모리 블록의 콘텐츠를 보안 엔클레이브로부터 수신하고, 콘텐츠를

커널 모드 애플리케이션으로 송신하기 위한 수단을 더 포함한다.

[0132] 예 66: 예 55 내지 65 중 어느 한 장치에 있어서, 보안 엔클레이브를 운영 시스템으로 전달하기 위한 수단을 더 포함한다.

[0133] 예 67: 예 59의 장치에 있어서, 보안 엔클레이브 페이지 캐시 사용을 운영 시스템으로 전달하기 위한 수단 - 운영 시스템은 보안 엔클레이브 페이지 캐시 사용에 적어도 부분적으로 기초하여 저장 구성요소로부터 하나 이상의 부가적인 메모리 페이지를 할당하도록 구성됨 - 과, 보안 엔클레이브에 대응하는 메모리 어드레스를 운영 시스템으로 전달하기 위한 수단 - 운영 시스템은 메모리 어드레스에 적어도 부분적으로 기초하여 보안 엔클레이브를 가상 메모리 위치로 맵핑하도록 구성됨 - 을 더 포함한다.

[0134] 예 68: 예 55 내지 67 중 어느 한 장치에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션 또는 도난-방지 애플리케이션 중 어느 하나이다.

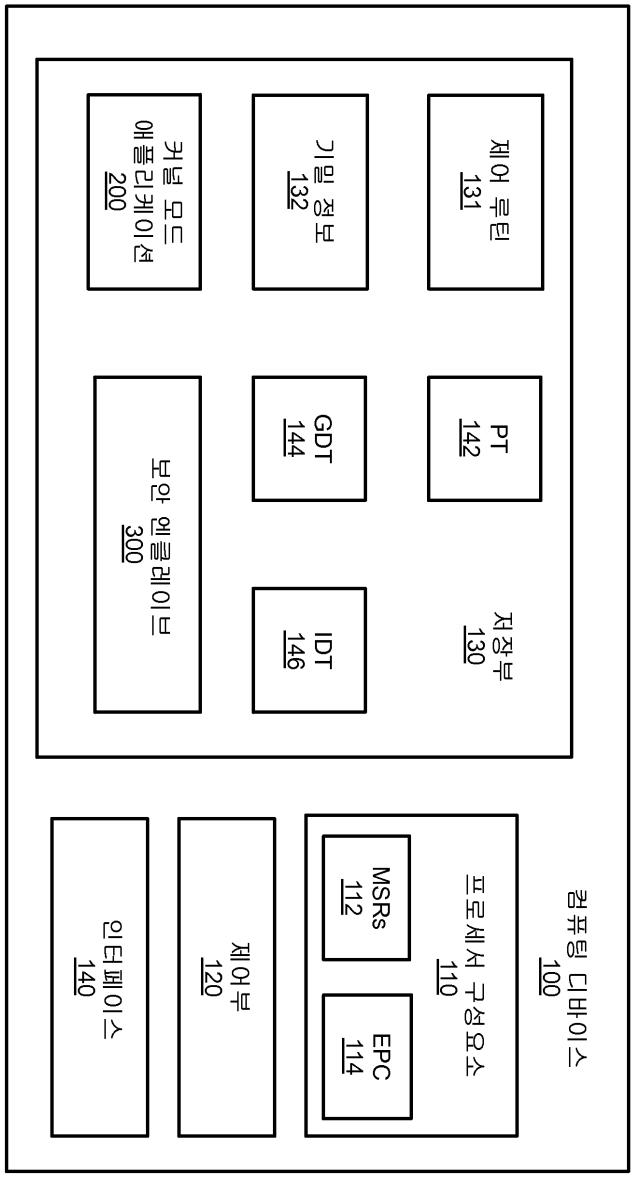
[0135] 예 69: 예 65의 장치에 있어서, 커널 모드 애플리케이션은 풀 디스크 암호화 애플리케이션이고, 암호화된 메모리 블록은 운영 시스템 로더, 운영 시스템 커널 및/또는 운영 시스템 부트 드라이버를 포함한다.

[0136] 예 70: 예 63의 장치에 있어서, 커널 모드 애플리케이션은 도난-방지 애플리케이션이고, 패스프레이즈는 사용자 검증 패스프레이즈에 대응한다.

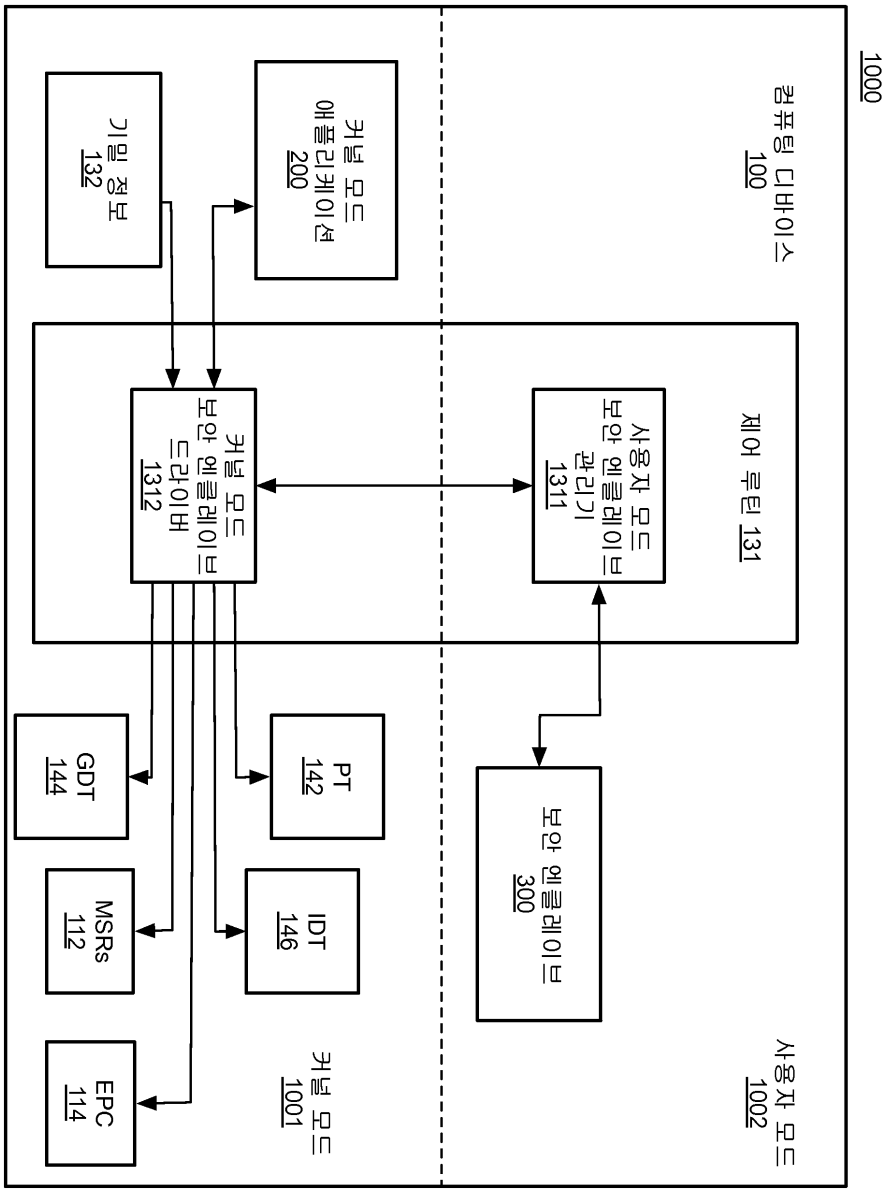
[0137] 예 71: 명령어를 포함하는 적어도 하나의 머신 판독 가능 저장 매체로서, 명령어는, 컴퓨팅 디바이스에 의해 실행될 때, 컴퓨팅 디바이스로 하여금 예 39 내지 54 중 어느 한 방법을 수행하게 한다.

도면

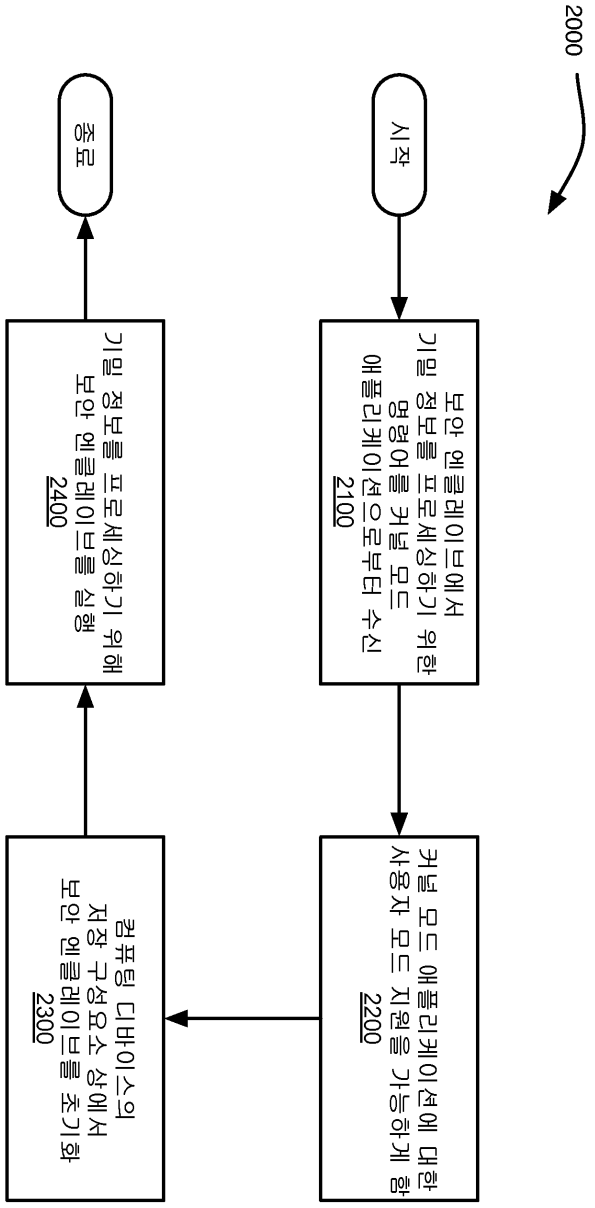
도면1


1000
컴퓨팅 디바이스
100
프로세서 구성요소
110
MSRs
112
EPC
114
제어부
120
인터페이스
140
저장부
130
제어 루틴
131
기밀 정보
132
커널 모드
애플리케이션
200
PT
142
GDT
144
IDT
146
보안 엔클레이브
300

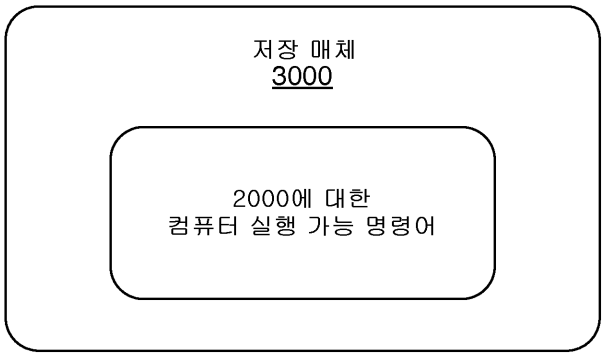
도면2


1000
컴퓨팅 디바이스
100
커널 모드
애플리케이션
200
기밀 정보
132
제어 루틴 131
커널 모드
보안 엔클레이브
드라이버
1312
사용자 모드
보안 엔클레이브
관리기
1311
보안 엔클레이브
300
GDT
144
PT
142
MSRs
112
IDT
146
EPC
114
커널 모드
1001
사용자 모드
1002

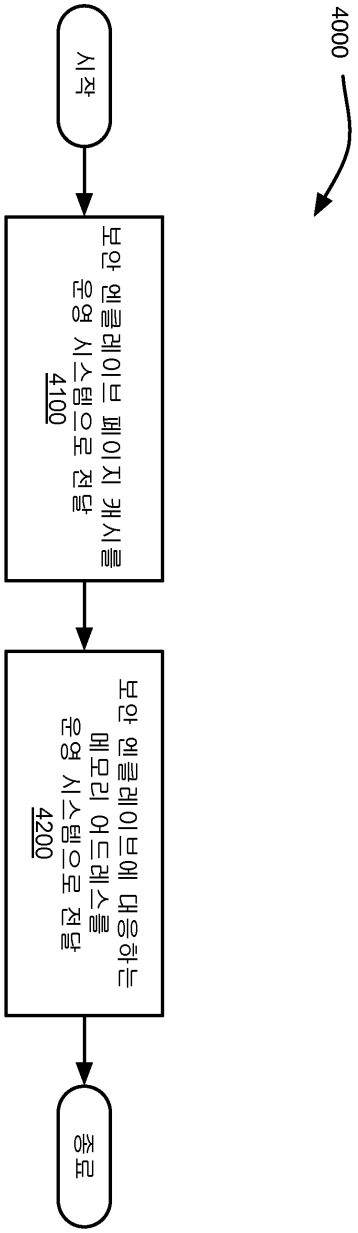
도면3


2000
시작
보안 엔클레이브에서
기밀 정보를 프로세싱하기 위한
명령어를 커널 모드
애플리케이션으로부터 수신
2100
커널 모드 애플리케이션에 대한
사용자 모드 지원을 가능하게 함
2200
컴퓨팅 디바이스의
저장 구성요소 상에서
보안 엔클레이브를 초기화
2300
기밀 정보를 프로세싱하기 위해
보안 엔클레이브를 실행
2400
종료

도면4


저장 매체
3000
2000에 대한
컴퓨터 실행 가능 명령어

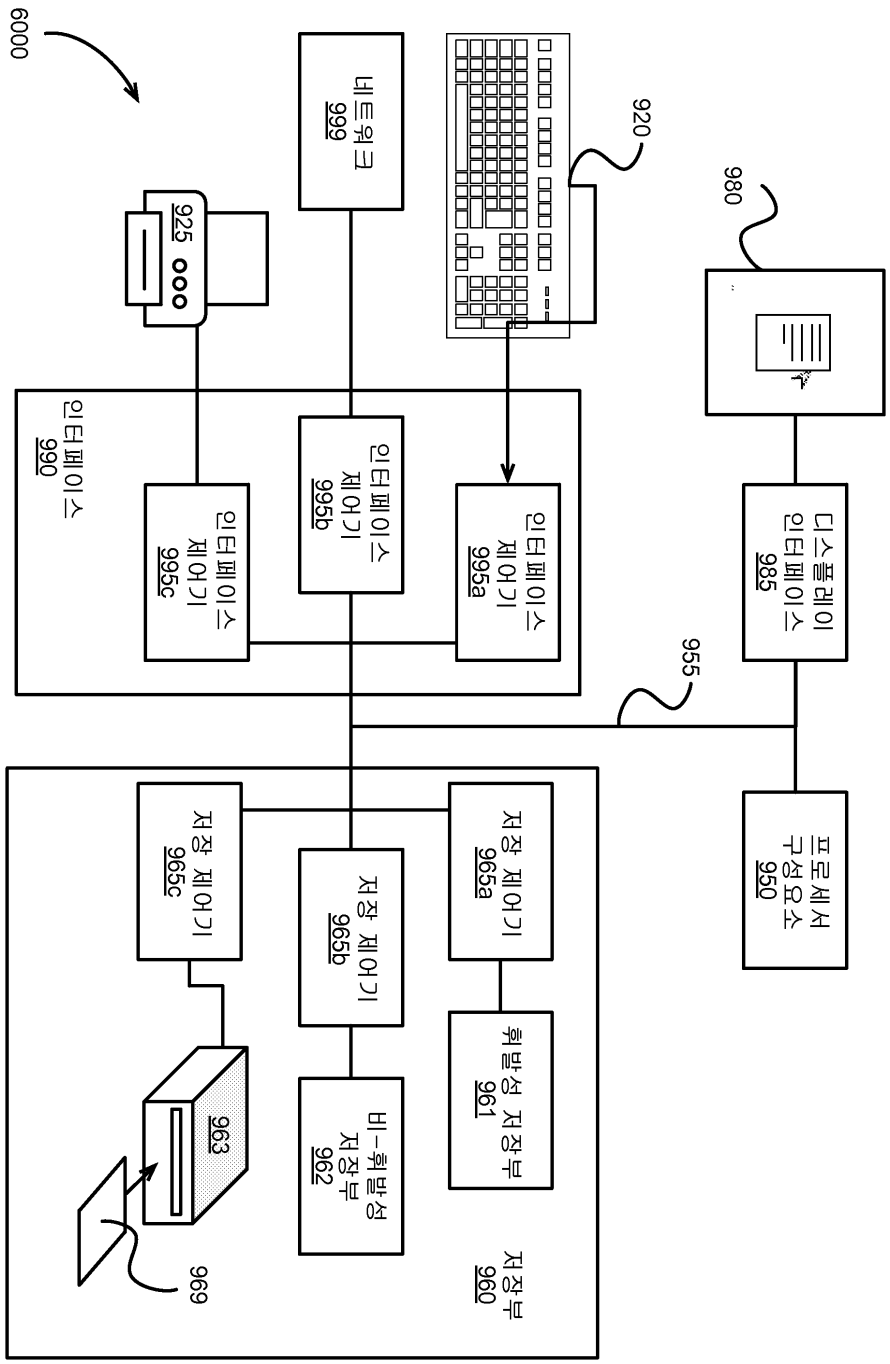
도면5


시작
4000
보안 엘리베이트 페이지 캐시를
운용 시스템으로 전달
4100
보안 엘리베이트에 대응하는
메모리 어드레스를
운용 시스템으로 전달
4200
종료

도면6


저장 매체
5000
4000에 대한
컴퓨터 실행 가능 명령어

도면7


6000
네트워크
999
920
980
925
인터페이스
990
인터페이스
제어기
995b
인터페이스
제어기
995a
인터페이스
제어기
995c
디스플레이
인터페이스
985
955
저장 제어기
965c
저장 제어기
965b
저장 제어기
965a
프로세서
구성요소
950
963
휘발성 저장부
961
비-휘발성
저장부
962
969
저장부
960