(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년05월17일
(11) 등록번호 10-1953444
(24) 등록일자 2019년02월22일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 21/64* (2013.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
G06F 21/604 (2013.01)
(21) 출원번호 10-2016-0178785
(22) 출원일자 2016년12월26일
심사청구일자 2016년12월26일
(65) 공개번호 10-2018-0074967
(43) 공개일자 2018년07월04일
(56) 선행기술조사문헌
KR1020150051813 A*
KR1020150055934 A*
KR1020130120985 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 지곡로 155, 6동 1105호
박우람
경상북도 포항시 남구 청암로 77, 11동 112호
신재복
경상북도 포항시 남구 지곡로 319, 342동 403호
(74) 대리인
특허법인이상

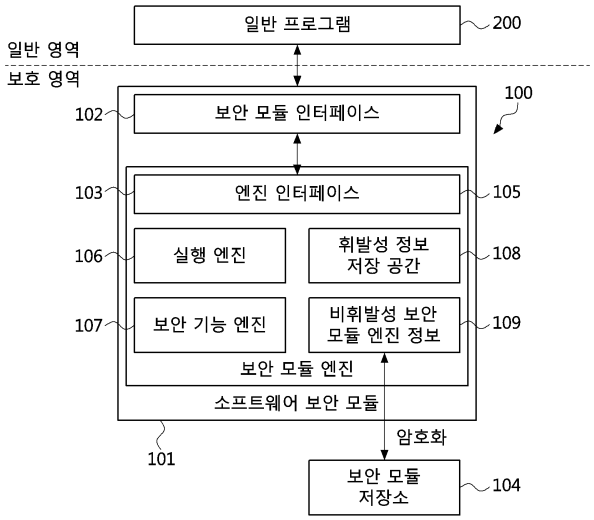
전체 청구항 수 : 총 20 항 심사관 : 구대성

(54) 발명의 명칭 **하드웨어 수준 보안을 보장하는 가상화 기반 소프트웨어 보안 방법 및 이를 이용하는 장치**

(57) 요 약

하드웨어 수준의 보안을 보장해줄 수 있는 가상화 기반 소프트웨어 보안 방법 및 장치가 개시된다. 가상화 기반 소프트웨어 보안 장치는, 암호화 및 보안 프로토콜 수행을 위한 보안 모듈 엔진, 응용프로그램에서 소프트웨어 보안 모듈에 명령 및 데이터를 전송하는 보안 모듈 인터페이스, 및 보안 모듈 엔진에서 사용하는 정보를 보관할 수 있는 보안 모듈 저장소를 포함하며, 하드웨어 보안 칩이 제공하는 모든 기능을 고성능의 중앙처리장치에서 동작하는 소프트웨어 보안 모듈 엔진을 이용하여 하드웨어 수준 보안을 보안 소프트웨어로 제공할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/64 (2013.01)
H04L 9/0877 (2013.01)
H04L 2209/12 (2013.01)

명 세 서

청구범위

청구항 1

컴퓨터에 의해 실행되고, 운영체제의 소프트웨어 보안 설정에 따라 생성된 보호 영역을 포함하는 가상화 기반의 소프트웨어 보안 장치에 있어서,

상기 컴퓨터에서 실행되는 응용프로그램의 명령을 수신하고 상기 명령에 대응하는 결과 데이터를 전송하는 보안 모듈 인터페이스 및 수신된 상기 명령을 암호화하고 사전에 정의된 보안 프로토콜에 따라 상기 명령을 수행하여 상기 결과 데이터를 추출하는 보안 모듈 엔진을 포함하는 소프트웨어 보안 모듈; 및

상기 소프트웨어 보안 모듈에서 사용하는 암호화된 적어도 하나의 비휘발성 보안 모듈 엔진 정보를 저장하는 보안 모듈 저장소를 포함하되,

상기 소프트웨어 보안 모듈은 상기 보호 영역에 위치하는, 가상화 기반 소프트웨어 보안 장치.

청구항 2

청구항 1에 있어서,

상기 소프트웨어 보안 모듈은, 상기 운영체제 및 상기 응용프로그램으로부터 독립성을 보장받거나 또는 허용되지 않은 상기 운영체제의 접근 및 허용되지 않은 상기 응용프로그램의 접근이 제한되는, 가상화 기반 소프트웨어 보안 장치.

청구항 3

청구항 2에 있어서,

상기 보호 영역은, 상기 운영체제의 소프트웨어 보안 설정에 따라 가상화 기술을 이용하여 생성되는, 가상화 기반 소프트웨어 보안 장치.

청구항 4

청구항 2에 있어서,

상기 보안 모듈 인터페이스는, 상기 응용프로그램이 발생시킨 명령 이벤트를 감지하는, 가상화 기반 소프트웨어 보안 장치.

청구항 5

청구항 2에 있어서,

상기 보안 모듈 인터페이스는, 상기 보호 영역에 위치한 상기 소프트웨어 보안 모듈에 미리 정의된 프로토콜에 따라서 외부의 운영체제와 응용프로그램의 명령을 상기 보안 모듈 엔진에 전송하고 상기 명령에 대한 결과를 상기 보안 모듈 엔진으로부터 전달받는, 가상화 기반 소프트웨어 보안 장치.

청구항 6

청구항 5에 있어서,

상기 보안 모듈 엔진은 상기 보안 모듈 인터페이스를 통하여 전달된 외부의 데이터를 프로토콜에 따라 처리하는 실행 엔진을 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 7

청구항 6에 있어서,

상기 보안 모듈 엔진은 보안 기능 엔진을 더 포함하고, 상기 보안 기능 엔진은 상기 실행 엔진이 상기 명령을

수행하는 과정에서 필요로 하는 암호화 엔진, 해시 (Hash) 엔진, 인증기, 변수 생성기, 대칭키/비대칭키 생성기를 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 8

청구항 7에 있어서,

상기 보안 모듈 엔진은 상기 보안 모듈 인터페이스로부터 명령을 전달받고 상기 보안 모듈 엔진의 상태를 표시할 수 있는 엔진 인터페이스를 더 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 9

청구항 8에 있어서,

상기 보안 모듈 엔진은 상기 실행 엔진과 상기 엔진 인터페이스를 연동 제어하여 하드웨어 보안 칩 수준의 보안을 수행하는, 가상화 기반 소프트웨어 보안 장치.

청구항 10

청구항 9에 있어서,

상기 보안 모듈 엔진은 소프트웨어 보안 수행 과정에서 사용된 키 및 소프트웨어 보안 장치에 설정된 사용정책에 대한 정보를 저장하는 휘발성 정보 저장 공간을 더 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 11

청구항 10에 있어서,

상기 보안 모듈 엔진은, 상기 소프트웨어 보안 모듈이 관리하는 상기 비휘발성 보안 모듈 엔진 정보를 임시 저장하는 비휘발성 보안 모듈 엔진 정보 공간을 더 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 12

청구항 11에 있어서,

상기 비휘발성 보안 모듈 엔진 정보는 상기 소프트웨어 보안 모듈이 키 체계(key hierarchy)의 구성에 필요로 하는 루트 키와, 상기 소프트웨어 보안 모듈이 사용하는 인증서 또는 비밀키 정보를 포함하는, 가상화 기반 소프트웨어 보안 장치.

청구항 13

청구항 11에 있어서,

상기 보안 모듈 엔진은, 상기 비휘발성 보안 모듈 엔진 정보 공간에 저장되는 상기 비휘발성 보안 모듈 엔진 정보가 변경될 경우, 변경된 상기 비휘발성 보안 모듈 엔진 정보를 상기 보안 모듈 저장소에 저장하는, 가상화 기반 소프트웨어 보안 장치.

청구항 14

청구항 13에 있어서,

상기 보안 모듈 엔진은 기밀성 보장을 위해 상기 비휘발성 보안 모듈 엔진 정보를 암호화하여 상기 보안 모듈 저장소에 저장하는, 가상화 기반 소프트웨어 보안 장치.

청구항 15

청구항 11 내지 14 중 어느 한 항에 있어서,

상기 보안 모듈 엔진은, 상기 비휘발성 보안 모듈 엔진 정보가 상기 보안 모듈 저장소에 저장될 때, 혹은 상기 보안 모듈 저장소에서 상기 보안 모듈 엔진으로 상기 비휘발성 보안 모듈 엔진 정보가 등록될 때, 상기 소프트웨어 보안 모듈의 무결성 정보를 획득하는, 가상화 기반 소프트웨어 보안 장치.

청구항 16

청구항 15에 있어서,

상기 보안 모듈 엔진은, 상기 무결성 정보를 기반으로 하여 상기 비휘발성 보안 모듈 엔진 정보를 암호화하거나 복호화하는데 사용하는 엔진 정보 암호화 대칭키를 생성하는, 가상화 기반 소프트웨어 보안 장치.

청구항 17

청구항 16에 있어서,

상기 보안 모듈 엔진은, 상기 엔진 정보 암호화 대칭키를 이용하여 안전한 기기에서만 상기 비휘발성 보안 모듈 엔진 정보를 암호화하거나 복호화하는, 가상화 기반 소프트웨어 보안 장치.

청구항 18

청구항 1에 있어서,

상기 보안 모듈 저장소는 상기 보안 모듈 인터페이스에 연결되는 일반 프로그램의 접근을 제한하는, 가상화 기반 소프트웨어 보안 장치.

청구항 19

컴퓨터에서 수행되는 가상화 기반 소프트웨어 보안 방법에 있어서,

상기 컴퓨터 내 운영체제의 소프트웨어 보안 설정에 의해 일반 프로그램과 독립적으로 동작하는 보호 영역을 생성하는 단계;

보안 모듈 엔진 및 상기 보안 모듈 엔진과 상기 일반 프로그램을 연결하는 보안 모듈 인터페이스를 포함하고, 상기 보호 영역에 위치하는 소프트웨어 보안 모듈을 로드(load)하는 단계;

상기 보안 모듈 엔진을 구동하고 상기 보안 모듈 인터페이스를 등록하는 단계;

상기 소프트웨어 보안 모듈의 무결정 정보를 수집하는 단계;

상기 무결정 정보를 기반으로 엔진 정보 암호화 대칭키를 생성하는 단계;

상기 소프트웨어 보안 모듈에 연결되는 보안 모듈 저장소로부터 암호화된 적어도 하나의 비휘발성 보안 모듈 엔진 정보를 획득하는 단계;

상기 암호화된 보안 모듈 엔진의 적어도 하나의 정보를 상기 엔진 정보 암호화 대칭키를 이용하여 복호화하는 단계; 및

상기 복호화된 보안 모듈 엔진 정보를 상기 보안 모듈 엔진에 등록하는 단계를 포함하는, 가상화 기반 소프트웨어 보안 방법.

청구항 20

청구항 19에 있어서,

상기 보안 모듈 엔진 정보를 상기 보안 모듈 엔진에 등록하는 단계 이후에,

상기 보안 모듈 인터페이스에서 명령 이벤트를 감지하는 단계;

상기 보안 모듈 엔진의 상태를 확인하는 단계;

상기 보안 모듈 엔진의 엔진 인터페이스에 명령을 전달하는 단계;

상기 보안 모듈 엔진의 상태를 업데이트하는 단계;

상기 보안 모듈 엔진의 실행 엔진에 명령을 전달하는 단계;

상기 실행 엔진에 의한 명령 수행이 성공인지를 판단하는 단계;

상기 명령 수행이 성공이면, 상기 보안 모듈 엔진의 상태를 업데이트하는 단계; 및

상기 보안 모듈 엔진에서 상기 보안 모듈 인터페이스를 통해 상기 일반 프로그램으로 상기 명령 수행의 결과를 전달하는 단계를 포함하는, 가상화 기반 소프트웨어 보안 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 가상화 기술을 활용한 소프트웨어 보안 기법에 관한 것으로, 더욱 상세하게는, 하드웨어 수준의 보안을 보장해줄 수 있는 가상화 기반 소프트웨어 보안 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 최근 사용자는 PC(Personal Computer) 뿐 아니라 스마트폰(Smart Phone), 태블릿 PC(Tablet PC)와 같은 휴대기기, 스마트워치(Smart Watch)와 같은 웨어러블 기기 등 다양한 기기를 소유하고 사용하고 있다. 각 기기에서 사용자는 많은 데이터를 생성하고 사용하고 있으며, 사용자는 각 기기에서 생성된 사진, 동영상, 문서와 같은 데이터나 혹은 응용프로그램을 자신이 소유한 기기에서 자유롭게 공유하여 사용할 수 있기를 원한다.

[0003] 이러한 기기 간 공유는 클라우드와 같은 네트워크 서비스를 통하여 이루어지고 있다. 사용자 본인뿐 아니라 수많은 사용자와 관리자가 접근할 수 있는 클라우드에 공유를 목적으로 저장된 데이터는 보안을 위하여 기밀성(confidentiality)이 보장되어야 한다.

[0004] 이와 같은 데이터의 기밀성 보장을 위하여 신뢰 플랫폼 모듈(Trusted Platform Module)과 같은 하드웨어 보안 칩이 사용되고 있다. 하드웨어 보안 칩은 데이터의 기밀성 보장을 위해 사용되는 대칭키(symmetric key)를 보안 하드웨어 내부에서만 사용할 수 있는 비대칭키(asymmetric key)를 이용하여 보호할 수 있다. 또한, 비대칭키가 사용될 수 있는 컴퓨팅 환경의 상태나 정책을 정의함으로써 데이터 소유자가 요구하는 환경이 구성되지 않았을 경우, 비대칭키의 사용을 제한할 수 있는 기능을 하드웨어 칩으로 지원함으로써 데이터 기밀성을 보장할 수 있다.

[0005] 그러나 하드웨어 보안 칩은 성능과 확장성에서 문제점을 가지고 있다. 하드웨어 보안 칩은 전력 및 코스트의 제약에 따라 낮은 성능의 암호화 연산 장치를 탑재하고 있다. 이에 따라, 사용자의 기기가 높은 성능을 가지고 있더라도 데이터 보안을 위해 하드웨어 보안 칩을 빈번하게 사용하여야 하는 경우, 하드웨어 보안 칩의 낮은 성능에 의하여 높은 성능 오버헤드를 보이게 된다.

[0006] 또한, 하드웨어의 특성으로 인하여 새롭게 발견된 보안 위협에 따른 보안 프로토콜의 업데이트와 같은 새로운 기술의 추가 및 기존에 하드웨어 보안 칩에 탑재된 기술의 변경이 불가능하다. 따라서, 이러한 하드웨어 보안 칩의 확장성 문제는 지속적으로 증대되고 있는 보안 위협에 대하여 능동적으로 대처하는 것을 어렵게 만든다.

발명의 내용

해결하려는 과제

[0007] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 가상화(Virtualization) 기술을 활용하여 하드웨어 보안 칩과 동일한 수준의 보안을 보장하면서 하드웨어 보안 칩의 성능 및 확장성 문제를 해결할 수 있는 가상화 기반 소프트웨어 보안 방법 및 이를 수행하는 장치를 제공하는데 있다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위한 본 발명의 일 측면에서는, 가상화 기반의 소프트웨어 보안 방법을 수행하는 장치로서, 암호화 및 보안 프로토콜 수행을 위한 보안 모듈 엔진, 응용프로그램에서 소프트웨어 보안 모듈에 명령 및 데이터를 전송하는 보안 모듈 인터페이스, 및 보안 모듈 엔진에서 사용하는 정보를 보관할 수 있는 보안 모듈 저장소를 포함하는, 가상화 기반 소프트웨어 보안 장치가 제공된다.

[0009] 여기에서, 보안 모듈 엔진과 보안 모듈 인터페이스를 포함하는 소프트웨어 보안 모듈은, 같은 기기 내에서 동작중인 운영체제와 응용프로그램으로부터 독립성을 보장받거나 운영체제 및 응용프로그램의 허용되지 않은 접근이 제한되는 중앙처리장치의 보호 영역에 위치할 수 있다.

[0010] 여기에서, 소프트웨어 보안 모듈은, 운영체제 또는 상기 응용프로그램이 실행되는 중앙처리장치의 보호 영역에

서 동작하며, 보호 영역은 가상화 기술을 이용하여 생성될 수 있다.

[0011] 여기에서, 보안 모듈 인터페이스는, 일반 프로그램이 발생시킨 명령 이벤트를 감지할 수 있다.

[0012] 여기에서, 보안 모듈 인터페이스는, 보호 영역에 위치한 소프트웨어 보안 모듈에 미리 정의된 프로토콜에 따라서 외부의 운영체제와 응용프로그램의 명령을 보안 모듈 엔진에 전송하고 명령에 대한 결과를 보안 모듈 엔진으로부터 전달받을 수 있다.

[0013] 여기에서, 보안 모듈 엔진은 보안 모듈 인터페이스를 통하여 전달된 외부의 데이터를 프로토콜에 따라 처리하는 실행 엔진을 포함할 수 있다.

[0014] 여기에서, 보안 모듈 엔진은 보안 기능 엔진을 더 포함할 수 있다. 보안 기능 엔진은 실행 엔진이 명령을 수행하는 과정에서 필요로 하는 암호화 엔진, 해시 (Hash) 엔진, 인증기, 변수 생성기, 대칭키/비대칭키 생성기를 포함할 수 있다.

[0015] 여기에서, 보안 모듈 엔진은 보안 모듈 인터페이스로부터 명령을 전달받고 보안 모듈 엔진의 상태를 표시할 수 있는 엔진 인터페이스를 더 포함할 수 있다.

[0016] 여기에서, 보안 모듈 엔진은 실행 엔진과 엔진 인터페이스를 연동 제어하여 하드웨어 보안 칩 수준의 보안을 수행할 수 있다. 이를 위해, 보안 모듈 엔진은 소프트웨어 보안 수행 과정에서 사용된 키 및 소프트웨어 보안 장치에 설정된 사용정책에 대한 정보를 저장하는 휘발성 정보 저장 공간을 더 포함할 수 있다. 또한, 보안 모듈 엔진은, 소프트웨어 보안 모듈이 관리하는 비휘발성 보안 모듈 엔진 정보를 임시 저장하는 비휘발성 보안 모듈 엔진 정보 공간을 더 포함할 수 있다.

[0017] 여기에서, 비휘발성 보안 모듈 엔진 정보는 소프트웨어 보안 모듈이 키 체계(key hierarchy)의 구성에 필요로 하는 루트 키와, 소프트웨어 보안 모듈이 사용하는 인증서 또는 비밀키 정보를 포함할 수 있다.

[0018] 여기에서, 보안 모듈 엔진은 사전 정의에 따라 비휘발성 보안 모듈 엔진 정보 공간에 저장되는 비휘발성 보안 모듈 엔진 정보의 변경 시 해당 비휘발성 보안 모듈 엔진 정보를 보안 모듈 저장소에 저장할 수 있다.

[0019] 여기에서, 보안 모듈 엔진은 기밀성 보장을 위해 비휘발성 보안 모듈 엔진 정보를 암호화하여 보안 모듈 저장소에 저장할 수 있다.

[0020] 여기에서, 보안 모듈 엔진은, 비휘발성 보안 모듈 엔진 정보가 보안 모듈 저장소에 저장될 때, 혹은 보안 모듈 저장소에서 보안 모듈 엔진으로 비휘발성 보안 모듈 엔진 정보가 등록될 때, 소프트웨어 보안 모듈의 무결성 정보를 획득할 수 있다.

[0021] 여기에서, 보안 모듈 엔진은, 무결성 정보를 기반으로 하여 비휘발성 보안 모듈 엔진 정보를 암호화하거나 복호화하는데 사용하는 엔진 정보 암호화 대칭키를 생성할 수 있다.

[0022] 여기에서, 보안 모듈 엔진은, 엔진 정보 암호화 대칭키를 이용하여 안전한 기기 또는 미리 지정된 기기에서만 비휘발성 보안 모듈 엔진 정보를 암호화하거나 복호화할 수 있다.

[0023] 여기에서, 보안 모듈 저장소는 보안 모듈 인터페이스에 연결되는 일반 프로그램의 접근을 제한하도록 구현된다.

[0024] 본 발명의 다른 측면에 의하면, 컴퓨터에서 수행되는 가상화 기반 소프트웨어 보안 방법으로서, 컴퓨터의 가상화 기술을 이용하여 일반 프로그램과 독립적으로 동작하는 보호 영역을 생성하는 단계; 보안 모듈 엔진과 일반 프로그램을 연결하는 보안 모듈 인터페이스 및 보안 모듈 엔진을 포함하는 소프트웨어 보안 모듈을 로드(load)하는 단계; 보안 모듈 엔진을 구동하고 보안 모듈 인터페이스를 등록하는 단계; 소프트웨어 보안 모듈의 무결정 정보를 수집하는 단계; 무결성 정보를 기반으로 엔진 정보 암호화 대칭키를 생성하는 단계; 소프트웨어 보안 모듈에 연결되는 보안 모듈 저장소로부터 암호화된 보안 모듈 엔진 정보를 획득하는 단계; 암호화된 보안 모듈 엔진 정보를 엔진 정보 암호화 대칭키를 이용하여 복호화하는 단계; 및 복호화된 보안 모듈 엔진 정보를 등록하는 단계를 포함하는, 가상화 기반 소프트웨어 보안 방법을 제공한다.

[0025] 여기에서, 가상화 기반 소프트웨어 보안 방법은, 상기 보안 모듈 엔진 정보를 등록하는 단계 이후에, 보안 모듈 인터페이스에서 명령 이벤트를 감지하는 단계; 보안 모듈 엔진의 상태를 확인하는 단계; 보안 모듈 엔진의 엔진 인터페이스에 명령을 전달하는 단계; 보안 모듈 엔진의 상태를 업데이트하는 단계; 보안 모듈 엔진의 실행 엔진에 명령을 전달하는 단계; 실행 엔진에 의한 명령 수행이 성공인지를 판단하는 단계; 명령 수행의 성공시, 보안 모듈 엔진의 상태를 업데이트하는 단계; 및 보안 모듈 엔진에서 보안 모듈 인터페이스를 통해 일반 프로그램으

로 명령 수행의 결과를 전달하는 단계를 더 포함할 수 있다.

발명의 효과

[0026] 상술한 바와 같은 본 발명의 일 실시예에 따른 하드웨어 수준 보안을 보장하는 가상화 기반 소프트웨어 보안 방법이나 이를 수행하는 장치를 이용할 경우에는, 하드웨어 보안 칩이 제공하는 모든 기능을 고성능의 중앙처리장치에서 동작하는 소프트웨어 보안 모듈 엔진을 이용하여 하드웨어 수준 보안을 보안 소프트웨어로 제공할 수 있다. 그리고 보안 모듈 인터페이스를 통해서 하드웨어 보안 칩과 동일하게 생성된 보안 결과를 일반 프로그램이 획득하도록 할 수 있다.

[0027] 또한, 본 실시예에 의하면, 가상화 기술을 통해 독립된 보호 영역에서 동작하여 기존 운영체제와 응용프로그램의 접근을 제한하고, 하드웨어 보안 칩과 동일한 인터페이스와 프로토콜을 통해서 명령을 소프트웨어 보안 모듈에 전송할 수 있도록 하며, 보안 모듈 저장소에 저장되는 소프트웨어 보안 모듈 엔진 정보는 소프트웨어 보안 모듈이 안전하게 구성된 환경에서만 사용 가능하도록 하여, 하드웨어 보안 칩과 동일한 수준의 기밀성을 유지하면서 하드웨어 보안 칩의 확장성 문제를 해결할 수 있다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 일실시예에 따른 가상화 기반 소프트웨어 보안 장치를 개략적으로 나타낸 블록도이다.

도 2는 도 1의 가상화 기반 소프트웨어 보안 장치의 작동 과정을 설명하기 위한 흐름도이다.

도 3은 도 1의 가상화 기반 소프트웨어 보안 장치의 보안 명령 및 결과 전송 동작을 설명하기 위한 흐름도이다.

도 4는 비교예에 따른 하드웨어 보안 칩 중 하나인 하드웨어 기반 신뢰 플랫폼 모듈에서 대칭키를 관리하는 방법을 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0030] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0031] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 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 아니하는 것으로 이해되어야 할 것이다.

[0032] 본 명세서에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다", "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0033] 본 명세서에서 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함하여 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 나타내는 것으로 보아야 한다. 그리고 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 나타내는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0035] 도 1은 본 발명의 일 실시예에 따른 가상화 기반 소프트웨어 보안 장치를 개략적으로 나타낸 블록도이다.

[0036] 도 1을 참조하면, 본 실시예에 따른 가상화 기반 소프트웨어 보안 장치(100)는 하드웨어 수준 보안을 보장하며 가상화 기술을 활용하는 소프트웨어 보안 방법을 수행하는 장치로서, 소프트웨어 보안 모듈(101) 및 보안 모듈 저장소(104)를 포함한다.

[0037] 소프트웨어 보안 모듈(101)은 보안 모듈 인터페이스(102) 및 보안 모듈 엔진(103)을 포함하고, 보안 모듈 저장소(104)와 연결된다. 소프트웨어 보안 모듈(101)은 가상화 기술을 이용하여 일반 프로그램(200)으로부터 독립된 보호 영역에서 동작한다. 일반 프로그램(200)는 소프트웨어 보안 모듈(101)과 달리 일반 영역에서 동작한다. 일반 프로그램(200)은 부트로더(bootloader), 운영체제, 응용프로그램 등을 포함할 수 있다. 응용프로그램은 가상 머신, 신뢰 컴퓨팅 그룹(Trusted Computing Gourp, TCG) 소프트웨어 스택, 신뢰 컴퓨팅 모듈(TPM) 드라이버 등을 포함할 수 있다.

[0038] 가상화 기반 소프트웨어 보안 장치(100)의 각 구성요소를 좀 더 상세히 설명하면 다음과 같다.

[0039] 보안 모듈 인터페이스(102)는 일반 프로그램(200)에서 소프트웨어 보안 모듈(101)에서 정의한 프로토콜에 따라 명령을 전달받고 받은 명령을 보안 모듈 엔진(103)으로 전달하며, 보안 모듈 엔진(103)으로부터 생성된 결과를 정해진 프로토콜에 따라 일반 프로그램(200)으로 전달하는 기능을 수행한다.

[0040] 보안 모듈 인터페이스(102)는 일반 프로그램(200)으로부터 발생한 인터럽트(interrupt), MMIO(memory mapped input/output) 혹은 미리 정의된 다른 이벤트를 감지하여 일반 프로그램(200)으로부터 명령을 전달받을 수 있다.

[0041] 전술한 보안 모듈 인터페이스(102)는 가상 인터럽트를 위한 제1 수단과 이벤트 감지를 위한 제2 수단을 포함할 수 있다. 제1 수단은 가상 신뢰 컴퓨팅 그룹 인터럽트 핸들러(Virtual Trusted Computing Group Interrupt Handler)를 포함할 수 있고, 제2 수단은 신뢰 컴퓨팅 그룹 MMIO 핸들러(TCG MMIO Handler)를 포함할 수 있다.

[0042] 일반 프로그램(200)의 명령을 감지하는 데 있어서 퍼스널 컴퓨터(PC)의 신뢰 플랫폼 모듈을 예로 들면, 특정 인터럽트 벡터인 인터럽트 1AH를 통해 발생하는 명령과 0xFED40000에서 0xFED44FFF 메모리 주소까지 MMIO를 통해 발생하는 명령을 감지하고 처리할 수 있다. 이외의 다른 하드웨어 보안 칩의 경우, 각 하드웨어 보안 칩의 표준 프로토콜에 따라 신뢰 플랫폼을 구성할 수 있다.

[0043] 보안 모듈 엔진(103)은 엔진 인터페이스(105), 실행 엔진(106), 보안 기능 엔진(107), 휘발성 정보 저장 공간(108), 및 비휘발성 보안 모듈 엔진 정보 공간(109)을 포함한다.

[0044] 엔진 인터페이스(105)는 보안 모듈 인터페이스(102)로부터 명령을 받거나 보안 모듈 인터페이스(102)로 결과, 예컨대 명령 수행 결과를 전달하는 기능을 담당한다. 또한, 엔진 인터페이스(105)는 보안 모듈 엔진(103)의 상태를 표기하여 일반 프로그램(200)이 명령을 내리거나 결과를 받아오는데 참조할 수 있는 기능을 포함할 수 있다. 이러한 엔진 인터페이스(105)는 신뢰 컴퓨팅 그룹 바이오스 평션 인터페이스(TCG BIOS Function Interface)를 포함할 수 있다.

[0045] 실행 엔진(106)은 미리 정의된 프로토콜에 따라 전송된 명령을 해석하고 해석된 명령에 따라 결과를 생성하는 기능을 수행한다.

[0046] 보안 기능 엔진(107)은 실행 엔진(106)이 명령을 수행하는 과정에서 필요로 하는 암호화 엔진, 해시 엔진, 인증기, 키 생성기 등을 포함한다.

[0047] 휘발성 정보 저장 공간(108)은 소프트웨어 보안 모듈(101)에서 관리하는 휘발성 정보를 저장한다. 휘발성 정보는 보안 수행 과정에서 사용된 키, 현재 소프트웨어 보안 모듈에 설정된 사용정책 등의 정보를 포함할 수 있다.

[0048] 비휘발성 보안 모듈 엔진 정보 공간(109)은 소프트웨어 보안 모듈(101)이 동작함에 있어서 지속적으로 관리하고 갱신될 필요가 있는 비휘발성 정보를 임시 저장하는 공간(예컨대, 임시 저장 공간)으로서 키 체계(key hierarchy)를 구성함에 있어 필요로 하는 루트 키(root key), 소프트웨어 보안 모듈(101)에서 사용하는 인증서, 비밀키 등의 정보를 저장할 수 있다.

[0049] 전술한 휘발성 정보 저장 공간(108) 및/또는 비휘발성 보안 모듈 엔진 정보 공간(109)은 가상화 기반 소프트웨어 신뢰 컴퓨팅 모듈 레지스터(Virtualization-based Software Trusted Computing Module Registers: VS-TCM Registers) 또는 여기에 저장되는 정보를 포함할 수 있다.

[0050] 보안 모듈 저장소(104)는 소프트웨어 보안 모듈(101)이 동작할 때 필요로 하는 비휘발성 보안 모듈 엔진 정보를 저장한다. 보안 모듈 저장소(104)는 소프트웨어 보안 모듈(101)이 동작 중일 때 일반 프로그램(200)의 접근이 차단되도록 설정 또는 설계될 수 있다. 비휘발성 보안 모듈 엔진 정보가 변경되면, 보안 모듈 엔진(103)에 의하여 갱신된 정보가 보안 모듈 저장소(104)에 저장될 수 있다. 이때, 보안 모듈 저장소의 TCG 메모리 영역 내 특정 영역에 저장되는 정보와 TCM 레지스터 내 특정 영역에 저장되는 정보가 서로 대응되도록 시스템의 운영체제는 어느 하나에서 읽고 나머지 다른 하나에 기록하거나 그 역으로 데이터 읽기 및 쓰기 동작을 수행할 수 있다.

[0051] 또한, 보안 모듈 저장소(104)에 있어서, 비휘발성 보안 모듈 엔진 정보가 보안 모듈 저장소(104)에 저장될 때 보안 모듈 엔진(103)은 소프트웨어 보안 모듈(101)의 무결성(integrity) 정보를 기반으로 엔진 정보 암호화 대칭키를 생성할 수 있다. 일례로, 가상화 기반 소트프웨어 보안 장치(10)는 하드웨어 정보와 VS-TCM 무결성 측정값(integrity measurement value)을 이용하여 PIK(Permanent Information Key)를 생성하고, PIK를 이용하여 정보 또는 데이터를 암호화 및/또는 복호화할 수 있다. 이와 같이, 보안 모듈 엔진(103)은 엔진 정보 암호화 대칭키를 사용하여 암호화 및/또는 복호화를 수행함으로써 가상화 기반 소프트웨어 보안 장치(100)에서 기밀성을 보장할 수 있다. 복호화된 보안 모듈 엔진 정보는 비휘발성 보안 모듈 엔진 정보로서 보안 모듈 엔진에 등록될 수 있다.

[0052] 도 2는 본 발명의 일 실시예에 따른 가상화 기반 소프트웨어 보안 장치의 작동 과정을 설명하기 위한 흐름도이다.

[0053] 도 2를 참조하면, 본 실시예에 따른 가상화 기반 소프트웨어 보안 장치는 컴퓨터의 운영체제상의 소프트웨어 보안 설정에 따라 소프트웨어 보안 모듈이 구동되기 전에 가상화 기술을 이용하여 일반 프로그램과 독립적으로 동작할 수 있는 보호 영역을 생성한다(S100).

[0054] 보호 영역이 생성된 이후 보호 영역으로 소프트웨어 보안 모듈을 로드한다(S101). 소프트웨어 보안 모듈은 보안 모듈 엔진과 보안 모듈 인터페이스를 포함한다. 상기의 두 단계들(S100 및 S101)에 의하면, 가상화 기반 소프트웨어 보안 장치는 넓은 의미에서 컴퓨터의 운영체제의 적어도 일부를 포함할 수 있다.

[0055] 보호 영역에서 동작하는 소프트웨어 보안 모듈은 보안 모듈 엔진을 구동한다(S102). 그리고 소프트웨어 보안 모듈은 보안 모듈 인터페이스를 시스템에 등록한다(S103).

[0056] 등록된 보안 모듈 인터페이스를 이용하면, 일반 프로그램은 소프트웨어 보안 모듈에 명령을 내리고 결과를 받을 수 있다. 이와 관련하여 퍼스널 컴퓨터(PC)의 신뢰 플랫폼 모듈을 예로 들면, 신뢰 플랫폼 모듈은 인터럽트 벡터의 하나인 인터럽트 1AH와 0xFED40000 내지 0xFED44FFF의 메모리 영역까지 발생하는 이벤트를 감지할 수 있도록 컴퓨터 또는 컴퓨터의 보안 시스템에 등록되는데, 보안 모듈 인터페이스도 이와 유사하게 시스템에 등록될 수 있다.

[0057] 소프트웨어 보안 모듈 또는 보안 모듈 엔진은 소프트웨어 보안 모듈의 보안 동작에 필요한 구성요소를 모두 구동한 후, 구동된 구성요소의 무결성 정보를 수집한다(S104).

[0058] 그리고 수집한 무결성 정보를 기반으로 하여 엔진 정보 암호화 대칭키를 생성한다(S105). 엔진 정보 암호화 대칭키를 PIK를 포함할 수 있으나, 이에 한정되지는 않는다. 무결성 정보가 훼손되지 않았다면, 비휘발성 엔진 정보를 암호화할 때 사용한 암호화 대칭키와 동일한 대칭키가 생성된다.

[0059] 다음, 보안 모듈 저장소로부터 암호화된 비휘발성 보안 모듈 엔진 정보를 획득한다(S106). 보안 모듈 저장소는 보호 영역을 통해서만 접근이 가능하다. 용어 "비휘발성"은 시스템의 전원이 차단되어도 저장된 정보를 유지하는 기능을 지칭하는 것으로서, 이러한 용어가 전원 차단시 저장된 정보를 유지하는 휘발성 저장 수단이나 이러한 수단에 상응하는 기능을 수행하는 구성부를 배제하고자 하는 것은 아니다.

[0060] 무결성 정보를 기반으로 생성된 엔진 정보 암호화 대칭키를 이용하여 암호화 된 비휘발성 보안 모듈 엔진 정보를 복호화한다(S107).

[0061] 소프트웨어 보안 모듈이 정상적으로 동작하여 무결성 정보가 훼손되지 않았다면, 동일한 대칭키가 생성되었기 때문에 복호화를 정상적으로 수행할 수 있으며, 그 경우 소프트웨어 보안 모듈 또는 보안 모듈 엔진은 복호화된 비휘발성 보안 모듈 엔진 정보를 보안 모듈 엔진에 등록한다(S108).

[0062] 비휘발성 보안 모듈 엔진 정보가 등록되면, 일반 프로그램으로부터 보안 명령을 전달받고 결과를 생성할 준비가 완료되었기 때문에 소프트웨어 보안 모듈은 준비 동작을 완료한다(S109).

[0063] 한편, 상기의 단계(S107)에서 복호화가 실패하면, 즉 소프트웨어 보안 모듈이 비정상적으로 동작하거나 악의적인 목적으로 훼손되었을 경우, 무결성 정보가 훼손되기 때문에 상기의 단계(S105)에서 다른 대칭키가 생성되며, 이에 따라 복호화를 정상적으로 수행할 수 없다. 그 경우, 보안 모듈 엔진에 비휘발성 보안 모듈 엔진 정보를 등록할 수 없기 때문에 현재의 소프트웨어 보안 모듈의 동작은 종료된다(S110).

[0064] 도 3은 본 발명의 일 실시예에 따른 가상화 기반 소프트웨어 보안 장치의 보안 명령 및 결과 전송 과정을 설명하기 위한 흐름도이다.

[0065] 도 3을 참조하면, 본 실시예에 따른 가상화 기반 소프트웨어 보안 장치는, 먼저 컴퓨터의 일반 프로그램에서 보안 명령 이벤트가 발생할 때(S200) 이를 감지한다. 즉, 보안 모듈 인터페이스는 일반 프로그램에서 발생시킨 보안 명령 이벤트를 감지하고 명령 내용을 수집한다(S201).

[0066] 다음, 보안 모듈 인터페이스는 엔진 인터페이스를 통해서 현재 보안 모듈 엔진의 상태를 확인한다(S202).

[0067] 확인 결과, 보안 모듈 엔진이 명령을 수행할 수 있는 상태(엔진 상태 정상)이면, 보안 모듈 인터페이스는 수집한 보안 명령을 엔진 인터페이스에 전달한다(S203).

[0068] 다음, 엔진 인터페이스는 보안 명령을 실행 엔진에 전달하기 전에 현재 상태를 업데이트하여 명령이 현재 수행중임을 보안 모듈 인터페이스 등에 알린다(S204).

[0069] 상태 업데이트를 완료한 후, 엔진 인터페이스는 전달받은 보안 명령을 실행 엔진에 전달한다(S205).

[0070] 실행 엔진은 보안 명령을 정해진 프로토콜에 따라 수행한다(S206). 실행 엔진이 보안 명령을 정상적으로 수행하였다면, 보안 모듈 엔진은 엔진 상태를 업데이트하여 결과가 생성되었음을 보안 모듈 인터페이스 등에 알린다(S207).

[0071] 다음, 보안 모듈 엔진은 보안 모듈 인터페이스에 생성된 결과를 전달한다(S208). 일반 프로그램은 보안 모듈 인터페이스를 통해서 생성된 결과를 받을 수 있다.

[0072] 한편, 상기의 확인 결과, 현재 보안 모듈 엔진이 다른 명령을 수행 중(엔진 상태 비정상에 대응함)이거나, 상기 단계(S206)의 명령 또는 명령어 수행에 실패하였다면, 보안 모듈 인터페이스에 명령 수행 실패 결과를 전달한다(S210). 일반 프로그램은 보안 모듈 인터페이스를 통해 보안 명령의 수행이 실패하였음을 알 수 있다.

[0073] 전술한 가상화 기반 소프트웨어 보안 장치의 소프트웨어 보안 모듈은 컴퓨터의 중앙처리장치인 마이크로프로세서 또는 프로세서에 탑재될 수 있다.

[0074] 프로세서는 하나 이상의 코어, 캐시 메모리, 메모리 인터페이스 및 주변장치 인터페이스를 포함할 수 있다. 프로세서가 멀티 코어 구조를 구비하는 경우, 멀티 코어(multi-core)는 두 개 이상의 독립 코어를 단일 집적 회로로 이루어진 하나의 패키지로 통합한 것을 지칭한다. 단일 코어는 중앙 처리 장치를 지칭할 수 있다. 중앙처리장치(CPU)는 MCU(micro control unit)와 주변 장치(외부 확장 장치를 위한 집적회로)가 함께 배치되는 SOC(system on chip)로 구현될 수 있으나, 이에 한정되지는 않는다. 코어는 처리할 명령어를 저장하는 레지스터(register), 비교, 판단, 연산을 담당하는 산술논리연산장치(arithmetic logical unit, ALU), 명령어의 해석과 실행을 위해 CPU를 내부적으로 제어하는 컨트롤 유닛(control unit), 버스 인터페이스 등을 구비할 수 있다.

[0075] 또한, 프로세서는 하나 이상의 데이터 프로세서, 이미지 프로세서, 또는 코덱(CODEC)을 포함할 수 있으나, 이에 한정되지는 않는다. 데이터 프로세서, 이미지 프로세서 또는 코덱은 별도로 구성될 수도 있다. 또한, 프로세서는 주변장치 인터페이스와 메모리 인터페이스를 구비할 수 있고, 그 경우 주변장치 인터페이스는 프로세서와 입출력 시스템 및 여러 다른 주변 장치를 연결하고, 메모리 인터페이스는 프로세서와 메모리를 연결할 수 있다.

[0076] 전술한 구성의 프로세서는 여러 가지의 소프트웨어 프로그램을 실행하여 가상화 기반 소프트웨어 보안 방법을 수행하기 위하여 데이터 입력, 데이터 처리 및 데이터 출력을 수행할 수 있다. 또한, 프로세서는 메모리에 저장되어 있는 특정한 소프트웨어 모듈(명령어 세트)을 실행하여 해당 모듈에 대응하는 특정한 여러 가지의 기능을 수행할 수 있다. 모듈은 명령어들의 집합으로서 명령어 세트(instruction set) 또는 프로그램으로 표현될 수 있다.

[0077] 메모리는 하나 이상의 자기 디스크 저장 장치와 같은 고속 랜덤 액세스 메모리 및/또는 비휘발성 메모리, 하나 이상의 광 저장 장치 및/또는 플래시 메모리를 포함할 수 있다.

[0078] 메모리는 소프트웨어, 프로그램, 명령어 집합 또는 이들의 조합을 저장할 수 있다. 본 실시예에서 메모리는 암

호화된 가상화 기반 소프트웨어 신뢰 플랫폼 모듈 영구 정보, 암호화된 가상화 기반 소프트웨어 신뢰 컴퓨팅 그룹 정보, 보안 모듈 엔진 정보, 소프트웨어 보안 모듈 정보, 가상화 기반 보안 장치 정보 등을 저장할 수 있다.

[0079] 운영 체제는 예컨대 MS WINDOWS, LINUX, 다윈(Darwin), RTXC, UNIX, OS X, iOS, 맥 OS, VxWorks, 구글 OS, 안드로이드(android), 바다(삼성 OS), 플랜 9 등과 같은 내장 운영 체제를 포함하고, 모바일 장치 등을 포함하는 사용자 단말의 시스템 작동(system operation)을 제어하는 여러 가지의 구성요소를 구비할 수 있다. 전술한 운영 체제는 여러 가지의 하드웨어(장치)와 소프트웨어 구성요소(모듈) 사이의 통신을 수행하는 기능도 구비할 수 있으나, 이에 한정되지는 않는다.

[0080] 가상화 기반 소프트웨이 보안 방법을 구현하는 기능들의 제어를 제외하고 일반적인 시스템 작동이나 기능의 제어를 위하여 소프트웨어 보안 장치 또는 컴퓨터는 예를 들어 메모리 관리, 저장 하드웨어 제어, 전력 제어, 네트워크 접속 제어 등을 위한 하나 이상의 수단이나 이러한 수단에 상응하는 기능을 수행하는 구성부를 포함할 수 있다.

[0081] 네트워크는, 예를 들어, GSM(Global System for Mobile Communication) 네트워크, EDGE(Enhanced Data GSM Environment) 네트워크, CDMA(Code Division Multiple Access) 네트워크, W-CDMA(W-Code Division Multiple Access) 네트워크, LTE(Long Term Evolution) 네트워크, OFDMA(Orthogonal Frequency Division Multiple Access) 네트워크, WiMax 네트워크, Wi-Fi(Wireless Fidelity) 네트워크, Bluetooth 네트워크 등을 포함할 수 있으나, 이에 한정되지는 않는다.

[0082] 한편, 본 실시예에 있어서, 가상화 기반 소프트웨어 보안 방법의 구성요소들은 컴퓨터 장치에 탑재되는 기능 블록 또는 모듈일 수 있으나, 이에 한정되지 않는다. 전술한 구성요소들은 이들이 수행하는 일련의 기능을 구현하기 위한 소프트웨어 형태로 컴퓨터 판독 가능 매체(기록매체)에 저장되거나 혹은 캐리어 형태로 원격지에 전송되어 다양한 컴퓨터 장치에서 동작하도록 구현될 수 있다. 여기서 컴퓨터 판독 가능 매체는 네트워크를 통해 연결되는 복수의 컴퓨터 장치나 클라우드 시스템을 포함할 수 있고, 복수의 컴퓨터 장치나 클라우드 시스템 중 적어도 하나 이상은 메모리 시스템에 본 실시예의 가상화 기반 소프트웨어 보안 방법을 수행하기 위한 프로그램이나 소스 코드 등을 저장할 수 있다.

[0083] 즉, 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하는 형태로 구현될 수 있다. 컴퓨터 판독 가능 매체에 기록되는 프로그램은 본 발명을 위해 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것을 포함할 수 있다.

[0084] 또한, 컴퓨터 판독 가능 매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 하드웨어 장치는 본 실시예의 소음 제거 방법을 수행하기 위해 적어도 하나의 소프트웨어 모듈로 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0085] 도 4는 비교예에 따른 하드웨어 보안 칩 중 하나인 신뢰 플랫폼 모듈에서 데이터 암호화에 사용된 대칭키를 관리하는 방법을 설명하기 위한 블록도이다.

[0086] 도 4를 참조하면, 비교예에 따른 신뢰 플랫폼 모듈(10)은 내부에 비대칭 비밀키(11)와 비대칭 공개키(12)를 가지고 있다. 비대칭 비밀키(11)는 신뢰 플랫폼 모듈(10) 내부에만 존재하며 비밀키 생성 시 미리 정의된 비밀키 사용정책(13)에 따라 사용 여부가 결정된다. 그리고 비대칭 공개키(12)는 신뢰 플랫폼 모듈(10) 외부로 전달되어서 소정의 대칭키를 암호화하여 암호화된 대칭키(14)를 생성하는데 사용된다.

[0087] 암호화된 대칭키(14)를 사용하기 위해서는 복호화에 필요한 비대칭 비밀키(11)를 가지고 있는 신뢰 플랫폼 모듈(10)에 암호화된 대칭키를 전달해야 한다.

[0088] 암호화된 대칭키가 전달되면, 신뢰 플랫폼 모듈(10)은 비대칭 비밀키(11)를 사용하기에 앞서서 현재 신뢰 플랫폼 모듈(10)에 설정되어 있는 사용정책(15)이 비대칭 비밀키(11)의 사용정책에 부합되는지를 검사한다.

[0089] 사용정책에 부합된다면, 신뢰 플랫폼 모듈(10)은 비대칭 비밀키(11)를 이용하여 복호화된 대칭키(16)를 생성하여 외부로 전달한다. 만약, 사용정책에 부합되지 않는다면 신뢰 플랫폼 모듈(10)은 비밀키의 사용을 금지하고 대칭키를 복호화 하지 않는다.

[0090] 이와 같이, 비교예에 따른 하드웨어 기반 신뢰 플랫폼 모듈이나 이러한 하드웨어 기반 신뢰 플랫폼 모듈을 포함

하는 하드웨어 보안 칩은 성능과 확장성에서의 문제, 하드웨어 보안 칩의 확장성 문제 등의 문제점을 가진다.

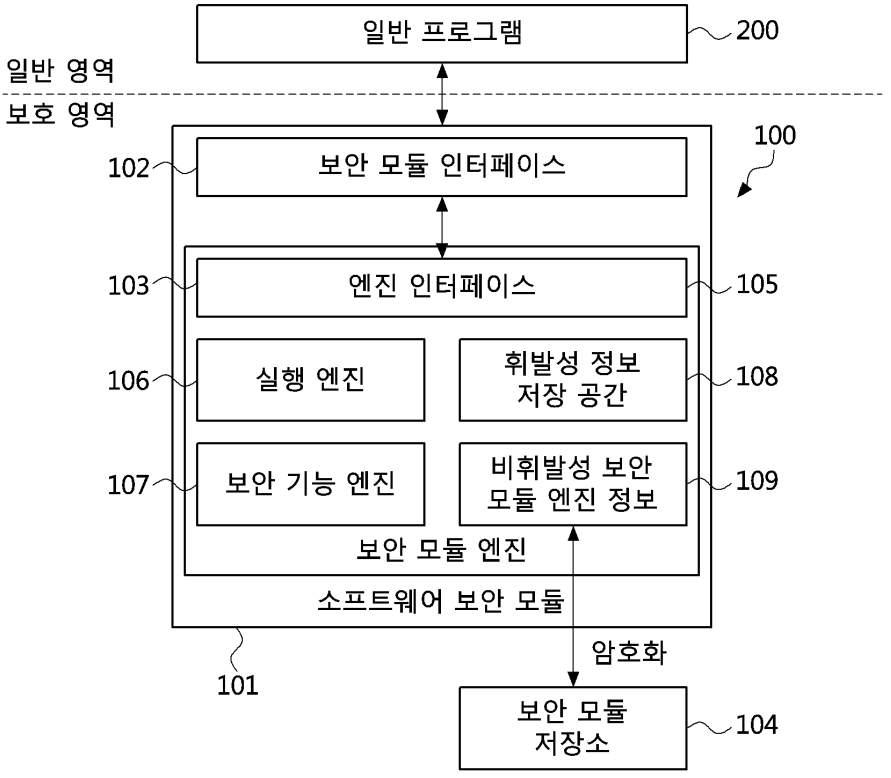
[0091] 한편, 도 1 내지 도 3을 참조하여 앞서 설명한 본 실시예의 소프트웨어 보안 방법이나 가상화 기반 소프트웨어 보안 장치는 소프트웨어 기반 신뢰 플랫폼 모듈을 포함하는 것으로서 사용자의 기기가 높은 성능을 가지고 있는 만큼 성능 오버헤드를 미연에 제거하면서 빠르고 신속하게 하드웨어 보안 수준의 데이터 보안을 소프트웨어적으로 수행할 수 있다. 또한, 하드웨어의 특성으로 인하여 새롭게 발견된 보안 위협에 따른 보안 프로토콜의 업데이트를 실질적으로 실시간 수행할 수 있다. 즉, 새로운 보안 기술의 추가 및 기탑재된 보안 기술의 변경을 용이하게 수행할 수 있고, 그에 의해 하드웨어 보안 칩의 확장성 문제와 같은 단점을 제거하면서 지속적으로 증대되는 보안 위협에 대하여 능동적으로 대처할 수 있다.

[0092] 상기에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

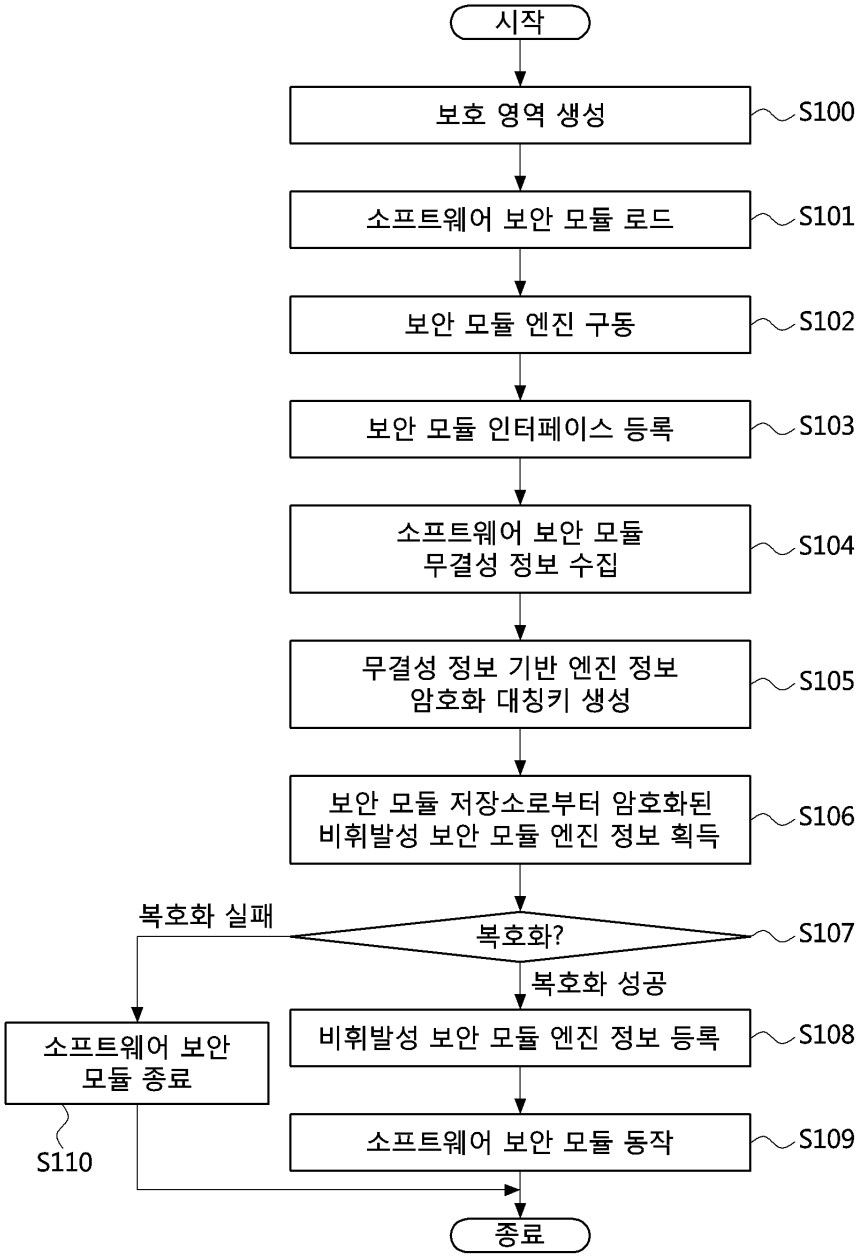
부호의 설명

도면

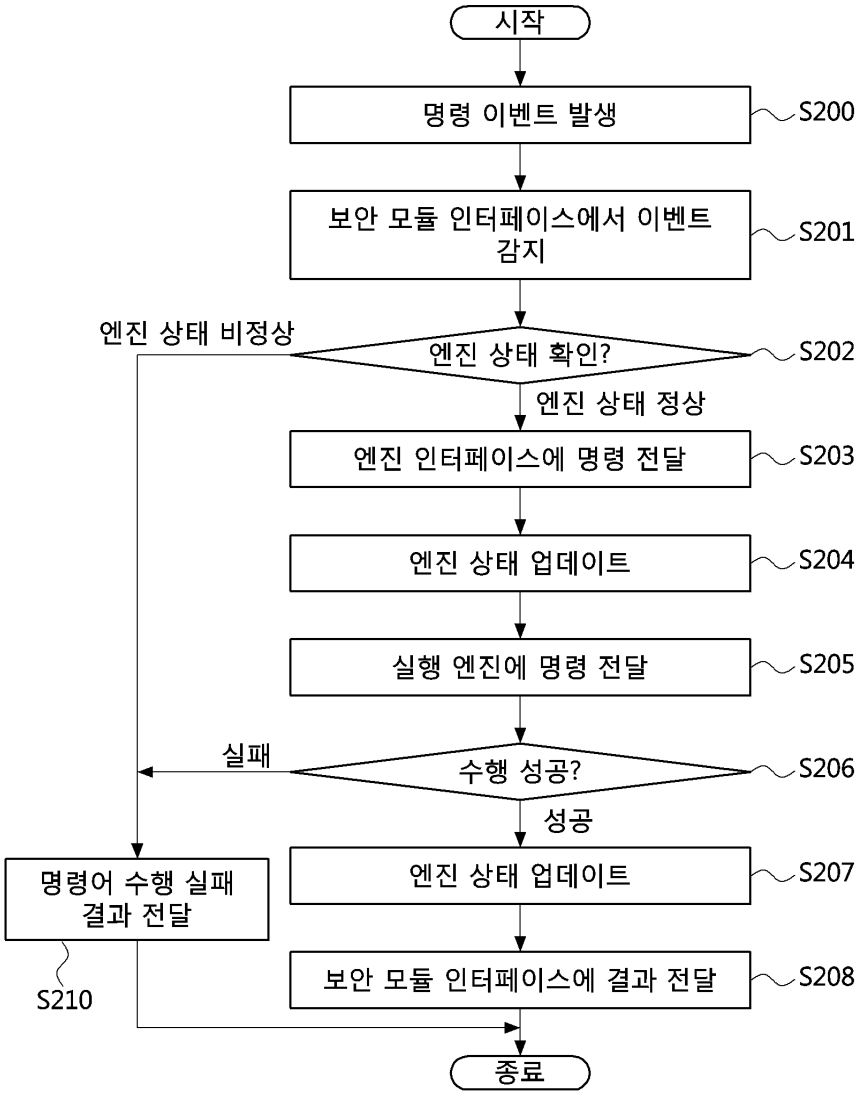
도면1



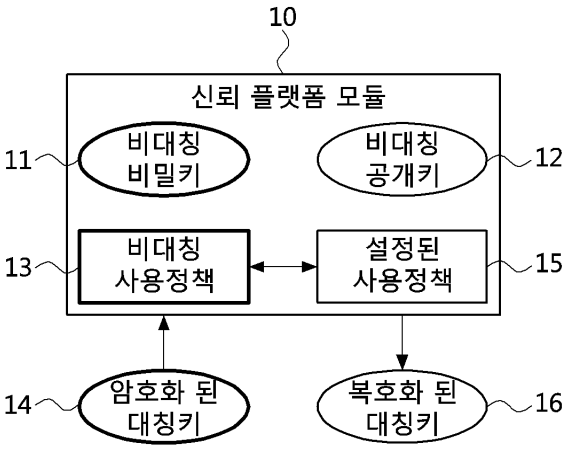
도면2


시작
보호 영역 생성
S100
소프트웨어 보안 모듈 로드
S101
보안 모듈 엔진 구동
S102
보안 모듈 인터페이스 등록
S103
소프트웨어 보안 모듈
무결성 정보 수집
S104
무결성 정보 기반 엔진 정보
암호화 대칭키 생성
S105
보안 모듈 저장소로부터 암호화된
비휘발성 보안 모듈 엔진 정보 획득
S106
복호화 실패
복호화?
S107
복호화 성공
소프트웨어 보안
모듈 종료
S110
비휘발성 보안 모듈 엔진 정보 등록
S108
소프트웨어 보안 모듈 동작
S109
종료

도면3



도면4



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 제19항

【변경전】

상기 무결성 정보

【변경후】

상기 무결정 정보