(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0051813
(43) 공개일자 2015년05월13일

(51) 국제특허분류(Int. Cl.)
*G06F 21/00* (2006.01) *G06F 9/06* (2006.01)
(21) 출원번호 10-2013-0133792
(22) 출원일자 2013년11월05일
심사청구일자 없음

(71) 출원인
**한국전자통신연구원**
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
**김영호**
서울특별시 성동구 뚝섬로 310 한진아파트 105동 2102호
**김정녀**
대전광역시 유성구 문지로 22 우성아파트 101동 103호
**조현숙**
대전광역시 유성구 관평1로 12 대덕테크노밸리7단지 금성백조아파트 702동 601호
(74) 대리인
**특허법인이지**

전체 청구항 수 : 총 10 항

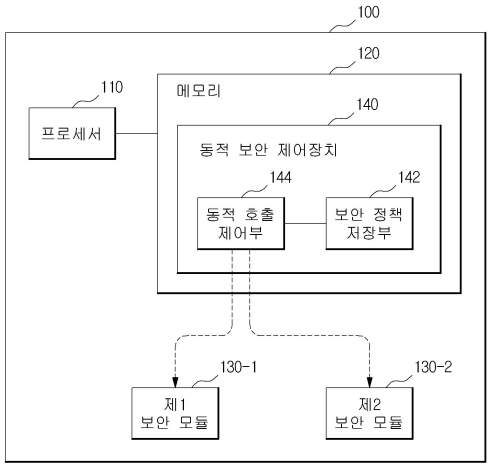
(54) 발명의 명칭 **복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하는 장치 및 방법**

## (57) 요 약

본 발명은 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하는 장치 및 방법에 관한 것이다.

본 발명에 따른 동적 보안 제어 장치는, 컴퓨팅 장치의 상태 및 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하는 정책 저장부와, 응용 프로그램으로부터 보안 함수가 호출됨을 인식하고 상기 저장된 보안 정책에 따라 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하는 동적 호출 제어부를 포함한다.

*대 표 도* - 도1



# 명 세 서

## 청구범위

### 청구항 1

복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하기 위한 동적 보안 제어 장치로서,

상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하는 보안 정책 저장부와,

상기 응용 프로그램으로부터 보안 함수가 호출됨을 인식하고 상기 설정된 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하는 동적 호출 제어부

를 포함하는 동적 보안 제어 장치.

### 청구항 2

제1항에 있어서, 상기 보안 정책 저장부에 저장된 보안 정책은 응용 프로그램 각각에 대한 보안 레벨 정보를 포함하는 동적 보안 제어 장치.

### 청구항 3

제1항에 있어서, 상기 보안 정책은 외부 관리 서버를 통해 관리자에 의해 원격으로 변경 가능한 동적 보안 제어 장치.

### 청구항 4

제1항에 있어서, 상기 복수의 보안 모듈은 소프트웨어로 구현된 보안 라이브러리 및 하드웨어 보안 모듈을 포함하는 동적 보안 제어 장치.

### 청구항 5

제1항에 있어서, 상기 응용 프로그램이 상기 보안 라이브러리에서 제공하는 보안 함수를 호출하더라도 상기 동적 호출 제어부의 결정에 따라 상기 하드웨어 보안 모듈에서 제공하는 보안 함수가 호출될 수 있는 동적 보안 제어 장치.

### 청구항 6

복수의 보안 모듈,

프로세서 및 상기 프로세서에 의해 실행되는 명령어를 포함하는 메모리를 포함하고, 상기 명령어는 상기 프로세서에 의해 실행될 때 상기 프로세서로 하여금,

상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하고,

상기 응용 프로그램으로부터 보안 함수가 호출되는 것에 응답하여 상기 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하도록 하는 컴퓨팅 장치.

### 청구항 7

복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하기 위한 동적 보안 제어 방법으로서,

상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하는 단계와,

상기 응용 프로그램으로부터 보안 함수가 호출됨을 인식하는 단계와,

상기 보안 함수 호출에 응답하여, 상기 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하

는 보안 함수를 호출할지 판단하는 단계

를 포함하는 동적 보안 제어 방법.

**청구항 8**

제7항에 있어서, 상기 보안 정책은 응용 프로그램 각각에 대한 보안 레벨 정보를 포함하는 동적 보안 제어 방법.

**청구항 9**

제7항에 있어서, 상기 보안 정책은 외부 관리 서버를 통해 관리자에 의해 원격으로 변경가능한 동적 보안 제어 방법.

**청구항 10**

제7항에 있어서, 상기 복수의 보안 모듈은 소프트웨어로 구현된 보안 라이브러리 및 하드웨어 보안 모듈을 포함하는 동적 보안 제어 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하는 장치 및 방법에 관한 것으로서, 구체적으로는 컴퓨팅 장치내에 하드웨어/소프트웨어 방식으로 구현된 복수의 보안모듈에서 제공하는 보안 함수를 보안 정책에 따라 동적으로 호출할 수 있도록 하기 위한 장치 및 방법에 관한 것이다.

### *배 경 기 술*

[0002] 현재, 모바일 단말, 데스크톱, 노트북 등의 다양한 컴퓨팅 장치들은 보안을 위해 하드웨어칩로 구현된 보안 모듈 또는 가상화 기반의 소프트웨어로 구현된 보안 모듈을 이용하고 있다. 응용 프로그램에서 이러한 하드웨어 보안 모듈 또는 가상화 기반의 소프트웨어 보안 모듈을 이용하고자 하는 경우에는 해당 보안 모듈과의 연계를 위해 별도의 소프트웨어 API(Application Programming Interface)를 이용한 프로그래밍이 필요하다.

[0003] 따라서, 이미 구현된 응용 프로그램은 새로운 보안 모듈을 채용하기 위해서는 재프로그래밍되어야 하므로 새로운 보안 모듈을 적용하는데 한계점을 갖는다.

[0004] 이에, 기존 응용 프로그램들도 재프로그래밍 과정 없이 해당 장치에 새롭게 적용되는 보안 모듈을 이용할 수 있도록 하는 방안이 요구된다. 더욱이, 응용 프로그램 개발 당시 개발자가 해당 프로그램이 실행될 단말의 보안 환경(즉, 하드웨어 또는 가상화 기반의 소프트웨어 보안 모듈 장착 여부)에 상관없이 프로그램을 작성하더라도 해당 프로그램이 단말에서 제공하는 보안 모듈을 용이하게 이용할 수 있도록 하는 방안이 요구된다.

## *발명의 내용*

### *해결하려는 과제*

[0005] 따라서, 본 발명은 프로그램 개발자가 프로그램이 실제로 실행될 컴퓨팅 장치 환경에 상관없이 프로그램을 개발하더라도 해당 장치에 장착된 보안 모듈에서 제공하는 높은 보안성을 제공 받을 수 있도록 하는 데 그 목적이 있다.

[0006] 특히, 기존의 소프트웨어/하드웨어 보안 모듈을 이용하여 보안 기능을 제공하는 컴퓨팅 장치에 새로운 하드웨어 기반의 보안 모듈이 장착되는 경우에 기존 프로그램의 재작성없이 컴퓨팅 장치 환경과 보안 정책(접근제어 정책)에 따라 프로그램의 보안을 동적으로 제어하는 데 그 목적이 있다.

### *과제의 해결 수단*

[0007] 본 발명의 일실시예에 따르면, 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하기 위한 동적 보안 제어 장치가 제공된다. 상기 장치는, 상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응

용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하는 보안 정책 저장부와, 상기 응용 프로그램으로부터 보안 함수가 호출됨을 인식하고 상기 설정된 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하는 동적 호출 제어부를 포함할 수 있다.

[0008] 본 발명의 일실시예에 따르면, 동적 보안 제어가 가능한 컴퓨팅 장치가 제공된다. 상기 컴퓨팅 장치는, 복수의 보안 모듈, 프로세서 및 상기 프로세서에 의해 실행되는 명령어를 포함하는 메모리를 포함하고, 상기 명령어는 상기 프로세서에 의해 실행될 때 상기 프로세서로 하여금, 상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하고, 상기 응용 프로그램으로부터 보안 함수가 호출되는 것에 응답하여 상기 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하도록 할 수 있다.

[0009] 본 발명의 일실시예에 따르면, 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하기 위한 동적 보안 제어 방법이 제공된다. 상기 방법은, 상기 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장하는 단계와, 상기 응용 프로그램으로부터 보안 함수가 호출됨을 인식하는 단계와, 상기 보안 함수 호출에 응답하여, 상기 보안 정책에 따라 상기 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단하는 단계를 포함할 수 있다.

## *발명의 효과*

[0010] 본 발명의 일실시예에 따르면, 컴퓨팅 장치의 보안성을 높이기 위해 하드웨어 또는 가상화 기반의 보안 모듈을 장착하는 경우 이미 작성된 응용 프로그램도 소스코드 변경 없이 해당 하드웨어 또는 가상화 기반의 보안 모듈을 호출할 수 있게 된다. 따라서, 기존에 개발된 프로그램들과의 호환성을 제공하면서 동시에 새롭게 추가된 보안 모듈의 활용을 통해 원래 의도한 보안성을 높여줄 수 있다.

## *도면의 간단한 설명*

[0011] 도 1은 본 발명의 일실시예에 따른 보안 제어 장치가 적용되는 컴퓨팅 장치의 구조를 개략적으로 도시한 도면이다.

도 2는 본 발명의 일실시예에 따라 응용 프로그램의 키생성함수(keyGen()) 동적 호출 과정을 개념적으로 도시한 도면이다.

도 3은 본 발명의 일실시예에 따라 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하는 방법을 도시한 흐름도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0012] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 이를 상세한 설명을 통해 상세히 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.

[0013] 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0014] 또한, 본 명세서 및 청구항에서 사용되는 단수 표현은, 달리 언급하지 않는 한 일반적으로 "하나 이상"을 의미하는 것으로 해석되어야 한다.

[0015] 또한, 본 명세서에서 사용되는 용어들중 "모듈", "부", "인터페이스"등은 일반적으로 컴퓨터 관련 객체를 의미하며, 예를 들어, 하드웨어, 소프트웨어 및 이들의 조합을 의미할 수 있다.

[0016] 도 1은 본 발명의 일실시예에 따른 보안 제어 장치가 적용되는 컴퓨팅 장치의 구조를 개략적으로 도시한 도면이다.

[0017] 도 1에 도시된 바와 같이, 컴퓨팅 장치(100)는 프로세서(110) 및 메모리(120)에 부가하여 제1 및 제2 보안 모듈(130-1, 130-2)을 구비하고, 메모리(120) 내에 본 발명의 일실시예에 따라 보안 모듈들(130-1, 130-2)을 선택적으로 이용하여 컴퓨팅 장치(100)의 보안을 동적으로 제어할 수 있는 동적 보안 제어 장치(140)가 명령어 형태로

저장될 수 있다.

[0018] 상기 도면에는 보안 모듈이 2개만 도시되어 있으나, 이는 단지 설명의 편의를 위한 것으로서, 본 발명이 보안 모듈의 개수에 제한되는 것은 아니다.

[0019] 일실시예에서, 제 1 보안 모듈(130-1)은 가상화 기반의 소프트웨어 보안 모듈로서 보안 함수 라이브러리 형태로 구현된 모듈이며, 제2 보안 모듈(130-2)은 하드웨어칩으로 구현된 하드웨어 보안 모듈일 수 있다. 일반적으로, 하드웨어칩으로 구현된 제2 보안 모듈(130-2)이 소프트웨어로 구현된 제 1 보안 모듈(130-1)에 비해 더 높은 보안성을 컴퓨팅 장치에 제공해줄 수 있다.

[0020] 일실시예에서, 동적 보안 제어 장치(140)는 보안 정책 저장부(142) 및 동적 호출 제어부(144)를 포함할 수 있다.

[0021] 보안 정책 저장부(142)는 컴퓨팅 장치(100)의 상태 및/또는 컴퓨팅 장치(100)에서 실행되는 응용 프로그램 특성 중 적어도 하나에 따라 동적으로 설정되는 보안 정책을 저장한다. 일실시예에서, 보안 정책은 컴퓨팅 장치(100)의 사용자의 의해 직접 설정될 수 있다. 또는, 해당 장치를 관리하는 관리자가 외부 관리 서버를 통해 보안 정책을 원격으로 설정 및/또는 변경할 수 있다. 이에 따라, 컴퓨팅 장치를 관리하는 기업 입장에서 다양한 보안 정책에 따라 컴퓨팅 장치의 보안을 동적으로 제어할 수 있게 된다.

[0022] 보안 정책은 컴퓨팅 장치(100)의 상태 및 상기 장치(100)에서 실행되는 특정 응용 프로그램에 대해 어느 정도의 보안 레벨을 제공할지 정하는 정보로서, 이에 따라 어느 보안 모듈의 보안 함수가 호출될 지 판단될 수 있다. 일실시예에서, 컴퓨팅 장치(100)의 상태(예, 회사 내부 사용/회사 외부 사용/신뢰된 단말/신뢰 안되는 단말) 및/또는 응용 프로그램 특성(예, 높은 보안성이 요구되는 업무용 프로그램/보통 수준의 업무용 프로그램/개인 용도 프로그램 등)에 따라 상이하게 설정되는 보안 레벨을 포함할 수 있다. 예를 들어, 회사 외부에서 높은 보안성이 요구되는 업무용 프로그램을 컴퓨팅 장치(100)에서 실행시킬 때에는 가장 높은 수준의 보안 레벨을 설정하고, 반면 개인 용도의 프로그램을 실행시킬 때에는 소프트웨어 보안 모듈만으로도 충분한 보안성이 제공될 수 있기 때문에 상대적으로 낮은 보안 레벨을 설정할 수 있다.

[0023] 동적 호출 제어부(144)는 특정 응용 프로그램으로부터 보안 함수가 호출됨을 인식하고, 보안 정책 저장부(142)에 의해 저장된 보안 정책에 따라 복수의 보안 모듈(131-1, 131-2) 중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단할 수 있다. 동적 호출 제어부(144)는 다양한 응용 프로그램들에 동일한 인터페이스를 제공하는 라이브러리 형태로 구현될 수 있으며, 복수의 보안 모듈에 의해 제공되는 보안 함수중 어느 하나로 동적으로 분기할 수 있는 함수 포인터 형태로 구현가능하식으로 보안 함수의 호출을 구현할 수 있음은 본 기술분야의 당업자에게 자명하다.

[0024] 도 2를 참조하여, 본 발명의 일실시예에 따라 응용 프로그램인 키생성함수(KeyGen())를 호출하는 경우에 실제 함수가 호출되는 과정을 설명하고자 한다.

[0025] 도 2에 도시된 바와 같이, 응용 프로그램(210)이 키생성함수(KeyGen())를 호출한다고 가정한다. 응용 프로그램(210)은 신규 보안 모듈(240)이 컴퓨팅 장치에 장착되기 이전에 개발된 프로그램으로서 기존의 보안 라이브러리(240)에서 제공하는 키생성함수(KeyGen())를 호출하도록 프로그래밍되어 있다. 그러나, 본 발명의 일실시예에 따르면, 기존의 보안 라이브러리(240)에서 제공하는 키생성함수(KeyGen()) 및 신규 보안 모듈(250)에서 제공하는 키생성함수(KeyGen())중 실제 어느 함수가 호출될지 여부는 보안 정책 저장부(230)에 저장된 보안정책에 근거하여 동적 호출 제어부(220)에 의해 결정될 것이다. 가령, 해당 응용 프로그램에 대한 보안 정책이 보안 정책 저장부(230)에 하위 보안 레벨(low security)로 저장된 경우에는, 키생성 함수 호출 시 기존 보안 라이브러리(240) 내부에 있는 keyGen() 함수가 호출될 수 있다. 그러나, 보안 정책 저장부(230)에 의해 상위 보안 레벨(high security)로 저장된 경우에는 신규 보안 모듈(250) 내부의 keyGen() 함수가 호출되어 보다 안전한 방식으로 보안키를 생성할 수 있게 된다.

[0026] 이와 같이, 본 발명의 일실시예에 따르면, 응용 프로그램에서 실제로 호출되는 보안 함수는 개발자에 의해 개발 당시에 결정되는 것이 아니라, 보안 정책의 동적 설정을 통해 컴퓨팅 장치 사용자 또는 해당 장치를 원격 관리하는 관리자(서버)에 의해 결정될 것이다. 따라서, 응용 프로그램 개발자 입장에서는 앞으로 등장할 신규 보안 모듈에 상관없이 프로그램을 개발할 수 있으며, 신규 보안 모듈이 단말에 적용되더라도 기존 프로그램 수정없이 호환성을 유지할 수 있다.

[0027] 본 발명에 따른 보안 제어가 실제 서비스 환경에 적용시킬 수 있는 또다른 사례로서, 최근 BYOD(Bring Your Own Device)와 같이 모바일 단말을 회사 업무 용도 및 개인 용도도 사용하는 경우의 보안 제어이다. 가령, 사

용자가 모바일 단말을 회사 내에서 업무 용도로 이용할 경우에는 응용 프로그램에서 업무용 데이터를 저장하기 위해 저장 함수(store())를 호출할 때, 높은 보안 레벨로 설정된 보안 정책에 따라 모바일 단말에 장착된 하드웨어 보안 모듈에 업무용 데이터가 저장되도록 할 수 있다. 한편, 사용자가 업무를 마치고 퇴근하여 회사 밖에서 동일한 응용 프로그램을 이용하여 개인 데이터를 저장하는 경우에는 높은 보안성이 요구하지 않기 때문에 낮게 설정된 보안 레벨에 따라 기존 보안 라이브러리를 사용하여 업무용 데이터와 분리된 형태로 개인 데이터가 저장되도록 제어할 수 있다. 응용 프로그램 개발자에게는 항상 동일한 인터페이스를 통해 프로그램을 개발할 수 있는 장점을 제공하고, 컴퓨팅 장치 사용자 또는 컴퓨팅 장치를 관리하는 기업 입장에서는 다양한 보안 정책에 따라 컴퓨팅 장치를 안전하게 유지할 수 있는 방법을 제공한다.

[0028] 도 3은 본 발명의 일실시예에 따라 복수의 보안 모듈을 구비하는 컴퓨팅 장치의 보안을 동적으로 제어하는 방법을 도시한 흐름도이다.

[0029] 단계(S310)에서, 컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 동적으로 설정되는 보안 정책이 저장된다.

[0030] 일실시예에서, 보안 정책은 컴퓨팅 장치(100)에서 실행되는 응용 프로그램 각각에 대한 보안 레벨 정보를 포함할 수 있다.

[0031] 일실시예에서, 보안 정책은 컴퓨팅 장치의 사용자에 의해 직접 설정되거나, 외부 관리 서버를 통해 관리자에 의해 원격으로 설정 및/또는 변경가능하다.

[0032] 단계(S320)에서, 응용 프로그램으로부터 보안 함수가 호출됨을 인식한다.

[0033] 단계(S330)에서, 응용 프로그램의 보안 함수 호출에 응답하여, 상기 보안 정책에 따라 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단한다.

[0034] 일실시예에서, 복수의 보안 모듈은 소프트웨어로 구현된 보안 라이브러리 및 하드웨어 보안 모듈을 포함할 수 있다.

[0035] 본 발명의 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

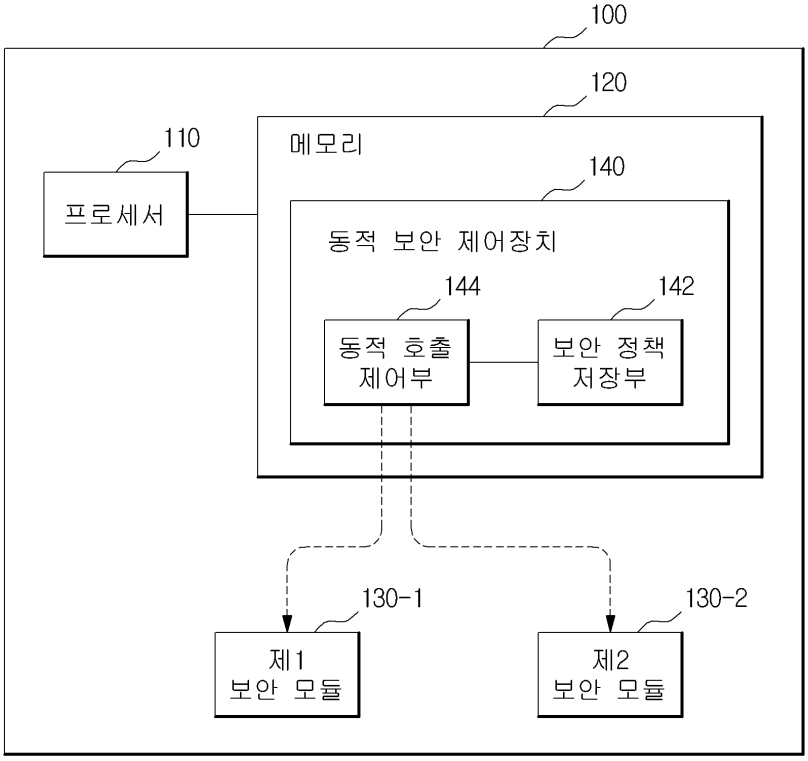
[0036] 컴퓨터 판독 가능 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media) 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 또한 상술한 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0037] 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

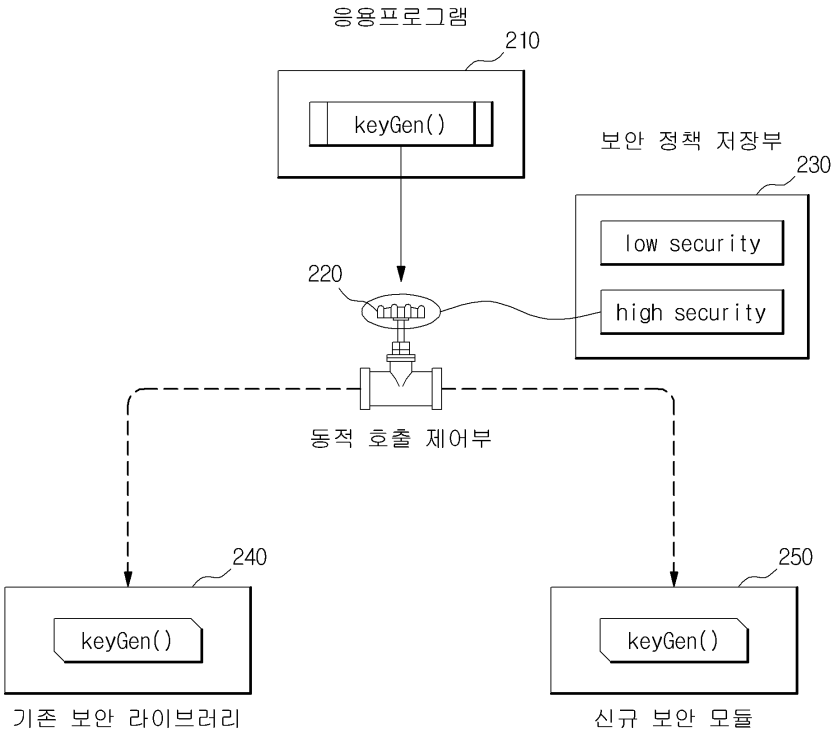
[0038] 이제까지 본 발명에 대하여 그 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

## 도면

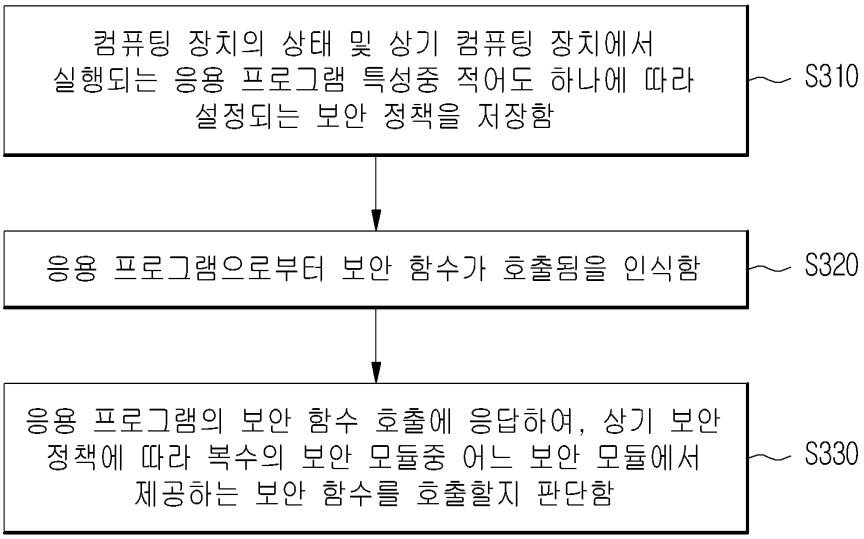
### 도면1


100
120
메모리
110
프로세서
140
동적 보안 제어장치
144
142
동적 호출
제어부
보안 정책
저장부
130-1
130-2
제1
보안 모듈
제2
보안 모듈

도면2


응용프로그램
210
keyGen()
보안 정책 저장부
230
low security
high security
220
동적 호출 제어부
240
keyGen()
기존 보안 라이브러리
250
keyGen()
신규 보안 모듈

도면3


컴퓨팅 장치의 상태 및 상기 컴퓨팅 장치에서 실행되는 응용 프로그램 특성중 적어도 하나에 따라 설정되는 보안 정책을 저장함
S310
응용 프로그램으로부터 보안 함수가 호출됨을 인식함
S320
응용 프로그램의 보안 함수 호출에 응답하여, 상기 보안 정책에 따라 복수의 보안 모듈중 어느 보안 모듈에서 제공하는 보안 함수를 호출할지 판단함
S330