



(19) 대한민국특허청(KR)  
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0134082  
(43) 공개일자 2017년12월06일

|                                                                                                                 |                                                            |
|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| (51) 국제특허분류(Int. Cl.)<br>G06F 21/57 (2013.01) G06F 17/30 (2006.01)<br>G06F 21/50 (2013.01) G06F 9/445 (2017.01) | (71) 출원인<br>충남대학교산학협력단<br>대전광역시 유성구 대학로 99 (궁동, 충남대학교)     |
| (52) CPC특허분류<br>G06F 21/57 (2013.01)<br>G06F 17/30144 (2013.01)                                                 | (72) 발명자<br>류재철<br>대전광역시 유성구 어은로 57, 132동 801호(어은동, 한빛아파트) |
| (21) 출원번호 10-2016-0065825                                                                                       | (74) 대리인<br>홍성욱, 심경식                                       |
| (22) 출원일자 2016년05월27일<br>심사청구일자 없음                                                                              |                                                            |

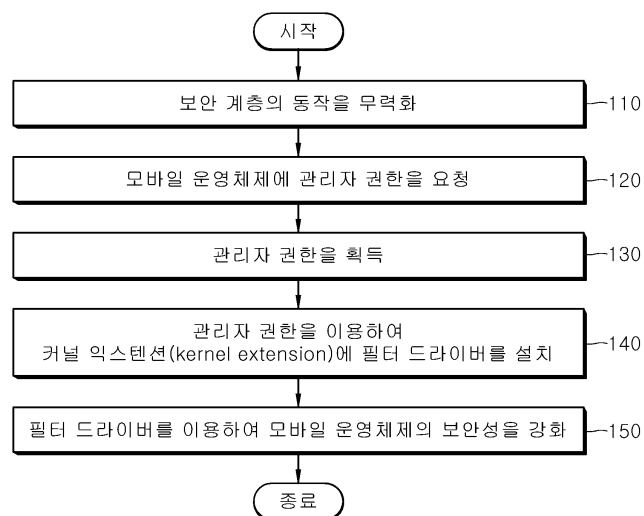
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 모바일 운영체제 보안성 강화 방법 및 장치

### (57) 요약

본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 방법은 모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시키는 단계; 상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청하여 관리자 권한을 획득하는 단계; 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버를 설치하는 단계; 및 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

**G06F 21/50** (2013.01)

**G06F 8/61** (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF2014M3C4A7030648

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 원천기술개발사업

연구과제명 미래 컴퓨팅 환경을 위한 암호와 기반 SW의 안전성 분석및 대응기술 연구

기 여 율 1/1

주관기관 충남대학교 산학협력단

연구기간 2014.07.01 ~ 2019.06.30

---

## 명세서

### 청구범위

#### 청구항 1

모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시키는 단계;  
 상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청하여 관리자 권한을 획득하는 단계;  
 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버를 설치하는 단계; 및  
 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화하는 단계  
 를 포함하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 방법.

#### 청구항 2

제1항에 있어서,  
 상기 커널 익스텐션은  
 외부 장치와의 네트워크 연결을 제어하는 네트워크 인터페이스이고,  
 상기 필터 드라이버는  
 상기 커널 익스텐션을 통해 상기 어플리케이션의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제의 보안성을 강화하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 방법.

#### 청구항 3

제1항에 있어서,  
 상기 커널 익스텐션은  
 상기 무력화된 보안 계층과 상기 모바일 운영체제 사이의 계층에 위치하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 방법.

#### 청구항 4

제1항에 있어서,  
 상기 어플리케이션이 특정 파일을 처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일에 기록하는 단계  
 를 더 포함하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 방법.

#### 청구항 5

제4항에 있어서,  
 상기 모니터링용 이벤트 파일은  
 상기 모바일 운영체제가 아이오에스(IOS)인 경우, '/dev/fsevents'인 것을 특징으로 하는 모바일 운영체제 보안

성 강화 방법.

#### 청구항 6

제4항에 있어서,

상기 모니터링용 이벤트 파일은

상기 모바일 운영체제와 하드웨어 사이의 계층에 위치하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 방법.

#### 청구항 7

모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시키는 보안 계층 무력화부;

상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청하여 관리자 권한을 획득하는 관리자 권한 획득부;

상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버를 설치하는 필터 드라이버 설치부; 및

상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화하는 보안성 강화부

를 포함하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

#### 청구항 8

제7항에 있어서,

상기 커널 익스텐션은

외부 장치와의 네트워크 연결을 제어하는 네트워크 인터페이스이고,

상기 필터 드라이버는

상기 커널 익스텐션을 통해 상기 어플리케이션의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제의 보안성을 강화하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

#### 청구항 9

제7항에 있어서,

상기 커널 익스텐션은

상기 무력화된 보안 계층과 상기 모바일 운영체제 사이의 계층에 위치하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

#### 청구항 10

제7항에 있어서,

상기 어플리케이션이 특정 파일을 처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일에 기록하는 로그 기록부

를 더 포함하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

## 청구항 11

제10항에 있어서,

상기 모니터링용 이벤트 파일은

상기 모바일 운영체제가 아이오에스(IOS)인 경우, '/dev/fsevents'인 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

## 청구항 12

제10항에 있어서,

상기 모니터링용 이벤트 파일은

상기 모바일 운영체제와 하드웨어 사이의 계층에 위치하는 것을 특징으로 하는 모바일 운영체제 보안성 강화 장치.

## 발명의 설명

### 기술 분야

[0001] 본 발명의 실시예들은 보안 기술에 관한 것으로서, 더욱 상세하게는 운영체제 보안 해제를 통해 모바일 운영체제의 보안성을 강화하는 방법 및 장치에 관한 것이다.

### 배경 기술

[0003] 스마트폰은 현대인의 필수품이 되었으며, 스마트폰의 기반이 되는 플랫폼은 IOS, 안드로이드, 윈도우폰, 심비안 등 여러 가지가 있다. 그 중에서 IOS와 안드로이드 기반의 스마트폰은 한국뿐 아니라 전세계 스마트폰의 가장 많은 비율을 차지하고 있으며, 특히 안드로이드 기반의 스마트폰은 점차 그 비율이 증가하고 있다.

[0004] 안드로이드 점유율이 급증하는 이유 중의 하나는 개방성이라고 볼 수 있으나, 이것은 공격자들의 주요 대상이 되도록 하는 요인으로도 작용한다. 안드로이드는 리눅스와 자바에 기반하고 있으며 다양한 보안 메커니즘을 제공하고 있지만, 개방된 소스들은 공격자들로 하여금 비교적 쉽게 취약점을 파악하게 하고 그로 인해 다양한 악성코드들이 급증하고 있다.

[0005] 이와 같이 시간이 지날수록 스마트폰 등의 IT 장치에 대한 악의적이 공격이 증가하고 있기에, IT 장치의 핵심인 운영체제는 강화된 보안/보호 기술을 적용하고 있다.

[0006] 하지만, 강화된 보안/보호 기술은 악의적인 공격도 차단하지만, 보안 프로그램이 운영체제를 제어하는 데에도 영향을 끼치고 있다. 또한, 운영체제의 보안/보호 기술에 문제점이 발생할 경우, 운영체제의 업데이트보다 보안 프로그램의 업데이트가 더 빠르기 때문에 운영체제의 보안/보호 기능을 해제하고 보안 프로그램의 기능을 강화할 수 있는 기술이 필요하다.

[0007] 관련 선행기술로는 일본 공개특허공보 특개2015-532756(발명의 명칭: 악의적 소프트웨어에 의한 공격으로부터 운영체제를 보호하는 방법, 공개일자: 2015.11.12)가 있다.

## 발명의 내용

### 해결하려는 과제

[0009] 본 발명의 일 실시예는 운영체제의 보안/보호 기술에 문제점이 발생할 경우 운영체제의 업데이트보다 보안 프로

그럼의 업데이트가 더 빠르기 때문에, 운영체제의 보안/보호 기능을 해제하고 보안 프로그램의 기능을 강화할 수 있도록 하는 모바일 운영체제 보안성 강화 방법 및 장치를 제공한다.

[0011] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

### 과제의 해결 수단

[0013] 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 방법은 모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시키는 단계; 상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청하여 관리자 권한을 획득하는 단계; 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버를 설치하는 단계; 및 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화하는 단계를 포함한다.

[0014] 상기 커널 익스텐션은 외부 장치와의 네트워크 연결을 제어하는 네트워크 인터페이스이고, 상기 필터 드라이버는 상기 커널 익스텐션을 통해 상기 어플리케이션의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제의 보안성을 강화할 수 있다.

[0015] 상기 커널 익스텐션은 상기 무력화된 보안 계층과 상기 모바일 운영체제 사이의 계층에 위치할 수 있다.

[0016] 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 방법은 상기 어플리케이션이 특정 파일을 처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일에 기록하는 단계를 더 포함할 수 있다.

[0017] 상기 모니터링용 이벤트 파일은 상기 모바일 운영체제가 아이오에스(IOS)인 경우, '/dev/fsevents'일 수 있다.

[0018] 상기 모니터링용 이벤트 파일은 상기 모바일 운영체제와 하드웨어 사이의 계층에 위치할 수 있다.

[0019] 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치는 모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시키는 보안 계층 무력화부; 상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청하여 관리자 권한을 획득하는 관리자 권한 획득부; 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버를 설치하는 필터 드라이버 설치부; 및 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화하는 보안성 강화부를 포함한다.

[0020] 상기 커널 익스텐션은 외부 장치와의 네트워크 연결을 제어하는 네트워크 인터페이스이고, 상기 필터 드라이버는 상기 커널 익스텐션을 통해 상기 어플리케이션의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제의 보안성을 강화할 수 있다.

[0021] 상기 커널 익스텐션은 상기 무력화된 보안 계층과 상기 모바일 운영체제 사이의 계층에 위치할 수 있다.

[0022] 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치는 상기 어플리케이션이 특정 파일을 처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일에 기록하는 로그 기록부를 더 포함할 수 있다.

[0023] 상기 모니터링용 이벤트 파일은 상기 모바일 운영체제가 아이오에스(IOS)인 경우, '/dev/fsevents'일 수 있다.

[0024] 상기 모니터링용 이벤트 파일은 상기 모바일 운영체제와 하드웨어 사이의 계층에 위치할 수 있다.

[0026] 기타 실시예들의 구체적인 사항들은 상세한 설명 및 첨부 도면들에 포함되어 있다.

### 발명의 효과

[0028] 본 발명의 일 실시예에 따르면, 운영체제의 보안/보호 기술에 문제점이 발생할 경우 운영체제의 업데이트보다

보안 프로그램의 업데이트가 더 빠르기 때문에, 운영체제의 보안/보호 기능을 해제하고 보안 프로그램의 기능을 강화할 수 있다.

### 도면의 간단한 설명

도 1은 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 방법을 설명하기 위해 도시한 흐름도이다.

도 2는 모바일 운영체제 보안성 강화를 위한 계층 구조를 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치를 설명하기 위해 도시한 블록도이다.

도 4 및 도 5는 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치의 동작을 설명하기 위해 도시한 도면이다.

### 발명을 실시하기 위한 구체적인 내용

본 발명의 이점 및/또는 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성요소를 지칭한다.

기존 PC는 관리자 권한의 요청 없이 바로 운영체제에 어플리케이션의 설치가 가능하지만, IOS나 안드로이드와 같은 운영체제(모바일 운영체제)에서는 관리자 권한을 허용하고 있지 않기 때문에 어플리케이션의 설치가 제한되며, 다만 관리자 권한을 요청하여 관리자 권한을 확인하여 IOS의 경우 탈옥이 되었는지, 안드로이드의 경우 루팅이 되었는지를 탐지하고 있다.

즉, IOS나 안드로이드와 같은 운영체제에서는 관리자 권한을 요청하여 획득할 수 없기 때문에 관리자 권한을 이용한 어플리케이션의 설치가 제한된다. 따라서, 본 발명의 일 실시예에서는 관리자 권한을 요청하여 획득하고, 이렇게 획득한 관리자 권한을 이용하여 필터 드라이버를 설치함으로써 운영체제의 보안성 강화를 위한 보안 솔루션을 제공하고자 한다.

이를 위해, 본 발명의 일 실시예에서는 운영체제에 존재하는 다양한 보안/보호 기술 중에서 보안 프로그램의 기능을 제한하는 주요 보안/보호 기술인 샌드박스, 코드사인, 관리자 권한 등의 3가지 보안/보호 기능을 해제하여 운영체제의 드라이버 기능을 추가할 수 있으며, 이를 통해 강화된 보안 프로그램의 개발이 가능하게 한다.

운영체제 안에서 보안 프로그램이 작동 가능한 환경일 경우, 보안 프로그램이 강화된 기능을 가질 수 있게 된다. 데스크톱(PC) 운영체제의 경우, 마이크로소프트사의 윈도우 10부터 보안/보호 기술에 의해 보안 프로그램(백신 등)이 모니터링 및 제어 가능한 기술에 한계가 발생하며, 모바일 운영체제의 경우 관리자 권한 자체를 사용하지 못하도록 하였기에 데스크톱 환경에서와 같은 소프트웨어 드라이버를 설치하는 것이 불가능하였다.

따라서, 본 발명의 일 실시예에서는 소프트웨어 드라이버의 설치가 제한된 모바일 운영체제에서 보안 프로그램의 설치 및 실행이 가능하도록 함으로써 보안성을 강화시킬 수 있는 방법을 제공한다.

이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 상세히 설명하기로 한다.

도 1은 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 방법을 설명하기 위해 도시한 흐름도이고, 도 2는 모바일 운영체제 보안성 강화를 위한 계층 구조를 도시한 도면이다. 상기 모바일 운영체제 보안성 강화 방법은 도 3의 모바일 운영체제 보안성 강화 장치(300)에 의해 수행될 수 있다.

도 1 내지 도 3을 참조하면, 단계(110)에서 상기 모바일 운영체제 보안성 강화 장치는 모바일 운영체제(240)에 어플리케이션(202, 203)의 설치를 제한하는 기능을 제공하는 보안 계층(220)의 동작을 무력화시킨다.

이를 위해, 상기 모바일 운영체제 보안성 강화 장치는 부팅 설정에 따른 보안 계층(220)의 무력화를 수행할 수

있다. 여기서, 상기 보안 계층(220)은 보안 프레임워크(220)로 구현될 수 있으며, 상기 모바일 운영체제 보안성 강화 장치는 상기 보안 프레임워크(220)의 보안/보호 기능을 해제할 수 있다.

- [0043] 다음으로, 단계(120)에서 상기 모바일 운영체제 보안성 강화 장치는 상기 보안 계층(220)의 무력화에 따라, 상기 모바일 운영체제(240)에 관리자 권한을 요청한다.
- [0044] 다음으로, 단계(130)에서 상기 모바일 운영체제 보안성 강화 장치는 상기 관리자 권한의 요청에 따라, 상기 모바일 운영체제(240)로부터 관리자 권한을 획득한다.
- [0045] 기존의 모바일 운영체제(IOS, 안드로이드 등)에서는 보안 계층(220)과의 연동을 통해 관리자 권한을 허용하고 있지 않기 때문에, 사용자가 관리자 권한을 획득할 수 없었다. 이러한 이유로 인해 기존의 모바일 운영체제에서는 어플리케이션(개인 프로그램)의 설치가 제한되었다.
- [0046] 다만, 기존의 모바일 운영체제에서는 관리자 권한을 요청하여 관리자 권한을 확인할 수 있는 정도까지만 허용하였으며, 이러한 관리자 권한의 확인은 IOS의 경우 탈옥이 되었는지, 안드로이드의 경우 루팅이 되었는지를 탐지하기 위한 용도로 활용되어 왔다.
- [0047] 즉, 기존의 모바일 운영체제에서는 관리자 권한을 요청하여 획득할 수 없기 때문에 관리자 권한을 이용한 어플리케이션의 설치가 제한되었다.
- [0048] 그러나, 본 발명의 일 실시예에서는 보안 계층(220)의 무력화를 통해, 모바일 운영체제(240)로부터 관리자 권한을 요청하여 획득할 수 있도록 함으로써, 이렇게 획득한 관리자 권한을 이용하여 필터 드라이버를 설치함으로써 운영체제(240)의 보안성 강화를 위한 보안 솔루션을 제공할 수 있는 환경을 제공할 수 있다.
- [0049] 여기서, 상기 필터 드라이버는 보안 어플리케이션(201)의 설치 시 함께 설치될 수 있다. 상기 보안 어플리케이션(201)은 운영체제(240)의 보안/보호 기술에 문제점이 발생할 경우, 운영체제(240)의 업데이트보다 먼저 업데이트를 수행하게 된다. 이로써, 본 발명의 일 실시예에 따르면, 상기 보안 어플리케이션(201)의 보안 기능을 강화할 수 있으며, 이를 통해 운영체제(240)의 보안성을 강화시킬 수 있는 환경을 제공할 수 있게 된다.
- [0050] 다음으로, 단계(140)에서 상기 모바일 운영체제 보안성 강화 장치는 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)(230)에 필터 드라이버(filter driver)를 설치한다.
- [0051] 여기서, 상기 커널 익스텐션(230)은 상기 무력화된 보안 계층(220)과 상기 모바일 운영체제(240) 사이의 계층에 위치하며, 외부 장치(앱스토어나 플레이스토어 등과 같은 서버)와의 네트워크 연결을 제어하는 네트워크 인터페이스로서 기능할 수 있다.
- [0052] 또한, 상기 필터 드라이버는 상기 커널 익스텐션(230)을 통해 상기 어플리케이션(201, 202, 203)의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제(240)의 보안성을 강화할 수 있다.
- [0053] 다음으로, 단계(150)에서 상기 모바일 운영체제 보안성 강화 장치는 상기 필터 드라이버를 이용하여 상기 어플리케이션(201, 202, 203)의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제(240)의 보안성을 강화할 수 있다.
- [0054] 이를 위해, 상기 모바일 운영체제 보안성 강화 장치는 상기 어플리케이션(201, 202, 203)의 설치 시, 상기 필터 드라이버를 이용하여 상기 어플리케이션(201, 202, 203)의 설치 여부에 대해 메시지를 출력할 수 있으며, 이때 상기 메시지를 통한 선택 여부에 따라 사용자가 설치에 동의한 경우에만 상기 어플리케이션(201, 202, 203)을 모바일 디바이스에 설치함으로써, 모바일 운영체제(240)의 보안성을 강화할 수 있다.
- [0055] 한편, 상기 모바일 운영체제 보안성 강화 장치는 상기 어플리케이션(201, 202, 203)이 특정 파일을 처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일(250)에 기록할 수 있다.
- [0056] 여기서, 상기 모니터링용 이벤트 파일(250)은 상기 모바일 운영체제(240)가 아이오에스(IOS)인 경우, '/dev/fsevents'(250)일 수 있다. 상기 모니터링용 이벤트 파일(250), 즉 '/dev/fsevents'(250)은 상기 모바일 운영체제(240)와 하드웨어(260) 사이의 계층에 위치할 수 있다.
- [0057] 참고로, 상기 보안 계층(220)의 상위 계층에 존재하는 라이브러리 계층(210)은 라이브러리 프레임워크로서 구현될 수 있으며, 상기 어플리케이션(201, 202, 203)의 구동을 위한 최소한의 기능을 할 수 있다.

- [0059] 도 3은 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치를 설명하기 위해 도시한 블록도이고, 도 4 및 도 5는 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치의 동작을 설명하기 위해 도시한 도면이다.
- [0060] 도 3을 참조하면, 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치(100)는 보안 계층 무력화부(310), 관리자 권한 획득부(320), 필터 드라이버 설치부(330), 보안성 강화부(340), 및 제어부(350)를 포함하여 구성될 수 있다.
- [0061] 상기 보안 계층 무력화부(310)는 모바일 운영체제에 어플리케이션의 설치를 제한하는 기능을 제공하는 보안 계층의 동작을 무력화시킨다. 이를 위해, 상기 보안 계층 무력화부(310)는 부팅 설정에 따른 보안 계층의 무력화를 수행할 수 있다. 즉, 상기 보안 계층 무력화부(310)는 도 4에 도시된 바와 같이 '(A) 무력화'의 기능을 수행하여 상기 보안 계층의 기능을 해제시킬 수 있다.
- [0062] 상기 관리자 권한 획득부(320)는 상기 보안 계층의 무력화에 따라, 상기 모바일 운영체제에 관리자 권한을 요청한다. 즉, 상기 관리자 권한 획득부(320)는 도 4에 도시된 바와 같이 '(B) 관리자 권한 요청' 기능을 수행하여 상기 모바일 운영체제에 상기 관리자 권한을 요청할 수 있다. 상기 관리자 권한 획득부(320)는 상기 관리자 권한의 요청에 따라, 상기 모바일 운영체제로부터 관리자 권한을 획득한다.
- [0063] 기존의 모바일 운영체제(IOS, 안드로이드 등)에서는 보안 계층과의 연동을 통해 관리자 권한을 허용하고 있지 않기 때문에, 사용자가 관리자 권한을 획득할 수 없었다. 이러한 이유로 인해 기존의 모바일 운영체제에서는 어플리케이션(개인 프로그램)의 설치가 제한되었다.
- [0064] 다만, 기존의 모바일 운영체제에서는 관리자 권한을 요청하여 관리자 권한을 확인할 수 있는 정도까지만 허용하였으며, 이러한 관리자 권한의 확인은 IOS의 경우 탈옥이 되었는지, 안드로이드의 경우 루팅이 되었는지를 탐지하기 위한 용도로 활용되어 왔다.
- [0065] 즉, 기존의 모바일 운영체제에서는 관리자 권한을 요청하여 획득할 수 없기 때문에 관리자 권한을 이용한 어플리케이션의 설치가 제한되었다.
- [0066] 그러나, 본 실시예에서는 보안 계층의 무력화를 통해, 상기 관리자 권한 획득부(320)가 모바일 운영체제로부터 관리자 권한을 요청하여 획득할 수 있도록 함으로써, 이렇게 획득한 관리자 권한을 이용하여 도 5에 도시된 바와 같이 모니터링 도구(예: 필터 드라이버, 프로그램 등)를 설치함으로써 운영체제의 보안성 강화를 위한 보안 솔루션을 제공할 수 있는 환경을 제공할 수 있다.
- [0067] 상기 필터 드라이버 설치부(330)는 상기 관리자 권한을 이용하여 커널 익스텐션(kernel extension)에 필터 드라이버(filter driver)를 설치한다.
- [0068] 여기서, 상기 커널 익스텐션은 상기 무력화된 보안 계층과 상기 모바일 운영체제 사이의 계층에 위치하며, 외부 장치(앱스토어나 플레이스토어 등과 같은 서버)와의 네트워크 연결을 제어하는 네트워크 인터페이스로서 기능할 수 있다.
- [0069] 또한, 상기 필터 드라이버는 상기 커널 익스텐션을 통해 상기 어플리케이션의 설치와 관련하여 상기 외부 장치와 송수신하는 데이터를 필터링함으로써 상기 모바일 운영체제의 보안성을 강화할 수 있다.
- [0070] 상기 보안성 강화부(340)는 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부를 선택 가능하도록 하여 상기 모바일 운영체제의 보안성을 강화할 수 있다.
- [0071] 이를 위해, 상기 보안성 강화부(320)는 상기 어플리케이션의 설치 시, 상기 필터 드라이버를 이용하여 상기 어플리케이션의 설치 여부에 대해 메시지를 출력할 수 있으며, 이때 상기 메시지를 통한 선택 여부에 따라 사용자가 설치에 동의한 경우에만 상기 어플리케이션을 모바일 디바이스에 설치함으로써, 모바일 운영체제의 보안성을 강화할 수 있다.
- [0072] 상기 제어부(350)는 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치(100), 즉 상기 보안 계층 무력화부(310), 상기 관리자 권한 획득부(320), 상기 필터 드라이버 설치부(330), 상기 보안성 강화부(340) 등의 동작을 전반적으로 제어할 수 있다.
- [0073] 한편, 본 발명의 일 실시예에 따른 모바일 운영체제 보안성 강화 장치(300)는 상기 어플리케이션이 특정 파일을

처리하려고 하는 이벤트가 발생할 때, 상기 이벤트의 신속한 모니터링을 위해 상기 이벤트에 해당하는 로그(log)를 모니터링용 이벤트 파일에 기록하는 로그 기록부(미도시)를 더 포함할 수 있다.

[0074] 여기서, 상기 모니터링용 이벤트 파일은 상기 모바일 운영체제가 아이오에스(IOS)인 경우, '/dev/fsevents'일 수 있다. 상기 모니터링용 이벤트 파일, 즉 '/dev/fsevents'은 상기 모바일 운영체제와 하드웨어 사이의 계층에 위치할 수 있다.

[0076] 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0078] 지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다. 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구의 범위뿐 아니라 이 특허 청구의 범위와 균등한 것들에 의해 정해져야 한다.

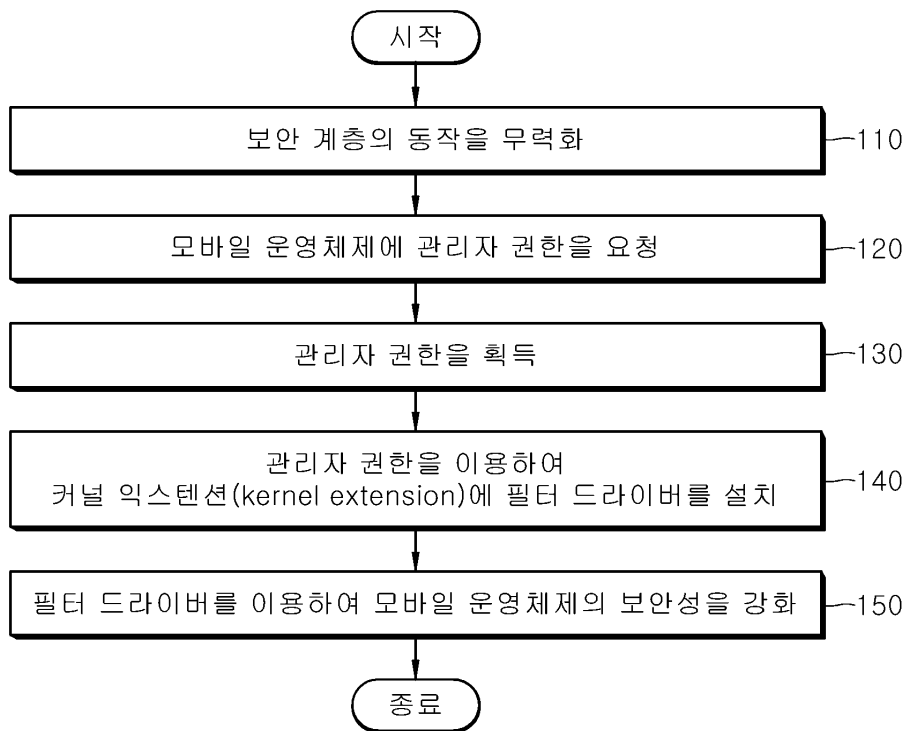
[0079] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

## 부호의 설명

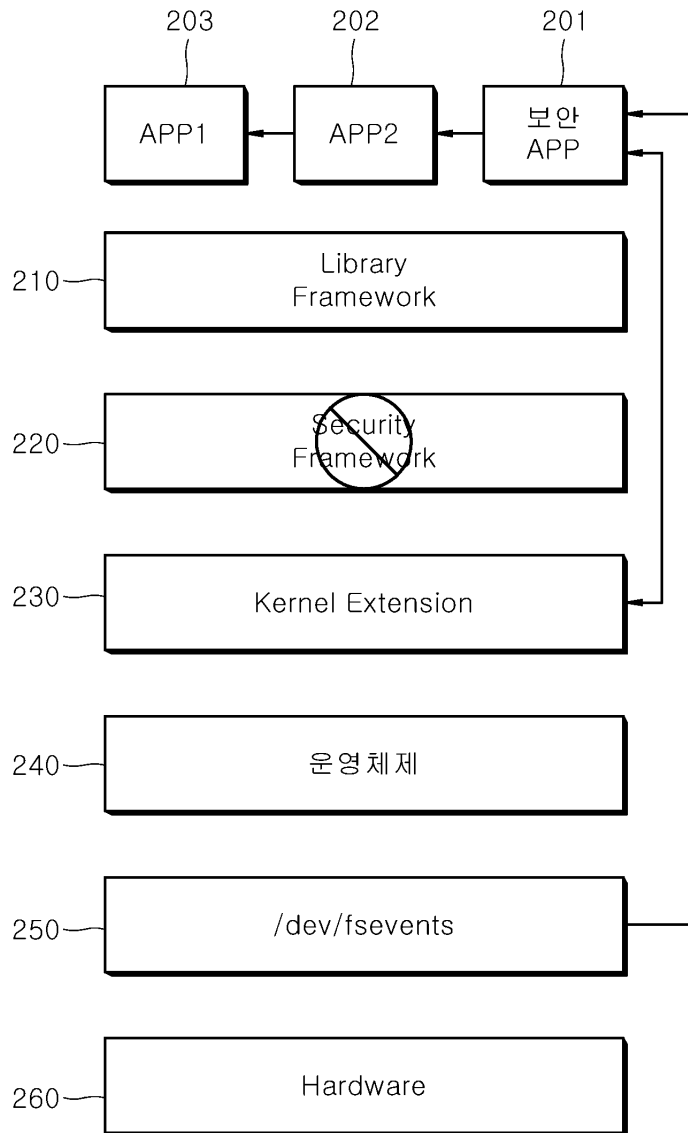
[0081] 310: 보안 계층 무력화부  
320: 관리자 권한 획득부  
330: 필터 드라이버 설치부  
340: 보안성 강화부  
350: 제어부

도면

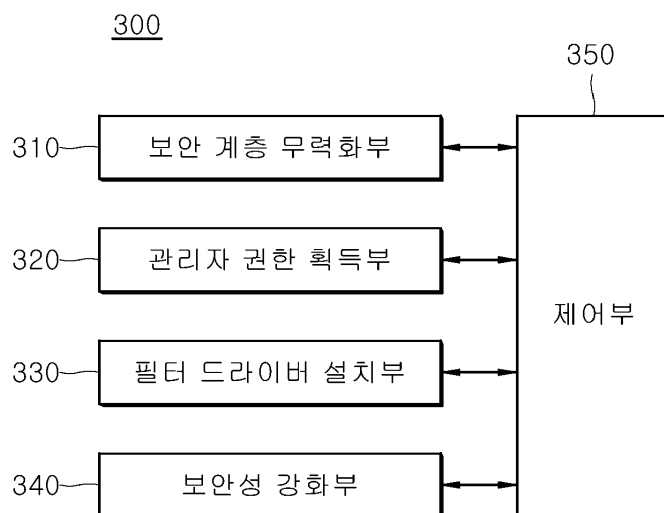
도면1



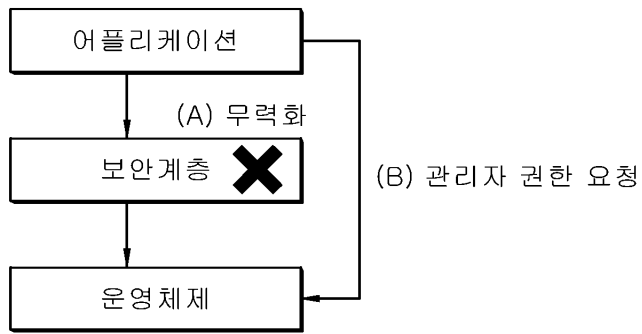
도면2



도면3



도면4



도면5

