(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2015-0047707
(43) 공개일자 2015년05월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 9/22* (2006.01)
G06F 9/44 (2006.01)
(21) 출원번호 10-2013-0127447
(22) 출원일자 2013년10월24일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
(72) 발명자
하준호
경북 구미시 진평2길 15-3, 507호 (진평동, 개성시대빌라)
엘리스 리 초우
미국 캘리포니아주 95070 사라토가 아르고너트 드라이브 20200
(뒷면에 계속)
(74) 대리인
윤동열

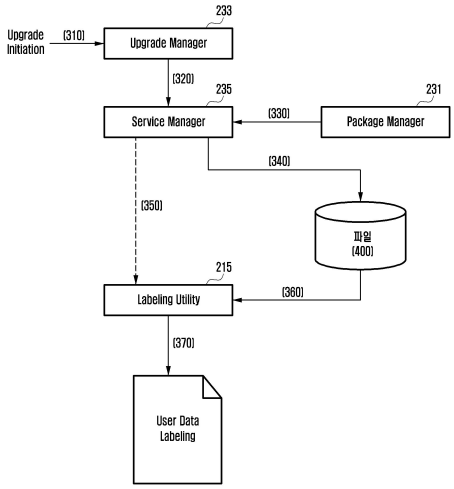
전체 청구항 수 : 총 26 항

(54) 발명의 명칭 **전자 장치의 운영체제 업그레이드 방법 및 장치**

(57) 요 약

본 발명은 운영체제(OS, Operating System)를 구비한 전자 장치에서 유저 데이터(user data)의 삭제 없이 보안성이 강화된 운영체제로 업그레이드 할 수 있는 전자 장치 및 그 운영 방법에 관한 것으로, 이러한 본 발명의 실시 예에 따른 전자 장치의 운영체제 업그레이드 방법은, 운영체제의 업그레이드 개시를 감지하는 과정, 유저 데이터별 레이블링 정보를 생성하는 과정, 및 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 과정을 포함할 수 있다. 본 발명은 상기한 한 실시 예를 기반으로 다양한 다른 실시 예들이 가능하다.

대 표 도 - 도3



(72) 발명자

이창욱

경기 화성시 영통로50번길 27, 105동 204호 (반월동, 두산위브아파트)

장 씽웬

미국 캘리포니아주 94583, 샌 라몬 카르도 CIR 348

문성환

서울 강남구 논현로 205, 3동 1105호 (도곡동, 도곡한신아파트)

배국진

경기 수원시 영통구 영통로154번길 51-16, 308동 603호 (망포동, 센트럴하이츠아파트)

양수용

서울 송파구 토성로17길 3, 202호 (풍납동)

명 세 서

청구범위

청구항 1

전자 장치의 운영체제 업그레이드 방법에 있어서,

운영체제의 업그레이드 개시를 감지하는 과정,

유저 데이터별 레이블링(labeling) 정보를 생성하는 과정, 및

상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링(relabeling) 하는 과정을 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 2

제1항에 있어서, 상기 레이블링 정보를 생성하는 과정은

상기 유저 데이터의 플레인 텍스트(plain text)를 획득하는 과정,

상기 플레인 텍스트에 기초하여 유저 데이터를 식별하는 과정, 및

식별된 유저 데이터에 대한 레이블링 정보를 생성하는 과정을 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 3

제1항에 있어서, 상기 레이블링 정보는

상기 운영체제의 보안 정책(Security Policy)에 따른 보안 속성을 포함하는 것을 특징으로 하는 전자 장치의 운영체제 업그레이드 방법.

청구항 4

제3항에 있어서, 상기 보안 속성은

타입(Type) 속성을 포함하는 것을 특징으로 하는 전자 장치의 운영체제 업그레이드 방법.

청구항 5

제1항에 있어서, 상기 레이블링 정보를 생성하는 과정은

유저 데이터별 레이블링 정보를 파일로 저장하는 과정을 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 6

제1항에 있어서, 상기 리레이블링 하는 과정은

상기 유저 데이터의 보안 컨텍스트(Security Context)를 상기 운영체제의 보안 정책을 기반으로 변경하는 과정을 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 7

제1항에 있어서, 상기 리레이블링 하는 과정은

상기 유저 데이터의 보안 컨텍스트에 상기 운영체제의 보안 정책에 대응하는 타입 속성을 추가하는 과정을 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 8

제1항에 있어서,

상기 운영체제의 업그레이드는 일반 운영체제에서 보안 운영체제(Secure OS)로 업그레이드 하는 것을 특징으로

하는 전자 장치의 운영체제 업그레이드 방법.

청구항 9

제1항에 있어서,

전자 장치의 동작 중에 유저 데이터를 리레이블링 하는 과정을 더 포함하는 전자 장치의 운영체제 업그레이드 방법.

청구항 10

전자 장치의 운영 방법에 있어서,

프레임워크(framework)에서, 유저 데이터의 리레이블링(relabeling)을 위한 레이블링(labeling) 정보를 저장하고 상기 유저 데이터의 리레이블링 명령을 커널(kernel)에 전달하는 과정, 및

상기 커널에서, 상기 리레이블링 명령에 반응하여 상기 레이블링 정보에 따라 상기 유저 데이터를 리레이블링 하는 과정을 포함하는 전자 장치의 운영 방법.

청구항 11

제10항에 있어서, 상기 레이블링 정보를 저장하는 과정은

서비스 매니저(Service Manager)에 의해 수행하는 것을 특징으로 하고,

상기 서비스 매니저는

유저 데이터의 플레인 텍스트(plain text)를 획득하는 과정,

상기 플레인 텍스트에 기초하여 식별된 유저 데이터의 레이블링 정보를 보안 정책(Security Policy)에 기초하여 생성하는 과정, 및

상기 식별된 유저 데이터의 레이블링 정보를 저장하는 과정을 실행하는 것을 특징으로 하는 전자 장치의 운영 방법.

청구항 12

제10항에 있어서, 상기 전달하는 과정은

서비스 매니저가 상기 리레이블링 명령을 상기 커널의 레이블링 유틸리티(Labeling Utility)에게 전달하는 것을 특징으로 하는 전자 장치의 운영 방법.

청구항 13

제10항에 있어서, 상기 리레이블링 하는 과정은

레이블링 유틸리티에 의해 수행하는 것을 특징으로 하고,

상기 레이블링 유틸리티는

보안 정책에 따른 타입 속성을 상기 유저 데이터의 보안 컨텍스트(Security Context)에 추가하는 것에 의해 상기 리레이블링을 실행하는 것을 특징으로 하는 전자 장치의 운영 방법.

청구항 14

제11항에 있어서, 상기 플레인 텍스트를 획득하는 과정은

상기 서비스 매니저에 의해 수행하는 것을 특징으로 하고,

상기 서비스 매니저는

상기 프레임워크의 패키지 매니저가 관리하는 플레인 텍스트를 획득하거나, 또는 상기 서비스 매니저가 상기 유저 데이터로부터 추출하여 획득하는 것을 특징으로 하는 전자 장치의 운영 방법.

청구항 15

제10항에 있어서,

일반 운영체제에서 보안 운영체제(Secure OS)로 업그레이드 시 리레이블링 동작을 개시하는 것을 특징으로 하는 전자 장치의 운영 방법.

청구항 16

제10항에 있어서,

전자 장치의 동작 중에 유저 데이터의 리레이블링을 위한 인터럽트를 감지하는 과정; 및

상기 레이블링 정보에 따라 상기 유저 데이터를 리레이블링 하는 과정을 더 포함하는 전자 장치의 운영 방법.

청구항 17

전자 장치에 있어서,

운영체제의 업그레이드를 위한 패키지를 수신하는 통신부,

상기 패키지를 저장하고, 유저 데이터의 레이블링을 위한 레이블링 정보를 저장하는 저장부, 및

상기 운영체제의 업그레이드 시 상기 레이블링 정보를 생성하고, 상기 레이블링 정보에 기초하여 유저 데이터의 리레이블링에 의한 상기 운영체제의 업그레이드를 제어하는 제어부를 포함하는 것을 특징으로 하는 전자 장치.

청구항 18

제17항에 있어서, 상기 제어부는

상기 유저 데이터의 리레이블링에 의해, 상기 유저 데이터의 삭제 없이 상기 운영체제 업그레이드를 제어하는 것을 특징으로 하는 전자 장치.

청구항 19

제17항에 있어서, 상기 제어부는

유저 데이터에서 플레인 텍스트(plain text)를 추출하고, 추출된 플레인 텍스트를 관리하는 유저 데이터 관리 모듈,

상기 플레인 텍스트에 기초하여 유저 데이터를 식별하고, 식별된 유저 데이터를 리레이블링 하기 위한 레이블링 정보를 생성하는 서비스 처리 모듈, 및

상기 레이블링 정보에 기초하여 상기 유저 데이터에 대한 리레이블링을 처리하는 레이블링 실행 모듈을 포함하는 것을 특징으로 하는 전자 장치.

청구항 20

제19항에 있어서, 상기 레이블링 실행 모듈은

상기 유저 데이터의 보안 컨텍스트(Security Context)에 보안 정책(Security Policy)에 따른 타입 속성을 추가하는 것을 특징으로 하는 전자 장치.

청구항 21

제19항에 있어서, 상기 레이블링 정보는

보안 정책에 따른 타입 속성을 포함하는 것을 특징으로 하는 전자 장치.

청구항 22

제19항에 있어서, 상기 서비스 처리 모듈은

유저 데이터별로 생성하는 레이블링 정보를 파일로 저장하는 것을 특징으로 하는 전자 장치.

청구항 23

제17항에 있어서, 상기 제어부는

전자 장치의 동작 중에 유저 데이터의 리레이블링을 위한 인터럽트를 감지하고, 상기 레이블링 정보에 따라 상기 유저 데이터의 리레이블링을 제어하는 것을 특징으로 하는 전자 장치.

청구항 24

제17항에 있어서,

상기 운영체제의 업그레이드는 일반 운영체제에서 보안 운영체제(Secure OS)로 업그레이드인 것을 특징으로 하는 전자 장치.

청구항 25

전자 장치에 있어서,

운영체제 업그레이드 진행과 관련된 화면을 표시하는 표시부;

전자 장치의 통신을 수행하고 운영체제 업그레이드를 위한 패키지를 수신하는 통신부;

하나 또는 그 이상의 프로그램이 저장되는 저장부; 및

상기 하나 또는 그 이상의 프로그램을 실행하여 상기 전자 장치의 운영체제 업그레이드를 제어하는 하나 또는 그 이상의 프로세서들을 포함하고,

상기 하나 또는 그 이상의 프로그램들은,

상기 패키지에 따른 보안 운영체제 업그레이드 시 유저 데이터별 레이블링 정보를 생성하는 과정, 및

상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 과정을 실행하는 프로그램을 포함하는 것을 특징으로 하는 전자 장치.

청구항 26

운영체제의 업그레이드 개시를 감지하는 동작, 유저 데이터별 레이블링(labeling) 정보를 생성하는 동작, 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링(relabeling) 하는 동작을 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 운영체제(OS, Operating System)를 구비한 전자 장치에서 상기 운영체제의 업그레이드 방법 및 이를 지원하는 장치에 관한 것이다.

배 경 기 술

[0002] 전자 장치는 다양한 운영체제(OS, Operating System)들 중 적어도 하나의 운영체제에 기초하여 동작할 수 있다. 상기 운영체제는 보안 위협을 극복하기 위하여 다양한 보안 방식을 사용하여 시스템을 보호하고 있다.

발명의 내용

해결하려는 과제

[0003] 전자 장치에 보안 운영체제에 따라 정의되는 정책(policy)은 사용자, 프로그램, 프로세스 그리고 이들의 동작 대상인 파일과 디바이스를 포함한 시스템 전체, 즉, 모든 주체(subject)들과 객체(object)들에 대한 접근 허가(access permissions)를 기술하게 된다. 따라서 보안 운영체제에 따른 정책은 관련 소스(source)와 함께 패키지로 공급될 수 있다. 따라서 전자 장치는 패키지에 기초하여 보안 운영체제를 설치하게 된다. 보안 운영체제가 설치되어 생산되는 전자 장치에서는 보안 운영체제에 따른 정책이 적용되어 사용하는 데에는 문제가 없다. 하지만, 기존 운영체제를 가지는 전자 장치에서 보안성이 강화된 새로운 운영체제(보안 운영체제)를 적용하기 위해서는 전자 장치에 포함된 모든 객체(예컨대, 파일시스템(FS, File System), 프로세스, 유저 데이터 등)에 대한

레이블링(labeling)이 이루어져야 한다.

[0004] 본 발명의 실시 예에 따르면, 운영체제를 구비한 전자 장치에서 기존 운영체제에 보안 운영체제를 적용할 때 유저 데이터의 삭제 없이 보안 운영체제를 적용할 수 있는 전자 장치 및 그 운영 방법을 제공할 수 있다.

[0005] 본 발명의 실시 예에서 전자 장치는 정보통신기기, 멀티미디어기기, 웨어러블(wearable) 기기 및 그에 대한 응용기기와 같이 AP(Application Processor), GPU(Graphic Processing Unit), 및 CPU(Central Processing) 중 하나 또는 그 이상을 사용하는 모든 장치를 포함할 수 있다.

[0006] 본 발명의 실시 예에 따르면, 운영체제를 구비한 전자 장치에서 기존 운영체제에 보안성이 강화된 운영체제로 업그레이드할 시 유저 데이터를 초기화해야 하는 전자 장치의 공장 초기화를 거치지 않고 운영체제 업그레이드를 지원할 수 있는 전자 장치 및 그 운영 방법을 제공할 수 있다.

[0007] 본 발명의 실시 예에 따르면, 전자 장치가 동작하는 중에 유저 데이터의 리레이블링을 위한 인터럽트를 감지할 수 있고, 상기 인터럽트에 반응하여 해당 유저 데이터를 운영체제의 보안 정책에 따라 리레이블링 할 수 있는 전자 장치 및 그 운영 방법을 제공할 수 있다.

[0008] 본 발명의 실시 예에 따르면, 전자 장치의 보안 강화를 지원하기 위한 최적의 환경을 구현하여 사용자의 편의성 및 전자 장치의 사용성을 향상시킬 수 있는 전자 장치 및 그 운영 방법을 제공할 수 있다.

과제의 해결 수단

[0009] 본 발명의 실시 예에 따르면, 운영체제의 업그레이드 개시를 감지하는 과정, 유저 데이터별 레이블링(labeling) 정보를 생성하는 과정, 및 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 과정을 포함할 수 있다.

[0010] 본 발명의 실시 예에 따르면, 프레임워크(framework)에서, 유저 데이터의 리레이블링을 위한 레이블링 정보를 저장하고 상기 유저 데이터의 리레이블링 명령을 커널(kernel)에 전달하는 과정, 및 상기 커널에서, 상기 리레이블링 명령에 반응하여 상기 레이블링 정보에 따라 상기 유저 데이터를 리레이블링(relabeling) 하는 과정을 포함할 수 있다.

[0011] 본 발명의 실시 예에 따르면, 상기 방법을 프로세서에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체를 포함할 수 있다.

[0012] 본 발명의 실시 예에 따르면, 운영체제의 업그레이드 개시를 감지하는 동작, 유저 데이터별 레이블링 정보를 생성하는 동작, 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 동작을 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체를 포함할 수 있다.

[0013] 본 발명의 실시 예에 따르면, 운영체제의 업그레이드를 위한 패키지를 수신하는 통신부, 상기 패키지를 저장하고, 유저 데이터의 레이블링을 위한 레이블링 정보를 저장하는 저장부, 및 상기 운영체제의 업그레이드 시 상기 레이블링 정보를 생성하고, 상기 레이블링 정보에 기초하여 유저 데이터의 리레이블링에 의한 상기 운영체제의 업그레이드를 제어하는 제어부를 포함할 수 있다.

[0014] 본 발명의 실시 예에 따르면, 운영체제 업그레이드 진행과 관련된 화면을 표시하는 표시부, 전자 장치의 통신을 수행하고 운영체제 업그레이드를 위한 패키지를 수신하는 통신부, 하나 또는 그 이상의 프로그램이 저장되는 저장부, 및 상기 하나 또는 그 이상의 프로그램을 실행하여 상기 전자 장치의 운영체제 업그레이드를 제어하는 하나 또는 그 이상의 프로세서들을 포함하고, 상기 하나 또는 그 이상의 프로그램들은, 상기 패키지에 따른 보안 운영체제 업그레이드 시 유저 데이터별 레이블링 정보를 생성하는 과정, 및 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 과정을 실행하는 프로그램을 포함할 수 있다.

[0015] 전술한 바와 같은 내용들은 당해 분야 통상의 지식을 가진 자가 후술되는 본 발명의 구체적인 설명으로부터 보다 잘 이해할 수 있도록 하기 위하여 본 발명의 실시 예에 따른 특징들 및 기술적인 장점들을 다소 넓게 약술한 것이다. 이러한 특징들 및 장점들 이외에도 본 발명의 청구범위의 주제를 형성하는 추가적인 특징들 및 장점들이 후술되는 본 발명의 실시 예에 따른 구체적인 설명으로부터 잘 이해될 것이다.

발명의 효과

[0016] 본 발명의 실시 예에서는, 운영체제를 구비하는 전자 장치에서 기존 운영체제에 보안성이 강화된 보안 운영체제의 설치를 지원할 수 있어, 사용자의 편의성을 향상시키고, 전자 장치의 사용성, 편의성, 접근성 및 경쟁력을

향상시키는데 기여할 수 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명의 실시 예에 따른 전자 장치의 구성을 개략적으로 도시한 도면이다.

도 2는 본 발명의 실시 예에 따른 기능을 처리하는 전자 장치의 플랫폼 구조의 예시를 개략적으로 도시한 도면이다.

도 3 및 도 4는 본 발명의 실시 예예 따른 전자 장치에서 운영체제 업그레이드 동작을 설명하기 위해 개략적으로 도시한 도면들이다.

도 5는 본 발명의 실시 예에 따른 전자 장치에서 운영체제 업그레이드를 위한 운영 방법을 도시한 흐름도이다.

도 6은 본 발명의 실시 예에 따른 전자 장치에서 업그레이드 방식에 따라 운영체제를 업그레이드하는 운영 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0018] 이하, 첨부된 도면들을 참조하여 본 발명의 다양한 실시 예들을 설명한다. 본 발명의 실시 예에서는 특정 실시 예들이 도면에 예시되고 관련된 상세한 설명이 기재되어 있으나, 다양한 변경을 가할 수 있고 여러 가지 실시 예들을 가질 수 있다. 따라서 본 발명의 다양한 실시 예들은 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 실시 예에 따른 사상 및 기술 범위에 포함되는 모든 변경 또는 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 도면의 설명과 관련하여, 유사한 구성 요소에 대해서는 유사한 참조부호가 사용되었다. 또한 본 발명의 요지를 흐리게 할 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략할 것이다. 하기의 설명에서는 본 발명의 다양한 실시 예들에 따른 동작을 이해하는데 필요한 부분만이 설명되며, 그 이외 부분의 설명은 본 발명의 요지를 흩트리지 않도록 생략될 것이라는 것을 유의하여야 한다.

[0019] 본 발명의 실시 예에서 사용될 수 있는"포함한다", "포함할 수 있다" 등의 표현은 개시된 해당 기능, 동작, 구성요소 등의 존재를 가리키며, 추가적인 하나 이상의 기능, 동작, 구성요소 등을 제한하지 않는다. 또한, 본 발명의 실시 예에서, "포함하다" 또는 "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.

[0020] 또한 본 발명의 실시 예에서 "및/또는" 등의 표현은 함께 나열된 단어들의 어떠한, 그리고 모든 조합을 포함한다. 예를 들어, A 및/또는 B는, A를 포함할 수도, B를 포함할 수도, 또는 A 와 B 모두를 포함할 수도 있다.

[0021] 또한 본 발명의 실시 예에서 "제 1", "제2", "첫째", "둘째" 등의 표현들이 본 발명의 실시 예에 따른 다양한 구성요소들을 수식할 수 있지만, 해당 구성요소들을 한정하지 않는다. 예를 들어, 상기 표현들은 해당 구성요소들의 순서 및/또는 중요도 등을 한정하지 않는다. 상기 표현들은 한 구성요소를 다른 구성요소와 구분 짓기 위해 사용될 수 있다. 예를 들어, 제1 사용자 기기와 제 2 사용자 기기는 모두 사용자 기기이며, 서로 다른 사용자 기기를 나타낸다. 예를 들어, 본 발명의 실시 예에 따른 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0022] 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 않는 것으로 이해될 수 있어야 할 것이다. 본 발명의 실시 예에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명의 실시 예를 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0023] 본 발명의 실시 예에 따른 전자 장치는, 통신 기능이 포함된 장치일 수 있다. 예를 들면, 전자 장치는 스마트폰(smartphone), 태블릿 PC(tablet personal computer), 이동전화기(mobile phone), 화상전화기, 전자북 리더기(e-book reader), 데스크탑 PC(desktop personal computer), 랩탑 PC(laptop personal computer), 넷북 컴퓨터(netbook computer), PDA(personal digital assistant), PMP(portable multimedia player), MP3 플레이어, 모바일 의료기기, 카메라(camera), 또는 웨어러블 장치(wearable device)(예: 전자 안경과 같은 head-mounted-device(HMD), 전자 의복, 전자 팔찌, 전자 목걸이, 전자 앱세서리(appcessory), 전자 문신, 또는 스마트 와치

(smart watch)) 중 적어도 하나를 포함할 수 있다.

[0024] 어떤 실시 예들에 따르면, 전자 장치는 통신 기능을 갖춘 스마트 가전 제품(smart home appliance)일 수 있다. 스마트 가전 제품은, 예를 들어, 텔레비전, DVD(digital video disk) 플레이어, 오디오, 냉장고, 에어컨, 청소기, 오븐, 전자레인지, 세탁기, 공기 청정기, 셋톱 박스(set-top box), TV 박스(예를 들면, 삼성 HomeSync™,애플TV™,또는 구글 TV™),게임 콘솔(game consoles), 전자 사전, 전자 키, 캠코더(camcorder), 또는 전자 액자 중 적어도 하나를 포함할 수 있다.

[0025] 어떤 실시 예들에 따르면, 전자 장치는 각종 의료기기(예: MRA(magnetic resonance angiography), MRI(magnetic resonance imaging), CT(computed tomography), 촬영기, 초음파기 등), 네비게이션(navigation) 장치, GPS 수신기(global positioning system receiver), EDR(event data recorder), FDR(flight data recorder), 자동차 인포테인먼트(infotainment) 장치, 선박용 전자 장비(예: 선박용 항법 장치 및 자이로 콤파스 등), 항공 전자기기(avionics), 또는 보안 기기, 또는 산업용 또는 가정용 로봇 중 적어도 하나를 포함할 수 있다.

[0026] 어떤 실시 예들에 따르면, 전자 장치는 통신 기능을 포함한 가구(furniture) 또는 건물/구조물의 일부, 전자 보드(electronic board), 전자 사인 입력장치(electronic signature receiving device), 프로젝터(projector), 또는 각종 계측 기기(예컨대, 수도, 전기, 가스, 또는 전파 계측 기기 등) 중 적어도 하나를 포함할 수 있다. 본 발명의 실시 예에 따른 전자 장치는 전술한 다양한 장치들 중 하나 또는 그 이상의 조합일 수 있다. 또한, 본 발명의 실시 예에 따른 전자 장치가 전술한 기기들에 한정되지 않음은 당업자에게 자명하다.

[0027] 제안하는 본 발명의 실시 예는 운영체제(OS, Operating System)에 기초하여 동작하는 전자 장치에서, 설치된 기존 운영체제를 보안성이 강화된 보안 운영체제(Security OS)로 업그레이드하기 위한 방법 및 장치에 관한 것이다.

[0028] 본 발명의 실시 예에서 보안 운영체제는, 예를 들어, 리눅스 보안 모듈을 이용하여 강제적 접근 제어(MAC, Mandatory Access Control)를 구현한 운영체제를 의미할 수 있다. 예를 들어, 보안 운영체제는 보안이 강화된 운영체제의 패치를 나타낼 수 있다.

[0029] 표준 리눅스 보안(Standard Linux Security)은 임의적 접근 제어(DAC, Discretionary Access Control) 모델이다. DAC 모델에서 파일과 자원에 대한 결정권은 오직 해당 객체(object)들(예컨대, 파일, 디바이스, 저장장치, 프린터, 메모리, CPU 등)의 사용자(user id)에게 있고 소유권(ownership)에 따라 이루어진다. 각 사용자와 그 사용자에 의해 실행된 프로그램은 자기에게 할당된 객체에 대해 전적으로 자유 재량권을 가질 수 있다. 따라서 이러한 상황에서는 악의 있는 일반 혹은 루트 사용자가 실행시킨 결함이 있는 소프트웨어를 통해 주어진 객체로 원하는 어떠한 일을 해도 막아낼 방법이 없으며 보안 정책을 시스템 전체에 걸쳐 시행되도록 할 방법이 없다. 이에, MAC 모델이 제안되었다. MAC 모델은 위와 같이 DAC 모델에서 빠져있는 요소들을 제공한다. 예를 들어, 보안 정책(security policy)을 모든 프로세스나 객체에 대하여 관리차원으로 규정지을 수 있고, 커널을 통해 보안 운영체제를 구현하면, 모든 프로세스와 객체를 제어할 수 있으며, 결정은 단지 인증된 사용자(user identity)에 의해서가 아니라 이용 가능한(available) 모든 보안 관련 정보에 근거하여 이루어지도록 할 수 있다.

[0030] 예를 들어, 보안 운영체제 하에서 MAC은 모든 주체(subject)들(예컨대, 사용자, 프로그램, 프로세스 등)과 객체들(예컨대, 파일, 디바이스 등)에 대해서 국부적으로 허가(granular permissions)해 줄 수 있다. 응용 프로그램(application program)에서 불필요한 부분은 제외하고 오직 필요한 기능에 대해서만 사용 권한을 안전하게 부여할 수 있다. 이러한 보안 운영체제의 구현은 타입 시행(TE, Type Enforcement)에 기초하여 추상적 사용자 수준 제어(abstracted user-level control)를 제공하는 역할 기반 접근 제어(RBAC, Role-Based Access Control)를 사용할 수 있다. TE는 접근 제어를 처리하기 위해서 테이블(매트릭스)을 이용할 수 있다. 주체는 도메인(domain)을 갖고 객체는 타입을 가지므로, 매트릭스에서 교차 조회하여 이들의 상호작용을 규정할 수 있다. 이는 전자 장치에서 모든 동작자(actor)에 대하여 극단적으로 국부 제어를 가능하게 할 수 있다.

[0031] 이와 같은 전자 장치에서의 보안 운영체제의 목적은, 어플리케이션에 의한 권한 획득 방지, 어플리케이션에 의한 데이터 누출 방지, 보안 모듈의 직접적 접근 방지, 정보에 대한 합법적 규제 시행, 어플리케이션과 데이터의 무결성 유지, 그리고 소비자, 사업자, 정보의 이득 등을 추구하고자 하는 것이고, 보안 운영체제에 의해 루트(root) 권한 획득을 금지할 수 있고, 루트 권한이 획득이 되더라도 시스템을 구성하는 주요 부분(예컨대, bootloader, kernel, user 등의 주요 정보 영역)을 지킬 수 있다.

[0032] 이러한 보안 운영체제에 따라 보안 정책(security policy)이 새롭게 정의되고 있다. 보안 운영체제에서 보안 정책은 사용자, 프로그램, 프로세스 그리고 이들의 동작 대상인 파일과 디바이스를 포함한 시스템 전체, 즉 모든 주체들과 객체들에 대한 접근 허가(access permission)를 기술할 수 있다. 이러한 보안 정책은 서버를 통해 관련 소스(source)와 함께 패키지로 공급될 수 있다. 따라서 전자 장치는 패키지에 기초하여 보안 운영체제를 설치할 수 있다.

[0033] 한편, 기존 운영체제를 가지는 전자 장치에서 보안 운영체제를 적용하기 위해서 전자 장치에 포함된 모든 객체(예컨대, 파일시스템(FS, File System), 프로세스, 유저 데이터 등)에 대한 레이블링(labeling)이 이루어질 수 있다. 객체에 대한 레이블링의 예시는 아래 <표 1>과 같이 나타낼 수 있다.

표 1

[0034]

/data/drm(/.*)? u: object_r: drm_data_file : s0

[0035] 상기 <표 1>의 예시에 따르면, '/data/drm' 아래에 속하는 모든 파일과 디렉토리는 'drm_data_file'로 레이블링 될 수 있다.

[0036] 예를 들어, ABC라는 어플리케이션이 있다고 가정하고, 파일 컨텍스트(file context)에 '/data/important'라는 디렉토리(dir)를 'imp_dir'으로 레이블링 되어 있고, ABC 어플리케이션의 타입 시행(TE)이 기술된 'ABC.te'라는 파일에 상기 ABC 어플리케이션을 my_app이라고 레이블링 하는 정책을 가정하면 아래 <표 2>과 같은 정책 파일이 기술될 수 있다.

표 2

[0037]

allow my_app imp_dir:dir create_dir_perms;

[0038] 상기 <표 2>의 예시와 같이 ABC 어플리케이션에 대한 정책을 명시하면, ABC 어플리케이션은 'my_app'이라는 도메인(domain)을 가지고 동작하는 주체를 나타내고, 'my_app'이라는 도메인은 'imp_dir'이라고 레이블링된 '/data/important/' 디렉토리 생성 권한이 부여된다. 이와 같이, '.te' 정책 파일에 허가(allow)가 명시되지 않은 곳에 대한 접근은 모두 차단(block)될 수 있다.

[0039] 한편, 현재 전자 장치의 기 설치된 기존 운영체제에 보안 운영체제를 적용하기 위해서는 유저 데이터 영역의 경우 공장 초기화(factory reset)를 거칠 수 있다. 예를 들어, 기존 운영체제에서는 해당 정책에 따른 컨텍스트에서는 보안 운영체제에 따른 보안 컨텍스트(Security Context)의 보안 속성(특히, 타입(Type) 속성)이 명시되어 있지 않다. 예를 들어, 아래 <표 3>에 나타낸 바와 같이 기존 운영체제에서의 보안 컨텍스트에서는 '타입 속성'이 기술되어 있지 않으며, 보안 운영체제에서의 보안 컨텍스트에서는 '타입 속성'이 기술된다.

[0040] 보안 운영체제에서의 보안 컨텍스트는 파일, 디렉토리, TCP 소켓 등과 연관되어 있는 모든 속성을 가질 수 있고, 보안 컨텍스트는 아이덴티티(identity), 역할(role), 도메인(domain) (identity:role:domain) 또는 아이덴티티, 역할, 타입(type) (identity:role:type)으로 구성될 수 있다. 도메인은 주체에게 어떠한 접근을 가질 것인가를 결정하는 부분으로, 해당 주체가 무엇을 할 수 있고, 타입에 따라서 주체가 어떤 행동을 취할 수 있도록 할 것인가 하는 목록을 나타낼 수 있다. 타입 속성은 객체에 주어진 보안 속성을 나타내며, 그 객체에 어떤 주체가 접근할 수 있는지를 결정하는 부분이다. 도메인과 타입의 보안 속성은 일반적으로 sysadm_t와 같이 마지막에 '_t'로 표시될 수 있다.

표 3

기존 운영체제	보안 운영체제
user_u:system_r (identity:role)	user_u:system_r:unconfined_t (identity:role:type)

[0041]

[0042] 따라서 이를 적용하기 위해서는 전자 장치의 공장 초기화 과정을 걸쳐 보안 패키지에 의한 설치가 이루어져야만 해당 정책이 적용될 수 있다. 만약, 공장 초기화 과정 없이 보안 패키지에 의한 보안 운영체제가 전자 장치에 탑재되는 경우 기존 유저 데이터들에 대한 정책 즉, 모든 주체와 객체에 대한 접근 허가(access permissions)가 기술되지 않아 모든 유저 데이터의 경우 레이블링이 되지 않는다. 따라서 전자 장치의 사용자도 유저 데이터에 대한 접근 권한을 가질 수 없기 때문에 유저 데이터 자체를 사용할 수 없게 된다. 예를 들어, 사용자가 전자 장치에서 기존에 사용하던 어플리케이션을 실행하고자 할 시 퍼미션 권한 설정이 되지 않았다는 등의 오류 메시지가 출력되면서 어플리케이션 사용이 차단될 수 있다.

[0043] 이에, 본 발명의 실시 예에서는 운영체제를 구비한 전자 장치에서 기존 운영체제에 보안 운영체제를 적용할 때 유저 데이터의 삭제 없이 보안 운영체제를 적용할 수 있는 전자 장치 및 그 운영 방법을 제공한다. 또한 본 발명의 실시 예에서는 전자 장치에서 보안 운영체제의 보안 정책에 따른 레이블링 정보를 가지지 않는 유저 데이터를 전자 장치의 동작 중에 리레이블링 할 수 있는 전자 장치 및 그 운영 방법을 제공한다.

[0044] 이하에서, 본 발명의 실시 예에 따른 전자 장치의 구성과 그의 운용 제어 방법에 대하여 하기 도면들을 참조하여 살펴보기로 한다. 본 발명의 실시 예에 따른 전자 장치의 구성과 그의 운용 제어 방법이 하기에서 기술하는 내용에 제한되거나 한정되는 것은 아니므로 하기의 실시 예들에 의거하여 다양한 실시 예들에 적용할 수 있음에 유의하여야 한다.

[0045] 도 1은 본 발명의 실시 예에 따른 전자 장치의 구성을 개략적으로 도시한 도면이다.

[0046] 상기 도 1을 참조하면, 본 발명의 실시 예에 따른 전자 장치는 무선 통신부(110), 사용자 입력부(120), 터치스크린(130), 오디오 처리부(140), 저장부(150), 인터페이스부(160), 제어부(170), 그리고 전원 공급부(180)를 포함할 수 있다. 본 발명의 실시 예에서 전자 장치는 도 1에 도시된 구성 요소들이 필수적인 것은 아니어서, 도 1에 도시된 구성 요소들보다 많은 구성 요소들을 가지거나, 또는 그보다 적은 구성 요소들을 가지는 것으로 구현될 수 있다. 예를 들어, 본 발명의 실시 예에 따른 전자 장치가 촬영 기능을 지원하는 경우 카메라 모듈의 구성이 더 포함될 수 있다. 또한 본 발명의 실시 예에 따른 전자 장치가 방송 수신 및 재생 기능을 지원하지 않는 경우 일부 모듈(예컨대, 상기 무선 통신부(110)의 방송 수신 모듈(119))의 구성이 생략될 수도 있다.

[0047] 상기 무선 통신부(110)는 전자 장치와 무선 통신 시스템 사이 또는 전자 장치와 다른 전자 장치 사이의 무선 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 예를 들어, 무선 통신부(110)는 이동통신 모듈(111), 무선 랜(WLAN, Wireless Local Area Network) 모듈(113), 근거리 통신 모듈(115), 위치 산출 모듈(117), 그리고 방송 수신 모듈(119) 등을 포함하여 구성될 수 있다.

[0048] 이동통신 모듈(111)은 이동통신 네트워크 상에서 기지국, 외부의 단말, 그리고 다양한 서버들(예컨대, 통합 서버(integration server), 프로바이더 서버(provider server), 컨텐츠 서버(content server), 인터넷 서버(internet server), 클라우드 서버(cloud server) 등) 중 적어도 하나와 무선 신호를 송수신할 수 있다. 상기 무선 신호는 음성통화 신호, 화상통화 신호 또는 문자/멀티미디어 메시지 송수신에 따른 다양한 형태의 데이터를 포함할 수 있다. 이동통신 모듈(111)은 전자 장치의 기존 운영체제의 업그레이드를 위한 상위 버전의 운영체제(예컨대, 보안 강화를 위한 보안 운영체제)를 수신할 수 있다. 한 실시 예에 따르면, 이동통신 모듈(111)은 전자 장치와 네트워크(예컨대, 이동통신 네트워크)를 통해 연결되어 있는 서버로부터 상위 버전의 운영체제를 수신할 수 있다. 전자 장치의 운영체제는 상기 이동통신 모듈(111)에 의한 무선 전송 기술(예컨대, OTA(Over-The-Air) 또는 FOTA(Firmware OTA))을 통해 업그레이드되거나, 유선 통신 기술(예컨대, USB(Universal Serial Bus) 기반 연결)을 통해 업그레이드될 수 있다.

[0049] 무선 랜 모듈(113)은 무선 인터넷 접속 및 다른 전자 장치와 무선 랜 링크(link)를 형성하기 위한 모듈을 나타낼 수 있다. 무선 랜 모듈(113)은 전자 장치에 내장되거나 외장될 수 있다. 무선 인터넷 기술로는 무선 랜(Wi-

Fi), Wibro(Wireless broadband), Wimax(World Interoperability for Microwave Access), 그리고 HSDPA(High Speed Downlink Packet Access) 등이 이용될 수 있다. 무선 랜 모듈(113)은 메신저를 통해 사용자로부터 입력된 데이터를 전송하거나, 또는 외부로부터 데이터를 수신할 수 있다. 무선 랜 모듈(113)은 전자 장치의 기존 운영체제의 업그레이드를 위한 상위 버전의 운영체제(예컨대, 보안 강화를 위한 보안 운영체제)를 수신할 수 있다. 한 실시 예에 따르면, 무선 랜 모듈(113)은 전자 장치와 네트워크(예컨대, 무선 인터넷 네트워크)를 통해 연결되어 있는 서버로부터 상위 버전의 운영체제를 수신할 수 있다. 또한 무선 랜 모듈(113)은 다른 전자 장치와 무선 랜 링크가 형성될 시 사용자 선택에 따른 다양한 데이터(예컨대, 이미지, 동영상, 음악 등)를 다른 전자 장치로 전송하거나 수신 받을 수 있다. 무선 랜 모듈(113)은 상시 온(On) 상태를 유지하거나, 사용자 설정 또는 입력에 따라 턴-온(turn-on)될 수 있다.

[0050] 근거리 통신 모듈(115)은 근거리 통신(short range communication)을 수행하기 위한 모듈을 나타낼 수 있다. 근거리 통신 기술로 블루투스(Bluetooth), 블루투스 저에너지(BLE, Bluetooth Low Energy), RFID(Radio Frequency Identification), 적외선 통신(IrDA, Infrared Data Association), UWB(Ultra Wideband), 지그비(ZigBee), 그리고 NFC(Near Field Communication) 등이 이용될 수 있다. 근거리 통신 모듈(115)은 다른 전자 장치와 근거리 통신이 연결될 시 사용자 선택에 따른 데이터(예컨대, 이미지, 동영상, 음악 등)를 다른 전자 장치로 전송하거나 수신 받을 수 있다. 근거리 통신 모듈(115)은 상시 온 상태를 유지하거나, 사용자 설정 또는 입력에 따라 턴-온될 수 있다.

[0051] 위치 산출 모듈(117)은 전자 장치의 위치를 획득하기 위한 모듈로서, 대표적인 예로는 GPS(Global Position System) 모듈을 포함할 수 있다. 위치 산출 모듈(115)은 3개 이상의 기지국들로부터 떨어진 거리 정보와 정확한 시간 정보를 산출한 다음 상기 산출된 정보에 삼각법을 적용함으로써, 위도(latitude), 경도(longitude), 및 고도(altitude)에 따른 3차원의 현 위치 정보를 산출할 수 있다. 또는 위치 산출 모듈(117)은 3개 이상의 위성들로부터 전자 장치의 위치 정보를 실시간으로 계속 수신함으로써 위치 정보를 산출할 수 있다. 전자 장치의 위치 정보는 다양한 방법에 의해 획득될 수 있다.

[0052] 방송 수신 모듈(119)은 방송 채널(예컨대, 위성 방송 채널, 지상파 방송 채널 등)을 통하여 외부의 방송 관리 서버로부터 방송 신호(예컨대, TV 방송 신호, 라디오 방송 신호, 데이터 방송 신호 등) 및/또는 상기 방송과 관련된 정보(예컨대, 방송 채널, 방송 프로그램 또는 방송 서비스 제공자에 관련한 정보 등)를 수신할 수 있다.

[0053] 사용자 입력부(120)는 전자 장치의 동작 제어를 위한 입력 데이터를 사용자 입력에 응답하여 발생시킬 수 있다. 사용자 입력부(120)는 키패드(key pad), 돔 스위치(dome switch), 터치패드(정압/정전), 조그셔틀(jog & shuttle), 센서(예컨대, 음성인식센서, 근접센서, 조도센서, 가속도센서, 자이로센서 등) 등을 포함할 수 있다. 또한 사용자 입력부(120)는 전자 장치의 외부에 버튼 형태로 구현될 수 있으며, 또는 터치 패널(touch panel)로 구현될 수도 있다. 본 발명의 실시 예에서 사용자 입력부(120)는 본 발명의 실시 예에 따른 운영체제 업그레이드 동작을 개시(initiation)하기 위한 사용자 입력을 수신하고 그에 따른 입력신호를 발생시킬 수 있다. 예를 들어, 사용자 입력부(120)는 전자 장치의 현재 운영체제 확인 및/또는 현재 운영체제의 업그레이드를 수행하기 위한 사용자 입력을 수신할 수 있고, 상기 사용자 입력에 따른 입력신호를 발생시킬 수 있다.

[0054] 터치스크린(130)은 입력 기능과 표시 기능을 동시에 수행하는 입출력 수단을 나타내며, 표시부(131)와 터치감지부(133)를 포함할 수 있다. 터치스크린(130)은 표시부(131)를 통해 전자 장치 운영에 따른 다양한 화면(예컨대, 메신저 및 그에 의해 운영되는 화면, 통화 발신을 위한 화면, 게임 화면, 동영상 재생 화면, 갤러리(gallery) 화면, 업그레이드 화면 등)을 표시할 수 있다. 터치스크린(130)은 표시부(131)를 통해 특정 화면을 표시하는 중에 터치감지부(133)에 의한 사용자의 터치 이벤트(touch event)가 입력되면, 상기 터치 이벤트에 따른 입력신호를 제어부(170)에게 전달할 수 있다. 제어부(170)는 터치 이벤트를 구분하고, 터치 이벤트에 따른 동작 수행을 제어할 수 있다.

[0055] 표시부(131)는 전자 장치에서 처리되는 정보를 표시(출력)할 수 있다. 예를 들어, 전자 장치가 통화모드인 경우 통화와 관련된 유저 인터페이스(UI, User Interface) 또는 그래픽 유저 인터페이스(GUI, Graphical UI)를 표시할 수 있다. 또한 표시부(131)는 전자 장치가 화상통화 모드 또는 촬영 모드인 경우에는 촬영 또는/및 수신된 영상과 해당 모드 운영과 관련된 UI, GUI를 표시할 수 있다. 표시부(131)는 전자 장치의 운영체제 업그레이드 시 업그레이드 진행과 관련된 UI 또는 GUI를 표시할 수 있다. 예를 들어, 표시부(131)는 업그레이드 진행 시 현재 설치된 운영체제 정보, 수신된 보안 패키지에 따른 보안 운영체제 정보, 업그레이드 실행 및 업그레이드 방식 선택을 위한 다양한 아이템(예컨대, 메뉴, 버튼 등)을 표시할 수 있다. 표시부(131)는 전자 장치의 회전 방향(또는 놓인 방향)에 따라 가로모드에 의한 화면 표시, 세로모드에 의한 화면 표시 및 가로모드와 세로모드 간

의 변화에 따른 화면 전환 표시를 지원할 수 있다.

[0056] 표시부(131)는 액정 디스플레이(LCD, Liquid Crystal Display), 박막 트랜지스터 액정 디스플레이(TFT LCD, Thin Film Transistor-LCD), 발광 다이오드(LED, Light Emitting Diode), 유기 발광 다이오드(OLED, Organic LED), 능동형 OLED(AMOLED, Active Matrix OLED), 플렉서블 디스플레이(flexible display), 벤디드 디스플레이(bended display), 그리고 3차원 디스플레이(3D display) 중에서 적어도 하나를 포함할 수 있다. 이들 중 일부 디스플레이는 투명형 또는 광투명형으로 구성되는 투명 디스플레이(transparent display)로 구현될 수 있다.

[0057] 터치감지부(133)는 상기 표시부(131)에 안착될 수 있으며, 상기 터치스크린(130) 표면에 접촉하는 사용자의 터치 이벤트(예컨대, 탭(tap), 드래그(drag), 스윕(sweep), 플릭(flick), 드래그앤드롭(drag&drop), 드로잉(drawing), 싱글터치(single-touch), 멀티터치(multi-touch), 제스처(gesture)(예컨대, 필기 등), 호버링(hovering) 등)를 감지할 수 있다. 터치감지부(133)는 터치스크린(130) 표면을 통해 사용자의 터치 이벤트를 감지할 시 상기 터치 이벤트가 발생된 좌표를 검출하고, 검출된 좌표를 상기 제어부(170)에게 전달할 수 있다. 즉, 터치감지부(133)는 사용자에 의해 발생되는 터치 이벤트를 감지하고, 감지된 터치 이벤트에 따른 신호를 생성하여 제어부(170)에게 전달할 수 있다. 제어부(170)는 터치감지부(133)에서 전달되는 신호에 의해 터치 이벤트가 발생된 영역에 해당하는 기능 수행을 제어할 수 있다.

[0058] 터치감지부(133)는 본 발명의 실시 예에 따른 운영체제 업그레이드 동작을 개시하기 위한 사용자 입력을 수신하고 그에 따른 입력신호를 발생시킬 수 있다. 예를 들어, 터치감지부(133)는 전자 장치의 현재 운영체제 확인 및/또는 현재 운영체제의 업그레이드를 수행하기 위한 사용자 입력을 수신할 수 있고, 상기 사용자 입력에 따른 입력신호를 발생시킬 수 있다.

[0059] 터치감지부(133)는 표시부(131)의 특정 부위에 가해진 압력 또는 표시부(131)의 특정 부위에 발생하는 정전 용량 등의 변화를 전기적인 입력신호로 변환하도록 구성될 수 있다. 터치감지부(133)는 터치되는 위치 및 면적뿐만 아니라, 적용한 터치 방식에 따라 터치 시의 압력까지도 검출할 수 있도록 구성될 수 있다. 터치감지부(133)에 대한 터치 입력이 있는 경우, 그에 대응하는 신호(들)는 터치 제어기(미도시)로 전달될 수 있다. 터치 제어기(미도시)는 그 신호(들)를 처리한 다음 해당 데이터를 제어부(170)로 전달할 수 있다. 이로써, 제어부(170)는 터치스크린(130)의 어느 영역이 터치되었는지를 확인할 수 있다.

[0060] 오디오 처리부(140)는 제어부(170)로부터 입력 받은 오디오 신호를 스피커(SPK, speaker)(141)로 전송하고, 마이크(MIC, microphone)(143)로부터 입력 받은 음성 등의 오디오 신호를 제어부(170)로 전달하는 기능을 수행할 수 있다. 오디오 처리부(140)는 음성/음향 데이터를 제어부(170)의 제어에 따라 스피커(141)를 통해 가청음으로 변환하여 출력하고 마이크(143)로부터 수신되는 음성 등의 오디오 신호를 디지털 신호로 변환하여 제어부(170)로 전달할 수 있다.

[0061] 스피커(141)는 무선 통신부(110)로부터 수신되거나, 또는 저장부(150)에 저장된 오디오 데이터를 출력할 수 있다. 스피커(141)는 전자 장치에서 수행되는 기능(예컨대, 메신저 실행, 대화 수신, 대화 발신, 이미지 표시, 이미지 변환, 통화 연결 수신, 통화 연결 발신, 촬영, 미디어 컨텐츠 파일 재생, 운영체제 업그레이드 등)과 관련된 음향 신호를 출력할 수도 있다.

[0062] 마이크(143)는 외부의 음향 신호를 입력 받아 전기적인 음성 데이터로 처리할 수 있다. 처리된 음성 데이터는 통화모드인 경우 이동통신 모듈(111)을 통하여 이동통신 기지국으로 송신 가능한 형태로 변환되어 출력될 수 있다. 마이크(143)에는 외부의 음향 신호를 입력 받는 과정에서 발생되는 잡음(noise)을 제거하기 위한 다양한 잡음 제거 알고리즘이 구현될 수 있다.

[0063] 저장부(150)는 제어부(170)의 처리 및 제어를 위한 하나 또는 그 이상의 프로그램들(one or more programs)을 저장할 수 있고, 입/출력되는 데이터들(예컨대, 메신저 데이터(예컨대, 대화 데이터), 컨택트(contact) 정보(예컨대, 유선 또는 무선 전화번호 등), 메시지, 컨텐츠(예컨대, 오디오, 동영상, 이미지) 등)의 임시 저장을 위한 기능을 수행할 수도 있다.

[0064] 상기 하나 또는 그 이상의 프로그램들은, 패키지에 따른 보안 운영체제 업그레이드 시 유저 데이터별 레이블링 정보를 생성하는 동작, 및 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 동작을 실행하는 프로그램을 포함할 수 있다. 또한 상기 하나 또는 그 이상의 프로그램들은 보안 운영체제 업그레이드 개시에 반응하여 유저 데이터에 설정된 플레인 텍스트(plain text)(암호화를 하지 않은 데이터)(예컨대, SEINFO, key value)를 획득하는 동작, 상기 플레인 텍스트에 기초하여 유저 데이터를 식별하는 동작, 및 상기 식별된 유저 데이터에 대한 레이블링 정보를 생성하는 동작을 실행하는 프로그램을 포함할 수 있다. 또한 상기 하나 또는 그

이상의 프로그램들은 유저 데이터의 보안 컨텍스트에 보안 운영체제에 따른 보안 정책에서 명시하는 보안 속성(예컨대, 타입 속성)을 추가하여, 유저 데이터의 기존 보안 컨텍스트를 변경하는 동작을 실행하는 프로그램을 포함할 수 있다.

[0065] 저장부(150)는 전자 장치의 펌웨어(firmware)/소프트웨어 업그레이드를 위해 무선 통신부(110) 또는 인터페이스부(160)를 통해 외부로부터 수신되는 업그레이드 데이터(예컨대, 패키지)를 저장할 수 있다. 또한 저장부(150)는 유저 데이터의 레이블링을 위한 레이블링 정보를 파일 형태로 저장할 수 있다. 또한 저장부(150)는 전자 장치의 기능 운영에 따른 사용 빈도(예컨대, 어플리케이션 사용빈도, 컨텐츠 사용빈도 등), 중요도 및 우선순위도 함께 저장할 수 있다. 저장부(150)에는 터치스크린(130) 상의 터치 입력에 응답하여 출력되는 다양한 패턴(pattern)의 진동 및 음향에 관한 데이터를 저장할 수도 있다. 저장부(150)는 전자 장치의 운영체제, 터치스크린(130)을 이용한 입력 및 표시 제어 동작과 관련된 프로그램, 운영체제의 업그레이드 제어 동작과 관련된 프로그램, 그리고 각 프로그램들의 동작에 의해 발생되는 데이터 등을 지속적으로 또는 일시적으로 저장할 수 있다. 또한 저장부(150)는 후술하는 도 2의 플랫폼(platform)을 저장할 수도 있다.

[0066] 저장부(150)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 마이크로 타입(micro type), 및 카드 타입(예컨대, SD 카드(Secure Digital Card) 또는 XD 카드(eXtream Digital Card)) 등의 메모리와, 디램(DRAM, Dynamic Random Access Memory), SRAM(Static RAM), 롬(ROM, Read-Only Memory), PROM(Programmable ROM), EEPROM(Electrically Erasable PROM), 자기 메모리(MRAM, Magnetic RAM), 자기 디스크(magnetic disk), 및 광디스크(optical disk) 타입의 메모리 중 적어도 하나의 타입의 저장 매체(storage medium)를 포함할 수 있다. 전자 장치는 인터넷 상에서 상기 저장부(150)의 저장 기능을 수행하는 웹 스토리지(web storage)와 관련되어 동작할 수도 있다.

[0067] 인터페이스부(160)는 전자 장치에 연결되는 모든 외부 기기와의 인터페이스 역할을 수행할 수 있다. 인터페이스부(160)는 외부 기기로부터 데이터를 전송 받거나, 전원을 공급받아 전자 장치 내부의 각 구성 요소에 전달하거나, 전자 장치 내부의 데이터가 외부 기기로 전송되도록 할 수 있다. 예를 들어, 유/무선 헤드셋 포트(port), 외부 충전기 포트, 유/무선 데이터 포트, 메모리 카드(memory card) 포트, 식별 모듈이 구비된 장치를 연결하는 포트, 오디오 입/출력(Input/Output) 포트, 비디오 입/출력 포트, 이어폰 포트 등이 인터페이스부(160)에 포함될 수 있다.

[0068] 제어부(170)는 전자 장치의 전반적인 동작을 제어할 수 있다. 예를 들어, 제어부(170)는 음성 통신, 데이터 통신, 화상 통신 등에 관련된 제어를 수행할 수 있다. 제어부(170)는 기존 운영체제 업그레이드 시 유저 데이터를 삭제하지 않으면서 기존 운영체제를 상위 버전의 운영체제(예컨대, 보안 운영체제)로 업그레이드 하는 기능과 관련된 동작을 처리할 수 있고, 이를 처리하는 업그레이드 관리 모듈(175)을 포함할 수도 있다. 상기 업그레이드 관리 모듈(171)은 유저 데이터 관리 모듈(173), 서비스 처리 모듈(175), 레이블링 실행 모듈(177)을 포함할 수 있다. 상기 업그레이드 관리 모듈(175)은 저장부(150) 및 제어부(170) 중 적어도 하나에 저장 또는 탑재(loading)되거나, 별도의 구성으로 구현될 수도 있다. 또한 제어부(170)는 저장부(150)에 저장되는 하나 또는 그 이상의 프로그램을 실행하여 본 발명의 운영체제 업그레이드를 제어하는 하나 또는 그 이상의 프로세서들(one or more processors)로 구현될 수 있다.

[0069] 본 발명의 실시 예에서 제어부(170)는 전자 장치에 설치된 기존 운영체제(예컨대, Android)를 업그레이드할 때, 사용자에 의해 자동 업그레이드 옵션(option)이 설정된 경우 보안 운영체제에 따라 정의된 정책(policy)에 기초하여 유저 데이터를 리레이블링(relabeling)하는 방식에 의한 업그레이드를 제어할 수 있다. 제어부(170)는 보안 운영체제 업그레이드 시 레이블링 정보를 생성하고, 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 것에 의해, 상기 유저 데이터의 삭제 없이 상기 보안 운영체제 업그레이드를 제어할 수 있다.

[0070] 또는 제어부(170)는 전자 장치에 설치된 기존 운영체제를 업그레이드할 때, 사용자에 의해 수동 업그레이드 옵션이 설정된 경우, 유저 데이터와 관계없이 공장 초기화(factory reset)와 같은 상태에서 새로운 운영체제(이하, 보안 운영체제(Security OS), 예컨대, SE(Security Enhanced) OS 등)로 설치하는 방식에 의한 업그레이드를 제어하거나, 보안 운영체제에 따라 정의된 정책에 기초하여 유저 데이터를 리레이블링 하는 방식에 의한 업그레이드를 제어할 수 있다. 이러한 업그레이드 방식은 사용자 선택에 따라 결정될 수 있다.

[0071] 예를 들어, 제어부(170)는 서버로부터 운영체제의 보안 업그레이드를 위한 보안 패키지(security package)가 수신되면, 상기 보안 패키지에 기초하여 운영체제의 업그레이드 개시를 판단할 수 있다. 제어부(170)는 업그레이드 개시를 판단하면, 운영체제의 업그레이드 이벤트 발생을 사용자에게 통지할 수 있다. 제어부(170)는 업그레이드 개시 판단 시 운영체제 업그레이드 정보를 표시부(131)를 통해 출력할 수 있고, 진동 및/또는 사운드 등을

통해 업그레이드 이벤트 발생을 피드백(feedback)할 수 있다. 상기 업그레이드 정보는 전자 장치에 현재 설치된 기존 운영체제 정보(예컨대, 운영체제 이름, 운영체제 버전, 최종 업그레이드 날짜 등), 보안 패키지에 따른 보안 운영체제 정보(예컨대, 운영체제 이름, 운영체제 버전 등) 등을 포함할 수 있다. 또한 제어부(170)는 업그레이드 정보와 함께 업그레이드 실행 여부를 선택받기 위한 선택 버튼, 업그레이드 실행 방식을 선택받기 위한 선택 버튼 등을 더 제공할 수 있다. 그리고 제어부(170)는 사용자에 의해 선택되는 업그레이드 방식에 따라 운영체제의 업그레이드 동작을 처리할 수 있다.

[0072] 제어부(170)(예컨대, 유저 데이터 관리 모듈(173))는 전자 장치에서 설치/저장되는 유저 데이터(예컨대, 어플리케이션 등), 각 유저 데이터가 수행하는 기능 등을 관리할 수 있다. 제어부(170)(예컨대, 유저 데이터 관리 모듈(173))는 유저 데이터를 기본 패키징 단위(예컨대, 특정 파일 포맷의 파일(예컨대, 안드로이드 플랫폼의 경우 APK 파일))에서 설정된 플레인 텍스트(plain text)(암호화를 하지 않은 데이터)(예컨대, SEINFO, key value)를 추출하고, 추출된 플레인 텍스트를 관리할 수 있다.

[0073] 제어부(170)(예컨대, 서비스 처리 모듈(175))는 기존 운영체제에 보안 운영체제를 적용하는 운영체제 업그레이드 시, 상기 보안 운영체제에서 명시된 보안 정책에 따라 상기 유저 데이터를 리레이블링 하기 위한 레이블링 정보를 생성할 수 있다. 제어부(170)(예컨대, 서비스 처리 모듈(175))는 플레인 텍스트에 기반하여 유저 데이터를 식별할 수 있고, 각 유저 데이터에 대한 레이블링 정보를 생성할 수 있다. 상기 레이블링 정보는 상기 보안 운영체제에 따른 보안 정책에서 명시되는 보안 컨텍스트의 타입 속성을 포함할 수 있다. 제어부(170)(예컨대, 서비스 처리 모듈(175))는 각 유저 데이터에 대응하게 생성하는 레이블링 정보를 특정 파일(예컨대, .xml)로 저장부(150)에 저장할 수 있다.

[0074] 제어부(170)(예컨대, 레이블링 실행 모듈(177))는 보안 운영체제의 업그레이드 시, 상기 레이블링 정보에 기초하여 전자 장치의 유저 데이터에 대한 리레이블링을 제어할 수 있다. 제어부(170)(예컨대, 레이블링 실행 모듈(177))는 유저 데이터의 보안 컨텍스트를 상기 레이블링 정보가 포함되도록 리레이블링할 수 있다. 예를 들어, 제어부(170)(예컨대, 레이블링 실행 모듈(177))는 유저 데이터의 보안 컨텍스트에 상기 보안 운영체제에 따른 보안 정책에서 명시하는 타입 속성을 추가할 수 있다.

[0075] 본 발명의 실시 예에 따른 제어부(170)는 전자 장치의 동작 중에 유저 데이터의 리레이블링을 위한 인터럽트를 감지할 수 있다. 예를 들어, 제어부(170)는 전자 장치가 동작하는 중에 운영체제의 보안 정책에 따라 리레이블링 되지 않은 유저 데이터를 검출할 수 있다. 또는 제어부(170)는 전자 장치가 동작하는 중에 변경(예컨대, 신규 설치 또는 업그레이드 등)되는 유저 데이터의 컨텍스트를 체크할 수 있고, 해당 유저 데이터가 운영체제의 보안 정책을 기반으로 동작될 수 있는지(예컨대, 보안 정책에 따른 레이블링 정보를 가지는지) 여부를 판단할 수도 있다. 제어부(170)는 상기 인터럽트에 반응하여 해당 유저 데이터를 위한 레이블링 정보에 따라 상기 유저 데이터의 리레이블링을 제어할 수 있다.

[0076] 본 발명의 실시 예에 따른 제어부(170)는 상기의 기능 외에 전자 장치의 통상적인 기능과 관련된 각종 동작을 제어할 수 있다. 예를 들어, 제어부(170)는 특정 어플리케이션 실행 시 그의 운영 및 화면 표시를 제어할 수 있다. 또한 제어부(170)는 터치 기반의 입력 인터페이스(예컨대, 터치스크린(130))에서 지원하는 다양한 터치 이벤트 입력에 대응하는 입력신호를 수신하고 그에 따른 기능 운용을 제어할 수 있다. 또한 제어부(170)는 유선통신 기반 또는 무선통신 기반으로 각종 데이터의 송수신을 제어할 수도 있다.

[0077] 전원 공급부(180)는 제어부(170)의 제어에 의해 외부의 전원, 내부의 전원을 인가받아 각 구성 요소들의 동작에 필요한 전원을 공급할 수 있다.

[0078] 본 발명의 다양한 실시 예들은 소프트웨어(software), 하드웨어(hardware) 또는 이들의 조합된 것을 이용하여 컴퓨터(computer) 또는 이와 유사한 장치로 읽을 수 있는 기록 매체 내에서 구현될 수 있다. 하드웨어적인 구현에 의하면, 본 발명의 실시 예들은 ASICs(Application Specific Integrated Circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서(processors), 제어기(controllers), 마이크로 컨트롤러(micro-controllers), 마이크로프로세서(microprocessors), 기타 기능 수행을 위한 전기적인 유닛(unit) 중 적어도 하나를 이용하여 구현될 수 있다.

[0079] 여기서, 상기 기록 매체는 보안 운영체제에 의한 운영체제 업그레이드 개시를 감지하는 동작, 유저 데이터별 레이블링 정보를 생성하는 동작, 상기 레이블링 정보에 기초하여 유저 데이터를 리레이블링 하는 동작을 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체를 포함할 수 있다.

[0080] 그리고 일부의 경우에 본 명세서에서 설명되는 실시 예들이 제어부(170) 자체로 구현될 수 있다. 또한 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시 예들은 별도의 소프트웨어 모듈들로 구현될 수도 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 동작을 수행할 수 있다.

[0081] 도 2는 본 발명의 실시 예에 따른 기능을 처리하는 전자 장치의 플랫폼 구조의 예시를 개략적으로 도시한 도면이다.

[0082] 상기 도 2에 도시된 바와 같이, 본 발명의 실시 예에 따른 전자 장치의 플랫폼은, 운영체제 기반의 소프트웨어를 구비할 수 있다.

[0083] 상기 도 2를 참조하면, 본 발명의 실시 예에 따른 전자 장치는 커널(Kernel)(210), 프레임워크(Framework)(230), 그리고 어플리케이션(Application)(250)을 포함하여 설계될 수 있다.

[0084] 상기 커널(210)은 운영체제의 핵심으로써, 전자 장치의 구동 시 하드웨어 드라이버(driver) 구동, 전자 장치 내의 하드웨어와 프로세서의 보안, 시스템 자원의 효율적 관리, 메모리 관리, 하드웨어 추상화(hardware abstraction)에 의한 하드웨어에 대한 인터페이스 제공, 멀티 프로세스, 그리고 서비스 연결 관리 등 중 적어도 하나를 수행할 수 있다. 상기 커널(210)은 본 발명의 실시 예에서 보안 운영체제 업그레이드와 관련된 동작을 처리하는 레이블링 유틸리티(labeling utility)(215)를 포함할 수 있다.

[0085] 상기 레이블링 유틸리티(215)는 업그레이드 하는 보안 운영체제의 정책에 대응하여, 유저 데이터들에 대한 리레이블링(relebeling)을 처리한다. 예를 들어, 레이블링 유틸리티(215)는 서비스 매니저(235)로부터 유저 데이터들에 대한 레이블링 실행 명령을 수신할 수 있다. 레이블링 유틸리티(215)는 레이블링 실행 명령에 응답하여, 서비스 매니저(235)에 의해 생성된 파일에 기초하여 유저 데이터들의 정책 타입(policy type)을 레이블링 할 수 있다. 즉, 레이블링 유틸리티(215)는 유저 데이터별 보안 컨텍스트에서 정책 타입을 추가하는 레이블링을 통해, 유저 데이터에 대한 리레이블링 처리할 수 있다. 상기 타입(type)은 객체에 주어진 보안 속성을 나타내며, 그 객체에 어떤 주체가 접근할 수 있는지를 결정하는 부분이다. 타입의 보안 속성은 일반적으로 sysadm_t와 같이 마지막에 '_t'로 표시될 수 있다.

[0086] 예를 들어, 레이블링 유틸리티(215)는 아래의 <표 4>와 같이 기존 운영체제의 정책을 가지는 유저 데이터의 컨텍스트를 리레이블링 하여, 보안 운영체제의 정책을 가지는 유저 데이터의 컨텍스트로 변경할 수 있다.

표 4

[0087]

user_u:system_r (identity:role)	->	user_u:system_r:unconfined_t (identity:role:type)

[0088] 상기 커널(210) 내의 하드웨어 드라이버는 디스플레이 드라이버(Display Driver), 입력 장치 드라이버(예컨대, 키패드 드라이버), 와이파이 드라이버(WiFi Driver), 블루투스 드라이버(Bluetooth Driver), USB 드라이버, 오디오 드라이버(Audio Driver), 파워 관리자(Power Management), 바인더(IPC) 드라이버(Binder Driver), 카메라 드라이버(Camera Driver), 메모리 드라이버(예컨대, 플래시 메모리 드라이버(Flash Memory Driver)) 등이 포함될 수 있다.

[0089] 본 발명의 실시 예에 따르면, 기존 운영체제를 보안 운영체제로 업그레이드할 시, 유저 데이터들에 대해 보안 운영체제에 따른 정책에 기초하여 유저 데이터들에 대응하는 모든 보안 컨텍스트들을 리레이블링 처리함으로써, 유저 데이터들의 모든 보안 컨텍스트들의 레이블링 정보를 사용할 수 있는 준비가 된 상태로 설정할 수 있다.

[0090] 본 발명의 실시 예에서는 유저 데이터들의 기존 보안 컨텍스트에 정책 타입(policy type)을 추가하고, 추가된 정책 타입에 따라 역할(role)과 사용자(user) 별로 제어가 이루어지도록 한다. 따라서 유저 데이터의 리레이블링을 통해 유저 데이터에 대해서도 보안 운영체제에 기초하는 보안을 적용할 수 있다. 예를 들어, 기존 리눅스 보안 방식(예컨대, DAC)으로 파일 퍼미션을 체크하여 허가 되었는지 검사하고, 허가된 경우 MAC 방식으로 보안 컨텍스트의 정책 타입을 검사하여 해당 접근에 대한 거부(denial) 또는 허가(allow)를 처리할 수 있다.

[0091] 상기 프레임워크(230)는 운영체제의 API(Application Program Interface)를 나타내며, 어플리케이션(250) 계층

내 어플리케이션들의 기반이 되는 프로그램을 포함할 수 있다. 프레임워크(230)는 어떠한 어플리케이션과도 호환 가능하며, 컴포넌트(component)의 재사용, 이동 또는 교환이 가능할 수 있다. 프레임워크(230)는 지원 프로그램, 다른 소프트웨어 구성 요소들을 연결시켜 주는 프로그램 등을 포함할 수 있다. 상기 프레임워크(230)는 본 발명의 실시 예에서 보안 운영체제 업그레이드와 관련된 동작을 처리하는 상기 패키지 매니저(231), 업그레이드 매니저(Upgrade Manager)(233), 그리고 서비스 매니저(235)를 포함할 수 있다.

[0092] 상기 패키지 매니저(231)는 전자 장치에 어떤 유저 데이터(예컨대, 어플리케이션)들이 설치되어 있는지, 각각의 유저 데이터들이 어떤 기능을 수행하는지 등을 관리할 수 있다. 본 발명의 실시 예에서 패키지 매니저(231)는 전자 장치에 설치/저장된 유저 데이터(예컨대, 어플리케이션 등)를 기본 패키징 단위(예컨대, 특정 파일 포맷의 파일(예컨대, APK 파일))로 분석할 수 있고, 상기 기본 패키징 단위에서 플레인 텍스트(예컨대, SEINFO, key value)를 추출하여 관리할 수 있다. 본 발명의 실시 예에서 패키지 매니저(231)는 주기적 또는 특정 이벤트(예컨대, 운영체제 업그레이드, 어플리케이션 설치) 발생 시 플레인 텍스트를 추출하여 관리할 수 있도록 한다.

[0093] 상기 업그레이드 매니저(233)는 무선 통신부(110)(예컨대, 이동통신 모듈(111)) 또는 인터페이스부(160)(예컨대, USB 포트)로부터 입력되어 상기 커널(210)을 통해 수신되는 패키지에 따라 운영체제 업그레이드를 결정한다. 업그레이드 매니저(233)는 유저 리레이블링하는 방식에 의한 업그레이드 시 서비스 매니저(235)에게 레이블링 정보 확보 동작을 개시하도록 명령할 수 있다. 업그레이드 매니저(233)의 역할은 서비스 매니저(235)에서 직접 수행될 수도 있고, 이러한 경우 업그레이드 매니저(233)의 구성은 생략될 수 있다.

[0094] 상기 서비스 매니저(235)는 운영체제의 업그레이드 개시를 감지되면, 유저 데이터에 대한 플레인 텍스트를 획득할 수 있다. 서비스 매니저(235)는 패키지 매니저(233)에 의해 추출 및 관리되는 플레인 텍스트를 서비스 매니저(235)로부터 호출하여 획득할 수 있다. 서비스 매니저(235)는 획득된 플레인 텍스트에 기초하여 유저 데이터에 대한 레이블링 정보를 생성하여 파일로 저장할 수 있다. 상기 레이블링 정보는 보안 운영체제에서 정의되는 보안 정책(예컨대, 보안 컨텍스트에서 타입 속성 부분 포함)에 기초하여 생성될 수 있다. 본 발명의 실시 예에서 서비스 매니저(235)는 패키지 매니저(233)의 플레인 텍스트 생성 및 관리 동작을 처리하도록 구현될 수도 있다. 이러한 경우 서비스 매니저(235)는 유저 데이터 분석, 유저 데이터들의 플레인 텍스트 추출, 추출된 플레인 텍스트 관리 등의 동작을 더 수행할 수 있다. 그리고 서비스 매니저(235)는 운영체제의 업그레이드 개시에 반응하여 레이블링 유틸리티(215)에 레이블링 실행 명령을 전달할 수 있다.

[0095] 또한 상기 프레임워크(230)는 그 도시는 생략하였으나, 액티비티 매니저(Activity Manager), 패키지 매니저(Package Manager)(231), 윈도우 매니저(Windows Manager), 전화통신 매니저(Telephony Manager), 컨텐츠 프로바이더(Content Provider), 자원 매니저(Resource Manager), 뷰 시스템(View System), 위치 매니저(Location Manager), 통지 매니저(Notification Manager), XMPP 서비스(Extensible Messaging and Presence Protocol Service) 등이 포함될 수 있다.

[0096] 상기 어플리케이션(250)은 전자 장치 내에서 구동되어 표시 가능한 다양한 프로그램을 포함할 수 있다. 예를 들어, 전자 장치 내의 다양한 메뉴 등에 관한 UI 어플리케이션과, 외부 장치 또는 네트워크를 통해 다운로드 되어 저장되며, 사용자에 의해 설치 또는 삭제가 자유로운 어플리케이션 등을 포함할 수 있다. 이러한 어플리케이션을 통해, 네트워크 접속에 의한 인터넷 전화 서비스, 주문형 비디오(VOD) 서비스, 웹 앨범 서비스, SNS, 위치기반 서비스(LBS), 지도 서비스, 웹 검색 서비스, 애플리케이션 검색 서비스, 문자/멀티미디어 메시지 서비스, 메일 서비스, 주소록 서비스, 미디어 재생 서비스 등이 수행될 수 있다. 또한, 게임, 일정관리 등 다양한 기능이 수행될 수 있다.

[0097] 이 외에도, 본 발명의 플랫폼은 미들웨어(middleware)(미도시)를 더 포함할 수 있다. 상기 미들웨어(미도시)는 커널(210)과 어플리케이션(250) 계층 사이에 위치할 수 있으며, 다른 하드웨어 또는 소프트웨어 간에 데이터를 주고받을 수 있도록 중간에서 매개 역할을 할 수 있다. 이에 의해, 표준화된 인터페이스 제공이 가능하며, 다양한 환경 지원, 및 체계가 다른 업무와 상호 연동이 가능해질 수 있다.

[0098] 한편, 이상에서 살펴본 바와 같은 플랫폼은 본 발명의 실시 예에 따른 전자 장치는 물론, 그 외 다양한 디바이스에서 범용으로 사용 가능하다. 그리고 본 발명의 실시 예에 따른 플랫폼은 앞서 살펴본 바와 같은 저장부(150) 및 제어부(170) 중 적어도 하나 또는 별도의 프로세서(미도시)에, 저장 또는 탑재(loading)될 수도 있다.

[0099] 도 3은 본 발명의 실시 예에 따른 전자 장치에서 운영체제 업그레이드 동작을 설명하기 위해 개략적으로 도시한 도면이다.

[0100] 상기 도 3을 참조하면, 업그레이드 매니저(233)는 운영체제 업그레이드 개시를 감지하면(310), 운영체제 업그레

이드 방식을 판단할 수 있다. 업그레이드 매니저(233)는 유저 데이터를 제외한 업그레이드인 경우 공장 초기화 과정에 의한 업그레이드가 이루어지도록 동작할 수 있다. 업그레이드 매니저(233)는 기존 운영체제에 새로운 운영체제(예컨대, 보안 운영체제)를 적용하는 업그레이드인 경우 서비스 매니저(235)에게 운영체제의 업그레이드에 따른 유저 데이터 리레이블링 동작을 수행하도록 명령할 수 있다(320).

[0101] 서비스 매니저(235)는 업그레이드 매니저(233)의 명령에 반응하여 패키지 매니저(231)로부터 플레인 텍스트(예컨대, SEINFO, key value)를 획득할 수 있다(330). 여기서, 패키지 매니저(231)는 유저 데이터에 대응하는 파일(예컨대, APK 파일)로부터 플레인 텍스트(예컨대, SEINFO, key value)를 추출하여 관리할 수 있다.

[0102] 서비스 매니저(235)는 획득된 플레인 텍스트에 기초하여 유저 데이터의 보안 컨텍스트 리레이블링에 필요한 레이블링 정보를 생성하여 파일(400)로 저장할 수 있다(340). 예를 들어, 서비스 매니저(235)는 플레인 텍스트에 기초하여 유저 데이터를 식별할 수 있고, 유저 데이터별 컨텍스트(특히, 보안 컨텍스트)에 보안 운영체제에 따른 새로운 보안 정책을 레이블링할 수 있는 레이블링 정보(특히, 보안 컨텍스트에서 타입 속성 부분)를 포함하는 유저 데이터별 컨텍스트들을 특정 파일(예컨대, .xml)로 저장부(150)에 저장할 수 있다.

[0103] 서비스 매니저(235)는 업그레이드 매니저(233)의 명령에 반응하여 상기 파일 생성과 함께 레이블링 유틸리티(215)에게 유저 데이터에 대한 레이블링을 실행하도록 명령할 수 있다(350).

[0104] 레이블링 유틸리티(215)는 서비스 매니저(235)의 레이블링 실행 명령에 응답하여, 저장부(150)로부터 레이블링 정보가 기록된 파일을 획득할 수 있다(360). 레이블링 유틸리티(215)는 획득된 파일에 기초하여 유저 데이터의 보안 컨텍스트를 리레이블링 할 수 있다. 예를 들어, 레이블링 유틸리티(215)는 유저 데이터의 컨텍스트에 상기 파일에 포함된 레이블링 정보에 따라 보안 운영체제에서 명시된 정책에 대응하는 타입을 추가하는 레이블링 동작을 처리할 수 있다. 레이블링 유틸리티(215)는 전자 장치에서 설치/저장된 모든 유저 데이터들의 보안 컨텍스트들을 리레이블링 함으로써, 유저 데이터들의 보안 컨텍스트들의 레이블링 정보를 사용할 수 있는 준비가 된 상태로 설정할 수 있다.

[0105] 도 4는 본 발명의 실시 예에 따른 전자 장치에서 운영체제 업그레이드 동작을 설명하기 위해 개략적으로 도시한 도면이다.

[0106] 상기 도 4에서는 서비스 매니저(235)가 패키지 매니저(231)와 업그레이드 매니저(233)의 역할을 모두 포함하는 경우의 동작 예시를 나타낸 것이다. 따라서 상기 도 4에서 서비스 매니저(235)의 동작을 제외하고는 앞서 설명한 바와 같은 도 3의 동작에 대응할 수 있으며, 그에 대한 설명은 생략하기로 한다.

[0107] 상기 도 4를 참조하면, 서비스 매니저(235)는 운영체제 업그레이드 개시를 감지하면(410), 유저 데이터에 대응하는 파일(예컨대, APK 파일)로부터 플레인 텍스트(예컨대, SEINFO, key value)를 추출할 수 있다. 서비스 매니저(235)는 전자 장치에 설치/저장된 유저 데이터를 분석하고 각 유저 데이터들의 플레인 텍스트를 추출할 수 있다. 상기 플레인 텍스트는 서비스 매니저(235)에 의해 미리 추출되어 관리될 수도 있다. 서비스 매니저(235)는 획득된 플레인 텍스트에 기초하여 유저 데이터의 보안 컨텍스트의 리레이블링에 필요한 레이블링 정보를 생성하여 파일(400)로 저장(340)하면서, 레이블링 유틸리티(215)에게 유저 데이터에 대한 레이블링을 실행하도록 명령할 수 있다(350).

[0108] 상기 도 4에 도시된 바와 같이, 서비스 매니저(235)가 패키지 매니저(231)와 업그레이드 매니저(233)의 동작을 수행함에 따라, 본 발명의 실시 예에 따른 전자 장치의 보안 강화를 지원하기 위한 보안 운영체제 업그레이드 동작에서 패키지 매니저(231)와 업그레이드 매니저(233)의 구성 및 그들에 의한 동작은 생략될 수 있다. 예를 들어, 도 3과 도 4를 살펴보면, 도 4에서는 도 3의 310동작이 410동작으로 대체되고, 업그레이드 매니저(233)와 320동작이 생략되며, 패키지 매니저(231)와 330동작이 생략됨을 알 수 있다.

[0109] 도 5는 본 발명의 실시 예에 따른 전자 장치에서 운영체제 업그레이드를 위한 운영 방법을 도시한 흐름도이다.

[0110] 상기 도 5를 참조하면, 제어부(170)는 운영체제 업그레이드 개시(OS Upgrade initiation)를 감지할 수 있다(501단계). 예를 들어, 제어부(170)는 무선 통신부(110) 또는 인터페이스부(160)를 통해 기존 운영체제의 보안 업그레이드를 위한 보안 패키지가 수신되면(예컨대, OTA에 의한 운영체제 업그레이드의 경우), 운영체제 업그레이드 개시인 것으로 판단할 수 있다.

[0111] 제어부(170)는 운영체제 업그레이드 개시에 응답하여 유저 데이터에 대응하는 플레인 텍스트를 획득할 수 있다(503단계). 예를 들어, 제어부(170)는 전자 장치에 설치/저장된 유저 데이터를 확인하고 각 유저 데이터의 파일(예컨대, APK 파일)로부터 플레인 텍스트(예컨대, SEINFO, key value)를 추출할 수 있다.

[0112] 제어부(170)는 획득된 플레인 텍스트에 기초하여 각 유저 데이터에 대한 레이블링 정보를 생성할 수 있고, 각 유저 데이터별로 레이블링 정보가 기록된 하나 또는 그 이상의 파일들을 생성할 수 있다(505단계). 상기 레이블링 정보는 상기 보안 패키지에 따른 보안 정책에서 정의된 보안 컨텍스트의 타입 속성을 포함할 수 있다.

[0113] 제어부(170)는 레이블링 정보를 포함하는 상기 파일에 기초하여 각 유저 데이터의 컨텍스트를 리레이블링 할 수 있다(507단계). 예를 들어, 제어부(170)는 각 유저 데이터의 보안 컨텍스트에 상기 파일의 레이블링 정보에 기초하여 타입 속성을 추가하여 유저 데이터의 기존 보안 컨텍스트를 새로운 보안 정책이 명시된 보안 컨텍스트로 변경할 수 있다.

[0114] 도 6은 본 발명의 실시 예에 따른 전자 장치에서 운영체제 업그레이드를 위한 운영 방법을 도시한 흐름도이다.

[0115] 상기 도 6을 참조하면, 제어부(170)는 운영체제 업그레이드 개시를 감지할 수 있다(601단계). 예를 들어, 제어부(170)는 외부로부터 운영체제의 업그레이드를 위한 패키지가 수신되면, 운영체제 업그레이드 개시인 것으로 판단할 수 있다.

[0116] 제어부(170)는 운영체제 업그레이드 개시를 감지하면, 운영체제 업그레이드가 기존 운영체제에 보안성 강화를 위한 보안 운영체제를 적용하는 업그레이드인지, 또는 보안 운영체제의 설치인지 판단할 수 있다. 이는 사용자 입력에 따라 선택될 수 있다.

[0117] 제어부(170)는 보안 운영체제의 업그레이드인 것으로 판단하면(603단계의 YES), 전자 장치에 설치/저장된 유저 데이터를 확인하고(605단계), 확인된 각 유저 데이터의 보안 컨텍스트를 리레이블링하기 위한 레이블링 정보를 생성할 수 있다(607단계). 상기 레이블링 정보는 상기 보안 운영체제의 패키지에 따른 보안 정책에서 명시된 보안 컨텍스트의 타입 속성을 포함할 수 있다.

[0118] 제어부(170)는 생성된 레이블링 정보에 따라 유저 데이터를 리레이블링 할 수 있다(609단계). 예를 들어, 제어부(170)는 유저 데이터의 보안 컨텍스트에 레이블링 정보에 따른 타입 속성을 추가할 수 있다.

[0119] 제어부(170)는 유저 데이터의 리레이블링 후 리부팅(rebooting)을 제어할 수 있다(611단계).

[0120] 제어부(170)는 보안 운영체제의 설치인 것으로 판단하면(603단계의 NO), 전자 장치에 미리 설치된 유저 데이터의 레이블링을 위한 공장 초기화를 제어할 수 있다(621단계).

[0121] 제어부(170)는 전자 장치가 공장 초기화 상태가 되면 전자 장치를 리부팅하고 유저 데이터를 설치할 수 있다(623단계). 여기서, 설치되는 유저 데이터는 보안 운영체제의 패키지에 따른 보안 정책이 명시된 보안 컨텍스트가 설정될 수 있다.

[0122] 이상에서 살펴본 바와 같이, 본 발명의 실시 예에서는 운영체제의 업그레이드 시 유지 데이터의 레이블링 정보를 생성하고, 상기 레이블링 정보에 기초하여 유지 데이터를 리레이블링 하도록 함으로써, 전자 장치에서 유저 데이터의 삭제 없이도 운영체제의 업그레이드를 지원할 수 있다. 또한 업그레이드된 운영체제의 보안 정책을 기반으로 유저 데이터를 리레이블링 함에 따라 업그레이드된 운영체제에서도 모든 유저 데이터의 사용이 가능하도록 할 수 있다.

[0123] 한편, 본 발명의 실시 예에 따르면, 전자 장치의 유저 데이터는 사용자 선택에 따라 설치되거나 업그레이드될 수 있다. 본 발명의 실시 예에 따르면, 전자 장치는 동작 중에 유저 데이터의 리레이블링을 위한 인터럽트를 감지할 수 있다. 예를 들어, 전자 장치는 동작 중에 운영체제의 보안 정책에 따라 리레이블링 되지 않은 유저 데이터를 검출할 수 있다. 또는 전자 장치는 동작 중에 변경(예컨대, 신규 설치 또는 업그레이드 등)되는 유저 데이터의 컨텍스트를 체크할 수 있고, 해당 유저 데이터가 운영체제의 보안 정책을 기반으로 동작될 수 있는지(예컨대, 보안 정책에 따른 레이블링 정보를 가지는지) 여부를 판단할 수도 있다.

[0124] 전자 장치는 동작 중에 상기 유저 데이터의 리레이블링을 위한 인터럽트가 감지되면, 상기 인터럽트에 반응하여 해당 유저 데이터를 운영체제의 보안 정책에 따라 리레이블링 할 수 있다. 예를 들어, 전자 장치는 해당 유저 데이터가 동작할 수 없는 것으로 판단하면, 해당 유저 데이터에 대한 레이블링 정보 생성 및 상기 레이블링 정보를 기반으로 해당 유저 데이터의 컨텍스트를 변경 즉, 유지 데이터의 리레이블링을 수행할 수도 있다.

[0125] 한편, 본 발명의 다양한 실시 예에 따르면, 각각의 모듈들은 소프트웨어, 펌웨어, 하드웨어 또는 그 조합으로 구성될 수 있다. 또한 일부 또는 전체 모듈은 하나의 개체(entity)에 구성되되, 각 해당 모듈의 기능을 동일하게 수행되도록 구성할 수 있다. 또한 본 발명의 다양한 실시 예에 따르면, 각각의 동작들은 순차적, 반복적 또는 병렬적으로 실행될 수 있다. 또한 일부 동작들은 생략되거나, 다른 동작들이 추가되어 실행될 수도 있다.

[0126] 상술한 바와 같은 본 발명의 다양한 실시 예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터로 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터로 판독 가능한 기록 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 기록 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0127] 상기 컴퓨터로 판독 가능한 기록 매체에는 하드디스크, 플로피디스크 및 자기 테이프와 같은 마그네틱 매체(Magnetic Media)와, CD-ROM(Compact Disc Read Only Memory), DVD(Digital Versatile Disc)와 같은 광기록 매체(Optical Media)와, 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media)와, 그리고 ROM(Read Only Memory), RAM(Random Access Memory), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함될 수 있다. 또한 프로그램 명령에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지다.

[0128] 그리고 본 명세서와 도면에 개시된 실시 예들은 본 발명의 내용을 쉽게 설명하고, 이해를 돕기 위해 특정 예를 제시한 것일 뿐이며, 본 발명의 범위를 한정하고자 하는 것은 아니다. 따라서 본 발명의 범위는 여기에 개시된 실시 예들 이외에도 본 발명의 기술적 사상을 바탕으로 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

부호의 설명

[0129] 110: 무선 통신부 120: 사용자 입력부

130: 터치스크린 131: 표시부

133: 터치감지부 140: 오디오 처리부

150: 저장부 160: 인터페이스부

170: 제어부 171: 업그레이드 관리 모듈

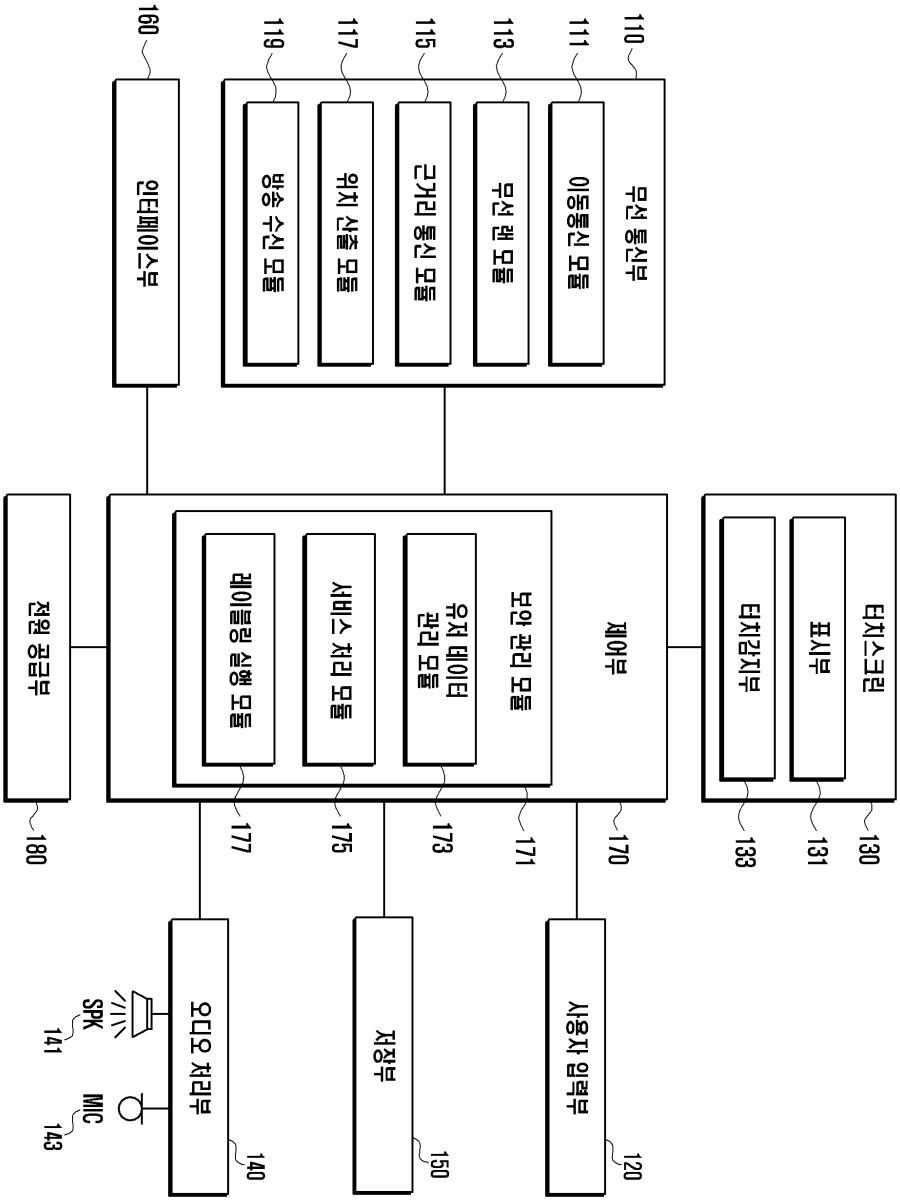
173: 유저 데이터 관리 모듈 175: 서비스 처리 모듈

177: 레이블링 실행 모듈 215: 레이블링 유틸리티

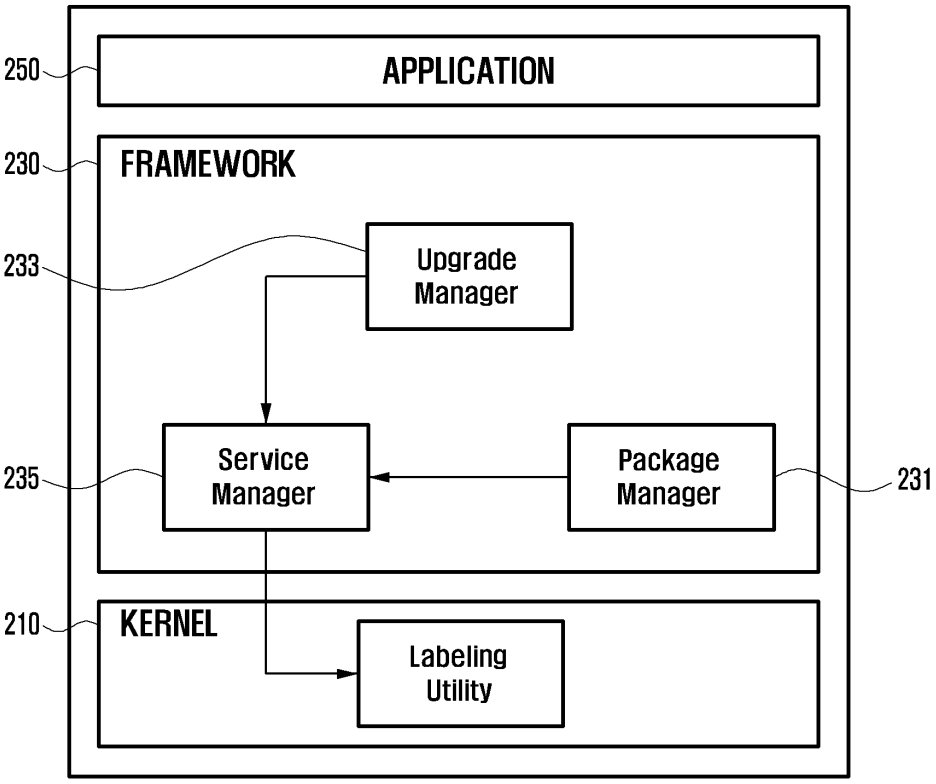
231: 패키지 매니저 235: 서비스 매니저

도면

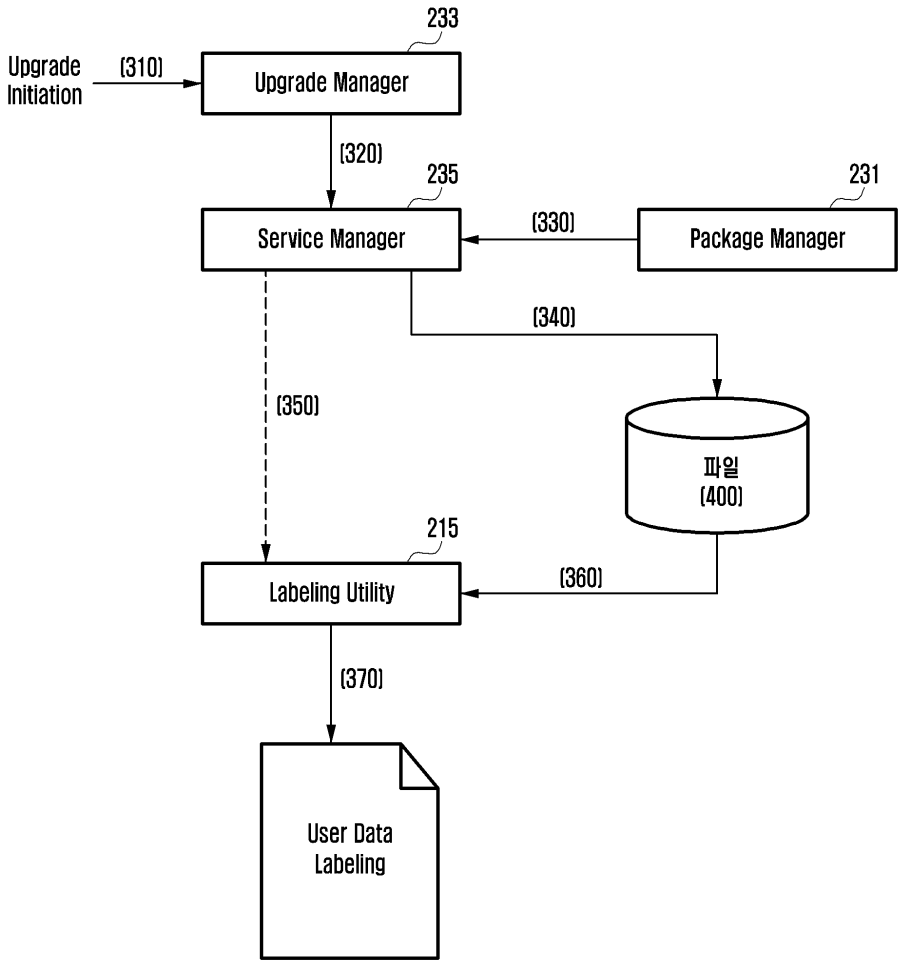
도면1


160
인터페이스부
119
방송 수신 모듈
117
위치 산출 모듈
115
근거리 통신 모듈
113
무선 랜 모듈
111
이동통신 모듈
110
무선 통신부
180
전원 공급부
177
레이블링 실행 모듈
175
서비스 처리 모듈
173
유저 데이터 관리 모듈
171
보안 관리 모듈
170
제어부
133
터치감지부
131
표시부
130
터치스크린
SPK
141
MIC
143
오디오 처리부
140
저장부
150
사용자 입력부
120

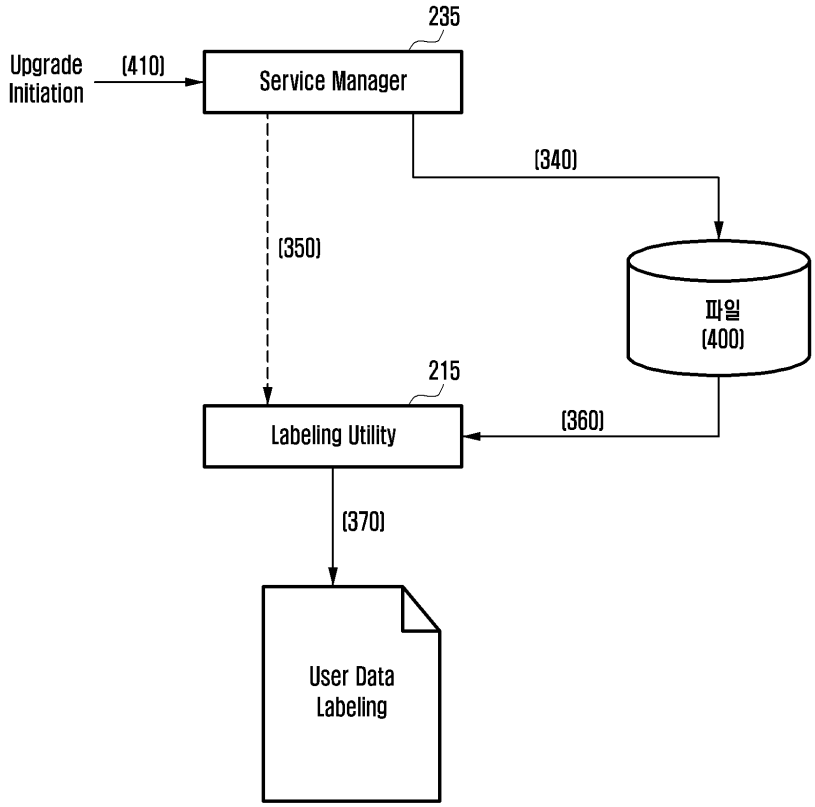
도면2


250
APPLICATION
230
FRAMEWORK
233
Upgrade Manager
235
Service Manager
Package Manager
231
210
KERNEL
Labeling Utility

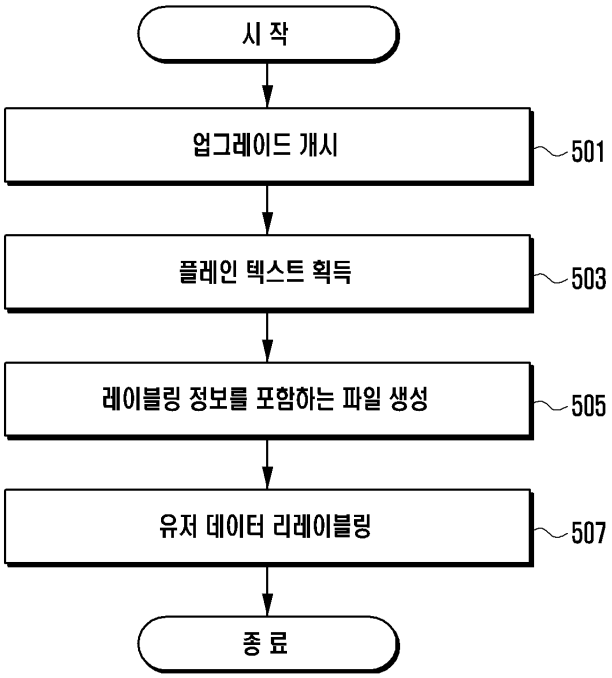
도면3


233
Upgrade Initiation
(310)
Upgrade Manager
(320)
235
231
Service Manager
(330)
Package Manager
(340)
(350)
파일
(400)
215
Labeling Utility
(360)
(370)
User Data Labeling

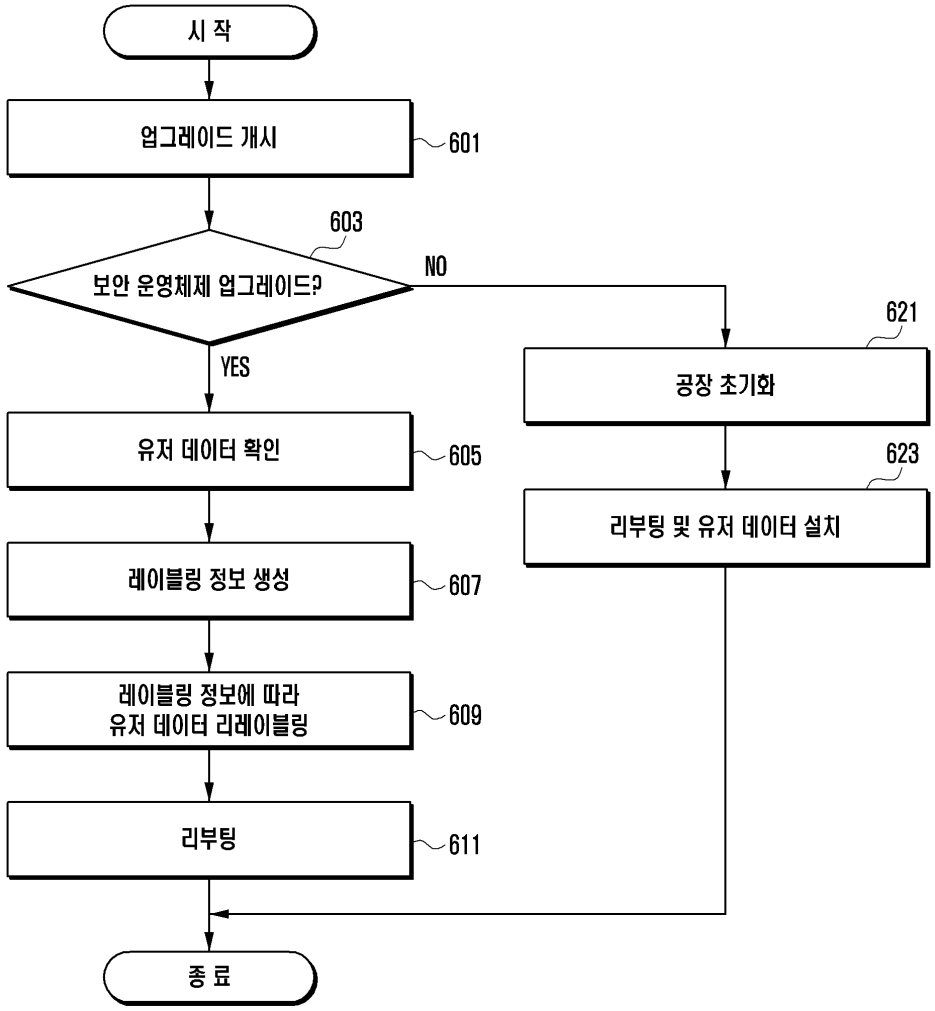
도면4


235
Upgrade Initiation
(410)
Service Manager
(340)
(350)
파일
(400)
215
Labeling Utility
(360)
(370)
User Data Labeling

도면5


시 작
업그레이드 개시
501
플레인 텍스트 획득
503
레이블링 정보를 포함하는 파일 생성
505
유저 데이터 리레이블링
507
종 료

도면6


시 작
업그레이드 개시
601
603
보안 운영체제 업그레이드?
NO
YES
621
공장 초기화
623
리부팅 및 유저 데이터 설치
유저 데이터 확인
605
레이블링 정보 생성
607
레이블링 정보에 따라
유저 데이터 리레이블링
609
리부팅
611
종 료