(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년12월06일
(11) 등록번호 10-1805310
(24) 등록일자 2017년11월29일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/60* (2013.01)
G06F 9/44 (2006.01)
(52) CPC특허분류
G06F 21/572 (2013.01)
G06F 21/60 (2013.01)
(21) 출원번호 10-2016-0089482
(22) 출원일자 2016년07월14일
심사청구일자 2016년07월14일
(56) 선행기술조사문헌
KR1020130114672 A*
JP2007133860 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
조진성
경기도 수원시 영통구 봉영로 1620, 101-1801호 (영통동, 대우 월드마크)
조성희
경기도 용인시 수지구 수지로113번길 15, 203동 1104호 (성복동, LG빌리지2차아파트)
(뒷면에 계속)
(74) 대리인
인비전 특허법인

전체 청구항 수 : 총 12 항 심사관 : 구대성

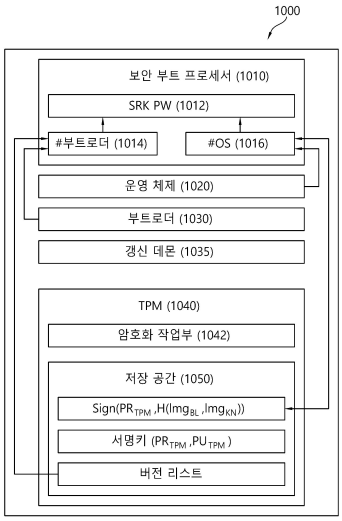
(54) 발명의 명칭 **TPM 기반의 사용자 장치 및 이를 이용한 펌웨어 갱신 방법**

(57) 요 약

본 발명은 TPM 기반의 사용자 장치에서 펌웨어 갱신 방법에 관한 것이다.

이러한 본 명세서는 펌웨어의 파일에 관한 해쉬값을 기반으로 상기 펌웨어의 이전 버전의 정보를 리스트화한 버전 리스트를 생성하는 보안 부트 프로세서, 상기 펌웨어에 새로운 업데이트가 존재하는지 확인하고, 상기 펌웨어의 업데이트 파일을 수신하여 상기 업데이트 파일의 무결성 검증을 수행하도록 구성되며, 상기 업데이트 파일의 버전에 대한 검사를 수행하고, 상기 검사의 결과를 기반으로 상기 펌웨어의 갱신을 수행하거나 취소하는 단계를 수행하는 갱신 데몬, 및 상기 버전 리스트를 저장하는 TPM을 포함하는 장치를 게시한다. 불법적으로 저사양 범용 IoT 디바이스의 커널, 부트로더 등의 펌웨어 이미지를 변경하는 공격에 효율적으로 대응할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06F 9/4401 (2013.01)
G06F 2221/033 (2013.01)
(72) 발명자
김병선
경기도 용인시 기흥구 덕영대로 1732 (서천동)
김지훈
경기도 수원시 영통구 청명로 47-1, 302호 (영통동)
황효선
경기도 부천시 송내대로205번길 70, 2502동 201호 (상동, 푸른마을 창보밀레시티)

명 세 서

청구범위

청구항 1

TPM(Trusted Platform Module) 기반의 사용자 장치로서,

펌웨어(firmware)의 파일에 관한 해쉬값(hash value)을 기반으로 상기 펌웨어의 이전 버전의 정보를 리스트화한 버전 리스트(version list)를 생성하는 보안 부트 프로세서(secure boot processor);

상기 펌웨어에 새로운 업데이트가 존재하는지 확인하고, 상기 펌웨어의 업데이트 파일을 수신하여 상기 업데이트 파일의 무결성 검증을 수행하도록 구성되며, 상기 업데이트 파일의 버전에 대한 검사를 수행하고, 상기 검사의 결과를 기반으로 상기 펌웨어의 갱신을 수행하거나 취소하는 단계를 수행하는 갱신 데몬(updater daemon); 및

상기 버전 리스트를 저장하는 TPM을 포함하고,

상기 보안 부트 프로세서는,

부트로더(bootloader)와 운영체제의 커널(kernel)을 실행하도록 구성되고, 상기 실행된 부트로더의 이미지(image)와 상기 실행된 커널의 이미지를 기반으로 적어도 하나의 무결성 검증(integrigy verification)을 수행하고, 상기 무결성 검증에 기반하여 상기 TPM의 저장공간에 접근하기 위한 SRK(storage root key) 암호를 생성하되,

시스템 레벨(system level)에서 상기 실행된 커널의 이미지(bootloader image)를 기반으로 제1 무결성 검증을 수행하고,

상기 제1 무결성 검증이 성공으로 판단되면 사용자 레벨(user level)에서 보안 부트 데몬을 실행하고 상기 실행된 부트로더의 이미지를 기반으로 제2 무결성 검증을 수행하는 것을 특징으로 하는 사용자 장치.

청구항 2

제 1 항에 있어서,

상기 펌웨어의 업데이트 파일은 상기 사용자 장치의 부팅에 사용되는 부트로더(bootloader), 커널(kernel), 보안 부트 데몬, 갱신 데몬 중 적어도 하나를 포함하는 것을 특징으로 하는, 사용자 장치.

청구항 3

제 2 항에 있어서, 상기 검사는,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나와, 상기 버전 리스트에 기록된 버전을 비교하는 단계를 포함함을 특징으로 하는, 사용자 장치.

청구항 4

제 3 항에 있어서,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전과 동일하거나 그 이전 버전일 경우, 상기 갱신 데몬은 상기 펌웨어의 업데이트 파일에 기반한 갱신을 취소하는 것을 특징으로 하는, 사용자 장치.

청구항 5

제 3 항에 있어서,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전에 비해 신규 버전일 경우, 상기 갱신 데몬은 상기 펌웨어의 업데이트 파일에 기반한 갱신을 수행하는 것을 특징으로 하는, 사용자 장치.

청구항 6

삭제

청구항 7

삭제

청구항 8

TPM(Trusted Platform Module) 기반의 사용자 장치에서 펌웨어(firmware)의 갱신을 수행하는 방법으로서,

펌웨어의 파일에 관한 해쉬값(hash value)을 기반으로 상기 펌웨어의 이전 버전의 정보를 리스트화한 버전 리스트(version list)를 생성하는 단계;

상기 펌웨어에 새로운 업데이트가 존재하는 경우 상기 펌웨어의 업데이트 파일을 수신하는 단계;

상기 업데이트 파일의 무결성 검증을 수행하는 단계;

상기 무결성 검증을 통과한 경우 상기 업데이트 파일의 버전에 대한 검사를 수행하는 단계;

상기 검사의 결과를 기반으로 상기 펌웨어의 갱신을 수행하거나 취소하는 단계

상기 펌웨어의 업데이트 파일에 기반한 갱신이 완료되면, 상기 사용자 장치를 재부팅하는 단계;

부트로더(bootloader)와 운영체제의 커널(kernel)을 실행하는 단계;

상기 실행된 부트로더의 이미지(image)와 상기 실행된 커널의 이미지를 기반으로 적어도 하나의 무결성 검증(integrigy verification)을 수행하는 단계; 및

상기 무결성 검증에 기반하여 상기 TPM의 저장공간에 접근하기 위한 SRK(storage root key) 암호를 생성하는 단계를 포함하고,

상기 무결성 검증은,

시스템 레벨(system level)에서 상기 실행된 커널의 이미지(bootloader image)를 기반으로 제1 무결성 검증을 수행하는 단계; 및

상기 제1 무결성 검증이 성공으로 판단되면 사용자 레벨(user level)에서 보안 부트 데몬을 실행하고 상기 실행된 부트로더의 이미지를 기반으로 제2 무결성 검증을 수행하는 단계를 포함함을 특징으로 하는, 방법.

청구항 9

제 8 항에 있어서,

상기 펌웨어의 업데이트 파일은 상기 사용자 장치의 부팅에 사용되는 부트로더(bootloader), 커널(kernel), 보안 부트 데몬, 갱신 데몬 중 적어도 하나를 포함하는 것을 특징으로 하는, 방법.

청구항 10

제 9 항에 있어서, 상기 검사는,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나와, 상기 버전 리스트에 기록된 버전을 비교하는 단계를 포함함을 특징으로 하는, 방법.

청구항 11

제 10 항에 있어서, 상기 펌웨어의 업데이트 파일에 기반한 갱신은,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전과 동일하거나 그 이전 버전일 경우에는 수행되지 않는 것을 특징으로 하는, 방법.

청구항 12

제 10 항에 있어서, 상기 펌웨어의 업데이트 파일에 기반한 갱신은,

상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전에 비해 신규 버전일 경우에 수행되는 것을 특징으로 하는, 방법.

청구항 13

제 10 항에 있어서, 상기 업데이트 파일의 무결성 검증은,

상기 수신된 업데이트 파일에 대한 제1 해쉬값과, 상기 수신된 업데이트 파일에 관한 서명과 개발자의 인증서를 통해 계산된 제2 해쉬값을 비교하는 단계를 포함함을 특징으로 하는, 방법.

청구항 14

제 13 항에 있어서, 상기 업데이트 파일의 무결성 검증은,

상기 제1 해쉬값과 상기 제2 해쉬값이 같을 경우 통과되고, 다를 경우 통과되지 않는 것을 특징으로 하는, 방법.

청구항 15

삭제

청구항 16

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자 장치에서의 안전한 펌웨어 갱신에 관한 것으로서, 보다 상세하게는 TPM 기반의 사용자 장치 및 이를 이용한 펌웨어 갱신 방법에 관한 것이다.

배 경 기 술

[0002] 펌웨어 업데이트를 진행하는 방법은 크게 디바이스에서 직접 업데이트 서버에 접속하여 업데이트를 진행하는 제1 방식과 디바이스를 PC에 연결하여 사용자가 업데이트 파일을 디바이스에 직접 설치하는 제2 방식으로 분류된다. 제1 방식에서는 해킹의 공격에 대비하여 인증 서버를 사용하는 방안이 제안되었으며, 이 기술은 업데이트 서버에서 디바이스를 검증하고, 인증된 디바이스에서만 복호화 가능한 암호화된 업데이트 파일을 만들어 제공한다. 반면 제2 방식에서는 해킹에 대비하여 별도의 업데이터를 사용하여 디바이스의 업데이트를 진행한다.

[0003] 범용(COTS; Commercial Off-The-Shelf) IoT(Internet of Things) 디바이스는 오픈소스(Open source) 기반의 인터넷에 연결 가능한 하드웨어 플랫폼을 제공한다. 범용 IoT 디바이스는 시중에서 쉽게 구매될 수 있기 때문에, 사용자는 범용 IoT 디바이스에 다양한 기능을 탑재하는 방식으로 손쉽게 제품을 개발하거나 사용할 수 있다. 범용 IoT 디바이스로서 라즈베리파이, 아두이노, 비글 본 블랙, 에디슨 등이 출시되어 있으며 여러 분야에서 사용되고 있다.

[0004] 이러한 범용 IoT 디바이스는 보편적으로 소형화 및 저사양으로 제작되기 때문에 일반 PC 환경과는 다르게 보안 요소 탑재에 제약이 있고, 업데이트 서버에서 개인화를 지원하지 않기 때문에 다양한 취약점과 위협들이 존재하고 있다. 이러한 보안 위협 중 펌웨어 교체 공격(Firmware replacement attack)은 펌웨어 업데이트 시, 변조된 부트로더, 커널, 루트 파일 시스템 등의 펌웨어를 디바이스에 강제로 업데이트하여 디바이스의 제어권을 획득하고 디바이스 내 저장된 암호화 키 교체/삭제/유출, 타 IoT 디바이스 공격을 위한 진입점으로 악용될 수 있다. 이러한 취약점을 해결하고자 각 부트 단계에 로드되는 이미지의 무결성을 단계적으로 검증하는 방안(Trust chain)이 있지만 취약점이 발견된 적법한 이전 버전의 펌웨어로 업데이트하는 경우, 무결성 검증을 통과할 가능성이 있다.

[0005] 위와 같은 공격이 실행되어 디바이스의 제어권이 탈취되면 디바이스에 저장된 암호화 키들이 유출될 가능성이 있다. 최근에는 이러한 소프트웨어 기반의 키 관리의 보안성을 강화하기 위해 TPM(Trusted Platform Module)과 같은 보안 하드웨어 모듈을 통해 암호화 키를 관리한다. TPM은 암호화 키, 암호화된 데이터, 암호화 방식 등을 제공하기 위한 목적으로 고안된 하드웨어 디바이스 모듈로서, 주로 개인용 컴퓨터(PC)의 주기판에 부착되며, 부

팅 단계에서부터 시스템의 무결성 검증에 이용된다. 그런데, TPM 기반의 사용자 장치에서 펌웨어 업데이트시 보안을 강화하기 위한 방법이 아직까지 게시된 바 없다. 따라서, TPM 기반의 사용자 장치에서 안전한 펌웨어 갱신 방법이 요구된다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 기술적 과제는 TPM(Trusted Platform Module)과 같은 보안 하드웨어 모듈을 포함하는 보안 장치 플랫폼에서, 불법적인 펌웨어 변조 또는 교체를 통한 TPM의 악의적 활용을 방지하는, 신뢰성 있는 펌웨어 업데이트 방법 및 장치를 제공함에 있다.

[0007] 본 발명의 다른 기술적 과제는 TPM을 포함하는 디바이스 플랫폼의 펌웨어 갱신 과정에서 기존 버전의 펌웨어 이미지의 설치를 차단하기 위한 사용자 장치 및 방법을 제공함에 있다.

과제의 해결 수단

[0008] 본 발명의 일 양태에 따르면, TPM(Trusted Platform Module) 기반의 사용자 장치를 제공한다. 상기 장치는 펌웨어(firmware)의 파일에 관한 해쉬값(hash value)을 기반으로 상기 펌웨어의 이전 버전의 정보를 리스트화한 버전 리스트(version list)를 생성하는 보안 부트 프로세서(secure boot processor), 상기 펌웨어에 새로운 업데이트가 존재하는지 확인하고, 상기 펌웨어의 업데이트 파일을 수신하여 상기 업데이트 파일의 무결성 검증을 수행하도록 구성되며, 상기 업데이트 파일의 버전에 대한 검사를 수행하고, 상기 검사의 결과를 기반으로 상기 펌웨어의 갱신을 수행하거나 취소하는 단계를 수행하는 갱신 데몬(updater daemon), 및 상기 버전 리스트를 저장하는 TPM을 포함한다.

[0009] 일 측면에서, 상기 펌웨어의 업데이트 파일은 상기 사용자 장치의 부팅에 사용되는 부트로더(bootloader), 커널(kernel), 보안 부트 데몬, 갱신 데몬 중 적어도 하나를 포함할 수 있다.

[0010] 여기서, 상기 검사는, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나와, 상기 버전 리스트에 기록된 버전을 비교하는 단계를 포함할 수 있다.

[0011] 다른 측면에서, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전과 동일하거나 그 이전 버전일 경우, 상기 갱신 데몬은 상기 펌웨어의 업데이트 파일에 기반한 갱신을 취소할 수 있다.

[0012] 또 다른 측면에서, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전에 비해 신규 버전일 경우, 상기 갱신 데몬은 상기 펌웨어의 업데이트 파일에 기반한 갱신을 수행할 수 있다.

[0013] 또 다른 측면에서, 상기 보안 부트 프로세서는 부트로더(bootloader)와 운영체제의 커널(kernel)을 실행하도록 구성되고, 상기 실행된 부트로더의 이미지(image)와 상기 실행된 커널의 이미지를 기반으로 적어도 하나의 무결성 검증(integrigy verification)을 수행하고, 상기 무결성 검증에 기반하여 상기 TPM의 저장공간에 접근하기 위한 SRK(storage root key) 암호를 생성할 수 있다.

[0014] 또 다른 측면에서, 상기 보안 부트 프로세서는, 시스템 레벨(system level)에서 상기 실행된 커널의 이미지(bootloader image)를 기반으로 제1 무결성 검증을 수행하고, 상기 제1 무결성 검증이 성공으로 판단되면 사용자 레벨(user level)에서 보안 부트 데몬을 실행하고 상기 실행된 부트로더의 이미지를 기반으로 제2 무결성 검증을 수행할 수 있다.

[0015] 본 발명의 다른 양태에 따르면, TPM(Trusted Platform Module) 기반의 사용자 장치에서 펌웨어(firmware)의 갱신을 수행하는 방법을 제공한다. 상기 방법은 펌웨어의 파일에 관한 해쉬값(hash value)을 기반으로 상기 펌웨어의 이전 버전의 정보를 리스트화한 버전 리스트(version list)를 생성하는 단계, 상기 펌웨어에 새로운 업데이트가 존재하는 경우 상기 펌웨어의 업데이트 파일을 수신하는 단계, 상기 업데이트 파일의 무결성 검증을 수행하는 단계, 상기 무결성 검증을 통과한 경우 상기 업데이트 파일의 버전에 대한 검사를 수행하는 단계, 및 상기 검사의 결과를 기반으로 상기 펌웨어의 갱신을 수행하거나 취소하는 단계를 포함한다.

[0016] 일 측면에서, 상기 펌웨어의 업데이트 파일은 상기 사용자 장치의 부팅에 사용되는 부트로더(bootloader), 커널(kernel), 보안 부트 데몬, 갱신 데몬 중 적어도 하나를 포함할 수 있다.

[0017] 여기서, 상기 검사는, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나와, 상기 버전 리스트에 기록된 버전을 비교하는 단계를 포함할 수 있다.

[0018] 다른 측면에서, 상기 펌웨어의 업데이트 파일에 기반한 갱신은, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전과 동일하거나 그 이전 버전일 경우에는 수행되지 않을 수 있다.

[0019] 또 다른 측면에서, 상기 펌웨어의 업데이트 파일에 기반한 갱신은, 상기 부트로더의 버전, 상기 커널의 버전, 상기 보안 부트 데몬의 버전, 상기 갱신 데몬의 버전 중 적어도 하나가 상기 기록된 버전에 비해 신규 버전일 경우에 수행될 수 있다.

[0020] 또 다른 측면에서, 상기 업데이트 파일의 무결성 검증은, 상기 수신된 업데이트 파일에 대한 제1 해쉬값과, 상기 수신된 업데이트 파일에 관한 서명과 개발자의 인증서를 통해 계산된 제2 해쉬값을 비교하는 단계를 포함할 수 있다.

[0021] 또 다른 측면에서, 상기 업데이트 파일의 무결성 검증은, 상기 제1 해쉬값과 상기 제2 해쉬값이 같을 경우 통과되고, 다를 경우 통과되지 않을 수 있다.

[0022] 또 다른 측면에서, 상기 방법은 상기 펌웨어의 업데이트 파일에 기반한 갱신이 완료되면, 상기 사용자 장치를 재부팅하는 단계, 부트로더(bootloader)와 운영체제의 커널(kernel)을 실행하는 단계, 상기 실행된 부트로더의 이미지(image)와 상기 실행된 커널의 이미지를 기반으로 적어도 하나의 무결성 검증(integrigy verification)을 수행하는 단계, 상기 무결성 검증에 기반하여 상기 TPM의 저장공간에 접근하기 위한 SRK(storage root key) 암호를 생성하는 단계를 더 포함할 수 있다.

[0023] 또 다른 측면에서, 상기 무결성 검증은, 시스템 레벨(system level)에서 상기 실행된 커널의 이미지(bootloader image)를 기반으로 제1 무결성 검증을 수행하는 단계, 및 상기 제1 무결성 검증이 성공으로 판단되면 사용자 레벨(user level)에서 보안 부트 데몬을 실행하고 상기 실행된 부트로더의 이미지를 기반으로 제2 무결성 검증을 수행하는 단계를 포함할 수 있다.

발명의 효과

[0024] 본 발명에 따른 사용자 장치 및 이를 이용한 펌웨어 갱신 방법은 불법적으로 저사양 범용 IoT 디바이스의 커널, 부트로더 등의 펌웨어 이미지를 변경하는 공격에 효율적으로 대응할 수 있다. 또한 불법적인 방법으로는 사용자 장치에 저장되어 있는 암호화된 데이터에 접근할 수 없기 때문에 본 발명은 범용 IoT 디바이스를 사용하는 모든 분야에서 디바이스의 제어권, 데이터 및 개인정보 등을 보호하는 목적으로 널리 활용될 수 있다.

도면의 간단한 설명

[0025] 도 1은 본 발명의 실시예에 따른 TPM을 포함하는 사용자 장치의 블록도이다.

도 2는 일 실시예에 따라 펌웨어의 갱신을 순차적으로 수행하는 방법을 개념적으로 도시한 도면이다.

도 3은 본 발명의 일 실시예에 따른 펌웨어 갱신을 수행하는 구체적인 방법과 알고리즘을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0026] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0027] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "~부" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0028] 범용 IoT 디바이스는 보편적으로 소형화 및 저사양으로 제작되기 때문에 일반 PC 환경과는 다르게 보안요소 탑재에 제약이 있고, 해킹 등 다양한 위협에 대한 취약점을 가진다. 보안을 위협하는 예로서 펌웨어 교체

(firmware replacement) 및 실행 공격이 있다. 이것은 범용 IoT 디바이스가 시스템 부트(boot) 단계에서 순차적으로 실행되는 부트로더(boot loader), 커널(kernel) 이미지의 무결성(integrity)을 보장하지 않는 취약점을 이용하여, 변조된 이미지로 교체 및 실행하여 시스템 제어권을 탈취하는 것이다. 이 경우 범용 IoT 디바이스는 디바이스 내 저장된 암호화 키 교체/삭제/유출, 타 IoT 디바이스 공격을 위한 진입점으로 악용될 수 있다.

[0029] 따라서, 본 실시예에 따른 사용자 장치는 소프트웨어 기반의 키 관리의 보안성을 강화하기 위해 TPM을 포함하며, TPM 기반하에서 펌웨어의 갱신시 추가적인 보안 방법을 수행한다.

[0030] 도 1은 본 발명의 실시예에 따른 TPM을 포함하는 사용자 장치의 블록도이다. TPM을 포함하는 사용자 장치는 TPM 기반의 범용 IoT 디바이스를 포함할 수 있으며, TPM 기반의 사용자 플랫폼, TPM 기반의 IoT 디바이스 플랫폼, TPM 기반의 범용 IoT 디바이스 플랫폼 또는 단순히 사용자 장치나 범용 IoT 디바이스라 불릴 수도 있다.

[0031] 도 1을 참조하면, 사용자 장치(user apparatus, 1000)는 보안 부트 프로세서(1010), 운영 체제(1020), 부트로더(1030), 갱신 데몬(1035, updater daemon), TPM(1040)을 포함한다. 사용자 장치(1000)는 메모리(memory) 또는 저장기기(storage device)를 더 포함할 수 있다(도면에 미도시). 상기 메모리 또는 저장기기는 운영 체제(1020), 부트로더(1030), 보안 부트 데몬(daemon), 갱신 데몬(1035) 중 적어도 하나를 저장할 수 있다. 보안 부트 프로세서(1010)는 보안 부트 데몬 또는 갱신 데몬(1035) 그 자체일 수도 있다.

[0032] 보안 부트 프로세서(1010)는 부트 실행의 이전 또는 부트 실행의 초기 단계에서 펌웨어의 갱신 절차를 수행하고, 부트 과정에서 부트로더 및 커널 이미지의 무결성을 검증하는 절차를 수행할 수 있다.

[0033] 우선, 펌웨어의 갱신 절차와 관련하여, 보안 부트 프로세서(1010)는 펌웨어 파일의 해쉬 또는 기타 정보 등을 기반으로 버전 리스트(version list)를 생성하고, 버전 리스트를 TPM(1040)의 저장 공간(1050)에 저장할 수 있다. 여기서, 버전 리스트는 부트로더, 커널 이미지, 보안 부트 데몬, 갱신 데몬 중 적어도 하나에 관한 이전 버전의 정보를 리스트화한 것으로 정의될 수 있다.

[0034] 갱신 데몬(1035)은 보안 부트 프로세서(1010)의 일부일 수도 있고, 소프트웨어 모듈로서 보안 부트 프로세서(1010)와 별개로 구비될 수 있다. 갱신 데몬(1035)은 펌웨어의 새로운 업데이트가 존재하는지 확인하는 단계, 업데이트 파일이 존재하는 경우 펌웨어의 업데이트 파일을 수신하는 단계, 업데이트 파일의 무결성 검증을 수행하는 단계. 펌웨어의 버전을 검사하는 단계, 검사결과를 기반으로 펌웨어의 갱신을 수행 또는 취소하는 단계를 수행한다. 펌웨어의 버전을 검사하는 단계는, 갱신 데몬(1035)는 수신된 부트로더의 버전, 커널 이미지의 버전, 보안 부트 데몬의 버전, 갱신 데몬의 버전 중 적어도 하나와, 이들의 버전 리스트상에 기록된 버전을 비교하는 단계를 포함할 수 있다. 검사결과, 수신된 펌웨어의 버전이 동일 또는 이전 버전일 경우, 갱신 데몬(1035)은 펌웨어의 갱신을 진행하지 않는다. 즉, 갱신 데몬(1035)는 이전 버전의 펌웨어 설치를 막는다. 반면, 검사결과, 수신된 펌웨어의 버전이 신규 버전일 경우, 갱신 데몬(1035)은 펌웨어의 갱신을 수행한다.

[0035] 펌웨어의 갱신이 완료되면, 보안 부트 프로세서(1010)는 사용자 장치(1000)를 재부트(reboot)하고 부트로더 및 커널 이미지의 무결성을 검증하는 과정을 수행한다. 구체적으로, 보안 부트 프로세서(1010)는 부트로더(1030)으로부터 해쉬값 #부트로더(1014), 운영 체제(1020)로부터 해쉬값 #OS(1016)를 계산 또는 처리하고, 부트로더와 OS(또는 커널)의 무결성을 식별하는 고유값을 이용하여 SRK 암호(1012)를 추출한다. 고유값은 해쉬값(Hash value)이라 불릴 수 있으며, 이하에서 해쉬값으로 통칭하도록 한다. 보안 부트 프로세서(1010)는 시스템 레벨(system level)에서의 커널 이미지의 제1 무결성 검증과, 사용자 레벨(user level)에서의 부트로더 이미지(1014)의 제2 무결성 검증을 수행하고, 상기 제1 및 제2 무결성 검증을 기반으로 SRK 암호(1012)를 생성한다. 이때, SRK 암호(1012)를 생성 또는 추출하는 연산과정은 제조사, 제품별로 상이하게 설정함으로써 보안성을 높일 수 있다.

[0036] TPM(1040)은 암호화 작업부(1042), 저장공간(storage space, 1050)을 포함한다. TPM(1040)은 사용자 장치(1000)의 부팅 단계에서부터 시스템의 무결성 검증을 수행하기 위한 정보를 보안 부트 프로세서(1010)에 제공한다.

[0037] 암호화 작업부(1042)는 암호화 키를 생성하는 동작과 같은 암호화 작업을 수행하며, CRYPTO 엔진(Engine)이라 불릴 수도 있다.

[0038] 저장 공간(1050)은 버전 리스트, 부팅에 사용된 부트로더 및/또는 커널 이미지의 무결성 검증을 위한 서명, 암호화 키, 암호화된 데이터 중 적어도 하나를 보관한다. 그리고 저장 공간(1050)은 보안 부트 프로세서(1010)의 요청에 의해 보안 부트 프로세서(1010)에 해당 정보를 제공할 수 있다. 저장 공간(1050)은 사용자 장치(1000)의 초기 설정 및 구성으로써 구비될 수 있다. 일례로서, 부팅에 사용된 부트로더 및/또는 커널 이미지의 무결성 검

증을 위한 서명은 비공개키를 사용하여 제작된 부트로더(1030)와 커널 이미지의 해쉬값에 대한 서명(Sign(PR_{TPM}, H(Img_{BL} + Img_{KN})))을 포함할 수 있다. 여기서, H(A)란 이미지 A의 해쉬값을 의미한다. 다른 예로서, 암호화 키 또는 암호화된 데이터는 서명 생성을 위한 비공개키(PR_{TPM})와, 서명 검증을 위한 공개키(PU_{TPM})를 포함할 수 있다. 여기서, 저장 공간(1050)에 보관된 암호화 키를 사용하기 위해서는 SRK(storage root key) 암호(Password)가 필요하며 이는 보안 부트 프로세서(1010)에 의해 획득된다. 한편 저장 공간(1050)은 NV(Non-Volatile) 타입의 저장소일 수 있다.

[0039] 도 2는 일 실시예에 따라 펌웨어의 갱신을 순차적으로 수행하는 방법을 개념적으로 도시한 도면이다.

[0040] 도 2를 참조하면, 사용자 장치(1000)는 갱신 데몬을 실행한 뒤(S200), 펌웨어 갱신절차를 수행한다. 펌웨어 갱신 절차는 도 1에서 설명된 갱신 데몬(1035)의 동작을 포함할 수 있다.

[0041] 펌웨어의 갱신이 완료되면, 사용자 장치(1000)는 재부트(reboot)을 실행하고(S210), 부트로더 및 커널 이미지의 무결성을 검증하는 과정을 수행한다. 제1 무결성 검증은 커널 이미지의 무결성 검증을 소프트웨어적으로 수행하는 단계로서 부트로더(1030)에 의해 수행될 수 있다(S220). 만약 커널 이미지의 무결성 검증(integrity verification)이 실패하면, 사용자 장치(1000) 또는 부트로더(1030)는 부팅을 더 이상 진행하지 않는다. 만약, 커널 이미지의 무결성 검증(integrity verification)이 성공하면, 사용자 장치(1000)는 OS 커널을 로드 및 실행하고(S230), 보안 부트 데몬에 의한 제2 무결성 검증을 수행한다(S240). 여기서, 제2 무결성 검증은 단계 S200에서 실행된 부트로더 이미지의 무결성 검증을 소프트웨어적으로 수행하는 단계로서 보안 부트 프로세서(1010) 또는 보안 부트 데몬에 의해 수행될 수 있다. 만약 부트로더 이미지의 무결성 검증(integrity verification)이 실패하면, 사용자 장치(1000) 또는 보안 부트 프로세서(1010)는 부팅을 더 이상 진행하지 않고, SRK 암호도 생성하지 않는다. 만약 부트로더 이미지의 무결성 검증(integrity verification)이 성공하면, 사용자 장치(1000) 또는 보안 부트 프로세서(1010)는 부팅을 계속 진행하며, SRK 암호를 생성하고 TPM(1040)을 정상적으로 사용할 수 있다.

[0042] 도 3은 본 발명의 일 실시예에 따른 펌웨어 갱신을 수행하는 구체적인 방법과 알고리즘을 도시한 순서도이다.

[0043] 먼저 펌웨어 갱신의 수행방법에서 사용되는 기술적 용어를 정리하면 다음과 같다.

표 1

[0044]

용어	설명
PR_a	a의 비공개키
PU_a	a의 공개키
$Cert_a$	a의 인증서
H(X)	X의 해쉬값
Sign(PR_a, H(X))	비공개키와 해쉬를 이용한 서명
D(PU_a, H(X))	공개키를 이용한 서명 복호화
Img	이미지 파일
Img_{KN_Cur}	부트로더에서 로드한 현재 커널 이미지
Img_{BL_Cur}	현재 부트로더 이미지
H(Img_{BL})	TPM에 저장된 부트로더 이미지의 해쉬값
H(Img_{KL})	TPM에 저장된 커널 이미지의 해쉬값
V_a	a의 버전
FW	펌웨어 파일

[0045] 도 3을 참조하면, 사용자 장치(1000)는 펌웨어의 업데이트 리스트를 확인하고(S300), 업데이트 파일이 존재하는지 판단한다(S305). 만약 펌웨어에 관한 새로운 업데이트 파일이 존재하면, 사용자 장치(1000)는 펌웨어에 관한 업데이트 파일을 다운로드한다(S310). 무결성 검증을 위해 다운받은 펌웨어 파일에 대한 제1 해쉬값 H(FW)과, 다운받은 서명과 개발자의 인증서를 통해 제2 해쉬값 H(FW_{Vrf})를 계산한다(S315).

[0046] 그리고 사용자 장치(1000)는 제1 해쉬값과 제2 해쉬값을 비교하여 업데이트 파일의 무결성을 검증한다(S320).

만약, 업데이트 파일이 무결성을 만족하지 않으면, 사용자 장치(1000)는 펌웨어의 갱신 절차를 중단한다(S325). 만약, 업데이트 파일이 무결성을 만족하면, 사용자 장치(1000)는 저장 공간(1050)에 보관된 버전 리스트를 로드한다(S330).

[0047] 사용자 장치(1000)는 버전 리스트상의 펌웨어의 버전과 다운로드된 업데이트 파일의 버전을 비교한다(S335). 업데이트 파일의 버전이 버전 리스트에 기록된 펌웨어의 버전과 같거나 그 이전 버전일 경우, 사용자 장치(1000)는 펌웨어의 갱신을 중단한다(S340). 즉, 사용자 장치(1000)는 이전 버전의 펌웨어 설치를 막는다. 반면, 업데이트 파일의 버전이 버전 리스트에 기록된 펌웨어의 버전보다 신규 버전일 경우, 사용자 장치(1000)는 펌웨어의 갱신을 수행하고, 기존 버전 리스트에서 새로운 펌웨어의 버전의 정보를 추가하여 버전 리스트의 갱신을 수행한 뒤 재부팅한다(S345).

[0048] 재부팅 단계는, 사용자 장치(1000)가 다음 부팅부터 무결성 검증을 수행하기 위해, 서명 $Sign(PR_{TPM}, H(Img_{BL_new}+Img_{KN_New}))$를 생성하고, TPM(1040)의 저장 공간(1050)에 저장하는 단계, 펌웨어의 나머지 업데이트를 실행하고 최종적으로 재부팅을 수행하는 단계를 포함한다.

[0049] 이러한 본 실시예에 따른 사용자 장치(1000) 및 보안 부트의 수행방법은 펌웨어 이미지 교체 공격에 대해 다음의 4가지 측면에서 강화된 보안성을 제공할 수 있다.

[0050] 첫째, 이전 버전으로의 커널 이미지 변조 및 교체 공격이 발생하면, 이전 버전의 커널 이미지가 수신된다. 사용자 장치(1000)가 펌웨어의 갱신을 진행할 때, 펌웨어의 버전을 검사하는 과정에서 펌웨어의 버전이 버전 리스트상의 버전에 존재하기 때문에, 사용자 장치(1000)는 펌웨어의 갱신을 중단한다. 따라서, 사용자 장치(1000)의 보안성의 강화된다. 갱신 데몬을 사용하지 않고 커널 이미지를 교체하였을 경우, 부팅 시 부트로더에서 커널을 검증하는 과정을 통과하지 못하여 부팅이 되지 않는다.

[0051] 둘째, 이전 버전으로의 부트로더 이미지 변조 및 교체 공격이 발생하면, 이전 버전 부트로더가 수신된다. 사용자 장치(1000)가 펌웨어의 갱신을 진행할 때, 펌웨어의 버전을 검사하는 과정에서 펌웨어의 버전이 버전 리스트상의 버전에 존재하기 때문에, 사용자 장치(1000)는 펌웨어의 갱신을 중단한다. 따라서, 사용자 장치(1000)의 보안성의 강화된다. 갱신 데몬을 사용하지 않고 부트로더 이미지를 교체하였을 경우, 부팅과정의 보안 부트 데몬에서 부트로더 무결성 검증에 실패하여 TPM의 SRK 암호가 생성되지 않아 TPM을 사용하지 못한다.

[0052] 셋째, 이전 버전으로의 부트로더 이미지와 커널 이미지의 변조 및 교체 공격이 발생하면, 사용자 장치(1000)가 펌웨어의 갱신을 진행할 때, 펌웨어의 버전을 검사하는 과정에서 펌웨어의 버전이 버전 리스트상의 버전에 존재하기 때문에, 사용자 장치(1000)는 펌웨어의 갱신을 중단한다. 또한 루트 파일 시스템을 변조 및 교체하여 갱신 데몬을 사용하지 않고 부트로더, 커널 이미지를 교체 하였을 경우, 보안 부트 데몬에서 부트로더, 커널 이미지의 무결성을 검증하는 과정에서 통과하지 못하여 TPM의 SRK 암호가 생성되지 않아 TPM을 사용하지 못한다.

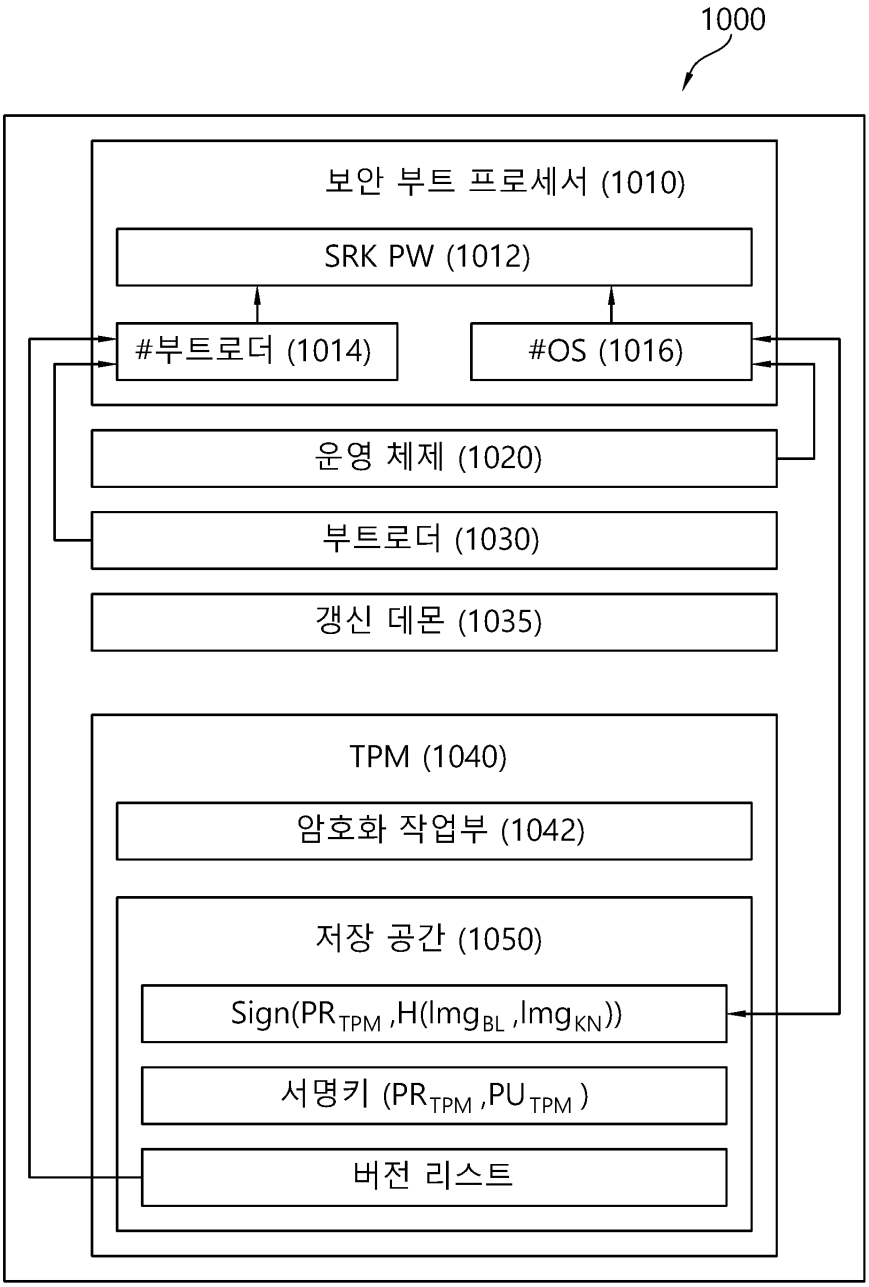
[0053] 이와 같이 본 발명에 따른 사용자 장치(1000) 및 펌웨어 갱신 수행방법은 이전 버전의 펌웨어 리스트와 업데이트 파일의 버전을 비교하여 이전 버전의 펌웨어 설치를 막을 수 있다. 또한, 시스템에서 제공되는 갱신 데몬을 사용하지 않고 우회적으로 업데이트를 진행하면 사용자 장치(1000)는 부팅을 막거나 TPM의 SRK 암호의 생성을 막기 때문에 키 보호 및 안전한 펌웨어 업데이트와 부팅이 가능하다.

[0054] 본 발명에 따를 때, 불법적인 방법으로는 사용자 장치(1000)에 저장되어 있는 암호화된 데이터에 접근할 수 없기 때문에 본 발명은 범용 IoT 디바이스를 사용하는 모든 분야에서 디바이스 및 데이터를 보호하는 목적으로 활용될 수 있다.

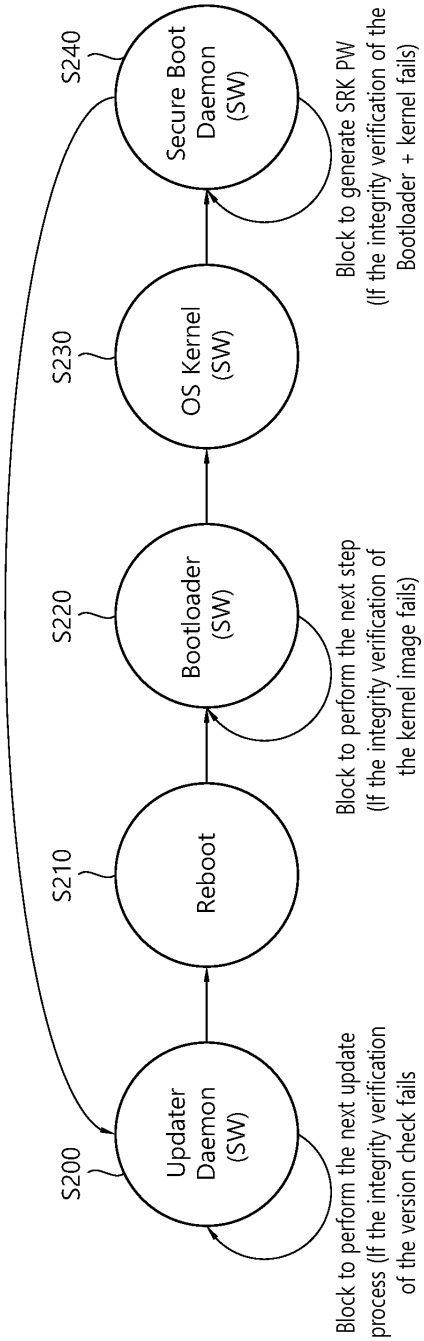
[0055] 상술한 예시적인 시스템에서, 방법들은 일련의 단계 또는 블록으로써 순서도를 기초로 설명되고 있지만, 본 발명은 단계들의 순서에 한정되는 것은 아니며, 어떤 단계는 상술한 바와 다른 단계와 다른 순서로 또는 동시에 발생할 수 있다. 또한, 당업자라면 순서도에 나타낸 단계들이 배타적이지 않고, 다른 단계가 포함되거나 순서도의 하나 또는 그 이상의 단계가 본 발명의 범위에 영향을 미치지 않고 삭제될 수 있음을 이해할 수 있을 것이다.

도면

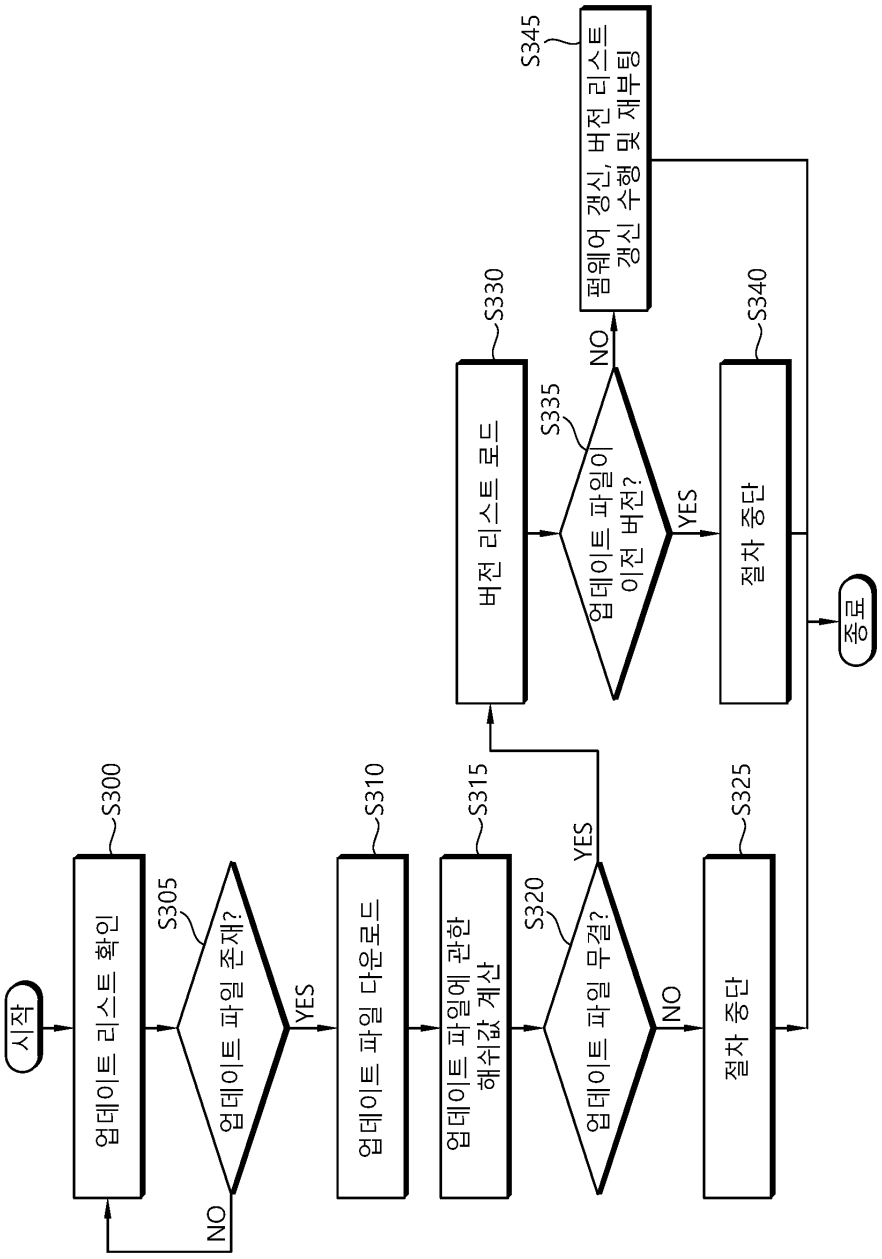
도면1


1000
보안 부트 프로세서 (1010)
SRK PW (1012)
#부트로더 (1014)
#OS (1016)
운영 체제 (1020)
부트로더 (1030)
갱신 데몬 (1035)
TPM (1040)
암호화 작업부 (1042)
저장 공간 (1050)
Sign(PR_TPM ,H(Img_BL ,Img_KN))
서명키 (PR_TPM ,PU_TPM)
버전 리스트

도면2


S200
Updater Daemon (SW)
S210
Reboot
S220
Bootloader (SW)
S230
OS Kernel (SW)
S240
Secure Boot Daemon (SW)
Block to perform the next update process (If the integrity verification of the version check fails or the update file fails)
Block to perform the next step (If the integrity verification of the kernel image fails)
Block to generate SRK PW (If the integrity verification of the Bootloader + kernel fails)

도면3


시작
업데이트 리스트 확인
S300
업데이트 파일 존재?
S305
NO
YES
업데이트 파일 다운로드
S310
업데이트 파일에 관한 해쉬값 계산
S315
업데이트 파일 무결?
S320
NO
YES
절차 중단
S325
버전 리스트 로드
S330
업데이트 파일이 이전 버전?
S335
NO
YES
펌웨어 갱신, 버전 리스트 갱신 및 재부팅
S345
절차 중단
S340
종료