(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0016280
(43) 공개일자 2014년02월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/50 (2013.01) *G06F 9/24* (2006.01)
(21) 출원번호 10-2013-7023086
(22) 출원일자(국제) 2012년03월01일
심사청구일자 없음
(85) 번역문제출일자 2013년08월30일
(86) 국제출원번호 PCT/US2012/027302
(87) 국제공개번호 WO 2012/118984
국제공개일자 2012년09월07일
(30) 우선권주장
13/037,962 2011년03월01일 미국(US)

(71) 출원인
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
앤더슨 스코트 디
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
린슬레이 데이비드 제이
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(뒷면에 계속)
(74) 대리인
제일특허법인

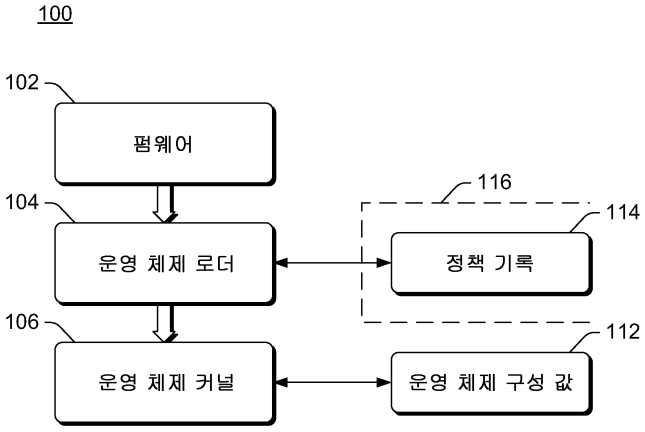
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **운영 체제 구성 값 보호**

(57) 요 약

디바이스 상에 운영 체제를 로딩하여 구동하기 전에 디바이스 상의 사전 운영 체제 환경에서, 운영 체제를 위한 구성 설정을 식별하는 정책이 획득된다. 운영 체제 그 자체는 이러한 정책을 변화시키지 못하지만, 정책은 소정의 상황에서 사전 운영 체제 환경의 컴포넌트에 의해 변화될 수 있다. 정책은 운영 체제에 의해 사용된 구성 값과 비교되며, 구성 값이 정책을 만족시키면 운영 체제는 구성 값을 이용하여 부팅하도록 허용된다. 그러나, 구성 값이 정책을 만족시키지 않으면, 응답 동작이 취해진다.

대 표 도 - 도1



(72) 발명자

니스트롬 매그너스 보 구스타프

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

맥시버 더글라스 엠

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

스피거 로버트 칼

미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션

특허청구의 범위

청구항 1

디바이스 상에서 운영 체제를 구동하기 전에 상기 디바이스 상의 사전 운영 체제 환경에서, 하나 이상의 운영 체제를 위한 구성 설정을 식별하는 정책을 획득하는 단계 - 상기 운영 체제는 상기 정책을 변화시키지 못하도록 방지됨 -,

상기 사전 운영 체제 환경에서, 상기 정책을 상기 운영 체제에 의해 사용된 구성 값과 비교하는 단계,

상기 구성 값이 상기 정책을 만족시키면, 상기 사전 운영 체제 환경에서, 상기 운영 체제가 상기 구성 값을 이용하여 부팅하도록 허용하는 단계, 및

상기 구성 값이 상기 정책을 만족시키지 않으면, 상기 사전 운영 체제 환경에서, 응답 동작을 취하는 단계를 포함하는

방법.

청구항 2

제 1 항에 있어서,

상기 정책은 또한 상기 운영 체제가 부팅하도록 허용되기 위해 상기 사전 운영 체제 환경이 만족시켜야 하는 구성 설정을 식별하는

방법.

청구항 3

제 1 항에 있어서,

상기 사전 운영 체제 환경에서, 상기 정책의 구성 설정을 위한 값을 캡처하는 단계,

상기 캡처된 값을 상기 정책의 일부분으로서 저장하는 단계, 및

상기 디바이스의 다음 부팅을 위해 상기 캡처된 값을 상기 정책의 상기 정책 설정의 일부분으로서 사용하는 단계를 포함하는

방법.

청구항 4

제 1 항에 있어서,

상기 정책의 신규 버전이 신뢰 개체인 정책 발행자로부터 유래되며 상기 정책의 상기 신규 버전이 상기 정책의 보다 신규한 버전이라고 판단되는 경우에만, 상기 정책이 상기 정책의 상기 신규 버전으로 대체되도록 허용하는 단계를 더 포함하는

방법.

청구항 5

제 4 항에 있어서,

상기 정책의 식별자가 상기 정책의 상기 신규 버전의 조상 리스트 내에 포함되면, 상기 정책의 상기 신규 버전

이 상기 정책의 보다 신규한 버전이라고 판단하는 단계를 더 포함하는

방법.

청구항 6

제 1 항에 있어서,

상기 사전 운영 체제 환경은 컴퓨팅 디바이스 상에서 구동되는 가상 머신의 사전 운영 체제 환경인

방법.

청구항 7

제 1 항에 있어서,

상기 정책은 상기 사전 운영 체제 환경의 컴포넌트가 상기 정책을 변화시킬 수 있지만 상기 운영 체제가 상기 정책을 변화시키지 못하게 방지되는 보안 방식으로 유지되는

방법.

청구항 8

제 1 항에 있어서,

상기 정책은 상기 응답 동작을 더 식별하는

방법.

청구항 9

하나 이상의 프로세서, 및

하나 이상의 컴퓨터 판독 가능 매체를 포함하며, 상기 하나 이상의 컴퓨터 판독 가능 매체는 상기 하나 이상의 프로세서에 의해 실행될 때 상기 하나 이상의 프로세서로 하여금 상기 컴퓨팅 디바이스의 사전 운영 체제 환경을 구현하게 하는 복수의 명령어를 저장하고, 상기 컴퓨팅 디바이스의 상기 사전 운영 체제 환경은

상기 운영 체제가 상기 컴퓨팅 디바이스 상에서 실행되기 위해 상기 운영 체제의 구성 값에 의해 만족되어야 하는 구성 설정을 식별하는 정책에 대한 변화를 수신하는 동작 - 상기 운영 체제는 상기 정책을 변화시키지 못하게 방지됨 -,

상기 컴퓨팅 디바이스에서, 상기 정책에 대한 상기 변화가 상기 사전 운영 체제 환경에 의해 신뢰되는 개체에 의해 승인되는지를 점검하는 동작, 및

상기 정책에 대한 상기 변화가 상기 사전 운영 체제 환경에 의해 신뢰되는 상기 개체에 의해 승인된 경우에만 상기 정책을 변화시키는 동작을 포함하는 동작을 수행하는

컴퓨팅 디바이스.

청구항 10

제 9 항에 있어서,

상기 정책은 상기 운영 체제에 액세스 가능하지 않은 보안 방식으로 유지되는

컴퓨팅 디바이스.

명 세 서

배 경 기 술

[0001] 컴퓨터는 인터넷과 같은 다양한 네트워크를 통해 점점 더 상호 연결되고 있다. 그러한 연결은 사용자로 하여금 다양한 상이한 서비스 및 데이터에 액세스하도록 허용하지만, 그러한 연결이 문제가 없는 것은 아니다. 그러한 한가지 문제는 이러한 접속이 악성 프로그램으로 하여금 이들 컴퓨터 상에서 구동되도록 허용할 수 있다는 것이다. 이들 악성 프로그램은 다른 컴퓨터에 대한 공격을 개시하는 것, 다른 사용자의 컴퓨터로 비밀 데이터를 송신하는 것, 사용자가 자신의 컴퓨터를 사용할 수 없게 하는 것 등과 같은 다양한 바람직하지 않은 동작을 수행할 수 있다. 이러한 악성 프로그램으로부터 컴퓨터를 보호하는 것은 여전히 어렵다.

발명의 내용

[0002] 본 요약은 아래의 상세한 설명에서 더 설명되는 개념들의 선택을 간단한 형태로 소개하기 위해 제공된다. 본 요약은 청구된 발명 대상의 중요한 특징들 또는 본질적인 특징들을 식별하도록 의도되지 않으며, 청구된 발명 대상의 범위를 한정하기 위해 사용되도록 의도되지도 않는다.

[0003] 하나 이상의 양태에 따라, 디바이스 상에 운영 체제를 로딩하여 구동하기 전에 디바이스 상의 사전 운영 체제 환경에서, 적어도 하나의 운영 체제를 위한 구성 설정을 식별하는 정책이 획득된다. 운영 체제는 이러한 정책을 변화시키지 못한다. 이러한 정책은 운영 체제에 의해 사용된 구성 값과 비교되며, 구성 값이 정책을 만족시키면 운영 체제는 구성 값을 이용하여 부팅하도록 허용된다. 그러나, 구성 값이 정책을 만족시키지 않으면, 응답 동작이 취해진다.

[0004] 하나 이상의 양태에 따라, 운영 체제가 컴퓨팅 디바이스 상에서 실행되기 위해 운영 체제의 구성 값에 의해 만족되어야 하는 구성 설정을 식별하는 정책에 대한 변화가 수신된다. 운영 체제 그 자체는 이러한 정책을 변화시키지 못한다. 정책에 대한 변화가 사전 운영 체제 환경에 의해 신뢰 개체에 의해 승인되는지에 대한 점검이 수행되며, 정책에 대한 변화가 사전 운영 체제 환경에 의해 승인된 경우에만 정책이 변화된다.

도면의 간단한 설명

[0005] 동일한 참조 번호가 유사한 특징을 지칭하기 위해 첨부 도면에 걸쳐 사용된다.

도 1은 하나 이상의 실시예에 따라 보호형 운영 체제 구성 값을 구현하는 예시적인 디바이스를 도시한다.

도 2는 하나 이상의 실시예에 따른 예시적인 정책을 도시한다.

도 3은 하나 이상의 실시예에 따라 운영 체제 구성 값을 보호하기 위한 예시적인 프로세스를 도시하는 흐름도이다.

도 4는 하나 이상의 실시예에 따라 디바이스 내의 정책을 변화시키기 위한 예시적인 프로세스를 도시하는 흐름도이다.

도 5는 하나 이상의 실시예에 따라 보호형 운영 체제 구성 값을 구현하도록 구성될 수 있는 예시적인 컴퓨팅 디바이스를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0006] 본 명세서에서 운영 체제 구성 값 보호(protecting operating system configuration values)가 논의된다. 디바이스를 부팅하는 프로세스 중에, 디바이스의 하나 이상의 운영 체제 중 적어도 일부분에 의해 사용되며 디바이스의 사전 운영 체제 환경의 컴포넌트에 의해 사용된 하나 이상의 구성 값을 선택적으로 포함하는 한 세트의 구성 값은 디바이스를 위한 정책과 대조되어 점검된다. 구성 값이 정책을 만족시키면 운영 체제는 디바이스 상에서 구동되도록 허여되지만, 구성 값이 정책을 만족시키지 않으면 하나 이상의 적절한 동작(예를 들어, 운영 체제를 구동하지 않음, 값을 변화시킴 등)이 취해진다. 정책은 컴퓨팅 디바이스 상에서 구동하는 운영 체제 및 다른 애플리케이션에 의한 인증되지 않은 변경(unauthorized modification)으로부터 보호하는 방식으로 저장된

다. 그러나, 하나 이상의 정책 발행자는 정책이 시간에 걸쳐 변화하도록 허용하면서 정책을 갱신할 수 있다.

[0007] 본 명세서에서는 대칭 키 암호법(symmetric key cryptography), 공개 키 암호법(public key cryptography), 및 공개/비밀 키 쌍(public/private key pairs)을 참조한다. 이러한 키 암호법이 당업자에게 주지되어 있지만, 독자에게 도움이 되도록 이러한 암호법의 간단한 개요가 본 명세서에 포함된다. 공개 키 암호법에서, (사용자, 하드웨어 또는 소프트웨어 컴포넌트, 디바이스, 도메인 등과 같은) 개체(entity)는 그에 연관된 공개/비밀 키 쌍을 갖는다. 공개 키는 공개적으로 입수 가능하게 될 수 있지만, 개체는 비밀 키를 비밀로 유지한다. 비밀 키가 없으면, 공개 키를 사용하여 암호화된 데이터를 컴퓨터를 이용하여 해독하는 것이 매우 어렵다. 따라서, 데이터는 공개 키를 이용하여 임의의 개체에 의해 암호화될 수 있으며, 상응하는 비밀 키를 이용하여 하나의 개체에 의해서만 해독될 수 있다. 또한, 데이터 및 비밀 키를 이용함으로써 데이터를 위한 디지털 서명이 생성될 수 있다. 비밀 키가 없으면, 공개 키를 사용하여 검증될 수 있는 서명을 컴퓨터를 이용하여 생성하는 것이 매우 어렵다. 공개 키를 갖는 임의의 개체는 공개 키, 서명, 및 서명되었던 데이터에 대한 적절한 디지털 서명 검증 알고리즘을 실행함으로써 디지털 서명을 검증하기 위해 공개 키를 사용할 수 있다.

[0008] 한편, 대칭 키 암호법에서, (대칭 키로서도 또한 지칭되는) 공유 키(shared key)가 두 개의 개체에게 알려지며 두 개의 개체에 의해 비밀로 유지된다. 공유 키를 갖는 임의의 개체는 그러한 공유 키를 이용하여 암호화된 데이터를 전형적으로 해독할 수 있다. 공유 키가 없으면, 공유 키를 이용하여 암호화된 데이터를 컴퓨터를 이용하여 해독하는 것이 매우 어렵다. 따라서, 두 개의 개체가 모두 공유 키를 알고 있으면, 각각의 개체는 다른 개체에 의해 해독될 수 있는 데이터를 암호화할 수 있지만, 다른 개체가 공유 키를 알고 있지 않으면 이 다른 개체는 데이터를 해독할 수 없다. 마찬가지로, 공유 키를 갖는 개체는 동일한 개체에 의해 해독될 수 있는 데이터를 암호화할 수 있지만, 다른 개체는 공유 키를 알고 있지 않으면 데이터를 해독할 수 없다. 또한, 디지털 서명은 키드-해시 메시지 인증 코드 메카니즘(keyed-hash message authentication code mechanism)을 사용하는 것과 같이 대칭 키 암호법에 기반하여 생성될 수 있다. 공유 키를 갖는 임의의 개체는 디지털 서명을 생성하여 검증할 수 있다. 예를 들어, 신뢰된 제 3 자는 특정 개체의 아이덴티티(identity)에 기반하여 대칭 키를 생성할 수 있으며, 그런 다음 (예를 들어, 대칭 키를 이용하여 데이터를 암호화하거나 해독함으로써) 그러한 특정 개체를 위한 디지털 서명을 생성할 수 있을 뿐만 아니라 검증할 수 있다.

[0009] 도 1은 하나 이상의 실시예에 따라 운영 체제 구성 값 보호를 구현하는 예시적인 디바이스(100)를 도시한다. 디바이스(100)는 펌웨어(firmware, 102), 운영 체제 로더(operating system loader, 104), 및 운영 체제 커널(operating system kernel, 106)을 포함하며, 이들은 각각 디바이스(100)가 다양한 동작을 수행하도록 허용하는 하나 이상의 컴포넌트 또는 모듈이다. 이들 컴포넌트 또는 모듈은 비휘발성 메모리 또는 저장 디바이스(예를 들어, 플래시 메모리, ROM(read only memory), 자기 디스크, 광 디스크, 네트워크를 거쳐 액세스되는 원격 디바이스 또는 저장소 등)내에 전형적으로 저장된 명령어 및/또는 데이터를 포함한다. 이들 컴포넌트 또는 모듈은 비휘발성 메모리 또는 저장 디바이스로부터 하나 이상의 휘발성 메모리(예를 들어, RAM(random access memory)) 내로 로딩되며, 하나 이상의 휘발성 메모리로부터 이들 컴포넌트 또는 모듈이 하나 이상의 프로세서에 의해 검색되고 실행된다.

[0010] 디바이스(100)가 전원 공급되거나 또는 이와 달리 리셋될 때, 디바이스(100)는 부팅된다. 디바이스(100)의 부팅은 디바이스(100)의 시작 동작, 전형적으로 디바이스(100)의 운영 체제를 로딩하여 실행하는 것을 지칭한다. 디바이스(100)의 부팅은 전형적으로 적어도 두 개의 단계를 포함한다. 첫 번째 단계에서, 사전 운영 체제 환경의 컴포넌트가 디바이스(100) 상에 로딩되어 구동된다. 사전 운영 체제 환경에서, 다양한 컴포넌트 또는 모듈은 운영 체제를 부팅하는 것을 포함한 다양한 동작을 수행하는 것을 구동한다. 두 번째 단계에서, 운영 체제 환경의 컴포넌트가 디바이스(100) 상에 로딩되어 구동된다. 운영 체제 환경에서, 운영 체제는 디바이스(100) 상에서 구동하고 있다.

[0011] 컴포넌트의 로딩은 컴포넌트를 휘발성(또는 대안적으로 비휘발성) 메모리 내로 복사하는 것을 지칭하며, 선택적으로 다른 컴포넌트 또는 데이터 저장고에 추가 구성을 수행하는 것을 지칭한다. 컴포넌트를 실행하는 것은 디바이스(100)의 프로세서 또는 제어기에 의한 컴포넌트의 명령어의 구동(실행)을 지칭한다. 디바이스(100)가 부팅된 후에, 다양한 다른 프로그램이 운영 체제에 의해 디바이스(100) 상에서 구동될 수 있다.

[0012] 디바이스(100)는 다양한 상이한 유형의 물리적 디바이스일 수 있다. 예를 들어, 디바이스(100)는 데스크탑 컴퓨터, 랩탑 또는 넷북 컴퓨터, 노트패드 또는 태블릿 컴퓨터, 이동국(mobile station), 오락 기기, 디스플레이 디바이스에 통신 가능하게 결합된 셋탑 박스, 텔레비전, 휴대 전화 또는 다른 무선 전화, 게임 콘솔, 자동차용 컴퓨터 등일 수 있다. 디바이스(100)는 또한 물리적 디바이스 상에서 구동되는 가상 머신과 같은 가상 디바이

스(virtual device)일 수 있다. 가상 머신은 임의의 다양한 상이한 유형의 물리적 디바이스 상에서 구동될 수 있다.

[0013] 부트 프로세스 동안에, 펌웨어(102)는 디바이스(100)에 의해 로딩되어 실행된다. 펌웨어(102)는 디바이스(100)의 비휘발성 메모리 내에 저장된다. 펌웨어(102)는 ROM 내에 저장될 수 있거나, 또는 대안적으로 (플래시 메모리와 같은) 쓰기 가능한 비휘발성 메모리 내에 저장될 수 있다. 펌웨어(102)가 쓰기 가능한 비휘발성 메모리 내에 저장되는 실시예에서, 이러한 펌웨어(102)가 간섭받지 않는 것을 (그리고 그에 따라 악성 프로그램에 의해 변경되지 않는 것을) 보장하기 위해 전형적으로 주의를 기울인다. 예를 들어, 쓰기 가능한 비휘발성 메모리 내에 저장된 펌웨어(102)에 대한 서명을 검증함으로써, 오직 펌웨어(102)에만 액세스 가능한 보호식 메모리(protected memory) 내에 펌웨어(102)를 저장함으로써, 다양한 통상적인 신뢰된 부팅 또는 비밀 부팅 기법을 사용함으로써, 이러한 주의를 기울일 수 있다.

[0014] 펌웨어(102)는 운영 체제 로더(104)의 실행을 개시한다. 운영 체제 로더(104)는 실행되기 전에 펌웨어(102)에 의해 전형적으로 로딩되어 검증된다. 운영 체제 로더(104)는 여러 방식으로 검증될 수 있는데, 예컨대 운영 체제 로더(104)의 (펌웨어(102)가 신뢰하도록 구성된(예를 들어, 프로그래밍된) 개체에 의해 생성된) 디지털 서명을 검증함으로써 검증될 수 있다.

[0015] 운영 체제 로더(104)는 운영 체제 커널(106)을 로딩하여 실행한다. 운영 체제 커널(106)은 실행되기 전에 운영 체제 로더(104)에 의해 전형적으로 로딩되어 검증된다. 운영 체제 커널(106)은 여러 방식으로 검증될 수 있는데, 예컨대 운영 체제 커널(106)의 (운영 체제 로더(104)가 신뢰하도록 구성된(예를 들어, 프로그래밍된) 개체의 의해 생성된) 디지털 서명을 검증함으로써 검증될 수 있다. 그런 다음, 운영 체제 커널(106)은 계속하여 다양한 상이한 운영 체제 컴포넌트 및/또는 사용자 모드 컴포넌트를 로딩하여 실행할 수 있다. 이들 운영 체제 컴포넌트 및 사용자 모드 컴포넌트는 이러한 컴포넌트를 실행하라는 사용자 요구에 응답하여 또는 또 다른 컴포넌트 또는 모듈로부터의 요구에 응답하여 실행될 수 있다.

[0016] 운영 체제 커널(106)은 다양한 운영 체제 구성 값(112)을 획득하고 그에 따라 동작한다. 비록 운영 체제 커널(106)에 의해 액세스되고 있는 것으로 도시되었지만, 운영 체제 구성 값(112)은 또한 운영 체제 로더(104) 및/또는 디바이스(100)의 다른 컴포넌트 또는 모듈에 의해서도 액세스될 수 있다. 운영 체제 구성 값(112)은 운영 체제 커널(106)(및/또는 운영 체제 로더(104))이 어떻게 동작하는지, 운영 체제 커널(106)(및/또는 운영 체제 로더(104))의 어떠한 컴포넌트가 로딩되어 실행되는지, 이들의 조합 등을 판단하기 위해 사용된 임의의 다양한 상이한 정보일 수 있다. 예를 들어, 운영 체제 구성 값(112)은 운영 체제 커널(106)(및/또는 운영 체제 로더(104))이 신뢰되지 않은 프로그램 또는 컴포넌트가 디바이스(100) 상에서 실행하도록 허여하여야 하는지 또는 운영 체제 커널(106)(및/또는 운영 체제 로더(104))이 디바이스(100) 상에서 구동하기 전에 프로그램 또는 컴포넌트를 인증하여야 하는지의 표시일 수 있다. 또 다른 예로서, 운영 체제 구성 값(112)은 악성코드 방지 애플리케이션(anti-malware application)(또는 특정 악성코드 방지 애플리케이션)이 디바이스(100) 상에서 구동되어야 하는지의 표시일 수 있다. 또 다른 예로서, 운영 체제 구성 값(112)은 디바이스(100) 상에서 구동되는 가상 머신을 관리하는 가상 머신 관리자를 위해 사용되는 구성 값 또는 설정의 표시일 수 있다. 또 다른 예로서, 운영 체제 구성 값(112)은 사용되는 특정 프로세서 또는 프로세서 코어 설정(예를 들어, 실행 가능하지 않는(non-executable)으로 표시되어야 하는 메모리 영역)의 표시일 수 있다.

[0017] 하나 이상의 실시예에서, 펌웨어(102) 및 운영 체제 로더(104)는 (사전 부트 환경(pre-boot environment) 또는 사전 운영 체제 환경(pre-operating system environment)으로서 또한 지칭된) 사전 실행 환경(pre-execution environment)의 일부분으로서 구현되며, 사전 실행 환경은 운영 체제가 부팅을 종료하여 구동하기 전에 디바이스(100) 상에서 구동하는 환경을 지칭한다. 이러한 실시예에서, 펌웨어(102) 및 운영 체제 로더(104)는 디바이스(100)의 네트워크 인터페이스 카드 상에서와 같이 디바이스(100)의 컴포넌트 상에(예를 들어, ROM 또는 플래시 메모리 내에) 저장될 수 있다. 대안적으로, 펌웨어(102) 및 운영 체제 로더(104)는 사전 실행 환경 중에 또 다른 디바이스 또는 서비스로부터 획득될 수 있다. 예를 들어, 펌웨어(102) 및 운영 체제 로더(104)는 또 다른 디바이스 또는 서비스로부터 디바이스(100)로 제공된 부트 이미지(boot image)의 일부분으로서 포함될 수 있다.

[0018] 사전 실행 환경은 다양한 상이한 방식으로 구현될 수 있으며 다양한 상이한 통상적인 기법에 기반될 수 있다. 예를 들어, 사전 실행 환경은 PXE(Preboot eXecution Environment) 표준 버전 2.0 또는 다른 버전에 따라 구현될 수 있다. 또 다른 예로서, 사전 실행 환경은 (UEFI)Unified Extensible Firmware Interface 표준 버전 2.3 또는 다른 버전에 따라 구현될 수 있다. 또 다른 예로서, 사전 실행 환경은 다양한 상이한 퍼스널 컴퓨터 BIOS(basic input/output system) 버전을 사용하여 구현될 수 있다.

[0019] 부트 프로세스 동안에, 운영 체제 로더(104)는 정책 기록(114)을 획득하며, 정책 기록(114)은 디바이스(100)가 따라야 하는 하나 이상의 정책의 기록이다. 정책의 이러한 기록은 운영 체제 구성 값(112)이 만족시켜야 하는 구성 설정 또는 값을 포함한다. 운영 체제 로더(104)는 정책 기록(114) 내의 하나 이상의 정책을 운영 체제 구성 값(112)과 비교하며, 운영 체제 구성 값(112)이 정책 기록(114) 내의 하나 이상의 정책을 만족시키면 계속하여 운영 체제 커널(106) 컴포넌트의 실행을 착수한다. 그러나, 하나 이상의 운영 체제 구성 값(112)이 정책 기록(114) 내의 정책을 만족시키지 않으면, 적절한 응답 동작(responsive action)이 취해진다. 운영 체제 커널(106)을 로딩하지 않는 것, 운영 체제 구성 값(112)을 변화시키는 것 등과 같은 다양한 상이한 응답 동작이 취해질 수 있다. 이들 응답 동작은 이하에서 보다 상세하게 논의된다. 따라서, 운영 체제 로더(104)는 운영 체제 구성 값(112)이 악성 프로그램에 의해 변화될 수 있을 상황을 식별하면서 운영 체제 구성 값(112)을 보호한다.

[0020] 하나 이상의 실시예에서, 정책 기록(114) 내의 하나 이상의 정책은 디바이스의 사전 운영 체제 환경의 하나 이상의 컴포넌트가 만족시켜야 하는 구성 설정 또는 값을 또한 포함한다. 사전 운영 체제 환경에 의해 만족되는 이들 구성 설정 또는 값은 사전 운영 체제 환경이 어떻게 동작해야 하는지, 사전 운영 체제 환경의 어떠한 컴포넌트가 로딩되어 실행되어야 하는지, 이들의 조합 등의 임의의 다양한 상이한 표시일 수 있다. 이들 구성 설정 또는 값은 운영 체제 구성 값(112)의 일부분으로서 포함될 수 있거나, 또는 대안적으로 다른 설정 또는 값일 수 있다. 예를 들어, 이들 구성 설정 또는 값은 오직 특정 운영 체제만이 로딩되어 실행되어야 한다는 것을 명시할 수 있다.

[0021] 비록 단일 운영 체제 커널(106)이 도 1에 도시되지만, 대안적으로 복수의 상이한 운영 체제 커널(106)이 디바이스(100) 상에 로딩되어 실행될 수 있다는 것을 주목해야 한다. 이들 상이한 운영 체제 커널은 각각 자체의 고유한 운영 체제 구성 값(112) 및 자체의 고유한 정책 기록(114)(또는 정책 기록(114) 내의 자체의 고유한 정책)을 가질 수 있으며, 운영 체제 로더(104)는 적절한 하나 이상의 정책을 부팅되어 있는 운영 체제 커널(106)을 위한 적절한 운영 체제 구성 값과 비교한다. 대안적으로, 이들 상이한 운영 체제 커널 중 두 개 이상의 운영 체제 커널은 운영 체제 구성 값(112) 및/또는 정책 기록(114)(및/또는 정책 기록(114) 내의 정책)의 적어도 일부분을 공유할 수 있다.

[0022] 도 2는 하나 이상의 실시예에 따른 예시적인 정책(200)을 도시한다. 정책(200)은 예를 들어 도 1의 정책 기록(114) 내의 정책으로서 포함될 수 있다. 정책(200)은 정책 식별자(202), 정책 조상 리스트(204), 및 하나 이상의 구성 값 및/또는 설정(206)을 포함한다. 정책 식별자(202), 정책 조상 리스트(204), 및 구성 값/설정(206) 중 하나 이상을 디지털 서명함으로써 정책(200) 상의 디지털 서명(208)도 또한 생성된다.

[0023] 정책 식별자(202)는 상이한 정책이 서로 구별되도록 허용하면서 정책(200)을 식별한다. 정책 식별자(202)는 예를 들어 정책(200)에 할당된 전역적 유일 식별자(globally unique identifier(GUID))일 수 있다. 정책 조상 리스트(204)는 정책(200)이 대체하는 0개 이상의 다른 정책의 리스트이다. 정책 조상 리스트(204)는 이하에서 보다 상세하게 논의되는 바와 같이 소정 유형의 공격을 방지하는 것을 용이하게 한다.

[0024] 구성 값 및/또는 설정(206)은 운영 체제 구성 값(예를 들어, 도 1의 값(112))이 만족시켜야 하는 값을 포함한다. 구성 값 및/또는 설정(206)은 정책(200) 내의 구성 값 중 하나 이상의 구성 값이 운영 체제 구성 값에 의해 만족되지 않으면 취할 응답 동작도 또한 포함할 수 있다. 이하에서 보다 상세하게 논의되는 바와 같이, 구성 값 및/또는 설정(206) 중 하나 이상의 구성 값 및/또는 설정이 운영 체제 로더 컴포넌트(operating system loader component)에 의해 선택적으로 설정될 수 있다.

[0025] 구성 값 및/또는 설정(206)은 하나 이상의 다른 정책의 식별자에 대한 참조도 또한 포함할 수 있다. 이들 하나 이상의 정책 내의 구성 값 및/또는 설정은 정책(200)의 일부분으로서 포함된다. 따라서, 정책(200)은 하나 이상의 다른 정책을 효율적으로 통합하거나 포함할 수 있다. 구성 값 및/또는 설정(206)은 하나 이상의 신뢰된 정책 발행자의 식별자도 또한 포함할 수 있다. 따라서, 정책 기록(예를 들어, 도 1의 정책 기록(114))에 정책을 추가하도록 허용된 신규 정책 발행자(new policy issuer)가 정책(200) 내에서 식별될 수 있다.

[0026] 도 1을 다시 참조하면, 운영 체제 로더(104)는 운영 체제 구성 값(112)이 정책 기록(114) 내의 하나 이상의 정책을 만족시키는지를 점검한다. 정책 기록(114)은 단일 정책을 포함할 수 있으며, 이러한 단일 정책은 이하에서 보다 상세하게 논의되는 바와 같이 하나 이상의 상이한 정책 발행자에 의해 변화될 수 있다. 대안적으로, 정책 기록(114)은 복수의 정책을 포함할 수 있으며, 이러한 복수의 정책은 각각 하나 이상의 정책 발행자에 의해 변화될 수 있다. 따라서, 상이한 정책 발행자는 예를 들어 정책 기록(114) 내에 포함시키기 위한 (정책 발

행자가 다음에 변화시킬 수 있는) 상이한 정책을 제공할 수 있다.

[0027] 구성 값은 다양한 상이한 방식으로 정책 내에서 식별될 수 있다. 하나 이상의 실시예에서, 정책은 정책을 만족시키기 위해 그러한 운영 체제 구성 값이 가져야 하는 하나 이상의 값 및 운영 체제 구성 값의 명칭(또는 다른 식별자)을 포함하면서 값을 명칭-값(name-value) 쌍으로 식별한다. 다른 실시예에서, 값은 상응하는 운영 체제 구성 값이 내재하는 순서 또는 다른 구조로 정책 내에 포함된다.

[0028] 운영 체제 구성 값(112)이 정책 기록(114) 내의 하나 이상의 정책을 만족시키는지에 대한 판단은 상이한 방식으로 수행될 수 있다. 하나 이상의 실시예에서, 운영 체제 구성 값이 정책을 만족시키는지를 판단하기 위해 수학 연산자가 사용된다. 등호, 초과, 미만 등과 같은 다양한 상이한 수학 연산자가 사용될 수 있다. 다른 실시예에서, 예를 들어 운영 체제 구성 값이 정책 내의 한 세트의 값 중 하나의 값으로서 포함되는지와 같이 운영 체제 구성 값이 정책을 만족시키는지를 판단하기 위해 다른 연산자 또는 논리 공식이 사용된다.

[0029] 복수의 정책이 정책 기록(114) 내에 포함되는 상황에서, 운영 체제 구성 값(112)이 정책 기록(114) 내의 정책을 만족시키는지에 대한 판단은 운영 체제 구성 값(112)이 정책 기록(114) 내의 복수의 정책 각각을 만족시키는지에 대한 판단이다. 따라서, 복수의 정책은 운영 체제 구성 값(112)이 정책 기록(114) 내의 정책을 만족시키는지를 판단하기 위해 조합되어 있는 것으로 생각될 수 있다.

[0030] 운영 체제 구성 값(112)이 정책 기록(114)을 만족시키면, 운영 체제 로더(104)는 계속하여 운영 체제 커널(106)의 실행을 착수한다. 그러나, 하나 이상의 운영 체제 구성 값(112)이 정책 기록(114)을 만족시키지 않으면, 정책 기록(114)을 만족시키지 않는 하나 이상의 운영 체제 구성 값(112)에 응답하여 적절한 동작이 취해진다. 상이한 운영 체제 구성 값을 위해 상이한 응답 동작이 취해질 수 있거나, 복수의 운영 체제 구성 값을 위해 동일한 응답 동작이 취해질 수 있다. 이들 응답 동작은 부트 프로세스를 중지시켜서 운영 체제가 디바이스(100) 상에 로딩되어 구동되지 않는 동작은 물론 부트 프로세스가 계속되도록 허용하여 운영 체제가 디바이스(100) 상에 로딩되어 구동되는 동작을 포함할 수 있다.

[0031] 하나 이상의 실시예에서, 취해지는 응답 동작이 정책 기록(114) 내에 포함된다. 정책 기록(114) 내의 각각의 정책은 정책의 적어도 일부분이 만족되지 않으면 (예를 들어, 특정 운영 체제 구성 값(112)이 정책을 만족시키지 않으면) 취해지는 응답 동작의 (예를 들어, 도 2의 구성 값 및/또는 설정(206)의 일부분으로서의) 표시를 포함할 수 있다. 다른 실시예에서, 취해지는 응답 동작은 운영 체제 로더(104) 내에 포함되거나(예를 들어, 구성 값 내에 프로그래밍되거나 구성 값으로서 설정됨) 또는 이와 달리 운영 체제 로더(104)에 의해 획득된다.

[0032] 응답 동작은 부트 프로세스를 중지시키는 것일 수 있으며, 그 결과 운영 체제 로더(104)는 운영 체제 커널(106)의 실행을 착수시키지 않아서 운영 체제가 디바이스(100) 상에 로딩되어 구동되지 않는다. 대안적으로, 응답 동작은 정책을 만족시키지 않는 운영 체제 구성 값(112)을 무시하는 것일 수 있으며, 대신에 (예를 들어, 정책 내에 포함된) 또 다른 값을 사용할 수 있다. 대안적으로, 응답 동작은 운영 체제 구성 값(112)을 정책으로부터의(또는 이와 달리 정책에 의해 식별된) 값으로 덮어쓰는 것일 수 있고, 부트 프로세스가 계속되도록 허용할 수 있다. 대안적으로, 응답 동작은 운영 체제 구성 값(112)을 사용하는 것일 수 있고, 부트 프로세스가 계속되도록 허용할 수 있지만, 운영 체제 구성 값(112)이 정책을 만족시키지 않았다는 통지(특정 운영 체제 구성 값 및/또는 정책의 표시가 통지 내에 포함될 수 있음)를 (예를 들어, 또 다른 컴포넌트, 디바이스 또는 서비스로) 기록하거나 발송하는 것과 같이 이벤트를 보고할 수 있다.

[0033] 대안적으로, 응답 동작은 디바이스(100)의 사용자를 프롬프트(prompt)하는 것(예를 들어, 부트 프로세스를 계속하기 위해 사용자 승인을 수신하는 것)일 수 있다. 이러한 프롬프팅(prompting)는 예를 들어 사용자에게 현재의 운영 체제 구성 값을 승인할 것을 요구하는 프롬프트(prompt)를 포함할 수 있다. 이러한 프롬프팅은 정책을 만족시키기 위해 구성 값이 어떤 값이 되어야 하는지의 표시도 또한 포함할 수 있다. 그런 다음, 사용자는 예를 들어 버튼 또는 키를 누르는 것, 스크린의 특정 부분을 접촉하는 것, 청취 가능한 입력을 제공하는 것, 운영 체제 로더(104)에 의해 신뢰된(또는 그에 의해 검증될 수 있는) 보안 토큰(security token)을 제공하는 것 등과 같이 현재의 운영 체제 구성 값을 계속하는 것을 승인(또는 반대)하기 위해 다양한 상이한 입력을 제공할 수 있다. 운영 체제 로더(104)는 입력이 원격 디바이스보다는 디바이스(100)의 사용자로부터 수신되는 것(예를 들어, 디바이스(100)의 키보드, 터치스크린, 마이크 등으로부터 수신되는 것)을 검증(예를 들어, 사용자 입력이 원격 디바이스로부터 수신된 요구보다는 키 누름 또는 국부 마이크로부터 수신되는 것을 검증)하는데 주의를 기울인다. 따라서, 이러한 상황에서, 부트 프로세스는 사용자가 디바이스(100)에 존재하고 부트 프로세스를 계속하는 것을 승인하는 경우에만 계속될 수 있으며, 악성 디바이스 또는 디바이스(100)의 악성 컴포넌트는 부트 프로세스를 계속하는 것을 승인할 수 없다.

[0034] 정책 기록(114)은 운영 체제 로더(104)가 정책 기록(114)을 변화시킬 수 있지만 운영 체제 로더(104) 후에 실행된 컴포넌트(특히, 운영 체제 커널(106)은 물론 다른 운영 체제 컴포넌트 및/또는 사용자 모드 컴포넌트)가 정책 기록(114)을 변화시키지 못하게 하는 보안 방식으로 유지된다. 이러한 보안을 반영하기 위해 정책 기록(114)은 점선(116)에 의해 둘러싸이는 것으로 도시된다. 정책 기록(114)은 다양한 상이한 방식의 이러한 보안 방식으로 유지될 수 있다.

[0035] 하나 이상의 실시예에서, 정책 기록(114)은 비휘발성 RAM(nonvolatile RAM(NVRAM))과 같은 쓰기 가능한 비휘발성 메모리 내에 저장된다. 쓰기 가능한 NVRAM은 오직 소정의 조건 및/또는 소정의 시간에서만 액세스될 수 있다. 하나 이상의 실시예에서, 쓰기 가능한 NVRAM은 TPM(Trusted Platform Module)을 통해 액세스된다. TPM에 관한 추가 정보는 오레곤 주, 비버톤의 트러스티드 컴퓨팅 그룹(Trusted Computing Group)으로부터 입수 가능하다. TPM은 쓰기 가능한 NVRAM이 소정의 시점 또는 소정의 이벤트가 발생할 때까지 읽혀지고 쓰여지도록 허용하며, 그러한 소정의 시점 또는 소정의 이벤트가 발생한 후에 TPM은 쓰기 가능한 NVRAM이 읽혀지도록 허용하지만 쓰여지도록 허용하지는 않는다. 이러한 소정의 시점 또는 이벤트는 예를 들어 쓰기 가능한 NVRAM을 폐쇄하거나 잠그라는 컴포넌트로부터의 요구일 수 있다. 따라서, 운영 체제 로더(104)는 쓰기 가능한 NVRAM 내의 정책 기록(114)을 변화시킬 수 있으며, 그런 다음 쓰기 가능한 NVRAM이 잠금 상태로 될 수 있다. 따라서, 쓰기 가능한 NVRAM이 잠금 상태이므로 운영 체제 로더(104)는 악성 프로그램이 정책 기록(114)을 간섭하지 못하게 할 수 있다. 디바이스(100)가 다시 부팅될 때까지 쓰기 가능한 NVRAM은 잠금 해제되지 않는다. 쓰기 가능한 NVRAM은 디바이스(100)가 부팅되는 다음 시기에 잠금 해제되지만, 운영 체제 로더(104)는 악성 프로그램이 쓰기 가능한 NVRAM을 실행시키고 쓰기 가능한 NVRAM에 쓸 수 있기 전에 쓰기 가능한 NVRAM을 다시 잠근다. 마찬가지로, 다른 유형의 저장 디바이스(예를 들어, 자기 디스크 드라이브)는 소정의 조건 및/또는 소정의 시간에서만 액세스되도록 구현될 수 있다.

[0036] 대안적으로, 정책 기록(114)은 변화가 신뢰 개체에 의해 서명된 경우에만 정책 기록(114)에 대한 변화를 허여하는 보호식 인터페이스(protected interface)(예를 들어, 애플리케이션 프로그래밍 인터페이스(application programming interface, API))를 통해서만 액세스 가능한 정책 기록(114)에 의해서와 같이 다른 기법을 사용하는 보안 방식으로 유지될 수 있다. 이러한 신뢰 개체는 운영 체제 로더(104)에 의해 신뢰 개체(예를 들어, 운영 체제 로더(104)에 의해 신뢰할 수 있는 것으로 알려진 개체로서, 운영 체제 로더(104)가 그러한 개체를 위한 공개 키를 갖고 있음)이다. 예를 들어, 정책 기록(114)은 UEFI 인증된 변수로서 저장될 수 있으며, UEFI 인증된 변수는 변화가 신뢰 개체에 의해 서명된 경우에만 변화될 수 있다. 정책 기록(114)에 대한 임의의 요구된 변화는 신뢰 개체에 의해 서명된 것으로 검증되며, 신뢰 개체에 의해 서명되면 이러한 요구된 변화가 수행되지만 신뢰 개체에 의해 서명되지 않으면 이러한 요구된 변화가 수행되지 않는다.

[0037] 또 다른 예로서, 디바이스(100)가 가상 머신으로서 구현되는 상황에서, 정책 기록(114)은 디바이스 상의 하나 이상의 가상 머신의 동작을 관리하는 가상 머신 관리자에 의해 보안 방식으로 유지될 수 있다. 가상 머신 관리자는 운영 체제 로더(104)가 정책 기록(114) 내의 정책을 변화시키도록 허여할 수 있지만 다른 컴포넌트가 그러한 정책을 변화시키도록 허여하지는 않는다.

[0038] 정책 기록(114)에 대한 변화는 정책 기록(114)에 정책을 추가하는 것, 정책 기록(114)으로부터 정책을 제거하는 것, 및/또는 정책 기록(114) 내의 정책을 신규 정책으로 대체하는 것을 포함한다. 하나 이상의 실시예에서, 정책 기록(114)에 대한 변화는 이러한 변화가 신뢰된 정책 발행자로부터 수신되면(예를 들어, 변화가 운영 체제 로더(104)에 의해 신뢰된 정책 발행자 개체에 의해 디지털 서명되면) 운영 체제 로더(104)에 의해 수행된다. 정책 기록(114) 내의 정책을 변화시키라는 요구는 운영 체제 로더(104)로 상이한 방식으로 제공될 수 있다. 하나 이상의 실시예에서, 운영 체제 커널(106) 또는 디바이스(100) 상에서 구동하는 또 다른 컴포넌트는 디바이스(100)의 다음 부트 상에서 운영 체제 로더(104)에 액세스 가능한 영구 위치 내에 정책에 대한 변화를 저장한다. 디바이스(100)의 다음 부트 상에서, 운영 체제 로더(104)는 변화를 획득하고, 적절하다면 그 변화를 구현한다. 운영 체제 커널(106) 또는 디바이스(100) 상에서 구동하는 다른 컴포넌트는 변화와 함께 특정 유형의 변화에 대한 요구(예를 들어, 특정 정책이 제거되어야 하거나 또 다른 정책을 대체해야 하는지의 표시)도 또한 저장할 수 있다. 대안적으로, 특정 유형의 변화에 대한 요구는 내재적(예를 들어, 영구 위치 내의 저장된 정책의 존재는 운영 체제 로더(104)에 의해 그러한 정책을 정책 기록(114)에 추가하라는 요구로 간주됨)일 수 있다.

[0039] 운영 체제 로더(104)는 정책을 제거하라는 (정책 발행자로부터의) 요구에 응답하여 정책 기록(114)으로부터 정책을 제거할 수 있다. 운영 체제 로더(104)는 요구가 신뢰 개체인 정책 발행자로부터 유래되는 것을 검증하며, 그런 다음 요구가 신뢰 개체인 정책 발행자로부터 유래되면 정책을 제거하고, 요구가 신뢰 개체인 정책 발행자

로부터 유래되지 않으면 정책을 제거하지 않는다.

[0040] 마찬가지로, 운영 체제 로더(104)는 정책을 추가하라는 (정책 발행자로부터의) 요구에 응답하여 정책 기록(114)에 신규 정책을 추가할 수 있다. 운영 체제 로더(104)는 신규 정책(및 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되는 것을 검증하며, 신규 정책(및 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되면 신규 정책을 추가하지만, 신규 정책(및/또는 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되지 않으면 신규 정책을 추가하지 않는다.

[0041] 추가로, 운영 체제 로더(104)는 정책 기록(114) 내의 정책(정책의 현재 버전으로도 또한 지칭됨)을 신규 정책(정책의 신규 버전으로도 또한 지칭됨)으로 대체할 수 있다. 신규 정책이 수신될 때, 운영 체제 로더(104)는 신규 정책(및 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되는 것을 검증한다. 신규 정책(및/또는 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되지 않으면 운영 체제 로더(104)는 정책의 현재 버전을 정책의 신규 버전으로 대체하지 않는다.

[0042] 그러나, 신규 정책(및 선택적으로 요구)이 신뢰 개체인 정책 발행자로부터 유래되면, 운영 체제 로더(104)는 정책의 신규 버전이 실제로 정책의 현재 버전의 보다 신규한 버전인지를 점검한다. 운영 체제 로더(104)는 정책의 현재 버전이 정책의 신규 버전의 조상 리스트 내에 포함되는지를 점검함으로써 정책의 신규 버전이 실제로 정책의 현재 버전의 보다 신규한 버전인지를 점검할 수 있다. 정책의 신규 버전은 정책의 신규 버전에 의해 대체되는 동일한 정책 발행자에 의해 발행된 0개 이상의 이전 정책을 식별하는 정책 조상 리스트를 포함한다. 정책 조상 리스트는 그들의 정책 식별자(예를 들어, GUID)에 의해 이전 정책을 식별할 수 있다. 정책의 신규 버전이 신뢰 개체인 정책 발행자로부터 유래되고 정책의 현재 버전이 정책의 신규 버전의 정책 조상 리스트 내에 포함되면, 운영 체제 로더(104)는 정책의 현재 버전을 정책의 신규 버전으로 대체한다. 그렇지 않으면, 운영 체제 로더(104)는 정책의 현재 버전을 정책의 신규 버전으로 대체하지 않는다.

[0043] 정책 조상 리스트의 사용이 악성 프로그램 또는 사용자에 의한 역행(rollback) 또는 재생(replay) 공격으로부터 보호하는 것을 용이하게 한다는 것을 주목해야 한다. 예를 들어, 악성 프로그램 또는 사용자는 (예를 들어, 신규 보안 관련 값 또는 설정을 포함하는) 정책의 현재 버전을 (예를 들어, 악성 프로그램 또는 사용자가 디바이스(100)의 컴포넌트에 부적절하게 액세스하도록 허용하는 구식 보안 관련 값 또는 설정을 포함하는) 정책의 보다 오래된 버전으로 대체하려고 시도할 수 있다. 정책의 현재 버전이 정책의 신규 버전의 정책 조상 리스트 내에 포함된 경우에만 정책의 현재 버전을 신규 정책으로 대체함으로써, 운영 체제 로더(104)는 정책의 현재 버전이 정책의 보다 오래된 버전에 의해 대체되지 않는 것을 보장한다. 비록 정책의 보다 오래된 버전이 신뢰 개체인 정책 발행자에 의해 입수 가능하게 될 수 있을지라도, 정책의 보다 오래된 버전은 정책의 현재 버전을 포함하는 조상 리스트를 갖지 않을 것이며, 따라서 운영 체제 로더(104)는 정책의 현재 버전을 정책의 보다 오래된 버전으로 대체하지 않을 것이다.

[0044] 또한, 하나 이상의 실시예에서, 정책 기록(114)에 대한 변화는 이러한 변화가 디바이스(100)의 사용자와 같이 (예를 들어, 운영 체제 로더(104) 및/또는 펌웨어(102)에 의해 신뢰된) 사전 운영 체제 환경에 의해 신뢰 개체 또는 다른 신뢰 개체에 의해 승인된 경우에만 운영 체제 로더(104)에 의해 수행된다. 개체가 디바이스(100)의 사용자일 때, 운영 체제 로더(104)는 예를 들어 디바이스(100)의 (또는 디바이스(100)에 결합된) 스크린 상에 시각 프롬프트를 디스플레이함으로써, 디바이스(100)의(또는 디바이스(100)에 결합된) 스피커 상에 청취 가능한 프롬프트를 재생함으로써 등과 같이 변화의 승인을 위해 디바이스(100)의 사용자를 프롬프트한다. 사용자는 버튼 또는 키를 누름으로써, 스크린의 특정 부분을 접촉함으로써, 청취 가능한 입력을 제공함으로써 등과 같이 다양한 상이한 입력을 제공함으로써 정책에 대한 변화를 승인할 수 있다. 운영 체제 로더(104)는 입력이 원격 디바이스보다는 디바이스(100)의 사용자로부터 수신되는 것(예를 들어, 디바이스(100)의 키보드, 터치스크린, 마이크 등으로부터 수신되는 것)을 검증(예를 들어, 사용자 입력이 원격 디바이스로부터 수신된 요구보다는 키 누름 또는 국부 마이크로부터 수신되는 것을 검증)하는데 주의를 기울인다. 따라서, 이러한 상황에서, 정책 기록(114)에 대한 변화는 사용자가 디바이스(100)에 존재하고 변화를 승인한 경우에만 수행될 수 있으며, 악성 디바이스 또는 디바이스(100)의 악성 컴포넌트는 이러한 변화를 승인할 수 없다.

[0045] 개체가 (사용자가 아닌) 사전 운영 체제 환경에 의해 신뢰된 또 다른 개체일 때, 정책 기록(114)에 대한 변화는 개체에 의해 디지털 서명된다. 운영 체제 로더(104)는 디지털 서명을 검증하며, 디지털 서명이 사전 운영 체제 환경에 의해 신뢰된 (예를 들어, 운영 체제 로더(104)에 의해 신뢰된) 개체로부터 유래된 것으로 검증되는 경우에만 정책 기록(114)에 대한 변화를 수행한다. 디지털 서명이 검증되지 않으면, 정책 기록(114)에 대한 변화는 수행되지 않는다.

[0046] 하나 이상의 실시예에서, 정책 기록(114) 내의 정책은 연관된 타임스탬프(timestamp)(예를 들어, 날짜 및 시간)를 갖는다. 정책에 연관된 타임스탬프는 정책의 일부분으로 포함될 수 있거나, 또는 대안적으로 별개로 유지될 수 있다. 예를 들어, 정책 식별자 및 타임스탬프의 별개의 기록은 운영 체제 로더(104)에 의해 유지될 수 있으며, 이러한 기록은 보안 방식으로 (예를 들어, 보안 방식으로 유지되고 있는 정책 기록(114) 내의 정책에 관하여 전술된 것과 유사한 다양한 상이한 보안 방식으로) 유지된다.

[0047] 운영 체제 로더(104)는 정책 기록(114)을 변화시키는지를 판단하는데(예를 들어 정책의 신규 버전이 실제로 정책의 현재 버전의 보다 신규한 버전인지를 판단하는데) 이들 타임스탬프를 사용할 수 있다. 정책 발행자는 상이한 타임스탬프 이외에 정책의 두 개의 버전을 위한 동일한 정책 식별자를 사용하여 정책의 하나의 버전을 그러한 정책의 신규 버전으로 대체하려고 의도할 수 있다. 운영 체제 로더(104)는 정책의 신규 버전(및 선택적으로 정책을 변화시키라는 요구)이 신뢰 개체인 정책 발행자로부터 유래되는지, 및 정책의 신규 버전이 정책의 현재 버전보다 최근의 타임스탬프를 갖는지를 점검한다. 정책의 신규 버전이 신뢰 개체인 정책 발행자로부터 유래되고 정책의 현재 버전이 정책의 현재 버전보다 최근의 타임스탬프를 가지면, 운영 체제 로더(104)는 정책의 현재 버전을 정책의 신규 버전으로 대체한다. 그렇지 않으면, 운영 체제 로더(104)는 정책의 현재 버전을 정책의 신규 버전으로 대체하지 않는다. 정책의 현재 버전과 정책의 신규 버전이 동일한 정책 식별자를 가지므로, 정책의 현재 버전을 정책의 신규 버전으로 대체하는지의 판단은 정책의 신규 버전의 조상 리스트보다는 정책들의 버전의 타임스탬프에 기반한다.

[0048] 마찬가지로, 정책 기록(114) 내의 정책은 정책 발행자에 의해 할당된 연관된 버전 번호를 가질 수 있다. 정책의 버전 번호는 정책의 각각의 신규 버전에 대해 증가된다(또는 한 세트 내에서 다음 버전 번호가 선택된다). 버전 번호는 타임스탬프와 유사하게 사용될 수 있지만, 타임스탬프와는 다른 숫자(및/또는 다른 문자)이다.

[0049] 대안적으로, 운영 체제 로더(104)는 정책 기록(114)을 변화시키는지를 판단하는데 타임스탬프 및/또는 버전 번호를 사용하지 않아도 된다. 이러한 상황에서, 정책 발행자가 정책의 하나의 버전을 그러한 정책의 신규 버전으로 대체하려고 의도하면, 정책 발행자는 정책의 두 개의 버전에 대해 상이한 정책 식별자를 사용하며, 대체되는 정책의 버전의 정책 식별자를 정책의 신규 버전의 조상 리스트 내에 포함한다.

[0050] 하나 이상의 실시예에서, 정책 기록(114)에 대한 변화는 부트 프로세스 동안에 운영 체제 로더(104)에 의해 쓰여지는 값도 또한 포함한다. 정책 내의 특정 구성 설정에 대해, 운영 체제 로더(104)는 부트 프로세스 동안에 디바이스(100) 내에서 하나 이상의 현재 값 또는 설정을 캡처한다. 이들 캡처된 값 또는 설정은 정책의 일부분으로서 저장되며(또는 이와 달리 정책에 연관되며), 디바이스(100)의 다음 부트 상에서 만족되는 정책의 일부분으로 취급된다. 따라서, 운영 체제 로더(104)는 디바이스(100)의 다음 부트 상에서 이들 캡처된 설정 또는 값이 운영 체제 구성 값(112)에 의해 만족되는 것을 검증한다.

[0051] 어떠한 설정이 부트 프로세스 동안에 캡처된 그들의 현재 값 또는 설정을 가져야 하는지는 상이한 방식으로 식별될 수 있다. 예를 들어, 정책은 부트 프로세스 동안에 특정 값이 운영 체제 로더(104)에 의해 캡처되어 저장되어야 하는 것을 표시하는 설정을 포함할 수 있다. 또 다른 예로서, 운영 체제 로더(104)는 부트 프로세스 동안에 어떠한 특정 값이 운영 체제 로더(104)에 의해 캡처되어 저장되어야 하는지의 표시를 이용하여 구성될 수 있거나(예를 들어, 그 표시를 이용하여 프로그래밍될 수 있거나) 또는 이와 달리 그 표시를 획득할 수 있다. 또 다른 예로서, 운영 체제 로더(104)는 디바이스(100)의 보안이 더 강해지거나 개선될 때(예를 들어, 악성코드 방지 프로그램이 설치될 때, 방화벽 프로그램이 설치될 때 등)를 검출할 수 있으며, 그러한 보다 강해지거나 개선된 보안에 연관된 값 또는 설정을 캡처하여 저장(예를 들어, 악성코드 방지 프로그램의 표시를 캡처하여 저장)할 수 있다.

[0052] 디바이스(100)가 여러 차례 부팅될 수 있으므로, 그들 복수의 부트 프로세스 중 어떠한 부트 프로세스가 값이 캡처되어 저장되어야 하는 부트 프로세스인지는 상이한 방식으로 식별될 수 있다. 값이 이미 캡처되어 저장되지 않으면(또는 어떠한 값도 이미 캡처되어 저장되어 있지 않다고 알게 되면) 값은 디바이스(100)가 부팅되는 첫 번째 기간 동안에 캡처되어 저장될 수 있다. 대안적으로, 운영 체제 로더(104)는 디바이스(100)의 어떠한 부트 상에서 값이 캡처되어 저장되어야 하는지의 표시를 이용하여 구성될 수 있거나(예를 들어, 그 표시를 이용하여 프로그래밍될 수 있거나) 또는 이와 달리 그 표시를 획득할 수 있다. 대안적으로, 정책 기록(114) 내의 정책은 디바이스(100)의 어떠한 부트 상에서 값이 캡처되어 저장되어야 하는지의 표시를 포함할 수 있다.

[0053] 대안적으로, (예를 들어, 현재 부트 프로세스 동안에 또는 디바이스(100)의 다음 부트 상에서) 값이 캡처되어 저장되어야 하는 것을 운영 체제 로더(104)에 표시하는 사용자 입력이 수신될 수 있다. 사용자 입력은 예를 들어 버튼 또는 키를 누름으로써, 스크린의 특정 부분을 접촉함으로써, 청취 가능한 입력을 제공함으로써 등과 같

이 사용자에 의해 상이한 방식으로 제공될 수 있다. 운영 체제 로더(104)는 입력이 원격 디바이스보다는 디바이스(100)의 사용자로부터 수신되는 것을 검증(예를 들어, 사용자 입력이 원격 디바이스로부터 수신된 요구보다는 키 누름 또는 국부 마이크로부터 수신되는 것을 검증)하는데 주의를 기울인다. 따라서, 이러한 상황에서, 값을 캡처하여 저장하라는 요구는 사용자가 디바이스(100)에 존재하고 이러한 캡처 및 저장을 승인한 경우에만 수행될 수 있으며, 악성 디바이스 또는 디바이스(100)의 악성 컴포넌트는 이러한 값의 캡처 및 저장을 승인할 수 없다.

[0054] 도 3은 하나 이상의 실시예에 따라 운영 체제 구성 값을 보호하기 위한 예시적인 프로세스(300)를 도시하는 흐름도이다. 프로세스(300)는 도 1의 디바이스(100)와 같은 디바이스에 의해 수행되며, 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합으로 구현될 수 있다. 프로세스(300)는 디바이스 상에 운영 체제를 구동하기 전에 디바이스 상에 사전 운영 체제 환경의 일부분으로서 수행된다. 프로세스(300)는 한 세트의 동작으로서 도시되어 있으며, 다양한 동작의 작동을 수행하기 위해 도시된 순서로 제한되지는 않는다. 프로세스(300)는 운영 체제 구성 값을 보호하기 위한 예시적인 프로세스이며, 운영 체제 구성 값을 보호하는 추가 논의는 상이한 도면을 참조하여 본 명세서에 포함된다.

[0055] 프로세스(300)에서, 운영 체제를 위한 구성 설정 및/또는 값을 식별하는 정책이 획득된다(동작 302). 정책은 운영 체제 로더에 의해 변화될 수 있지만, 전술된 바와 같이 운영 체제는 정책을 변화시키지 못한다.

[0056] 정책은 운영 체제에 의해 사용된 구성 값과 비교되며(동작 304), 운영 체제에 의해 사용된 구성 값이 정책을 만족시키는지에 대한 점검이 수행된다(동작 306). 운영 체제에 의해 사용된 구성 값이 정책을 만족시키는지는 전술된 바와 같이 다양한 상이한 방식으로 판단될 수 있다.

[0057] 구성 값이 정책을 만족시키면, 운영 체제는 구성 값을 이용하여 부팅하도록 허용된다(동작 308). 그러나, 구성 값이 정책을 만족시키지 않으면, 응답 동작이 취해진다(동작 310). 전술된 바와 같이 다양한 상이한 응답 동작이 취해질 수 있다.

[0058] 도 4는 하나 이상의 실시예에 따라 디바이스 내의 정책을 변화시키기 위한 예시적인 프로세스(400)를 도시하는 흐름도이다. 프로세스(400)는 도 1의 디바이스(100)와 같은 디바이스에 의해 수행되며, 소프트웨어, 펌웨어, 하드웨어 또는 이들의 조합으로 구현될 수 있다. 프로세스(400)는 디바이스 상에 운영 체제를 구동하기 전에 디바이스 상에 사전 운영 체제 환경의 일부분으로서 수행된다. 프로세스(400)는 한 세트의 동작으로서 도시되어 있으며, 다양한 동작의 동작을 수행하기 위해 도시된 순서로 제한되지는 않는다. 프로세스(400)는 디바이스 내의 정책을 변화시키기 위한 예시적인 프로세스이며, 디바이스 내의 정책을 변화시키는 추가 논의는 상이한 도면을 참조하여 본 명세서에 포함된다.

[0059] 프로세스(400)에서, 운영 체제가 실행되거나 구동되기 위해 운영 체제의 구성 값에 의해 만족되어야 하는 운영 체제를 위한 구성 설정 및/또는 값을 식별하는 정책에 대한 변화가 수신된다(동작 402). 전술된 바와 같이 운영 체제는 정책을 변화시키지 못한다.

[0060] 정책에 대한 변화가 신뢰 개체에 의해 승인되는지에 대한 점검이 수행된다(동작 404). 이러한 신뢰 개체는 사전 운영 체제 환경(예를 들어, 운영 체제 로더)에 의해 신뢰 개체이며, 이러한 점검은 전술된 바와 같이 변화를 승인하도록 사용자를 프롬프트함으로써, 또는 변화가 신뢰 개체에 의해 디지털 서명되는 것을 검증함으로써 수행될 수 있다. 변화가 신뢰 개체에 의해 승인되지 않으면, 정책이 변화되지 않는다. 그러나, 변화가 신뢰 개체에 의해 승인되면, 동작(402)에서 수신된 변화에 따라 정책이 변화된다(동작 406). 신뢰 개체 승인에 추가하여, 전술된 바와 같이 정책을 변화시키기 전에 타임스탬프, 조상 리스트 등을 점검하는 것과 같은 다양한 상이한 검증 또는 점검도 또한 수행될 수 있다.

[0061] 본 명세서에서 논의된 운영 체제 구성 값 보호 기법은 다양한 용도 시나리오를 지원한다. 예를 들어, 운영 체제 구성 값 및 정책은 다양한 제조자 또는 개발자 중 하나의 제조자 또는 개발자로부터의 악성코드 방지 프로그램이 디바이스 상에서 구동되어야 한다는 것을 표시할 수 있으며, 이러한 악성코드 방지 프로그램이 디바이스 상에서 구동하고 있지 않는 한 운영 체제가 디바이스 상에 로딩되어 구동하지 않아야 한다는 것을 표시할 수 있다. 운영 체제를 로딩하여 구동하기 위해 악성코드 방지 프로그램이 구동하도록 요구되지 않는다는 것을 표시하기 위해 악성 프로그램이 운영 체제 구성 값을 변경하도록 시도되었다면, 디바이스가 부팅되는 다음 시기에 운영 체제 로더 컴포넌트는 운영 체제 구성 값이 정책을 만족시키지 않는다는 것을 검출할 것이며, 따라서 악성코드 방지 프로그램이 없으면 운영 체제를 로딩하여 구동하지 않는다.

[0062] 또 다른 예로서, 디바이스는 디폴트(default) 운영 체제 정책을 갖는 제조자 또는 유통업자로부터 출하될 수 있

다. 디바이스의 구매자는 기업 환경에서 (예를 들어, 회사 또는 가정 네트워크의 일부분으로서) 디바이스를 사용하고 싶어할 수 있으며, 자신이 디폴트 운영 체제 정책 대신에 사용하고자 했던 기업 정책을 가질 수 있다. 이러한 기업 정책은 디폴트 운영 체제 정책 대신에 상이한 보안 관련 설정 등을 가질 수 있으며, 기업 정책은 디폴트 운영 체제 정책의 식별자를 포함하는 조상 리스트를 갖는다. 기업 환경의 관리자는 신뢰 개체일 수 있으며, 기업 정책에 대한 디지털 서명을 생성할 수 있고, 디지털 서명은 운영 체제 로더로 제공된다. 기업 정책이 신뢰 개체에 의해 서명되고 조상 리스트 상의 디폴트 운영 체제를 식별하므로, 기업 정책은 정책 기록 내의 디폴트 운영 체제 정책을 대체한다. 그러나, 다음 디폴트 운영 체제 정책이 조상 리스트 상의 기업 정책을 식별하지 않을 것이므로, 다음 디폴트 운영 체제 정책은 기업 정책을 실수로 대체하지는 않을 것이다.

[0063] 도 5는 하나 이상의 실시예에 따라 운영 체제 구성 값 보호를 구현하도록 구성될 수 있는 예시적인 컴퓨팅 디바이스(500)를 도시한다. 컴퓨팅 디바이스(500)는 예를 들어 도 1의 디바이스(100)일 수 있거나, 또는 디바이스(100)가 내부에 구현된 가상 머신을 구동시킬 수 있다.

[0064] 컴퓨팅 디바이스(500)는 하나 이상의 프로세서 또는 프로세싱 유닛(502), 하나 이상의 메모리 및/또는 저장소 컴포넌트(506)를 포함할 수 있는 하나 이상의 컴퓨터 판독 가능 매체(504), 하나 이상의 입력/출력(I/O) 디바이스(508), 및 다양한 컴포넌트 및 디바이스가 서로 통신하도록 허용하는 버스(510)를 포함한다. 컴퓨터 판독 가능 매체(504) 및/또는 하나 이상의 I/O 디바이스(508)는 컴퓨팅 디바이스(500)의 일부분으로서 포함될 수 있거나 또는 컴퓨팅 디바이스(500)에 결합될 수 있다. 버스(510)는 다양한 상이한 버스 아키텍처를 사용하는 메모리 버스 또는 메모리 제어기, 주변 버스(peripheral bus), 가속형 그래픽 포트(accelerated graphics port), 프로세서 또는 로컬 버스 등을 포함하는 몇 가지 유형의 버스 구조 중 하나 이상의 버스 구조를 표현한다. 버스(510)는 유선 및/또는 무선 버스를 포함할 수 있다.

[0065] 메모리/저장소 컴포넌트(506)는 하나 이상의 컴퓨터 저장 매체를 표현한다. 컴포넌트(506)는 (RAM과 같은) 휘발성 매체 및/또는 (ROM, 플래시 메모리, 광 디스크, 자기 디스크 등과 같은) 비휘발성 매체를 포함할 수 있다. 컴포넌트(506)는 고정식 매체(예를 들어, RAM, ROM, 고정식 하드 드라이브 등)는 물론 제거 가능형 매체(예를 들어, 플래시 메모리 드라이브, 제거 가능한 하드 드라이브, 광 디스크 등)를 포함할 수 있다.

[0066] 본 명세서에서 논의된 기법은 소프트웨어로 구현될 수 있으며, 명령어는 하나 이상의 프로세싱 유닛(502)에 의해 실행될 수 있다. 상이한 명령어가 프로세싱 유닛(502) 내에, 프로세싱 유닛(502)의 다양한 캐시 메모리 내에, 컴퓨팅 디바이스(500)의 다른 캐시 메모리(도시되지 않음) 내에, 다른 컴퓨터 판독 가능 매체 상에 등과 같이 컴퓨팅 디바이스(500)의 상이한 컴포넌트 내에 저장될 수 있다는 것이 이해되어야 한다. 또한, 컴퓨팅 디바이스(500) 내에 명령어가 저장되는 위치가 시간에 대해 변화할 수 있다는 것이 이해되어야 한다.

[0067] 하나 이상의 입력/출력 디바이스(508)는 사용자가 명령(command) 및 정보를 컴퓨팅 디바이스(500)로 입력하도록 허용하며, 또한 정보가 사용자 및/또는 다른 컴포넌트 또는 디바이스로 제시되도록 허용한다. 입력 디바이스의 예는 키보드, 커서 제어 디바이스(예를 들어, 마우스), 마이크, 스캐너 등을 포함한다. 출력 디바이스의 예는 디스플레이 디바이스(예를 들어, 모니터 또는 프로젝터), 스피커, 프린터, 네트워크 카드 등을 포함한다.

[0068] 다양한 기법이 본 명세서에서 소프트웨어 또는 프로그램 모듈의 일반적인 맥락으로 설명될 수 있다. 일반적으로, 소프트웨어는 특정 임무를 수행하거나 특정 추상 데이터 유형(particular abstract data type)을 구현하는 루틴(routine), 프로그램, 애플리케이션, 객체(object), 컴포넌트, 데이터 구조 등을 포함한다. 이들 모듈 및 기법의 구현은 어떤 형태의 컴퓨터 판독 가능 매체 상에 저장될 수 있거나 그러한 매체를 통해 송신될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨팅 디바이스에 의해 액세스될 수 있는 임의의 입수 가능한 매체일 수 있다. 예를 들어 그리고 제한 없이, 컴퓨터 판독 가능 매체는 "컴퓨터 저장 매체" 및 "통신 매체"를 포함할 수 있다.

[0069] "컴퓨터 저장 매체(computer storage media)"는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈, 또는 다른 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 제거 가능한 및 제거 가능하지 않은 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD(digital versatile disk) 또는 다른 광학 저장소, 자기 카세트, 자기 테이프, 자기 디스크 저장소 또는 다른 자기 저장 디바이스, 또는 요구된 정보를 저장하기 위해 사용될 수 있으면서 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만 그에 제한되지는 않는다.

[0070] "통신 매체(communicatioin media)"는 전형적으로 반송파(carrier wave) 또는 다른 수송 메카니즘과 같은 변조 데이터 신호(modulated data signal) 내에 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈, 또는 다른 데이터를 구현한다. 통신 매체는 임의의 정보 전달 매체도 또한 포함한다. 용어 "변조 데이터 신호"는 신호

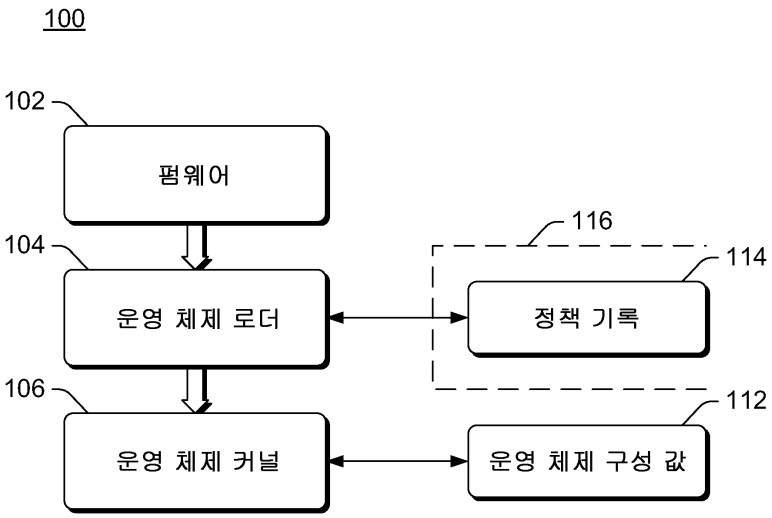
내에 정보를 부호화하는 것과 같은 방식으로 설정되거나 변화된 특징 중 하나 이상의 특징을 갖는 신호를 의미한다. 예를 들어 그리고 제한 없이, 통신 매체는 무선 네트워크 또는 다이렉트-와이어드(direct-wired) 접속과 같은 유선 매체, 및 음향, RF, 적외선 및 다른 무선 매체와 같은 무선 매체를 포함한다. 전술된 것의 임의의 조합도 또한 컴퓨터 판독 가능 매체의 범위 내에 포함된다.

[0071] 일반적으로, 본 명세서에서 설명된 임의의 기능 또는 기법은 소프트웨어, 펌웨어, 하드웨어(예를 들어, 고정식 논리 회로), 수동식 프로세싱, 또는 이들 구현의 조합을 사용하여 구현될 수 있다. 본 명세서에서 사용된 바와 같은 용어 "모듈" 및 "컴포넌트"는 일반적으로 소프트웨어, 펌웨어, 하드웨어, 또는 이들의 조합을 표현한다. 소프트웨어 구현의 경우에, 모듈 또는 컴포넌트는 프로세서(예를 들어, CPU 또는 CPU들) 상에서 실행될 때 명시된 임무를 수행하는 프로그램 코드를 표현한다. 프로그램 코드는 하나 이상의 컴퓨터 판독 가능 메모리 디바이스 내에 저장될 수 있으며, 이에 대해서는 도 5와 관련하여 설명되어 있다. 본 명세서에서 설명된 운영 체제 구성 값 보호 기법의 특징은 다양한 프로세서를 갖는 다양한 상업적인 컴퓨팅 플랫폼 상에서 기법이 구현될 수 있는 것을 의미한다는 점에서 플랫폼 독립적(platform-independent)이다.

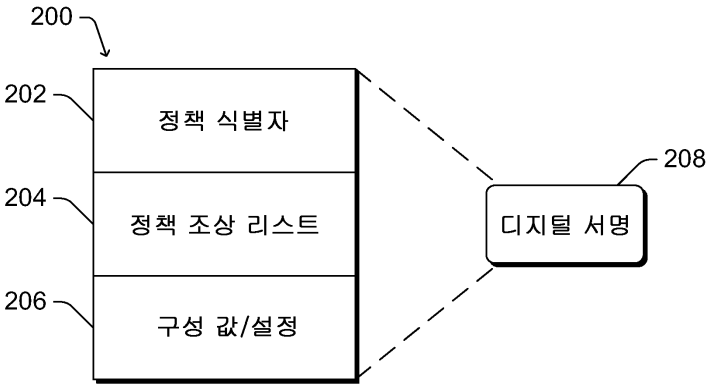
[0072] 발명 대상이 구조적 특징 및/또는 방법론적 동작에 특유한 언어로 설명되었지만, 첨부된 특허청구범위에서 정의되는 발명 대상이 전술된 특유한 특징 또는 동작으로 제한될 필요가 없다는 것이 이해되어야 한다. 오히려, 전술된 특유한 특징 및 동작은 특허청구범위를 구현하는 예시적인 형태로서 개시된다.

도면

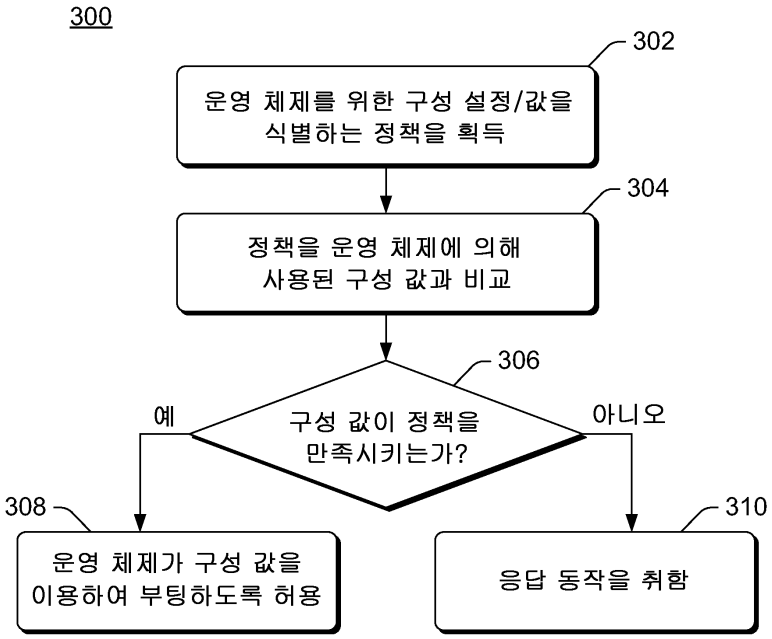
도면1



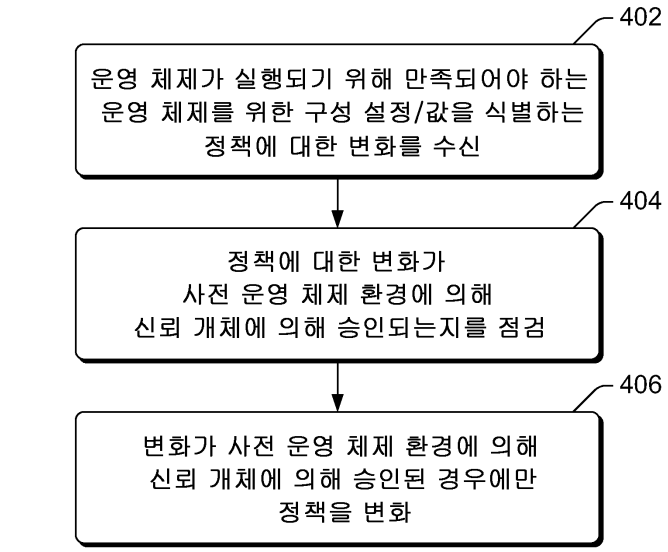
도면2



도면3


300
302
운영 체제를 위한 구성 설정/값을 식별하는 정책을 획득
304
정책을 운영 체제에 의해 사용된 구성 값과 비교
306
구성 값이 정책을 만족시키는가?
예
아니오
308
운영 체제가 구성 값을 이용하여 부팅하도록 허용
310
응답 동작을 취함

도면4


400
402
운영 체제가 실행되기 위해 만족되어야 하는 운영 체제를 위한 구성 설정/값을 식별하는 정책에 대한 변화를 수신
404
정책에 대한 변화가 사전 운영 체제 환경에 의해 신뢰 개체에 의해 승인되는지를 점검
406
변화가 사전 운영 체제 환경에 의해 신뢰 개체에 의해 승인된 경우에만 정책을 변화

도면5

500