(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년08월17일
(11) 등록번호 10-1889577
(24) 등록일자 2018년08월10일

(51) 국제특허분류(Int. Cl.)
G06F 21/30 (2013.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2013-7015803
(22) 출원일자(국제) 2011년12월19일
심사청구일자 2016년11월14일
(85) 번역문제출일자 2013년06월19일
(65) 공개번호 10-2013-0129224
(43) 공개일자 2013년11월27일
(86) 국제출원번호 PCT/US2011/065707
(87) 국제공개번호 WO 2012/087853
국제공개일자 2012년06월28일
(30) 우선권주장
12/972,534 2010년12월20일 미국(US)
(56) 선행기술조사문헌
US20030217137 A1*
US20080046965 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
바함 폴
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
피구에로아 조셉 엔
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(74) 대리인
제일특허법인(유)

전체 청구항 수 : 총 16 항 심사관 : 문남두

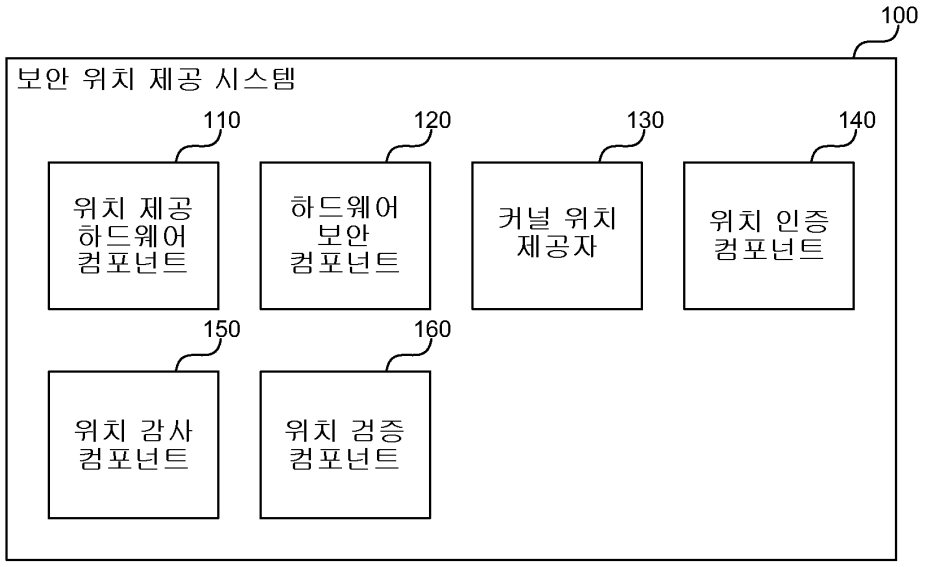
(54) 발명의 명칭 **부정조작 불가능한 위치 제공 서비스**

(57) 요 약

본 명세서에서는 액세스 결정을 내리기 위해 위치 기반 서비스 및 하드웨어를 이용하는 보안 위치 제공 시스템이 설명된다. 많은 이동식 컴퓨터가 GPS와 같은 위치 추적 장치를 갖는다. 이들 컴퓨터는 신뢰 플랫폼 모듈(TPM) 또는 다른 보안 장치도 갖는다. 현재는, 신뢰할 수 없는 애플리케이션 코드에서도 간단한 프로토콜을 사용하여 GPS

(뒷면에 계속)

대 표 도



위치 데이터에 직접 액세스할 수 있다. 보안 위치 제공 시스템은 보안 메커니즘을 제공하는데, 이에 의하여 운영 체제 커널 및 TPM은 특정 시간에 컴퓨터의 GPS 위치를 인증할 수 있다. 보안 위치 제공 시스템은 사용자 액티비티를 로그(log)함에 있어, 그 액티비티를 할 때 컴퓨팅 장치의 지리적 위치를 가리키는 레이블(label)을 이용한다. 보안 위치 제공 시스템은, 커널 모드 GPS 액세스와 TPM 보안 하드웨어의 결합을 통해, 위조하기 어려우면서(즉, 부정조작 불가능하고) 타임 스탬프된(time-stamped) 위치를 제공할 수 있다. 따라서, 보안 위치 제공 시스템은 보안 위치 정보를 인증 및 기타 운영 체제 결정에 통합시킨다.

명 세 서

청구범위

청구항 1

위치 정보에 기반하여 자원 상에 액세스 허가(access permission)를 설정하기 위한 컴퓨터로 구현된 방법으로서,

식별된 자원에 대한 허가가 위치 기반 허가 정보를 포함하도록 업데이트할 것을 요청하는 허가 업데이트 요청을 수신하는 단계 - 상기 위치 기반 허가 정보는 위치 기반 허가가 적용되는 지리적 영역을 정의하는 지리적 위치 정보를 적어도 포함함 - 와,

식별된 자원을 찾아내는(locate) 단계와,

상기 식별된 자원과 관련된 액세스 컨트롤 정보에 기초하여 위치를 찾아내는 단계와,

상기 자원이 저장되는 컴퓨팅 장치의 지리적 위치에 기반하여 목록(listing)에서 상기 자원이 판독되거나, 기록되거나, 또는 포함될 수 있는지 결정하는 것에 의해, 상기 요청에 동반하는 상기 위치 기반 허가 정보로부터 하나 이상의 허용된 위치 기반 액션(allowed location based actions)을 결정하는 단계와,

상기 하나 이상의 허용된 위치 기반 액션을 포함하도록 상기 위치 기반 액세스 컨트롤 정보를 업데이트하는 단계와,

상기 식별된 자원을 액세스하려는 차후의 시도(subsequent attempts)가 지정된 위치 기반 허가 정보를 따르도록(subject to), 상기 식별된 자원과 관련된 업데이트된 상기 위치 기반 액세스 컨트롤 정보를 저장하는 단계를 포함하되,

상기 단계들은 적어도 하나의 프로세서에 의해 수행되는

컴퓨터로 구현된 방법.

청구항 2

제 1 항에 있어서,

상기 식별된 자원은 적어도 하나의 액세스 컨트롤 리스트(ACL) 또는 액세스 컨트롤 엔트리(ACE)를 포함하는 연관 보안 정보(associated security information)를 포함하는 운영 체제에 의해 관리되는 객체(object)인

컴퓨터로 구현된 방법.

청구항 3

제 1 항에 있어서,

상기 허가 업데이트 요청을 수신하는 단계는 운영 체제 애플리케이션 프로그래밍 인터페이스(API)를 통해 애플리케이션으로부터 상기 요청을 수신하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 4

제 1 항에 있어서,

상기 허가 업데이트 요청을 수신하는 단계는 적어도 하나의 액세스 기준으로서 지리적 위치를 포함하는 액세스 컨트롤 정보를 수신하는 경로에 의해 상기 자원을 식별하는 정보를 수신하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 5

제 1 항에 있어서,

상기 식별된 자원을 찾아내는 단계는

환경설정 데이터베이스(configuration database) 또는 환경설정 디렉토리(configuration directory) 내에서 디스크 상의 상기 자원을 액세스하는 단계와,

상기 자원과 관련된 관련 액세스 컨트롤 메타데이터(related access control metadata)를 액세스하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 6

제 1 항에 있어서,

상기 액세스 컨트롤 정보를 찾아내는 단계는

위치 기반 정보를 포함하는 액세스 컨트롤 정보를 네비게이팅 및/또는 수정하기 위해 운영 체제 애플리케이션 프로그래밍 인터페이스(API)를 호출하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 7

제 1 항에 있어서,

상기 하나 이상의 허용된 위치 기반 액션을 결정하는 단계는 지리적 영역의 하나 이상의 지정된 경계에 기반하여 지리적 영역을 결정하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 8

제 1 항에 있어서,

상기 액세스 컨트롤 정보를 업데이트하는 단계는 상기 식별된 자원과 관련된 지정된 액션이 허가되는 지리적 영역을 나타내는 계층적 액세스 컨트롤 엔트리(ACE)를 추가하는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 9

제 1 항에 있어서,

상기 액세스 컨트롤 정보를 업데이트하는 단계는 상기 식별된 자원을 액세스하기 위한 하나 이상의 기준을 나타내도록 위치 기반 액세스 컨트롤 정보를 비-위치 기반 액세스 컨트롤 정보에 결합시키는 단계를 포함하는

컴퓨터로 구현된 방법.

청구항 10

부정조작 불가능한(tamper-proof) 위치 서비스를 소프트웨어 애플리케이션에 제공하기 위한 컴퓨터 시스템으로서,

상기 시스템의 현재 지리적 위치를 나타내는 하드웨어 신호를 제공하는 위치 제공 하드웨어 컴포넌트와,

상기 시스템 상에서 실행되는 소프트웨어 코드에 대한 신뢰할 수 있는 컴퓨팅 보증을 제공하는 하드웨어 보안 컴포넌트 - 상기 하드웨어 보안 컴포넌트는 상기 위치 제공 하드웨어 컴포넌트와 관련된 소프트웨어 드라이버에 대한 인증 정보를 검증하여 상기 위치 제공 하드웨어 컴포넌트로부터 운영 체제까지의 보안된 신뢰 체인(secure chain of trust)을 생성함 - 와,

운영 체제 커널로부터 지리적 위치 정보를 사용하는 사용자 모드 서비스 및 애플리케이션으로 인터페이스를 제공하는 커널 위치 제공자와,

상기 컴퓨터 시스템의 현재 지리적 위치를 나타내는 인증서(certificate)를 상기 위치 제공 하드웨어 컴포넌트 및 하드웨어 보안 컴포넌트로부터 정보와 함께 불러오는(retrieve) 위치 인증 컴포넌트 - 상기 위치 인증 컴포넌트에 의해 불려온 위치 인증서는 상기 인증서가 생성되었던 시간 및 상기 컴퓨터 시스템의 위치의 서명된 표시(a signed indication)를 포함함 - 와,

상기 컴퓨터 시스템과 관련된 보안 위치 정보의 감사 추적(audit trail)을 저장하는 위치 감사 컴포넌트(a location audit component) - 상기 위치 감사 컴포넌트는 상기 시스템의 현재 지리적 위치 정보를 획득하도록 상기 위치 제공 하드웨어 컴포넌트에 주기적으로 질의하도록 또한 구성되고, 상기 위치 감사 컴포넌트는 애플리케이션 또는 서비스가 상기 위치 인증 컴포넌트로부터 위치 인증서를 요청할 때마다 상기 시스템의 위치에 대한 표시를 저장하도록 또한 구성됨 - 와,

상기 커널 위치 제공자로부터 위치 정보를 요청하고 수신된 위치 정보에 기반하여 하나 이상의 액션을 수행하는 위치 검증 컴포넌트와,

상기 커널 위치 제공자, 상기 위치 인증 컴포넌트, 상기 위치 감사 컴포넌트 및 상기 위치 검증 컴포넌트 내에서 구현되는 소프트웨어 인스트럭션을 실행하도록 구성되는 프로세서 및 메모리를 포함하는

컴퓨터 시스템.

청구항 11

제 10 항에 있어서,

상기 위치 제공 하드웨어 컴포넌트는 글로벌 포지셔닝 시스템(GPS) 신호를 수신하고 상기 시스템의 위치를 판정하는 GPS 하드웨어 장치를 포함하는

컴퓨터 시스템.

청구항 12

제 10 항에 있어서,

상기 위치 제공 하드웨어 컴포넌트는 비-GPS 하드웨어를 포함하고, 상기 비-GPS 하드웨어로부터 지리적 위치가 보충 정보(supplemental information)에 기반하여 도출될 수 있는

컴퓨터 시스템.

청구항 13

제 10 항에 있어서,

상기 하드웨어 보안 컴포넌트는 컴퓨팅 장치의 보안과 관련된 암호화 기법에 의해 검증가능한 인증된 정보

(cryptographically verifiable authoritative information)를 제공하는 신뢰 플랫폼 모듈(TPM)을 포함하는

컴퓨터 시스템.

청구항 14

제 10 항에 있어서,

상기 하드웨어 보안 컴포넌트 및 상기 위치 제공 하드웨어 컴포넌트는 통신용 보안 채널을 통해 연결되는

컴퓨터 시스템.

청구항 15

제 10 항에 있어서,

상기 커널 위치 제공자는 애플리케이션과 서비스에 대해 공통적인 방식으로 보안 위치 정보를 노출시키도록 다양한 위치 및 보안 하드웨어 디바이스와 상호작용하는 드라이버 또는 다른 소프트웨어를 제공하는 플러그가능형 모델(pluggable model)을 포함하는

컴퓨터 시스템.

청구항 16

위치 기반 액세스 허가를 사용하여 컴퓨터 시스템이 자원에 액세스하는 것을 컨트롤하기 위한 인스트럭션을 포함한 컴퓨터 판독가능 저장 장치로서,

상기 인스트럭션은, 실행 시, 프로세서로 하여금,

컴퓨팅 장치 상의 식별된 자원에 액세스하라는 요청을 수신하는 것 - 상기 식별된 자원은 관련된 위치 기반 액세스 정보를 포함하고, 상기 요청은 상기 요청과 관련된 보안 원칙(security principal)을 식별하는 보안 토큰을 포함함 - 과,

위치 정보의 보안된 출처(a secure source)를 갖는 위치 제공 하드웨어 컴포넌트에 액세스하는 것과,

상기 위치 제공 하드웨어 컴포넌트가 부정조작되었는지 판정하기 위해 상기 위치 제공 하드웨어 컴포넌트에 질의하는 것(querying)과,

상기 요청이 수신된 상기 컴퓨팅 장치의 현재 지리적 위치를 나타내는 위치 정보의 상기 보안된 출처로부터 위치 인증서를 수신하는 것과,

상기 수신된 위치 인증서에 의해 제공된 상기 현재 지리적 위치 정보를 상기 식별된 자원과 관련된 액세스 컨트롤 정보 내의 적어도 하나의 위치 기반 제한(restirction)과 비교하는 것과,

상기 비교가 상기 자원의 요청된 액세스가 상기 현재 지리적 위치에서 허가된다는 것을 나타내는 경우, 액세스 요청을 허용하고 상기 자원에 대해 요청된 액세스를 제공하는 것

을 포함하는 액션을 수행하게 하는

컴퓨터 판독가능 저장 장치.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 위치 제공 서비스는 일반적인 컴퓨팅 장치의 더욱 평범한 부분이 되고 있다. 글로벌 포지셔닝 시스템(GPS) 칩이 처음에는 길 안내를 제공하는 장치에 전용으로 사용되었지만, 이동 전화, 휴대용 게임 장치, 및 랩톱 컴퓨터에서도 점차 흔해지고 있다. 컴퓨터 소프트웨어는 장치의 현재 위치를 사용하여 지역 목록(예컨대, 레스토랑 또는 기타 서비스에 관한 목록), 길 안내, 날씨 정보 등과 같은 다양한 서비스를 제공하고 있다. 일부 운영 체제는 일관된 방식으로(예컨대, 여러 하드웨어 유형에 대한 수정 없이) 위치 정보를 얻고자 할 때 소프트웨어 애플리케이션이 호출할 수 있는 위치 제공 서비스 애플리케이션 프로그래밍 인터페이스(API)를 포함하도록 업데이트되어 있다.

[0002] 지리적 위치는 단순히 사용자가 찾고자 하는 소매 업체의 유형 이상의 것에 영향을 미친다. 예를 들어, 많은 국가가 자국 내의 장치에 포함될 수 있는 암호화의 종류를 제한하는 수출 법규를 갖기도 한다. 다른 국가는 저작권으로 보호되는 콘텐트의 운송을 제한하기도 한다. 그러므로, 사용자가 컴퓨팅 장치를 어떤 방식으로 사용해도 되는지에 영향을 주는 법률 체계는 사용자의 위치에 따라 달라질 수도 있다.

[0003] 운영 체제는 데이터 및 서비스에 대한 액세스 컨트롤을 시행하는 것을 주로 책임지고, 가끔은 어떤 사용자가 어떤 액션을 수행했는지 보여주는 감사 추적(audit trail)을 제공하도록 기대되기도 한다. 현재, 액세스 컨트롤 결정은 일반적으로 보안 주체(security principal)라는 개념에 기반하는데, 가장 흔하게는 사용자 식별자(예컨대, 사용자 이름 및 패스워드)에 의해 식별되고, 가끔은 다른 방식이 될 수도 있다. 이동식 컴퓨팅 장치의 경우, 여러 다양한 유형의 지리적 위치에서 데이터 및 서비스가 액세스될 수도 있다. 아직까지 운영 체제는 어떤 결정을 내리기 위해 위치 정보를 사용하지 않고 있다. 특정 액션이 수행되었을 때 컴퓨터가 소정 위치에 존재했었다는 것을 인증할 수 있는 것이 바람직한 경우도 있는데, 오늘날의 위치 제공 서비스는 이러한 경우에는 사용되지 않고 있다.

발명의 내용

[0004] 본 명세서에서는 액세스 결정을 내리기 위해 위치 기반 서비스 및 하드웨어를 이용한 보안 위치 제공 시스템이 설명된다. 많은 이동식 컴퓨터가 GPS와 같은 위치 추적 장치를 갖는다. 이들 컴퓨터는 신뢰 플랫폼 모듈(TPM) 또는 다른 보안 장치도 갖는다. 현재는, 신뢰할 수 없는 애플리케이션 코드에서도 간단한 프로토콜을 사용하여 GPS 위치 데이터에 직접 액세스할 수 있다. 보안 위치 제공 시스템은 보안 메커니즘을 제공하는데, 이에 의하여 운영 체제 커널 및 TPM은 특정 시간에 컴퓨터의 GPS 위치를 인증할 수 있다. 일부 실시예에서, 보안 위치 제공 시스템은 사용자 액티비티를 로그(log)함에 있어, 그 액티비티를 할 때 컴퓨팅 장치의 지리적 위치를 가리키는 레이블(label)을 이용한다. 보안 위치 제공 시스템은, 커널 모드 GPS 액세스와 TPM 보안 하드웨어의 결합을 통해, 위조하기 어려우면서(즉, 부정조작 불가능하고) 타임 스탬프된(time-stamped) 위치를 제공할 수 있다.

[0005] 일부 실시예에서, 시스템은 특정 액션이 특정 위치에서 발생했었다는 것을 검증하는 데 사용될 수 있는 보안 감사 추적(secure audit trail)을 제공한다. 시스템은 지리적 위치 및/또는 시간에 기반하여 액세스 컨트롤 결정에 대한 변경을 제한하거나 운영 체제 서비스의 사용을 제한할 수도 있다. 보안 위치 제공 시스템은 오직 커널에 의해서만 GPS 하드웨어를 액세스할 수 있게 함으로써 이러한 액션을 수행한다. TPM은 운영 체제 및 부트 로더 코드(boot loader code)가 신뢰할 수 있는 출처로부터 왔다는 것을 보장한다. 운영 체제는 보안 GPS 위치를 판독하고, 인증된 GPS/시간 데이터를 사용자-공간 프로세스(user-space processes)로 제공한다. 시스템은 초기의 부트 프로세서에서부터 사용자 프로세스의 실행에 이르기까지 신뢰 체인(chain of trust)을 형성하는데, 이는 GPS 정보가 어떻게 제공되고 애플리케이션에 의해 어떻게 사용되는지 제어하고 감시한다. 따라서, 보안 위치 제공 시스템은 보안 위치 정보를 인증 및 기타 운영 체제 결정에 통합시킨다.

[0006] 본 요약부는 이하 발명의 상세한 설명에서 보다 자세히 기술될 개념을 단순화된 형식으로 소개하기 위해 제공되는 것이다. 본 요약부는 청구항에 기재된 청구대상의 주된 사항 또는 핵심 사항을 밝히기 위한 것이 아니며, 청구항에 기재된 청구대상의 범위를 한정하기 위한 것은 더더욱 아니다.

도면의 간단한 설명

[0007] 도 1은 일 실시예에 따른 보안 위치 제공 시스템의 컴포넌트를 도시하는 블록도이다.

도 2는 일 실시예에 따라 위치 정보에 기반하여 자원 허가를 설정하는 보안 위치 제공 시스템의 프로세싱을 도

시하는 흐름도이다.

도 3은 일 실시예에 따라 위치 기반 액세스 허가를 이용하여 자원에 액세스하는 보안 위치 제공 시스템의 프로세싱을 도시하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0008] 본 명세서에서는 액세스에 대한 결정을 내리기 위해 위치 기반 서비스 및 하드웨어에 사용하는 보안 위치 제공 시스템이 설명된다. 예를 들어, 운영 체제가 컴퓨터의 물리적 위치에 기반하여 서비스와 파일의 부분집합(subset)에 대한 액세스를 상이하게 허가해야 하는 경우를 상정할 수 있는데, 예컨대, 어떤 국가들 중 하나에 있거나 사무실 밖에 있으면 소정의 파일에 대한 액세스를 허용하지 않아야 하는 경우를 상정할 수 있다. 많은 이동식 컴퓨터가 GPS와 같은 위치 제공 장치를 갖는다. 이러한 컴퓨터는 신뢰 플랫폼 모듈(TPM) 또는 다른 보안 장치도 갖는다. 현재는, 신뢰할 수 없는 애플리케이션 코드에서도 간단한 프로토콜(예컨대, RS232 또는 USB)을 사용하여 GPS 위치 데이터에 직접 액세스할 수 있다. 보안 위치 제공 시스템은 보안 메커니즘을 제공하는데, 이에 의하여 운영 체제 커널 및 TPM은 특정 시간에 컴퓨터의 GPS 위치를 인증할 수 있다. 일부 실시예에서, 보안 위치 제공 시스템은 사용자 액티비티를 로그하는데, 그 액티비티를 할 때 컴퓨팅 장치의 지리적 위치를 가리키는 레이블을 이용한다.

[0009] 보안 위치 제공 시스템은, 커널 모드 GPS 액세스와 TPM(또는 유사한) 보안 하드웨어의 결합을 통해, 위조하기 어려우면서(즉, 부정조작 불가능하고) 타임 스탬프된 위치를 제공할 수 있다. 일부 실시예에서, 시스템은 특정 액션이 특정 위치에서 발생했었다는 것을 검증하는 데 사용될 수 있는 보안 감사 추적(secure audit trail)을 제공한다. 시스템은 지리적 위치 및/또는 시간에 기반하여 (파일) 액세스 컨트롤 결정에 대한 변경을 제한하거나 운영 체제 서비스의 사용을 제한할 수도 있다. 예를 들어, 어떤 회사는 랩톱 컴퓨터가 회사의 기업 본사 내에 있을 때는 그 컴퓨터 상에서 파일의 어떤 집합(set)에 대한 액세스를 제공하지만, 그 컴퓨터가 다른 곳에 있을 때는 파일의 더 작은 부분집합(subset)에 대한 액세스로 낮출 수 있다. 다른 예로서, 보안 위치 제공 시스템은 56 비트 암호화 제한을 허용하는 국가 내에 컴퓨팅 장치가 있을 때에는 암호화(예컨대, 보안 웹 페이지 액세스용)의 한 유형을 사용할 수 있지만, 더 높은 수준의 암호화를 허용하는 국가 내에 컴퓨팅 장치가 있을 때에는 다른 유형의 암호화를 사용할 수도 있다. 이 예에서, 여러 지역에 대해 공용(shared) 이진 모듈 집합이 출하되더라도, 운영 체제 판매자는 각각의 지역마다 운영 체제가 그 국가의 법률을 준수하도록 보증할 수 있다.

[0010] 보안 위치 제공 시스템은, 가능하다면 개인 암호화된 채널(private encrypted channel)로 GPS 하드웨어를 오직 커널에 의해서만 액세스할 수 있게 함으로써 이러한 액션을 수행한다. TPM은 운영 체제 및 부트 로더 코드가 신뢰할 수 있는 출처로부터 왔다는 것을 보장한다. 운영 체제는 보안 GPS 위치를 판독하고, 인증된 GPS/시간 데이터를 사용자 공간 프로세스로 제공한다. 시스템은 초기의 부트 프로세서에서부터 사용자 프로세스의 실행에 이르기까지 신뢰 체인(chain of trust)을 형성하는데, 이는 GPS 정보가 어떻게 제공되고 애플리케이션에 의해 어떻게 사용되는지 제어하고 감시한다. 시스템은 지리적 영역 내장형의 액세스 컨트롤 리스트를 포함하도록 수정된 파일, 디렉토리, 및 다른 자원 메타데이터를 포함할 수도 있다. 예를 들어, 관리자(administrator)는 단지 "누가" 뿐만 아니라 "어디서"(그리고 심지어 "언제") 파일이 액세스될 수 있는지 지정할 수 있다. 파일 및 디렉토리 타임 스탬프(atime, ctime, mtime)는 지리적 위치를 포함하도록 확장될 수도 있다. 운영 체제는 그것의 사용자 액티비티 로그(예컨대, 마이크로소프트(상표) 윈도우즈(상표) 보안 이벤트 로그)를 보안 GPS 위치 데이터를 갖추도록 확장한다. 애플리케이션은 위치에 대한 인증서(certificate)를 판독하고 획득할 수 있다. 애플리케이션이 파일을 판독할 때, 그것이 다시 돌려받는 데이터는 위치에 기반하여 더욱 보안된 레벨 또는 운영 체제에서 선택될 수 있다. 일부 실시예에서, 보안 위치 제공 시스템은 컴퓨터가 현재 속한 국가/지역이 어디인지에 근거하여 사용자 레벨에서의 전체 파일 시스템 모습을 대체할 수 있다(예컨대, 스테가노그래픽 파일 시스템(steganographic file system)을 사용함). 따라서, 보안 위치 제공 시스템은 보안 위치 정보를 인증 및 기타 운영 체제 결정에 통합시킨다.

[0011] 도 1은 일 실시예에 따른 보안 위치 제공 시스템의 컴포넌트를 도시하는 블록도이다. 시스템(100)은 위치 제공 하드웨어 컴포넌트(110), 하드웨어 보안 컴포넌트(120), 커널 위치 제공자(130), 위치 인증 컴포넌트(140), 위치 감사 컴포넌트(150), 및 위치 검증 컴포넌트(160)를 포함한다. 이러한 컴포넌트 각각이 본 명세서에서 더 자세하게 설명된다.

[0012] 위치 제공 하드웨어 컴포넌트(110)는 시스템의 현재 지리적 위치를 나타내는 하드웨어 신호를 제공한다. 예를 들어, 컴포넌트(110)는 위도 및 경도 좌표, 위도 및 경도를 계산하는 데 사용될 수 있는 삼각측량 정보, 또는 다른 위치 정보를 제공하는 GPS, Wi-Fi, 또는 셀룰러 칩을 포함할 수 있다. 이동식 장치는 컴퓨팅 장치의 대략

적 위치 또는 정밀한 위치를 판정하기 위해 하드웨어 및 다른 정보(예컨대, 할당된 인터넷 프로토콜(IP) 주소)의 결합을 사용할 수도 있다. 위치 제고 하드웨어 컴포넌트(110)는 시스템의 위치를 판정하는 루트 정보(root information)를 제공한다.

[0013] 하드웨어 보안 컴포넌트(120)는 시스템 상에서 실행되는 소프트웨어 코드에 대한 신뢰할 수 있는 컴퓨팅 보증을 제공한다. 컴포넌트(120)는 TPM, 프로세서 일련 번호, 암호화 신뢰 체인(cryptographic chain of trust), 또는 컴퓨팅 장치의 보안에 관한 인증된 정보를 제공하도록 설계된 다른 하드웨어와 소프트웨어 컴포넌트를 포함할 수 있다. 일부 경우에서, 시스템은 TPM 내의 키에 의해 암호화되고, 복호화되고, 저장되는 부트 로더 코드를 포함할 수 있다. 이것은 TPM으로 하여금 부트 로더 코드가 안전하고 신뢰할 수 있는 출처로부터 왔다는 것을 검증할 수 있게 해준다. 일부 경우에서, 키는 공개/개인키 페어(public/private key pair)의 공개 부분이고, 공개키에 의한 성공적인 복호화는 그 코드가 해당 개인 키 소유자에 의해 서명되었다는 것을 가리킨다. 부트 로더 코드를 복호화하고 나면, 하드웨어 보안 컴포넌트(120)는 실행중인 코드의 출처를 비슷한 방식으로 검증하면서 운영 체제를 계속해서 로드할 수 있다. 마찬가지로, 시스템은 위치 제공 하드웨어 컴포넌트(110)에 대한 드라이버를 검증하여, 위치 제공 하드웨어로부터 운영 체제까지의 보안된 신뢰 체인(secure chain of trust)이 생성되도록 한다.

[0014] 커널 위치 제공자(130)는 운영 체제 커널로부터 위치 정보를 사용하는 사용자 모드 서비스 및 애플리케이션으로의 인터페이스를 제공한다. 인터페이스는 보안 위치 정보를 수신하고 컴퓨팅 장치의 현재 위치에 기반한 결정을 내리기 위해 애플리케이션이나 운영체제 서비스가 사용할 수 있는 하나 이상의 API를 포함할 수 있다. 커널 위치 제공자(130)는 다양한 위치 및 보안 하드웨어 디바이스와 상호작용하는 드라이버 또는 다른 소프트웨어를 제공하는 플러그가능형 모델(pluggable model)을 포함하여, 애플리케이션과 서비스에 대해 공통적인 방식으로 보안 위치 정보를 노출시킬 수 있다.

[0015] 위치 인증 컴포넌트(140)는 현재 위치를 가리키는 인증서(certificate)를 위치 제공 하드웨어 컴포넌트(110) 및 하드웨어 보안 컴포넌트(120)로부터 불러온다. 인증서는 컴퓨팅 장치의 위치 및 인증서가 생성되었던 시간을 나타내는 서명된 표시(a signed indication)를 포함할 수 있다. 하드웨어 보안 컴포넌트(120)는 인증서에 대해 키(key)로 서명하거나 컴퓨팅 장치에 특유한 다른 암호화 식별자로 서명할 수 있는데, 컴퓨팅 장치 상에서 인증서는 위치 정보의 출처에 대한 서명으로서 생성된다. 애플리케이션은 취해진 액션이 검증가능한 위치 정보에 기반하여 수행되었다는 것의 증명(proof)으로서 인증서를 저장할 수 있다.

[0016] 위치 감사 컴포넌트(150)는 컴퓨팅 장치와 관련된 보안 위치 정보의 감사 추적(audit trail)을 저장한다. 이 컴포넌트는 하나 이상의 파일, 데이터베이스 엔트리, 또는 여러 시점에서의 장치의 하나 이상의 위치를 가리키는 다른 구조화된 데이터를 저장할 수 있다. 일부 실시예에서, 위치 감사 컴포넌트(150)는 애플리케이션 또는 서비스가 위치 인증 컴포넌트(140)로부터 위치 인증서를 요청할 때마다 장치의 위치에 대한 표시를 저장한다. 시스템(100)은 주기적으로 위치 감사 컴포넌트(150)가 위치 제공 하드웨어 컴포넌트(110)로부터 위치 정보를 획득하고, 감사 추적을 수신된 정보와 함께 저장하도록 지시한다. 이것은 관리자 또는 다른 사용자로 하여금 컴퓨팅 장치가 어디로 이동했는지, 잠재적으로 각 위치마다 어떤 액션이 수행되었는지 나중에 검증할 수 있게 해준다. 일부 실시예에서, 관리자는 중앙 저장소에 감사 추적을 주기적으로 업로드하는 소프트웨어를 컴퓨팅 장치 상에 설치하여, 조직(organization)이 그 조직과 관련된 장치가 어디서 어떻게 사용되었는지 추적할 수 있게 한다. 시스템(100)은 만약, 예를 들어, 장치가 정의된 허용 가능 위치 경계 밖에 있다면 IT 직원에게 경고 또는 통지를 제공할 수도 있다. 예를 들어, 회사는 공개되기 전의 컴퓨팅 장치가 시험 연구실 또는 회사 건물 밖으로 유출되는 것을 방지하는 것을 원할 수 있다.

[0017] 위치 검증 컴포넌트(160)는 커널 위치 제공자(130)로부터 위치 정보를 요청하고, 수신된 위치 정보에 기반하여 하나 이상의 액션을 수행한다. 컴퓨팅 장치는 장치의 현재 위치에 기반하여 결정을 내리는 위치 검증 컴포넌트(160)를 포함하는 많은 애플리케이션 및 서비스를 가질 수 있다. 예를 들어, 파일 시스템 필터는 장치의 현재 위치에 기반하여 어느 파일 애플리케이션이 액세스할 수 있는지 결정할 수도 있다. 맵핑 위치(mapping location)는 장치의 현재 위치에 기반하여 지도 및 다른 정보를 표시할 수 있다. 운영 체제는 장치의 위치에 기반하여 지역적 법률 또는 다른 제한에 따라 어떤 기능을 인에이블시키거나 디스에이블시킬 수 있다. 장치의 초기의 부트에서부터 커널 레이어까지 시행되는 신뢰 체인은, 애플리케이션 및 서비스로 하여금 운영 체제로부터 수신된 위치 정보를 신뢰할 수 있게 해준다.

[0018] 보안 위치 제공 시스템이 구현되는 컴퓨팅 장치는 중앙 처리 장치(central processing unit), 메모리, 입력 장치(예컨대, 키보드 및 포인팅 장치), 출력 장치(예컨대, 표시 장치), 및 저장 장치(예컨대, 디스크 드라이브 또

는 다른 비휘발성 저장 매체)를 포함할 수 있다. 메모리와 저장 장치는 시스템을 구현하거나 인에이블시키는 컴퓨터 실행가능한 인스트럭션(예컨대, 소프트웨어)으로 인코딩된 컴퓨터 판독가능한 저장 매체이다. 또한, 데이터 구조 및 메시지 구조는 저장되거나 통신 링크 상의 신호와 같이 데이터 전송 매체를 통해 전송될 수 있다. 인터넷, 근거리통신망(LAN), 광역통신망(WAN), 포인트-투-포인트 접화 접속 연결, 셀룰러 폰 네트워크 등과 같은 다양한 통신 링크가 사용될 수 있다.

[0019] 시스템에 대한 실시예는 개인용 컴퓨터, 서버 컴퓨터, 핸드헬드 또는 랩톱 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 프로그램 가능한 소비자 전자 기기, 디지털 카메라, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 전술된 시스템이나 장치 중 어느 것을 포함하는 분산 컴퓨팅 환경, 셋톱 박스, 시스템 온 칩(SOC) 등을 포함하는 다양한 동작 환경에서 구현될 수 있다. 컴퓨터 시스템은 셀룰러 폰, PDA(personal digital assistant), 스마트 폰, 개인용 컴퓨터, 프로그램 가능한 소비자 전자 기기, 디지털 카메라 등이 될 수도 있다.

[0020] 시스템은 하나 이상의 컴퓨터나 다른 장치에 의해 실행되는 프로그램 모듈과 같은 컴퓨터 실행 가능한 인스트럭션의 일반적인 맥락에 따라 설명될 수 있다. 일반적으로, 프로그램 모듈은 특별한 작업을 수행하거나 특별한 추상 데이터 타입을 구현하는 루틴, 프로그램, 객체(object), 컴포넌트, 데이터 구조 등을 포함한다. 일반적으로, 프로그램 모듈의 기능은 다양한 실시예에서 원하는대로 결합되거나 분산될 수 있다.

[0021] 도 2는 일 실시예에 따라 위치 정보에 기반하여 자원 허가를 설정하는 보안 위치 제공 시스템의 프로세싱을 도시하는 흐름도이다. 자원은 파일, 디렉토리, 프린터, 환경설정 엔트리, 사용자 계정, 또는 액세스 컨트롤 리스트(ACL)나 액세스 컨트롤 엔트리(ACE)와 같은 보안 정보를 일반적으로 포함하는 운영 체제 내의 임의의 다른 객체를 포함한다. 보안 위치 제공 시스템은 리소스에 액세스하기 위한 허가 기준으로서 위치 정보를 포함하도록 이러한 데이터 구조를 확장한다.

[0022] 블록(210)에서 시작하여, 시스템은 식별된 자원에 대한 허가가 위치 기반 허가 정보를 포함하도록 업데이트하라는 허가 업데이트 요청을 수신한다. 예를 들어, 애플리케이션이 운영 체제 API를 통해서 요청을 보낼 수도 있고, 또는 사용자가 쉘(shell) 프로그램이나 다른 수단으로 하여금 요청을 보내게 할 수도 있다. 요청은 경로나 다른 식별자에 의해 자원을 식별하고, 적어도 하나의 액세스 기준으로 지리적 위치를 포함하는 ACL 및/또는 ACE와 같은 액세스 컨트롤 정보를 포함한다. 예를 들어, 요청은 오직 미국에서만 액세스될 수 있는 파일에 대한 허가를 가리킬 수 있다.

[0023] 계속해서 블록(220)에서, 시스템은 식별된 자원의 위치를 찾는다. 자원은 디스크 상에 저장될 수 있고(예컨대, 파일 또는 폴더), 환경설정 데이터베이스(예컨대, 레지스트리 엔트리) 내에 저장될 수도 있으며, 디렉토리(예컨대, 액티브 디렉토리 자원) 내에 저장될 수도 있고, 기타 다른 곳에 저장될 수도 있다. 시스템은 자원의 위치를 찾아서, 엔트리와 연관된 임의의 관련 액세스 컨트롤 메타데이터(related access control metadata)를 불러올 수 있다. 예를 들어, 자원은, 자원과 인접하거나 자원과 관련되어 저장된 레코드를 포함할 수 있고, 그 레코드는 액세스 컨트롤 정보를 지정하게 된다.

[0024] 계속해서 블록(230)에서, 시스템은 식별된 자원과 관련된 액세스 컨트롤 리스트의 위치를 찾는다. 일부 실시예에서, 시스템은, 지리적 액세스 제한에 관한 액세스 컨트롤 정보의 위치를 찾아 불러오도록, 현존하는 운영 체제 API를 수정한다. 운영 체제는 다양한 유형의 자원과 관련된 액세스 컨트롤 정보를 네비게이트하고 수정하기 위한 보안 API의 강력한 집합(a robust set)을 일반적으로 포함한다.

[0025] 계속해서 블록(240)에서, 시스템은 요청을 동반하는 위치 기반 허가 정보로부터 하나 이상의 허용된 액션(allowed action)을 결정한다. 액션은 목록(listing)에서 자원이 판독되거나, 기록되거나, 또는 포함되거나, 기타 등등이 가능한지 여부를 포함한다. 위치 기반 허가 정보는 좌표에 의해 정의된 변(edge)을 갖는 직사각형이나 다른 적합한 영역과 같은 경계 있는 지리적 영역을 식별할 수 있다. 예를 들어, 시스템은 중심점 및 지리적 영역을 나타내는 그 중심점을 둘러싸는 반경을 수신할 수 있고, 그 영역 내에서 액션이 발생되는 것이 허용되거나 허용되지 않게 된다. 허가는 식별된 자원에 관하여 무엇인가가 허용됨과 허용되지 않음을 가리키도록 당연히 양(positive)과 음(negative) 모두로 표현될 수 있다.

[0026] 계속해서 블록(250)에서, 시스템은 허용된 위치 기반 액션을 포함하도록 위치가 찾아진 액세스 컨트롤 리스트를 업데이트한다. 액세스 컨트롤 리스트는 어떤 사용자가 어떤 액션을 수행할 수 있는지와 관련된 허가 데이터의 계층(hierarchy)을 흔히 포함하고, 시스템은 액션이 어디서 수행될 수 있는지 포함하도록 이 리스트를 수정한다. 위치 기반 액세스 컨트롤 정보는 다른 액세스 컨트롤 정보와 결합될 수 있고, 그에 따라, 예를 들어, 관리자는 어느 장소에서든 파일을 판독할 수 있으나, 제한된 사용자는 오직 지정된 지리적 영역 내에서만 파일

을 판독할 수 있도록 할 수도 있다.

[0027] 계속해서 블록(260)에서, 시스템은 식별된 자원을 액세스하는 차후의 시도가 지정된 위치 기반 액세스 정보를 따르도록, 식별된 자원과 관련된 업데이트된 액세스 컨트롤 리스트를 저장한다. 예를 들어, 만약 액세스 컨트롤 리스트가 어떤 액션이 수행될 수 있는 지정된 영역을 가리킨다면, 시스템은 액세스를 허용하기 이전에 그 영역 내에서 액세스 요청이 발생하였는지 검사할 것이다. 이 프로세스는 도 3을 참조하여 더 자세하게 설명된다. 블록(260) 이후에, 이들 단계는 종료한다.

[0028] 도 3은 일 실시예에 따라 위치 기반 액세스 허가를 갖는 자원에 액세스하는 보안 위치 제공 시스템의 프로세싱을 도시하는 흐름도이다. 컴퓨팅 시스템 내의 자원은 자원을 액세스하기 위한 다양한 기준 중 하나로서 위치 정보를 포함할 수 있다. 예를 들어, 특정 사용자가 지정된 위치에서만 파일에 액세스할 수 있도록, 파일은 사용자 및 위치 제한을 포함할 수도 있다.

[0029] 블록(310)에서 시작하여, 시스템은 식별된 자원을 액세스하라는 요청을 수신하는데, 식별된 자원에는 위치 기반 액세스 정보가 포함된다. 예를 들어, 자원은 파일, 디렉토리, 프린터, 컴퓨터 주변장치, 환경설정 데이터베이스 엔트리, 또는 다른 자원을 포함할 수 있는데, 이는 운영 체제가 액세스 컨트롤을 정의하고 시행하기 위한 것이다. 요청은 파일이나 다른 자원에 액세스하기 위한 운영 체제 API를 호출(call)하는 애플리케이션으로부터 수신될 수 있다. 요청은 그 요청과 관련된 보안 원칙을 식별하는 보안 토큰을 포함한다.

[0030] 계속해서 블록(320)에서, 시스템은 위치 정보의 보안된 출처(secure source)를 액세스한다. 예를 들어, 시스템은 검증가능하고(verifiable) 감사가능한(auditable) 위치 표시를 제공하는 GPS 및/또는 TPM 하드웨어로부터 위치 인증서를 요청하기 위하여 운영 체제 API를 호출할 수 있다. 위치 표시는, 타임 스탬프 및 위치 정보가 현재의 것이면서 부정조작되지 않았다는 것을 입증하는 다른 식별 정보뿐만 아니라, 위도와 경도 좌표 또는 다른 위치 세목(location specification)도 포함할 수 있다. 컴퓨팅 장치는 운영 체제가 위치 제공 하드웨어의 컨트롤을 가진다는 점과 운영 체제로부터 수신된 위치와 관련된 출력(output)이 신뢰할 수 있다는 점을 보장하는 신뢰 체인을 생성하는 보안 부트 프로세스(secure boot process)를 포함할 수 있다.

[0031] 계속해서 블록(330)에서, 시스템은 요청을 수신한 컴퓨팅 장치의 현재 지리적 위치를 가리키는 위치 정보의 보안된 출처로부터 위치 인증서를 수신한다. 인증서는 서명을 포함하거나, 이와 다른 방식으로 위치 정보의 출처에 대해 암호화 기법을 이용하여 검증가능한(cryptographically verifiable) 표시를 포함할 수 있다. 수신자는 서명을 검증하기 위해 TPM 또는 다른 보안 하드웨어에 질의하여(query), 인증서에 제공된 위치 정보에 관한 어떠한 부정조작도 발생하지 않았음을 보장할 수도 있다. 시스템은 특정 위치에서 수행된 액션에 대한 임의의 차후 조사를 위한 감사 추적(audit trail)을 형성하는 위치 인증서의 발행 로그(log of issued location certificates)를 생성할 수도 있다.

[0032] 계속해서 블록(340)에서, 시스템은 수신된 위치 인증서에 의해 제공된 위치 기반 정보와, 식별된 자원과 관련된 액세스 컨트롤 리스트 내의 적어도 하나의 위치 기반 제한을 비교한다. 예를 들어, 액세스 컨트롤 리스트는 미국 이외의 지역에서는 해당 자원이 판독되거나 기록될 수 없도록 하고, 미국 내에서는 어느 지역에서나 판독될 수 있게 하되, 자원에 대한 기록은 오직 특정 도시 내에서만 가능하게끔 지정할 수 있다. 이것은 단지 하나의 예시에 불과할 뿐이고, 본 기술분야의 통상의 지식을 가진 자는 액세스 컨트롤 리스트가 다양한 구체적인 목적에 따라 자원에 대한 액세스를 맞춤화하기 위해 액세스 제한에 관한 다양한 조합을 허용한다는 것을 이해할 것이다.

[0033] 계속해서 결정 블록(350)에서, 만약 비교 결과가 자원에 대해 요청된 액세스가 현재 위치에서는 허가되지 않음을 나타내면 시스템은 블록(360)으로 넘어가게 되고, 만약 그렇지 않다면 시스템은 블록(370)으로 넘어가게 된다. 계속해서 블록(360)에서는, 시스템이 액세스 요청을 거절한다. 시스템은 에러 메시지를 제공하거나 요청이 거절되었다는 것을 나타내는 다른 표시를 제공할 수 있다. 일부 실시예에 따르면 시스템은 위치나 다른 미충족 제한으로 인해 액세스 불가능한 경우에는 자원을 효과적으로 감추면서, 마치 자원이 존재하지 않는 것처럼 동작할 수도 있다. 일부 실시예에 따르면, 시스템은 어떤 조건하에서 자원이 액세스 될 수 있는지를 가리키는 에러 메시지를 제공할 수 있는데, 그 결과, 예를 들어, 사용자는 허용된 위치로 장치를 옮길 수 있게 된다.

[0034] 계속해서 블록(370)에서, 시스템은 액세스 요청을 허용하고 요청된 액세스를 자원에 제공한다. 예를 들어, 자원이 파일이라면, 시스템은 파일의 콘텐트를 열어서 보는 요청을 허용할 수 있다. 일부 실시예에서, 시스템은 액세스 요청을 허용할 수 있을 뿐만 아니라, 결정된 장치의 위치에 기반하여 파일 데이터를 대체하도록 허용할 수도 있다. 예를 들어, 시스템은 장치가 소정의 위치에 있을 때에는 평범한 데이터로 채워진 파일 시스템을 반환

(return)하지만, 장치가 다른 위치에 있을 때에는 비밀 정보를 반환할 수도 있다. 블록(370) 이후에, 이들 단계는 종료한다.

[0035] 일부 실시예에서, 보안 위치 제공 시스템은 스테가노그래픽 파일 시스템(steganographic file system)의 구현을 용이하게 한다. 스테가노그래픽 파일 시스템은 저장 장치 상의 데이터에 대한 여러 층(layers)의 액세스를 제공한다. 예를 들어, 베이스 레이어(base layer)는 키(key)가 없거나 아무 위치에서라도 액세스 가능하게 할 수 있고, 특별히 보안에 민감하지 않은 무해 데이터(benign data)를 포함할 수도 있다. TPM 또는 다른 보안된 하드웨어는 장치의 현재 위치에 따라 액세스 요청에 응답하여 암호화 키를 제공할 수 있다. 레이어가 높아질수록 적절한 키를 갖는 자에게만 민감한 데이터에 대한 액세스를 점점 더 많이 제공할 수도 있다. 이러한 방식에 따라, 컴퓨터가 어떤 위치에서는 무해 데이터로 채워진 것처럼 보이지만, 다른 위치에서는 보안에 민감한 정보를 갖는 것처럼 보일 수 있다. 이를 통해 만약 컴퓨팅 장치가 도난당하더라도, 악의적인 사용자가 민감한 사용자 정보에 액세스할 수 없도록 컴퓨터 사용자에게 보장할 수 있다.

[0036] 일부 실시예에서, 보안 위치 제공 시스템은 운영 체제가 시스템을 실행하는 컴퓨팅 장치의 위치에 기반하여 상이한 기능을 제공하도록 허용한다. 예를 들어, 보안 위치 제공 시스템은 만약 컴퓨팅 장치가 쿠키(cookie)의 사용을 제한하는 국가 내에 있으면 웹 브라우저 내의 쿠키를 꺼둘 수 있다. 다른 예로서, 운영 체제는 보안 소켓 계층(SSL) 또는 다른 암호화된 통신에 사용하는 암호화 레벨을, 그 장치가 사용되는 곳의 지역 법규에 기반하여 바꿀 수 있다. 현재 운영 체제 판매자는 특정 국가로 출하되는 운영 체제마다 수많은 상품 분류 단위(SKU)를 관리한다. 그러한 SKU는 관리가 어려울 뿐만 아니라, 특정 국가에서 특정 SKU만 판매하더라도 누군가가 그 국가에서 준수되지 않는 SKU를 반입하지 않을 것이라는 점까지 보증할 수는 없다. 보안 위치 제공 시스템을 사용하면, 운영 체제 판매자는 사용중인 위치의 보안 지식에 기반하여 동작을 자동적으로 수정하는 단일의 SKU를 출하할 수 있고, 이로써 여러 종류의 SKU에 대한 필요성을 감소시키거나 없애주며, 관리 비용을 줄일 수 있게 된다.

[0037] 일부 실시예에서, 보안 위치 제공 시스템은 위치 기반 결정을 용이하게 하도록 내장형 장치 내에서 사용될 수 있다. 예를 들어, 임대 자동차 회사는 차량을 운행할 수 있는 장소에 대한 지리적 제한을 구현하도록 임대 차량 내에 본 시스템을 구현하는 장치를 포함시킬 수 있다. 일부 임대 자동차 회사는 자동차가 특정 국가나 주를 벗어나는 것을 원하지 않을 수 있고, 본 시스템을 사용하여 이러한 유형의 제한을 구현할 수 있다. 다른 구현에 따르면, 회사는 다른 지리적 영역에서의 사용은 허용하지만, 정보를 로그(log)하여, 차량이 사용된 각 지역마다 상이한 렌탈 요금이 청구될 수 있게 할 수도 있다.

[0038] 일부 실시예에서, 보안 위치 제공 시스템은 여러 종류의 위치 기반 하드웨어와 함께 동작한다. 장치 내의 GPS 칩은 오늘날 여러 다양한 판매자로부터 용이하게 입수할 수 있게 되었고, 시스템은 이들 각각에 맞게 작동하도록 수정될 수 있다. 또한, 시스템은 위치 정보를 제공하는 특정한 위치 제공 기관을 식별하기 위하여, 위치 인증서의 일부로 포착될 수 있는 GPS 칩마다 실질적으로 고유한 식별자를 포함하는 GPS 하드웨어를 채용할 수 있다. 특정 인스턴스가 손상되면 이를 금지하거나 다른 이유로 인해 특정 인스턴스를 금지할 수 있도록, 프로세서와 TPM은 암호화 및 식별을 위해 고유한 일련 번호를 사용해왔다. 각각의 GPS 유닛을 고유하게 식별하고, 신뢰할 수 없는 인스턴스에 대한 액세스를 거절할 수 있도록, 유사한 기법이 GPS 하드웨어에 적용될 수 있다.

[0039] 일부 실시예에서, 보안 위치 제공 시스템은 GPS 모듈과 TPM과 같은 위치 제공 하드웨어 및 보안 하드웨어 사이에서 보안된 데이터 통신 채널을 사용한다. 채널은 TPM으로 하여금 GPS 칩의 출력(output)을 인증하게 해주고 신뢰 체인이 GPS 하드웨어와 운영 체제 또는 애플리케이션 사이에서 부정조작될 수 없다는 것을 보장해주는 암호화된 통신을 포함할 수 있다. 일부 실시예에서, 자원에 대한 액세스는 TPM이나 다른 보안 하드웨어에 의해 관리되는 암호화 키로 보호될 수 있고, TPM은 위치 제공 하드웨어로부터 얻을 수 있는 장치의 현재 위치에 기반하여 한시적(time-limited) 키를 배포할 수 있다.

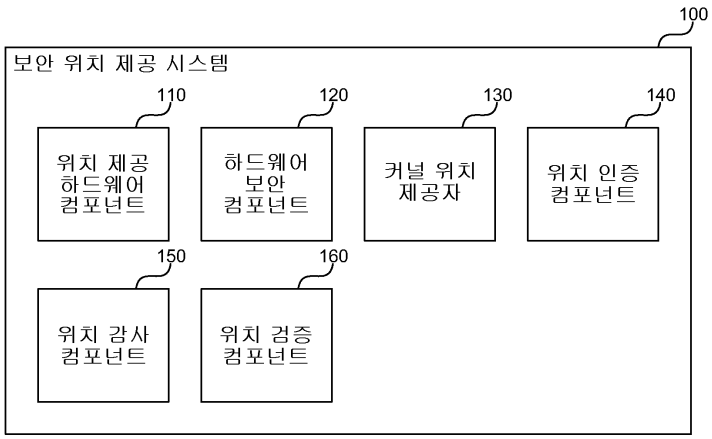
[0040] 일부 실시예에서, 보안 위치 제공 시스템은 위치 정보를 사용하여 이동식 컴퓨팅 장치 상에서 네트워크 보안 방침(network security policy)을 시행한다. 예를 들어, 시스템은 랩톱이 최근에 해외에 있었다는 정보를 사용하여, 그 장치가 회사 네트워크에 액세스하기 전에 바이러스 검사를 완료해야 한다고 결정할 수 있다. 이렇게 하기 위해, 네트워크 기반시설은, 만약 가능하다면, 컴퓨팅 장치 상에 저장되어 장치가 마지막 보안 점검 이후부터 어디에 있었는지에 대한 감사 추적을 제공하는 위치 정보 히스토리(historical location information)에 액세스한다. 시스템은 수신되거나(incoming) 송신되는(outgoing) 네트워킹 트래픽 중 어느 하나를 제한할 수도 있고, 또는 양자를 모두 제한할 수도 있다. 이러한 방침 및 다른 방침은 보안 위치 제공 시스템에 의해 시행될 수 있다.

[0041] 이상, 보안 위치 제공 시스템의 구체적인 실시예가 예시적 설명을 위해 본 명세서에서 기술되었으나, 본 발명의

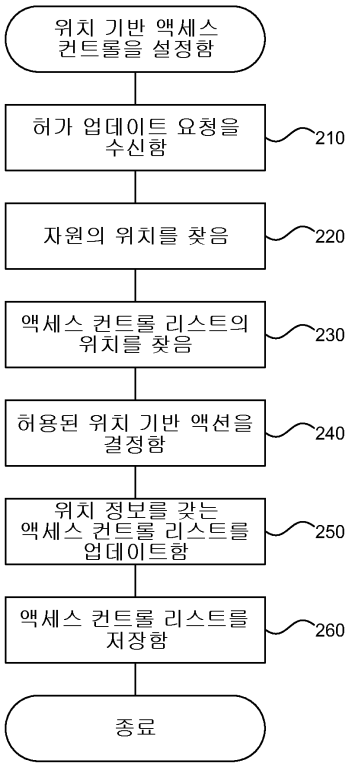
사상과 범주를 벗어나지 않는다면 다양한 변형도 가능한 것으로 이해될 수 있을 것이다. 따라서, 첨부된 특허청구범위로 본 발명이 제한되는 것은 아니고, 첨부된 특허청구범위 외의 것을 본 발명에서 배제하는 것도 아니다.

도면

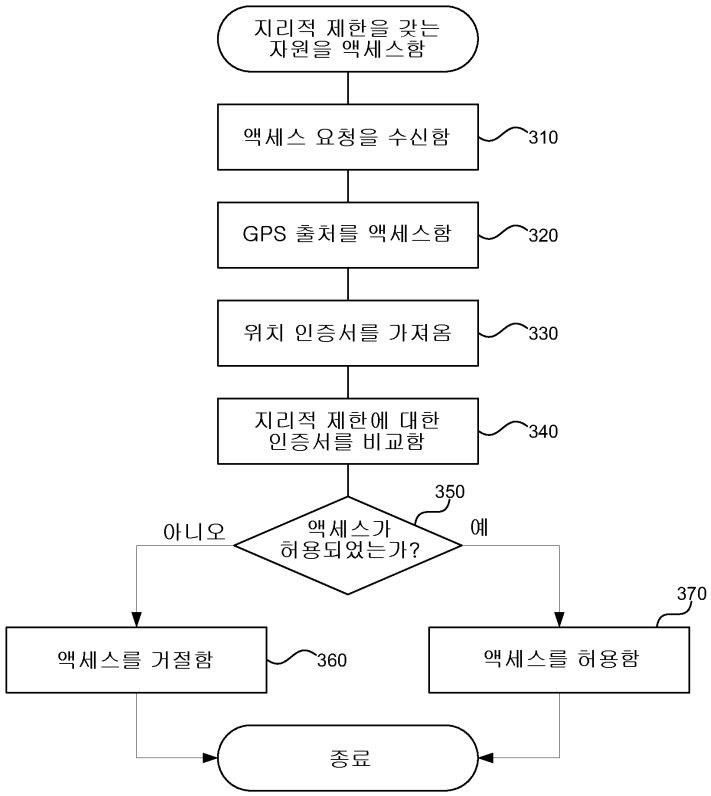
도면1



도면2



도면3


지리적 제한을 갖는 자원을 액세스함
액세스 요청을 수신함
310
GPS 출처를 액세스함
320
위치 인증서를 가져옴
330
지리적 제한에 대한 인증서를 비교함
340
350
액세스가 허용되었는가?
아니오
예
액세스를 거절함
360
액세스를 허용함
370
종료