(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년04월12일
(11) 등록번호 10-2386111
(24) 등록일자 2022년04월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 11/14* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/575 (2013.01)
G06F 11/1417 (2013.01)
(21) 출원번호 10-2019-7006214
(22) 출원일자(국제) 2017년08월25일
심사청구일자 2020년07월24일
(85) 번역문제출일자 2019년02월28일
(65) 공개번호 10-2019-0042018
(43) 공개일자 2019년04월23일
(86) 국제출원번호 PCT/US2017/048517
(87) 국제공개번호 WO 2018/044696
국제공개일자 2018년03월08일
(30) 우선권주장
15/253,521 2016년08월31일 미국(US)
(56) 선행기술조사문헌
JP2008226158 A*
US20060155988 A1*
US20070226505 A1*
US20130086383 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
킨슈만 -
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 마이크로소프트 테크놀로지 라이센싱, 엘엘씨
맥캐런 크리스토퍼
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 마이크로소프트 테크놀로지 라이센싱, 엘엘씨
삼소노프 예브게니 아나톨리예비치
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 마이크로소프트 테크놀로지 라이센싱, 엘엘씨
(74) 대리인
제일특허법인(유)

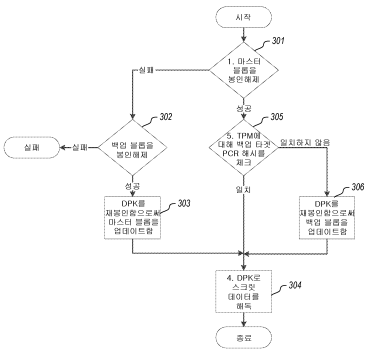
전체 청구항 수 : 총 20 항 심사관 : 구대성

(54) 발명의 명칭 **보호되는 시크릿을 보안 부팅 업데이트에 걸쳐 보존하는 기법**

(57) 요 약

봉인된 시크릿을 획득하는 방법이 개시된다. 이 방법은 컴퓨팅 시스템에서 복수의 상이한 BLOB 중의 하나 이상의 BLOB을 해독하는 단계를 포함한다. 복수의 BLOB 중의 각각의 BLOB는 시크릿을 포함한다. 복수의 BLOB 중의 각각의 BLOB는 복수의 조건 중 상이한 조건으로 봉인되어 있다. 주어진 조건은, 컴퓨팅 시스템이 시크릿을 수신하도록 신뢰될 수 있는지 여부를 나타내는, 시스템 상태를 반영하는 것이다. 방법은 조건들 중 하나 이상의 조건을 평가하여 이 하나 이상의 조건 중 적어도 하나의 조건이 충족되는지를 결정하는 단계를 더 포함한다. 이 방법은 하나 이상의 조건 중 적어도 하나가 충족되는 경우, 외부 엔티티에 시크릿을 제공하는 단계를 더 포함한다.

대 표 도 - 도3



(52) CPC특허분류
G06F 11/1433 (2013.01)
G06F 21/572 (2013.01)
H04L 9/085 (2013.01)
H04L 2209/127 (2013.01)

명 세 서

청구범위

청구항 1

보호된 시크릿을 보안 부팅 업데이트 동안 보존하는 컴퓨팅 시스템으로서,

하나 이상의 프로세서와,

봉인된 시크릿을 획득하게끔 상기 컴퓨팅 시스템을 구성하도록 상기 하나 이상의 프로세서에 의해 실행가능한 명령어를 저장한 하나 이상의 컴퓨터 판독가능 저장 장치를 포함하되, 상기 명령어는 동작들을 수행하게끔 상기 컴퓨팅 시스템을 구성하도록 실행가능한 명령어를 포함하고,

상기 동작들은 적어도,

복수의 BLOB(binary large object)를 유지하는 동작- 상기 복수의 BLOB 중 각각의 BLOB는 암호화된 데이터 및 상기 봉인된 시크릿을 포함하고, 각각의 BLOB 내의 각각의 봉인된 시크릿은 상이한 조건으로 봉인되었고, 각각의 조건은 상기 컴퓨팅 시스템이 상기 시크릿을 수신하기에 신뢰되는지 여부를 나타내는 시스템 상태의 반영임 -과,

제1 BLOB에 포함된 상기 봉인된 시크릿을 제1 조건을 사용하여 봉인해제하려 시도하는 동작과,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적인 것에 기초하여, 제2 BLOB가 업데이트될 필요가 있는지를 결정하고, 업데이트될 필요가 있는 경우, 상기 제2 BLOB를 업데이트하는 동작과,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적이지 못한 것에 기초하여, 상기 제2 BLOB에 포함된 상기 봉인된 시크릿을 제2 조건을 사용하여 봉인해제하려 시도하는 동작과,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도 또는 상기 제2 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적인 것에 기초하여, 상기 봉인해제된 시크릿을 엔티티에 제공하는 동작- 상기 봉인해제된 봉인된 시크릿을 통해 상기 엔티티는 상기 암호화된 데이터에 액세스할 수 있음 -을 포함하는

컴퓨팅 시스템.

청구항 2

제1항에 있어서,

상기 BLOB들 중 하나 이상의 BLOB가 업데이트될 필요가 있다고 결정되고, 그에 따라, 적어도 하나의 BLOB가 업데이트되는

컴퓨팅 시스템.

청구항 3

제2항에 있어서,

상기 하나 이상의 컴퓨터 판독가능 저장 장치는,

대응하는 조건이 충족되지 않게 하는 상기 컴퓨팅 시스템에서의 변화는 수용불가능한 변화인 것으로 결정됨에 따라, 상기 대응하는 조건이 만족되지 않는 BLOB를 업데이트하지 않기로 결정하게끔 상기 컴퓨팅 시스템을 구성하도록 상기 하나 이상의 프로세서에 의해 실행가능한 명령어를 더 저장한

컴퓨팅 시스템.

청구항 4

제1항에 있어서,

상기 하나 이상의 컴퓨터 판독가능 저장 장치는,

상기 조건들 중 적어도 하나가 충족되지 않는 것으로 판정됨에 따라, 충족되지 않는 조건과 연관된, 상기 BLOB들 중 하나 이상의 BLOB를 업데이트하게끔 상기 컴퓨팅 시스템을 구성하도록 상기 하나 이상의 프로세서에 의해 실행가능한 명령어를 더 저장한

컴퓨팅 시스템.

청구항 5

제1항에 있어서,

상기 조건들 중 적어도 하나는 서명자의 목록과 관련된

컴퓨팅 시스템.

청구항 6

제1항에 있어서,

상기 제1 조건 및 상기 제2 조건 중 적어도 하나는 운영 체제 컴포넌트의 목록과 관련된

컴퓨팅 시스템.

청구항 7

제1항에 있어서,

상기 하나 이상의 컴퓨터 판독가능 저장 장치는,

상기 복수의 BLOB 중 다수의 BLOB에 대한 조건들을 업데이트하게끔 상기 컴퓨팅 시스템을 구성하도록 상기 하나 이상의 프로세서에 의해 실행가능한 명령어를 더 저장하고, 상기 조건들의 업데이트는 반복적으로 행해지되 두 개 이상의 상이한 조건이 조건들을 업데이트하는 사이에 중간 재부팅 동작으로 업데이트되는

컴퓨팅 시스템.

청구항 8

제1항에 있어서,

상기 하나 이상의 컴퓨터 판독가능 저장 장치는,

중간 재부팅 동작없이 복수의 조건에 대한 업데이트가 요청되었음을 판정하고 그 결과로서 하나의 조건에 대해 적어도 하나의 업데이트를 수행하는 것을 거절하게끔 상기 컴퓨팅 시스템을 구성하도록 상기 하나 이상의 프로세서에 의해 실행가능한 명령어를 더 저장한

컴퓨팅 시스템.

청구항 9

봉인된 시크릿을 획득하는 컴퓨터 구현된 방법으로서,

컴퓨팅 시스템에서, 복수의 상이한 BLOB 중의 하나 이상의 BLOB에 액세스하는 단계- 상기 복수의 BLOB 중의 각각의 BLOB는 상기 시크릿을 포함하고, 상기 복수의 BLOB 중의 각각의 BLOB는 복수의 조건 중 상이한 조건으로 봉인되며, 주어진 조건은 시스템 상태의 반영이고 상기 시스템 상태는 상기 컴퓨팅 시스템이 상기 시크릿을 수신하기에 신뢰되는지 여부를 나타냄 -와,

제1 BLOB에 포함된 상기 봉인된 시크릿을 제1 조건을 사용하여 봉인해제하려 시도하는 단계와,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적인 것에 기초하여, 제2 BLOB가 업데이트될 필요가 있는지를 결정하고, 업데이트될 필요가 있는 경우, 상기 제2 BLOB를 업데이트하는 단계와,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적이지 못한 것에 기초하여, 상기 제2 BLOB에 포함된 상기 봉인된 시크릿을 제2 조건을 사용하여 봉인해제하려 시도하는 단계와,

상기 제1 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도 또는 상기 제2 BLOB에 포함된 상기 봉인된 시크릿을 봉인해제하려는 상기 시도가 성공적인 것에 기초하여, 상기 봉인해제된 시크릿을 엔티티에 제공하는 단계- 상기 봉인해제된 봉인된 시크릿을 통해 상기 엔티티는 암호화된 데이터에 액세스할 수 있음 -를 포함하는

컴퓨터 구현된 방법.

청구항 10

제9항에 있어서,

상기 복수의 조건 중 적어도 하나의 조건이 충족되지 않는다고 판정됨에 따라, 상기 복수의 BLOB 중 하나 이상의 BLOB가 업데이트될 필요가 있는지를 판정하는 단계를 더 포함하는

컴퓨터 구현된 방법.

청구항 11

제10항에 있어서,

대응하는 조건이 충족되지 않게 하는 상기 컴퓨팅 시스템에서의 변화는 수용불가능한 변화인 것으로 판정됨에 따라, 상기 대응하는 조건이 충족되지 않는 BLOB를 업데이트하지 않기로 결정하는 단계를 더 포함하는

컴퓨터 구현된 방법.

청구항 12

제9항에 있어서,

상기 복수의 조건 중 적어도 하나가 충족되지 않는 것으로 판정됨에 따라, 충족되지 않는 조건과 연관된, 상기 복수의 BLOB 중 하나 이상의 BLOB를 업데이트하는 단계를 더 포함하는

컴퓨터 구현된 방법.

청구항 13

제9항에 있어서,

상기 조건들 중 적어도 하나는 서명자의 목록과 관련된

컴퓨터 구현된 방법.

청구항 14

제9항에 있어서,

상기 제1 조건 및 상기 제2 조건 중 적어도 하나는 운영 체제 컴포넌트의 목록과 관련된

컴퓨터 구현된 방법.

청구항 15

제9항에 있어서,

상기 복수의 BLOB 중 다수의 BLOB에 대한 조건들을 업데이트하는 단계를 더 포함하되,

상기 조건들의 업데이트는 반복적으로 행해지되 두 개 이상의 상이한 조건이 조건들을 업데이트하는 사이에 중간 재부팅 동작으로 업데이트되는

컴퓨터 구현된 방법.

청구항 16

제9항에 있어서,

중간 재부팅 동작없이 상기 복수의 조건 모두에 대해 업데이트가 요청되었음을 판정하고 그 결과로서 하나의 조건에 대해 적어도 하나의 업데이트를 수행하는 것을 거절하는 단계를 더 포함하는

컴퓨터 구현된 방법.

청구항 17

시크릿을 봉인하는 컴퓨터 구현된 방법으로서,

시크릿을 획득하는 단계와,

컴퓨팅 시스템에서, 복수의 BLOB 중 제1 BLOB가 상기 시크릿을 포함하고 상기 제1 BLOB가 복수의 조건 중 제1 조건으로 봉인되도록 상기 시크릿을 상기 제1 BLOB 내에 봉인하는 단계- 상기 복수의 조건 중의 각각의 조건은 상기 컴퓨팅 시스템이 상기 시크릿을 수신하기에 신뢰되는지 여부를 나타내는 시스템 상태의 반영임 -와,

상기 복수의 BLOB 중 제2 BLOB가 상기 시크릿을 포함하고 상기 제1 BLOB가 상기 복수의 조건 중 제2 조건으로 봉인되도록 상기 시크릿을 상기 제2 BLOB 내에 봉인하는 단계를 포함하는

컴퓨터 구현된 방법.

청구항 18

제17항에 있어서,

상기 복수의 조건 중 적어도 하나가 변경되었다는 판정에 따라, 상기 적어도 하나의 변경된 조건과 연관된, 상기 복수의 BLOB 중 하나 이상의 BLOB를 업데이트하는 단계를 더 포함하는

컴퓨터 구현된 방법.

청구항 19

제17항에 있어서,

상기 조건들 중 적어도 하나는 서명자의 목록과 관련된

컴퓨터 구현된 방법.

청구항 20

제17항에 있어서,

상기 제1 조건 및 상기 제2 조건 중 적어도 하나는 운영 체제 컴포넌트의 목록과 관련된

컴퓨터 구현된 방법.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 최신 컴퓨터 시스템은 반드시 컴퓨터 시스템에 보안을 제공해야 한다. 바이러스 및 기타 방법이 컴퓨팅 시스템을 손상시키는 데 사용되었다. 따라서, 유효한 공격을 막거나 줄이기 위한 대책이 구현되었다.

[0002] 보호 유형 중 하나는 신뢰할 수 있는 플랫폼 모듈(TPM)에서 제공하는 보호에 관한 것이다. TPM은 암호화 키를 하드웨어 장치에 직접 통합하여 하드웨어 장치를 보호하는 기능을 제공한다. 단순한 예에서, TPM은 해독 키와 같은 시크릿(secret)을 저장할 수 있다. 시크릿은 시크릿 데이터의 잠금을 해제하는 데 사용될 수 있다. 예를 들어, 컴퓨터의 하드 드라이브는 하드 드라이브의 시크릿 데이터를 손상시키지 않도록 시크릿으로 암호화될 수 있다.

[0003] 시크릿은 봉인될 수 있다. 봉인이란, TPM이 해독을 가능하게 하도록 시크릿이 암호화되고, 외부 엔티티에 시크릿을 제공하는 TPM이 소정의 조건에 구속되어 있음을 의미한다. 따라서, TPM은 특정 조건이 충족되는 경우에만 시크릿을 해독 및/또는 제공한다. 즉, 봉인은 일반적으로 조건에 대한 암호화로 정의되는 반면 봉인해제는 조건을 해독 및 집행하는 것을 포함한다.

[0004] TPM에서 조건은 종종 하드웨어 또는 운영 체제 무결성과 관련된다. 예를 들어, 부팅 프로세스에서, 다양한 엔티티가 다양한 기능을 순차적으로 수행한다. 따라서, 엔티티(예를 들어, 부팅 모듈)는 무결성 검사를 수행할 것이고, 무결성 검사가 통과되면, 엔티티는 소정의 기능을 수행하고 프로세스 내의 다음 엔티티로 프로세싱을 전달할 것이다. 다음 엔티티는 무결성 검사를 수행하고 더 나아가 프로세싱을 또 다른 엔티티로 전달할 것이다. 이것은 모든 엔티티가 무결성 검사를 통과하고 원하는 처리를 수행할 때까지 계속된다. 프로세싱 또는 무결성 검사는 해당 결과가 검사 레지스터에 저장되는 반복적인 추가 및 해싱 프로세스와 같은 방식을 따라 누적될 수 있다. 프로세싱이 끝나면, 검사 레지스터는 계산된 조건 값을 가질 것이다. 이 조건 값은 알려진 양호한 조건 값과 비교될 수 있다. 알려진 양호한 조건 값은 알려진 정상적인 부팅 프로세스 중에 생성되었을 수 있다. 이 두 값이 일치하면, 암호가 해독되어 외부 엔티티에 제공된다. 따라서, 예를 들어, 운영 체제는 하드 드라이브를 해독하고 컴퓨팅 시스템이 사용될 수 있게 하는 시크릿을 얻을 수 있다.

[0005] 그러나, 조건 값이 일치하지 않으면(일반적으로 엔티티가 변조되었음을 나타냄), 시크릿은 TPM에 의해 해제되지 않을 것이다. 이것은 일반적으로 바람직한 결과이다. 그러나, 부팅 엔티티가 적법한 프로세스에 의해 업데이트되는 경우에도, 계산된 조건 값과 알려진 양호한 조건 값이 일치하지 않게 될 것이다. 이것은 TPM에 의해 시크릿이 유지되도록 할 것이며, 그에 따라 도시된 예에서, 하드 드라이브는 알려진 조건 값이 업데이트될 수 없으면 시스템이 손상되지 않더라도 컴퓨팅 시스템이 본질적으로 사용 불가능하게 되는 결과를 초래할 수 있다.

[0006] 본 명세서에서 청구된 대상은 임의의 단점을 해결하거나 전술한 바와 같은 환경에서만 동작하는 실시예에 한정되지 않는다. 오히려, 본 배경기술은 본 명세서에서 기술된 일부 실시예가 실시될 수 있는 하나의 예시적인 기술 영역을 설명하기 위해 제공된 것일 뿐이다.

발명의 내용

[0007] 본 명세서에서 예시된 일 실시예는 봉인된 시크릿을 획득하는 컴퓨터 구현 방법을 포함한다. 이 방법은 컴퓨팅 시스템에서 복수의 상이한 BLOB 중의 하나 이상의 BLOB을 해독하는 단계를 포함한다. 복수의 BLOB 중의 각각의 BLOB는 시크릿을 포함한다. 복수의 BLOB 중의 각각의 BLOB는 복수의 조건 중 상이한 조건으로 봉인되어 있다. 주어진 조건은, 시스템이 시크릿을 수신하도록 신뢰될 수 있는지 여부를 나타내는, 시스템 상태를 반영하는 것이다. 방법은 조건들 중 하나 이상의 조건을 평가하여 이 하나 이상의 조건 중 적어도 하나가 충족되는지를 결정하는 단계를 더 포함한다. 이 방법은 하나 이상의 조건 중 적어도 하나가 충족되는 경우, 외부 엔티티에 시크릿을 제공하는 단계를 더 포함한다.

[0008] 본 요약은 아래의 상세한 설명에서 더 자세히 설명되는 단순한 형태의 선정된 개념을 소개하기 위해 제공된다. 본 요약은 청구된 대상의 주요 특징이나 필수 기능을 식별하기 위한 것이 아니며 청구 대상의 범위를 결정하는 데 도움을 주기 위한 것도 아니다.

[0009] 추가의 특징 및 장점은 이하의 상세한 설명에서 설명될 것이고, 또한 부분적으로는 상세한 설명으로부터 명백해질 것이거나 또는 본 명세서의 교시의 실행에 의해 습득될 수 있다. 본 발명의 특징 및 이점은 특히 첨부된 청구 범위에 나타낸 수단 및 조합에 의해 실현되고 얻어질 수 있다. 본 발명의 특징은 하기의 상세한 설명 및 첨부된 청구 범위로부터보다 완전히 명백해질 것이며, 또는 후술되는 본 발명의 실시에 의해 습득될 것이다.

도면의 간단한 설명

[0010] 상술한 장점 및 다른 장점 및 특징이 얻어질 수 있는 방식을 설명하기 위해, 앞서 간략히 설명한 주제에 대한 보다 구체적인 설명은 첨부된 도면에 도시된 특정 실시예를 참조하여 설명될 것이다. 이들 도면은 단지 전형적인 실시예를 도시하고 있고 따라서 범위를 제한하는 것으로 간주되지 않는다는 것을 이해하면, 실시예는 첨부된 도면의 사용을 통해 추가적인 특이성 및 세부사항으로 기술되고 설명될 것이다.

도 1은 측정된 부팅 동작을 지원하는 장치를 도시한다.

도 2는 상이한 조건으로 동일한 시크릿을 봉인하는 상이한 BLOB를 도시한다.

도 3은 시스템 변경이 발생할 때 시크릿이 어떻게 봉인될 수 있는지를 도시하는 흐름도이다.

도 4는 시크릿을 획득하는 방법을 도시한다.

도 5는 시크릿을 봉인하는 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0011] 본 명세서에 도시된 실시예는 봉인과 관련된 조건이 충족되지 않는 경우에도, 키와 같은 봉인된 시크릿이 제공되게 할 수 있다. 이는 복수의 상이한 이진 대형 객체(BLOB)에 시크릿을 봉인함으로써 행해질 수 있는데, 각각의 BLOB는 상이한 조건으로 봉인된다. 따라서, 조건 중 하나가 충족되면 해당 조건과 관련된 BLOB로부터 시크릿이 제공될 수 있다. 이와 같이, 시스템 상태에 영향을 미치고 따라서, 계산된 시스템 조건 값에 영향을 미치는 여러 가지 업데이트가 구현될 수 있지만, 적어도 하나의 알려진 조건 값이 계산된 조건 값과 일치하는 한, 시크릿은 여전히 봉인해제되고 제공될 수 있다.

[0012] 또한, 계산된 조건 값이 알려진 조건 값과 일치하지 않는 경우, 이는 알려진 조건 값이 시스템 업데이트로 인해 업데이트될 필요가 있을 수도 있고, 및/또는 시스템 업데이트는 이 시스템 업데이트가 유효한지를 판정하기 위해 평가되어야 한다는 표시자로서 사용될 수 있다.

[0013] 일부 경우, 적어도 하나의 알려진 조건 값이 하나의 계산된 조건 값과 일치하는 한, 알려진 시스템 값은 일치하지 않는 계산된 조건 값으로 자동 업데이트될 수 있다.

[0014] 그러나, 알려진 조건 값이 반드시 자동으로 업데이트되는 것은 아니라는 것을 이해해야 한다. 특히, 때때로, 알려진 조건 값 및 계산된 조건 값의 불일치가 식별됨에 따라 업데이트가 신뢰가능하거나 유효함을 보장하기 위해 업데이트는 평가될 수 있다.

[0015] 상세한 예가 이제 도 1을 참조하여 도시된다.

[0016] 컴퓨팅 장치(100)가 (예를 들어, TCG 사양에 정의된 바와 같은) 측정된 부팅에 대한 지원을 구현하는 경우, 시스템 재부팅 간의 허가되지 않은 공개로부터 시크릿 데이터(114)를 보호하기 위한 목적으로 코드 무결성 수단을 이용하는 것이 가능하다. 이는 예를 들어 무작위 대칭 키(데이터 보호 키)와 같은 시크릿(104)으로 데이터스토어(102) 내의 데이터와 같은 시크릿 데이터(114)를 먼저 암호화한 후 시스템 신뢰 플랫폼 모듈(TPM)(106)을 통해 일반적으로 "봉인(sealing)" 동작으로 지칭되는 것을 사용하여 시크릿을 봉인함으로써 달성된다. 한 세트의 TPM 플랫폼 구성 레지스터(PCR)(108)가 후속 해독시 시스템 상태를 강제하는데 사용되며, TPM(106)은 PCR 세트(108)에서 선택된 PCR 중 임의의 하나가 예상 값과 일치하지 않는 경우 시크릿(104)을 해제하지 않을 것이다. TPM PCR(108)은 모든 로딩된 모듈의 연쇄 또는 누적된 해시 값 및 부팅 프로세스 구성을 포함하기 때문에, 방법은 컴퓨팅 장치가 봉인 동작에 의해 의도된 것과 동일한 상태로 부팅된 경우에만 시크릿(104)이 해제될 것이라는 것을 보장한다. 전술한 바와 같이, 구성 및/또는 임의의 로딩된 모듈로의 임의의 변경은 PCR 값을 변화시킬 것이므로, 단일 봉인 동작만이 사용되는 경우 부팅 사이클 동안 TPM(106)에 의한 시크릿(104)의 해제를 방지 할 것이다. 그러나, 본 명세서에 도시된 일부 실시예에서, 시크릿(104)을 포함하는 BLOB(110-1 내지 110-n)와 같은 다수의 봉인 동작 또는 다수의 봉인 BLOB가 사용되어 시크릿(104)이 제공될 수 있는 기회를 증가시킬 수 있다.

[0017] 또한, 컴퓨팅 장치(100)가 (UEFI 사양에 따라) 보안 부트에 대한 지원을 구현하는 경우, 시크릿 데이터를 보호하기 위해 사용되는 TPM PCR 세트를 제한하는 것이 가능하다. 예를 들어, 실시예는 레지스터를, 보안 부팅 데이터베이스의 구성 데이터를 포함하는 레지스터로만 제한할 수 있다. 대안적으로 또는 부가적으로, 실시예는 레지스터를, 로딩되는 모듈의 서명 권한을 포함하는 레지스터로만 제한할 수 있다. 이는 모듈(112)이 봉인 동작에 의해 목표된 동일한 원래의 기관에 의해 여전히 서명되는 한, 특정 부팅 사이클 동안 모듈(112)에 대한 임의의 업데이트가 개시되는 것을 허용한다. 대안적으로 또는 부가적으로, 실시예는 (시크릿(104)이 여전히 제공되는 것을 허용하면서) 보안 부팅 데이터베이스 자체의 콘텐츠가 업데이트되는 실시예를 용이하게 할 수 있는데, 이것은 희귀하지만 데이터베이스를 알려진 악성 모듈 및 서명자 목록을 갖는 최신 상태로 유지하는데 사용되는 매우 중요한 동작이다.

[0018] 실시예는 보안 부팅 데이터베이스 콘텐츠에 대한 업데이트에 걸쳐 TPM 봉인에 의해 보호되는 시크릿(104)을 보존하는 것을 용이하게 한다. 도시된 예에서, 데이터 스토어(104) 내의 시크릿 데이터는 이 경우 무작위 대칭 키(데이터 보호 키 또는 DPK)인 시크릿(104)으로 암호화되고, 시크릿(104)은 TPM(106)이 이 경우 보안 부팅 및 모듈 서명자의 상태를 반영하는 PCR 세트(108)의 서브 세트에 의해 반영된 제1 조건을 사용함으로써 봉인된다. 또한, 도시된 예에서, 실시예는 로딩되는 모듈의 해시를 반영하지만 보안 부팅 상태를 포함하지 않는 PCR 세트(108)에 봉인된 데이터 보호 키를 포함하는 추가의 봉인된 BLOB를 생성한다. 이 예에서는 두 개의 봉인된

BLOB(110-1,110-n)가 도시되어 있지만, 다른 실시 예에서는 다른 조건을 사용하여 추가적인 봉인된 BLOB가 생성될 수 있음을 이해해야 한다.

[0019] 도 2에 도시된 예시된 예에서, 시크릿(104)을 봉인해제할 때, 원래의 봉인된 BLOB(110-1)가 먼저 시도된다. 이 단계가 성공하면, 즉시 시크릿(104)을 이용할 수 있다. 백업 봉인된 BLOB(110-2)는 백업 BLOB(110-2)에 대한 봉인이 업데이트될 필요가 있는지의 여부를 결정하기 위해 자신의 타겟 PCR 값이 현재의 부팅 사이클과 여전히 일치하는 것에 대해 검증된다. 백업 PCR 값이 현재 사이클과 일치하지 않는 경우, 이는, 동일한 권한에 의해 여전히 서명된 동안 하나 이상의 모듈이 업데이트되었음을 나타내고, 그런 다음 백업된 봉인된 BLOB(110-2)는 현재 로딩된 모듈의 누적된 해시를 반영하도록 업데이트된다. 원래의 봉인된 BLOB(110-1)이 봉인해제되지 못하면, 이것은 보안 부팅 구성에 대한 잠재적 변화를 나타내며, 그런 다음 백업 BLOB(110-2)가 시도된다. 부팅 사이클 동안 동일한 세트의 모듈이 로딩되는 한, 백업 BLOB(110-1)은 성공적으로 봉인해제되어, 예컨대 데이터 보호 키와 같은 시크릿(104)을 해제할 것이고, 이것은 시크릿 데이터(114)를 해독할 수 있게 한다. 원래 봉인된 BLOB(110-1)는 보안 부팅 데이터베이스의 새로운 구성을 반영하도록 업데이트된다. 보안 부팅 데이터베이스 콘텐츠가 시크릿 데이터(114)를 보호하는 일부로서 사용되는 임의의 모듈과 별도로 업데이트되는 한, 이는 보안 부팅 구성에 대한 업데이트에 걸쳐 시크릿 데이터(114)가 보존될 수 있게 할 것이다.

[0020] 따라서, 실시예는 시크릿 데이터(114)를 위한 데이터 보호 키와 같은 시크릿(104)을 포함하는 데이터 BLOB를 생성 및 유지하되, 보안 부팅 구성 상태를 포함하지 않으나 하나 이상의 다른 조건으로 봉인된 동일한 데이터 보호 키를 포함하는 원래의 BLOB에 대한 백업 보호자로서 역할을 하는 로딩된 모듈의 누적된 해시를 포함하는 PCR 세트(108)의 상태, 보안 부팅 구성 상태 및 모듈 서명자를 반영하나 로딩된 모듈의 누적된 해시를 포함하지 않는 PCR 세트(108)의 상태와 같은 조건으로 봉인된 데이터 BLOB를 생성 및 유지하도록 구성된다.

[0021] 실시예는 전술한 백업 BLOB(110-2)의 경우와 같이, 현재의 부팅 사이클에서로딩된 모듈의 누적된 해시와 같은 조건을 항상 반영하기 위해 봉인된 BLOB를 업데이트하는 기능을 포함할 수 있다.

[0022] 설명한 예시에서, 실시예는 원래의 봉인된 BLOB(110-1)이 보안 부팅 상태의 변경 또는 다른 조건으로 인해 봉인해제 하지 못할 때 시크릿(104)(예를 들어, 데이터 보호 키)를 봉인해제하기 위해 백업 봉인된 BLOB(110-2)를 사용할 수 있다.

[0023] 실시예는 백업 BLOB(110-2)를 사용하여 시크릿(104)을 봉인해제한 후에 원래의 봉인된 BLOB(110-1)를 업데이트할 수 있다.

[0024] 도 2에 도시된 예에서, 시크릿 데이터(114)는 이 예에서, 무작위 대칭 데이터 보호 키(DPK)인 시크릿(104)로 암호화되고, DPK는 2개의 상이한 TPM PCR 세트로봉인되는데, 즉 도 2에 도시된 예에서, 마스터 봉인된 BLOB(110-1)는 (암호화된 시크릿 데이터(114)가 대안적으로 또는 추가적으로 다른 위치에 저장될 수 있지만) PCR(7,11)에 봉인된 DPK와 함께 암호화된 시크릿 데이터(114)를 포함하는 한편, 백업 봉인된 BLOB는 PCR(0,2,4, 11)에 봉인된 동일한 DPK를 포함한다. 측정된 부팅 TCG 사양 및 UEFI 사양에 따라, PCR(7)은 장치의 보안 부팅 구성을 반영하는 반면, PCR(4)은 부팅 관리자 모듈의 축적된 해시를 포함한다. 나머지 PCR은 본 명세서에서 다루지 않는 다른 목적으로 사용된다. 2개의 봉인된 BLOB 각각은 또한 타겟 축적된 해시 값, 즉 그 각각의 PCR 세트의 계산된 조건 값을 포함한다.

[0025] 도 3은 보안 부팅 구성의 변경에 걸쳐 시크릿 데이터(114)를 보존하기 위해 수행되는 하나의 특정 실시예에 대한 단계들을 나타내는 흐름도이다. 시크릿 데이터(114)가 획득될 필요가 있는 실행 시점에서, 제어는 먼저 (301에 도시된 바와 같이) 마스터 BLOB를 사용하여 DPK를 봉인해제하려 시도할 것이다. 마지막 부팅 사이클 이후에 보안 부팅 구성이 변경된 경우, 이 단계는 실패할 것으로 예상되며, 그러면 제어는 (302에 도시된 바와 같이) 백업 BLOB를 사용하여 DPK를 봉인해제하려 시도할 것이다. 이 단계에서의 실패는 마지막 부팅 사이클 이후에 보안 부팅 구성과 부팅 관리자 모듈이 모두 변경되었음을 나타내며 이로 인해 시크릿 데이터(114)는 보존되지 않는다. 다른 실시예에서, 시크릿 데이터(114)가 복구될 확률을 증가시키기 위해 추가적인 BLOB가 사용될 수 있다.

[0026] 그러나, 본 예에서, 부팅 관리자 모듈이 마지막 부팅 사이클 이후에 변경되지 않으면, 이 단계는 성공적이며 DPK를 제공할 것이다. 그 다음, 제어는 단계(303)로 진행되고 여기서 마스터 BLOB(110-1)은 PCR(7,11)의 현재 값에 대해 방금 획득한 DPK를 재봉인함으로써 업데이트된다. 그 다음, 제어는 단계(304)로 넘어가고, 방금 획득된 DPK는 현재 및 미래의 부팅 사이클에 이용가능한 시크릿 데이터(114)를 해독하는데 사용된다.

[0027] 단계(301)에서 마스터 BLOB(110-1)이 성공적으로 봉인해제된 경우, 다음 단계는 (305에서 도시된 바와 같이) 현

재의 TPM PCR에 대해 백업 BLOB의 타겟 PCR 누적된 해시 값을 검사하고 (306에서 도시된 바와 같이) 타겟 PCR 누적된 해시 값이 현재의 TPM PCR(108)과 일치하지 않으면 DPK를 재봉인함으로써 백업 BLOP를 업데이트한다(부팅 관리자 모듈이 마지막 부팅 사이클 이후에 업데이트되었을 가능성이 있음을 나타내다). 그 다음, 제어는 단계(304)로 넘어가서 단계(301)에서 획득된 DPK가 시크릿 데이터를 해독하는데 사용된다.

[0028] 다음의 논의는 수행될 수 있는 다수의 방법 및 방법 동작에 관한 것이다. 방법 동작은 특정 순서로 논의되거나 흐름도에서 특정 순서로 발생하는 것으로 설명될 수 있지만, 구체적으로 명시되거나 요구되는 경우를 제외하고는 특별한 순서가 필요하지 않는데, 그 이유는 하나의 동작이 그 동작이 수행되기 전에 완료된 다른 동작에 의존하기 때문이다.

[0029] 이제 도 4를 참조하면, 방법(400)이 도시된다. 방법(400)은 봉인된 시크릿을 획득하는 컴퓨터 구현 방법이다. 이 방법은 컴퓨팅 시스템에서 복수의 상이한 BLOB 중의 하나 이상의 BLOB를 해독하는 단계(동작 402)를 포함한다. 복수의 BLOB 중의 각각의 BLOB는 시크릿을 포함한다. 복수의 BLOB 중의 각각의 BLOB는 복수의 조건 중 상이한 조건으로 봉인된다. 주어진 조건은, 컴퓨팅 시스템이 시크릿을 수신하도록 신뢰될 수 있는지 여부를 나타내는, 시스템 상태를 반영하는 것이다. 예를 들어,이러한 시스템 상태는 BLOB의 서명자 또는 시스템 컴포넌트의 목록을 포함할 수 있다. 선택적으로 또는 부가적으로, 시스템 상태는 운영 체제 컴포넌트의 세트를 포함할 수 있다.

[0030] 방법(400)은 조건들 중 하나 이상의 조건을 평가하여 이 하나 이상의 조건 중 적어도 하나가 충족되는지를 판정한다(동작 404). 일부 실시예에서, 이것은 상술한 바와 같이 BLOB를 봉인해제함으로써 수행될 수 있다. 예를 들어, 축적된 해시 값은 계산되고 이전에 획득된 누적된 해시 값과 비교될 수 있다.

[0031] 하나 이상의 조건 중 적어도 하나가 충족되면, 방법은 외부 엔티티에 시크릿을 제공하는 단계(동작 406)를 더 포함한다. 예를 들어, 암호화된 하드 드라이브의 잠금을 해제할 수 있는 키가 잠금해제될 수 있다. 키는 TPM에 대해 외부 엔티티인 운영 체제시스템에 제공될 수 있다. 또 다른 예는 다양한 비디오 온 디맨드 공급자와 같은 상업적 스트리밍 미디어 공급자로부터 제공되는 미디어 스트림과 같이 장치 상의 특정 미디어 스트림을 해독하는데 사용되는 키를 잠금해제하는 것을 포함할 수 있다.

[0032] 방법(400)은 하나 이상의 조건 중 적어도 하나가 충족되지 않는다고 판정되면, BLOB 중 하나 이상이 업데이트될 필요가 있는지를 판정하는 단계를 더 포함할 수 있다. 예를 들어, 운영 체제 컴포넌트에 대한 타당한 변경도 조건들 중 하나가 이전에 알려진 조건과 일치하지 않게 할 수 있다. 그런 다음, 조건은 이러한 변경을 반영하도록 업데이트될 수 있고, 시크릿은 업데이트된 조건으로 재봉인될 수 있다.

[0033] 방법(400)은 조건이 충족되지 않게 하는 컴퓨팅 시스템에서의 변화는 수용할 수 없는 변화인 것으로 판정됨에 따라 대응하는 조건이 충족되지 않는 BLOB를 업데이트하지 않기로 판정하는 단계를 더 포함할 수 있다. 예를 들어, 운영 체제에 대한 변경이 허용되지 않거나 특정 서명이 충분하지 않다는 결정이 내려질 수 있다. 실시예는 조건이 롤백(roll-back)될 필요가 있는 경우에 업데이트된 조건으로의 재봉인을 방지할 수 있다.

[0034] 방법(400)은 하나 이상의 조건 중 적어도 하나가 충족되지 않는다고 판정됨에 따라, 충족되지 않은 조건과 관련된 하나 이상의 BLOB를 업데이트하는 단계를 더 포함할 수 있다. 따라서, 예를 들어, 시크릿이 제공될 수 있게 하는 하나의 조건은 충족되지만 또 다른 조건이 충족되지 않는 경우, 충족되지 않는 조건은 이 조건이 충족되도록 업데이트될 수 있고 시크릿은 업데이트된 조건으로 재봉인될 수 있다.

[0035] 방법(400)은 조건들 중 적어도 하나가 서명자, 예를 들어 운영 체제에 로딩되는 모듈의 서명 기관의 목록과 관련있는 경우 실시될 수 있다. 선택적으로 또는 부가적으로, 방법(400)은 조건들 중 적어도 하나가 운영 체제 컴포넌트의 목록과 관련있는 경우 실시될 수 있다.

[0036] 방법(400)은 복수의 BLOB에 대한 조건을 업데이트하는 단계를 더 포함할 수 있다. 이러한 일부 실시예에서, 조건들을 업데이트하는 것은 반복적으로 행해지므로, 2개 이상의 상이한 조건들은 조건들을 업데이트하는 사이의 중간 재부팅 동작으로 업데이트된다. 대안으로 또는 부가적으로, 방법(400)은 중간 재부팅 동작없이 복수의 조건 중의 모든 조건에 대해 업데이트가 요청되었음을 판정하고 그 결과로서 하나의 조건에 대한 적어도 하나의 업데이트를 수행하는 것을 거절하는 단계를 더 포함할 수 있다. 특히, 모든 조건이 변경되도록 업데이트가 수행되며 다음에 재부팅할 때, 시크릿을 얻을 수 있는 조건은 존재하지 않을 것이다. 따라서, 일부 실시예는 조건들 중 적어도 2개 사이에서 중간 재부팅없이 모든 조건들이 변경되는 것을 방지할 수 있다. 다시 부팅하면 하나 이상의 변경되지 않은 조건을 기반으로 시크릿을 여전히 복구할 수 있으면서 변경된 조건을 업데이트할 수 있을 것이다. 재부팅이 발생하고 변경된 조건이 업데이트되면, 변경되지 않은 조건은 변경될 수 있지만 이전에 변경

된 조건이 충족되어 업데이트되어 조건이 충족될 수 있게 할 수 있으므로 시크릿은 계속 복구될 수 있다.

[0037] 이제 도 5를 참조하면, 시크릿을 봉인하는 컴퓨터 구현 방법(500)이 도시되어 있다. 방법(500)은 시크릿을 획득하는 단계를 포함한다(동작 502). 예를 들어, 일부 실시예에서, 컴퓨팅 시스템의 하드 드라이브는 해독 키로 암호화될 수 있다. 해독 키는 시크릿일 수 있다. 해독 키는 TPM에 제공될 수 있다.

[0038] 방법(500)은 복수의 BLOB 중의 각각의 BLOB가 시크릿을 포함하고 복수의 BLOB 중의 각각의 BLOB가 복수의 조건 중의 상이한 조건으로 봉인되도록 컴퓨팅 시스템에서 복수의 BLOB 중의 각각의 다른 BLOB에 시크릿을 봉인하는 단계를 더 포함할 수 있다(동작 506). 주어진 조건은 시스템 상태를 반영한 것이다. 시스템 상태는 컴퓨팅 시스템이 시크릿을 수신하도록 신뢰될 수 있는지 여부를 나타낸다.

[0039] 방법(500)은 하나 이상의 조건 중 적어도 하나가 변경된 것으로 판정함에 따라, 변경된 조건과 관련된 하나 이상의 BLOB를 업데이트하는 단계를 더 포함할 수 있다.

[0040] 방법(500)은 조건들 중 적어도 하나가 서명자들의 목록과 관련있는 경우에 실행될 수 있다. 선택적으로 또는 부가적으로, 방법(500)은 제1 조건 및 제2 조건 중 적어도 하나가 운영 체제 컴포넌트의 목록과 관련있는 경우 실시될 수 있다.

[0041] 또한, 본 방법은 하나 이상의 프로세서 및 컴퓨터 메모리와 같은 컴퓨터 판독가능 매체를 포함하는 컴퓨터 시스템에 의해 실시될 수 있다. 특히, 컴퓨터 메모리는 하나 이상의 프로세서에 의해 실행될 때 실시예들에서 기술된 동작들과 같은 다양한 기능들이 수행되도록 하는 컴퓨터 실행가능 명령어를 저장할 수 있다.

[0042] 본 발명의 실시예는 아래에서보다 상세히 설명되는 바와 같이 컴퓨터 하드웨어를 포함하는 특수 목적 또는 범용 컴퓨터를 포함하거나 이용할 수 있다. 본 발명의 범위 내의 실시예는 또한 컴퓨터 실행가능 명령어 및/또는 데이터 구조를 운반하거나 저장하기 위한 물리적 및 다른 컴퓨터 판독가능 매체를 포함한다. 이러한 컴퓨터 판독가능 매체는 범용 또는 특수 목적 컴퓨터 시스템에 의해 액세스될 수 있는 임의의 이용 가능한 매체일 수 있다. 컴퓨터 실행가능 명령어를 저장하는 컴퓨터 판독가능 매체는 물리적 저장 매체이다. 컴퓨터 실행가능 명령어를 운반하는 컴퓨터 판독가능 매체는 전송 매체이다. 따라서, 제한이 아닌 예로서, 본 발명의 실시예는 적어도 두 개의 명백하게 상이한 종류의 컴퓨터 판독가능 매체, 즉 물리적 컴퓨터 판독가능 저장 매체 및 전송 컴퓨터 판독가능 매체를 포함할 수 있다.

[0043] 물리적 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장 장치(CD, DVD 등), 자기 디스크 저장 장치 또는 다른 자기 저장 장치, 또는 컴퓨터 실행가능 명령어 또는 데이터 구조 형태의 원하는 프로그램 코드 수단을 저장하는데 사용될 수 있고 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함한다.

[0044] "네트워크"는 컴퓨터 시스템 및/또는 모듈 및/또는 다른 전자 장치 간의 전자 데이터 전송을 가능하게 하는 하나 이상의 데이터 링크로 정의된다. 정보가 네트워크 또는 다른 통신 연결(유선, 무선 또는 유선과 무선의 조합)을 통해 컴퓨터로 전송되거나 제공되는 경우, 컴퓨터는 그 연결을 전송 매체로 적절하게 간주한다. 전송 매체는 컴퓨터 실행가능 명령어 또는 데이터 구조의 형태를 갖는 원하는 프로그램 코드 수단을 운반하는데 사용될 수 있고 또한 범용 또는 특수 목적 컴퓨터에 의해 액세스될 수 있는 네트워크 및/또는 데이터 링크를 포함할 수 있다. 상기의 조합 또한 컴퓨터 판독가능 매체의 범위 내에 포함된다.

[0045] 또한, 다양한 컴퓨터 시스템 컴포넌트에 도달하면, 컴퓨터 실행가능 명령어 또는 데이터 구조의 형태의 프로그램 코드 수단이 전송 컴퓨터 판독가능 매체로부터 물리적 컴퓨터 판독가능 저장 매체(또는 그 반대)로 자동 전송될 수 있다. 예를 들어, 네트워크 또는 데이터 링크를 통해 수신된 컴퓨터 실행가능 명령어 또는 데이터 구조는 네트워크 인터페이스 모듈(예를 들어, "NIC") 내의 RAM에 버퍼링될 수 있고, 결국 컴퓨터 시스템의 RAM 및/또는 컴퓨터 시스템의 난휘발성 컴퓨터 판독가능 물리적 저장 매체로 전송된다. 따라서, 컴퓨터 판독가능 물리적 저장 매체는 또한 전송 매체를 또한(또는 주로) 이용하는 컴퓨터 시스템 컴포넌트에 포함될 수 있다.

[0046] 컴퓨터 실행가능 명령어는, 예를 들어, 범용 컴퓨터, 특수 목적 컴퓨터 또는 특수 목적 프로세싱 장치로 하여금 특정 기능 또는 기능 그룹을 수행하게 하는 명령어 및 데이터를 포함한다. 컴퓨터 실행 가능 명령어는 예를 들어 바이너리, 어셈블리 언어와 같은 중간 포맷 명령어 또는 심지어 소스 코드일 수 있다. 본 발명이 구조적 특징 및/또는 방법론적 동작들에 특정한 언어로 기술되었지만, 첨부된 청구 범위에서 한정된 청구대상은 상술한 특징 또는 동작에 반드시 제한되는 것은 아니라는 것을 이해해야 한다. 오히려, 설명된 특징 및 동작은 청구 범위를 구현하는 예시적인 형태로서 개시된다.

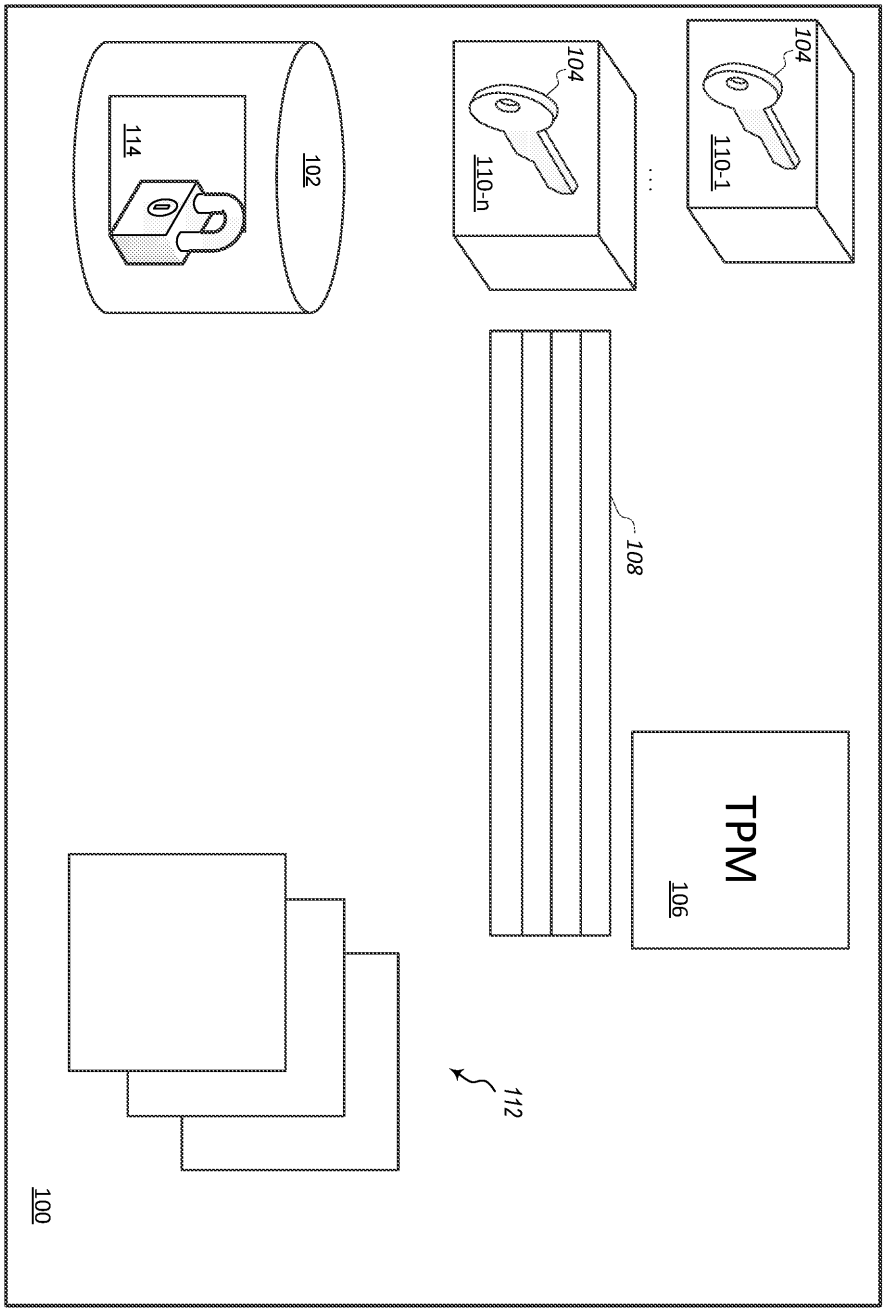
[0047] 당업자라면, 본 발명이 퍼스널 컴퓨터, 데스크톱 컴퓨터, 랩톱 컴퓨터, 메시지 프로세서, 핸드헬드 장치, 멀티프로세서 시스템, 마이크로프로세서 기반 또는 프로그램가능한 소비자 전자기기, 네트워크 PC, 미니 컴퓨터, 메인 프레임 컴퓨터, 이동 전화, PDA, 호출기, 라우터, 스위치 등을 포함하는 여러 유형의 컴퓨터 시스템 구성을 갖는 네트워크 컴퓨팅 환경에서 실시될 수 있음을 인식할 것이다. 본 발명은 또한 네트워크를 통해 (유선 데이터 링크, 무선 데이터 링크 또는 유선과 무선 데이터 링크의 결합에 의해) 연결된 로컬 및 원격 컴퓨터 시스템 모두가 작업을 수행하는 분산 시스템 환경에서도 실시될 수 있다. 분산 시스템 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 모두에 위치할 수 있다.

[0048] 대안으로, 또는 부가적으로, 본 명세서에 설명된 기능은 적어도 부분적으로 하나 이상의 하드웨어 로직 컴포넌트에 의해 수행될 수 있다. 예를 들어, 제한없이, 사용될 수 있는 예시적인 유형의 하드웨어 로직 컴포넌트는 필드 프로그래머블 게이트 어레이(FPGA), 프로그램 특정 집적 회로(ASIC), 프로그램 특정 표준 제품(ASSP), 시스템 온 칩 시스템(SOC), 컴플렉스 프로그래머블 로직 장치(CPLD) 등을 포함한다.

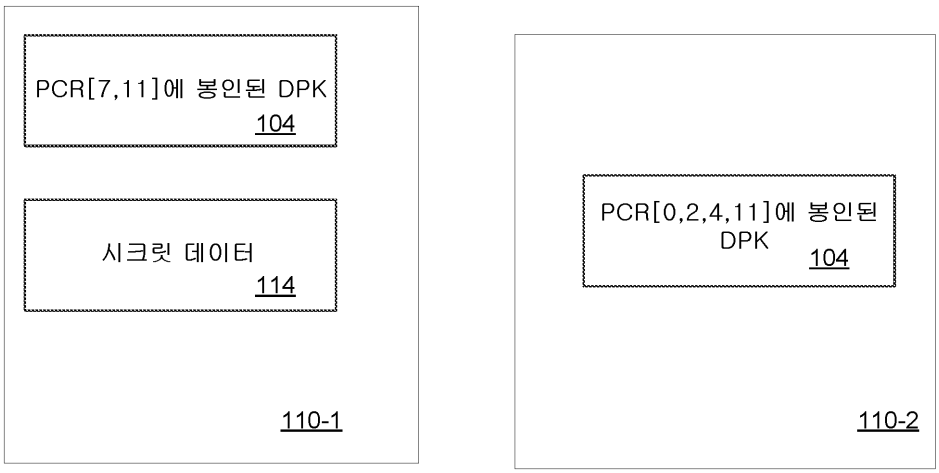
[0049] 본 발명은 본 발명의 사상 또는 특성으로부터 벗어나지 않으면서 다른 특정 형태로 구현될 수 있다. 기술된 실시예는 모든면에서 단지 예시적인 것으로서 제한적이지는 않다. 그러므로, 본 발명의 범위는 전술한 설명보다는 첨부된 청구 범위에 의해 표시된다. 청구 범위와 균등한 의미 및 범위 내에 있는 모든 변경은 그 범위 내에 포함되어야 한다.

도면

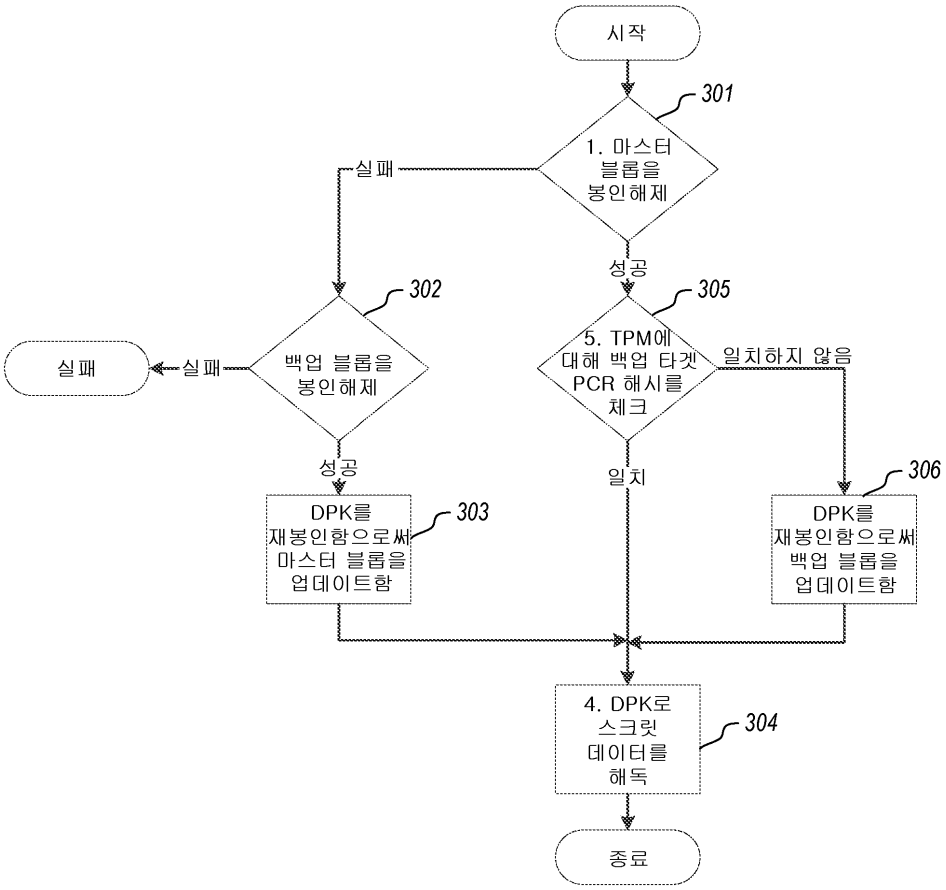
도면1



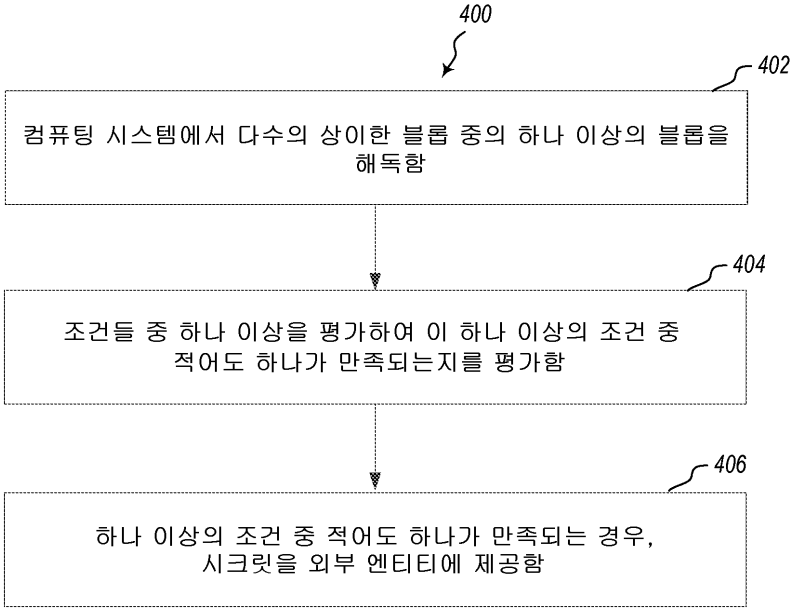
도면2


PCR[7,11]에 봉인된 DPK
104
시크릿 데이터
114
110-1
PCR[0,2,4,11]에 봉인된 DPK
104
110-2

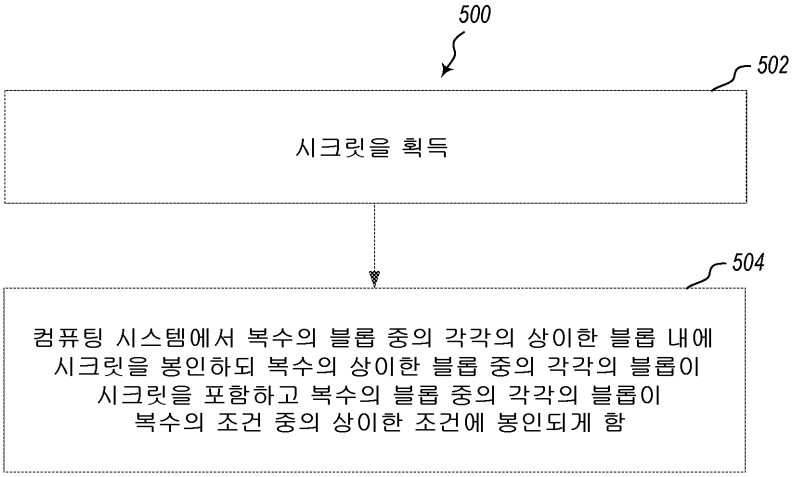
도면3


시작
301
1. 마스터 블롭을 봉인해제
실패
성공
302
백업 블롭을 봉인해제
실패
실패
성공
303
DPK를 재봉인함으로써 마스터 블롭을 업데이트함
305
5. TPM에 대해 백업 타겟 PCR 해시를 체크
일치하지 않음
일치
306
DPK를 재봉인함으로써 백업 블롭을 업데이트함
4. DPK로 스크릿 데이터를 해독
304
종료

도면4


400
402
컴퓨팅 시스템에서 다수의 상이한 블롭 중의 하나 이상의 블롭을 해독함
404
조건들 중 하나 이상을 평가하여 이 하나 이상의 조건 중 적어도 하나가 만족되는지를 평가함
406
하나 이상의 조건 중 적어도 하나가 만족되는 경우, 시크릿을 외부 엔티티에 제공함

도면5


500
502
시크릿을 획득
504
컴퓨팅 시스템에서 복수의 블롭 중의 각각의 상이한 블롭 내에 시크릿을 봉인하되 복수의 상이한 블롭 중의 각각의 블롭이 시크릿을 포함하고 복수의 블롭 중의 각각의 블롭이 복수의 조건 중의 상이한 조건에 봉인되게 함