(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2017년01월25일
(11) 등록번호 10-1699998
(24) 등록일자 2017년01월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/34 (2013.01) *G06F 21/57* (2013.01)
G06F 21/62 (2013.01) *G06F 21/72* (2013.01)
(21) 출원번호 10-2012-7009366
(22) 출원일자(국제) 2010년09월24일
심사청구일자 2015년08월24일
(85) 번역문제출일자 2012년04월12일
(65) 공개번호 10-2012-0087128
(43) 공개일자 2012년08월06일
(86) 국제출원번호 PCT/US2010/050275
(87) 국제공개번호 WO 2011/046731
국제공개일자 2011년04월21일
(30) 우선권주장
12/577,846 2009년10월13일 미국(US)
(56) 선행기술조사문헌
JP2008035449 A*
KR1020090079917 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 테크놀로지 라이센싱, 엘엘씨
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
톰 스테판
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
일락 크리스찬 마리우스
미국 워싱턴주 98052-6399 레드몬드 원 마이크로소프트 웨이 엘씨에이 - 인터내셔널 페이턴츠 마이크로소프트 코포레이션
(74) 대리인
제일특허법인

전체 청구항 수 : 총 14 항 심사관 : 문남두

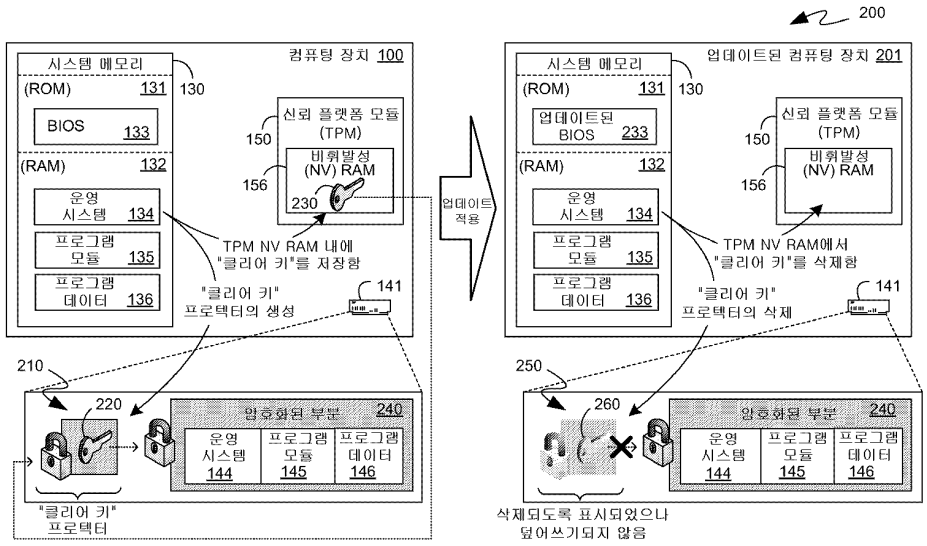
(54) 발명의 명칭 **일시적 중요정보의 보안 저장**

(57) 요 약

일시적으로 중요 정보는 TPM의 비휘발성 저장부 내에 저장될 수 있고, 그곳으로부터 그 정보는 안전하며, 복원 불가능하게 삭제될 수 있다. 추가하여, TPM 내에 저장된 정보는 통신적으로 접속 해제 가능한 저장 매체에 저장된 정보의 보안을 유지하여 통신적으로 접속 해제될 때, 이러한 매체에 저장된 정보가 액세스 불가능하게 할 수

(뒷면에 계속)

대 표 도



있다. 전체 볼륨(whole volume) 암호화 서비스 키는 TPM 내에 저장된 키에 의해 보호될 수 있고, 프로텍터가 액세스 가능하게 유지된다고 해도, TPM에서 키를 안전하게 삭제하는 것은 전체 볼륨 암호화 서비스 키의 비허가 노출을 방지한다. 추가하여, PCR에 의해 결정된 바와 같이 컴퓨팅 장치가 특정한 상태에 있을 때에만 데이터를 저장한 TPM이 공개될 수 있다. 휴지 상태 화상은 암호화될 수 있고, 그 상태가 휴지 상태(hibernation) 동안에 크게 변경되지 않은 경우에만 화상을 복호화하고 활성 컴퓨팅을 복원하기 위해 키가 공개되는 방식으로 그 키를 TPM에 저장한다.

명 세 서

청구범위

청구항 1

TPM(Trusted Platform module)을 포함하는 컴퓨팅 장치의 상태에 결부된 기존 암호화 메커니즘을 일시적으로 중지시키기 위한 컴퓨터 실행가능 명령어를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체로서,

상기 컴퓨터 실행가능 명령어는

제1 키를 암호화하는 단계- 상기 제1 키는 상기 기존 암호화 메커니즘의 일부이고, 상기 TPM은 상기 컴퓨팅 장치의 상태가 사전정의된 상태와 동일한 경우에만 상기 제1 키에 대한 액세스를 제공하도록 상기 기존 암호화 메커니즘의 일부로서 상기 TPM에 의해 보호되며, 상기 암호화하는 단계는 상기 컴퓨팅 장치의 상태에 결부된 상기 기존 암호화 메커니즘의 일시적 중지를 야기함 -와,

암호화된 상기 제1 키를 상기 컴퓨팅 장치에 통신가능하게 연결된 저장 매체에 저장하는 단계- 상기 저장 매체는 상기 TPM 외부에 있음 -와,

상기 TPM 외부에 있는 상기 저장 매체에 저장된 상기 암호화된 제1 키를 복호화하는 데 이용가능한 제2 키를 상기 TPM 내부에 있는 저장 매체에 저장하는 단계- 이 저장하는 단계는 상기 컴퓨팅 장치의 구체적인 상태와 무관하게 상기 TPM 내부에 있는 상기 저장 매체로부터 제2 키가 얻어질 수 있도록 행해짐 -와,

상기 제2 키가 저장된 상기 TPM의 저장 매체 상에서의 위치를 식별하는 인덱스를 상기 암호화된 제1 키와 함께 상기 TPM 외부에 있는 상기 저장 매체 상에 저장하는 단계와,

상기 TPM의 저장 매체에 상기 제2 키를 저장한 후, 상기 TPM에게 상기 제2 키를 요청하는 단계- 이 요청하는 단계는 상기 인덱스를 지정함 -와,

상기 요청에 응답하여 상기 TPM으로부터 획득된 상기 제2 키를 활용하여 상기 암호화된 제1 키를 복호화하는 단계와,

상기 TPM으로부터 획득된 상기 제2 키를 활용하여 상기 암호화된 제1 키를 복호화하는 단계 이후에, 상기 TPM의 저장 매체로부터 상기 제2 키를 삭제하도록 상기 TPM에게 명령함으로써, 상기 암호화된 제1 키가 상기 TPM 외부에 있는 상기 저장 매체로부터 검색되더라도 상기 제1 키에 대한 액세스를 방지하여 상기 기존 암호화 메커니즘이 복원되도록 하는 단계

를 수행하는

컴퓨터 판독가능 저장 매체.

청구항 2

제 1 항에 있어서,

상기 제2 키를 상기 TPM의 저장 매체에 저장하는 단계는 상기 TPM의 플랫폼 구성 레지스터(Platform Configuration Registers: PCRs)의 값과 무관하게 상기 제2 키에 대한 후속 요청에 응답하여 상기 TPM의 저장 매체로부터 상기 제2 키를 제공할 것을 상기 TPM에 명령하는 단계를 포함하는

컴퓨터 판독가능 저장 매체.

청구항 3

제 1 항에 있어서,

상기 TPM의 저장 매체에 상기 제2 키를 저장하는 단계 이후에 상기 TPM에게 상기 제2 키를 요청하는 단계는 상

기 컴퓨팅 장치의 상태가 변경된 후에 발생하고,

상기 기존 암호화 메커니즘의 일시적 중지는 상기 컴퓨팅 장치의 상태에 대한 변경이 예측되는 경우 수행되는

컴퓨터 판독가능 저장 매체.

청구항 4

제 1 항에 있어서,

상기 컴퓨터 실행가능 명령어는 상기 암호화된 제1 키를 저장하는 단계와, 상기 인덱스를 저장하는 단계 및 상기 제2 키를 저장하는 단계 이후, 상기 제2 키를 요청하는 단계 이전에, 상기 컴퓨팅 장치를 재부팅하는 단계를 더 수행하는

컴퓨터 판독가능 저장 매체.

청구항 5

제 1 항에 있어서,

상기 기존 암호화 메커니즘은 상기 TPM 외부에 있는 상기 저장 매체에 적용된 전체 볼륨 암호화(whole volume encryption) 메커니즘인

컴퓨터 판독가능 저장 매체.

청구항 6

TPM(Trusted Platform module)을 포함하는 컴퓨팅 장치의 상태에 결부된 기존 암호화 메커니즘을 일시적으로 중지시키기 위한 방법으로서,

제1 키를 암호화하는 단계- 상기 제1 키는 상기 기존 암호화 메커니즘의 일부이고, 상기 TPM은 상기 컴퓨팅 장치의 상태가 사전정의된 상태와 동일한 경우에만 상기 제1 키에 대한 액세스를 제공하도록 상기 기존 암호화 메커니즘의 일부로서 상기 TPM에 의해 보호되며, 상기 암호화하는 단계는 상기 컴퓨팅 장치의 상태에 결부된 상기 기존 암호화 메커니즘의 일시적 중지를 야기함 -와,

암호화된 상기 제1 키를 상기 컴퓨팅 장치에 통신가능하게 연결된 저장 매체에 저장하는 단계- 상기 저장 매체는 상기 TPM 외부에 있음 -와,

상기 TPM 외부에 있는 상기 저장 매체에 저장된 상기 암호화된 제1 키를 복호화하는 데 이용가능한 제2 키를 상기 TPM 내부에 있는 저장 매체에 저장하는 단계- 이 저장하는 단계는 상기 컴퓨팅 장치의 구체적인 상태와 무관하게 상기 TPM 내부에 있는 상기 저장 매체로부터 제2 키가 얻어질 수 있도록 행해짐 -와,

상기 제2 키가 저장된 상기 TPM의 저장 매체 상에서의 위치를 식별하는 인덱스를 상기 암호화된 제1 키와 함께 상기 TPM 외부에 있는 상기 저장 매체 상에 저장하는 단계와,

상기 TPM의 저장 매체에 상기 제2 키를 저장한 후, 상기 TPM에게 상기 제2 키를 요청하는 단계- 이 요청하는 단계는 상기 인덱스를 지정함 -와,

상기 요청에 응답하여 상기 TPM으로부터 획득된 상기 제2 키를 활용하여 상기 암호화된 제1 키를 복호화하는 단계와,

상기 TPM으로부터 획득된 상기 제2 키를 활용하여 상기 암호화된 제1 키를 복호화하는 단계 이후에, 상기 TPM의 저장 매체로부터 상기 제2 키를 삭제하도록 상기 TPM에게 명령함으로써, 상기 암호화된 제1 키가 상기 TPM 외부에 있는 상기 저장 매체로부터 검색되더라도 상기 제1 키에 대한 액세스를 방지하여 상기 기존 암호화 메커니즘이 복원되도록 하는 단계

를 포함하는 방법.

청구항 7

제 6 항에 있어서,

상기 제2 키를 상기 TPM의 저장 매체에 저장하는 단계는 상기 TPM의 플랫폼 구성 레지스터(Platform Configuration Registers: PCRs)의 값과 무관하게 상기 제2 키에 대한 후속 요청에 응답하여 상기 TPM의 저장 매체로부터 상기 제2 키를 제공할 것을 상기 TPM에 명령하는 단계를 포함하는

방법.

청구항 8

제 6 항에 있어서,

상기 TPM의 저장 매체에 상기 제2 키를 저장하는 단계 이후에 상기 TPM에게 상기 제2 키를 요청하는 단계는 상기 컴퓨팅 장치의 상태가 변경된 후에 발생하고,

상기 기존 암호화 메커니즘의 일시적 중지는 상기 컴퓨팅 장치의 상태에 대한 변경이 예측되는 경우 수행되는

방법.

청구항 9

제 8 항에 있어서,

상기 암호화된 제1 키를 저장하는 단계와, 상기 인덱스를 저장하는 단계 및 상기 제2 키를 저장하는 단계 이후, 상기 제2 키를 요청하는 단계 이전에, 상기 컴퓨팅 장치를 재부팅하는 단계를 더 포함하는 방법.

청구항 10

제 6 항에 있어서,

상기 기존 암호화 메커니즘은 상기 TPM 외부에 있는 상기 저장 매체에 적용된 전체 볼륨 암호화(whole volume encryption) 메커니즘인

방법.

청구항 11

휴지 화상(hibernation image)을 보호하기 위한 컴퓨터 실행가능 명령어를 포함하는 하나 이상의 컴퓨터 판독가능 저장 매체로서,

상기 컴퓨터 실행가능 명령어는

TPM(Trusted Platform module)을 포함하는 컴퓨팅 장치의 휘발성 메모리로부터 콘텐츠를 포함하는 휴지 화상을 암호화하는 단계와,

상기 암호화된 휴지 화상을 상기 컴퓨팅 장치에 통신가능하게 연결된 저장 매체에 저장하는 단계- 상기 저장 매체는 상기 TPM 외부에 있음 -와

상기 컴퓨팅 장치의 상태가 사전정의된 상태와 동일한 경우에만 상기 암호화된 휴지 화상을 복호화하는 데 이용가능한 키가 상기 TPM으로부터 얻어질 수 있도록 상기 키를 상기 TPM 내부에 있는 저장 매체에 저장하는 단계와,

상기 키가 저장된 상기 TPM의 저장 매체 상에서의 위치를 식별하는 인덱스를 상기 암호화된 휴지 화상과 함께 상기 TPM 외부에 있는 상기 저장 매체 상에 저장하는 단계와,

상기 TPM의 저장 매체에 상기 키를 저장한 후 그리고 상기 컴퓨팅 장치의 휴지 이후에, 상기 TPM에게 상기 키를 요청하는 단계- 이 요청하는 단계는 상기 인덱스를 지정함 -와,

상기 요청에 응답하여 상기 TPM으로부터 획득된 상기 키를 활용하여 상기 암호화된 휴지 화상을 복호화하는 단계와,

상기 복호화된 휴지 화상의 적어도 일부를 상기 컴퓨팅 장치의 상기 휴발성 메모리에 복원하기 이전에 상기 TPM의 저장 매체로부터 상기 키를 삭제하도록 상기 TPM에게 명령함으로써, 상기 복호화된 휴지 화상이 두 번 이상 성공적으로 복호화되지 않도록 하는 단계

를 수행하는

컴퓨터 판독가능 저장 매체.

청구항 12

제 11 항에 있어서,

상기 키를 상기 TPM 내부에 있는 저장 매체에 저장하는 단계는 상기 TPM의 하나 이상의 플랫폼 구성 레지스터(Platform Configuration Registers: PCRs)가 예상되는 값을 포함하는 경우에만 상기 키를 제공할 것을 상기 TPM에 명령하는 단계를 포함하는

컴퓨터 판독가능 저장 매체.

청구항 13

제 12 항에 있어서,

상기 PCR의 예상되는 값은 상기 휴지 화상이 생성되었을 때의 상기 PCR의 값과 동일한

컴퓨터 판독가능 저장 매체.

청구항 14

제 11 항에 있어서,

상기 컴퓨터 실행가능 명령어는 상기 TPM에게 상기 키를 요청하는 단계가 실패하는 경우 상기 컴퓨팅 장치를 재부팅하는 단계를 더 수행하는

컴퓨터 판독가능 저장 매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 컴퓨팅 장치에 저장된 중요 정보의 보안을 유지하는 기술에 관한 것이다.

배 경 기 술

[0002] 컴퓨팅 장치가 더욱 유비쿼터스화(ubiquitous)될수록, 이러한 컴퓨팅 장치에 의해 더 많은 양의 중요 정보가 저장 및 활용되고 있다. 결과적으로, 이러한 컴퓨팅 장치의 사용자는 이러한 중요 정보의 보안을 유지하는 데 상당한 양의 시간 및 노력을 투자할 것이다. 중요 정보의 보안을 유지하는 메커니즘 중에는, 패스워드 기반의 메커니즘이 보편화되고 있다. 당업자라면 인식할 수 있듯이, 패스워드 기반의 보호 기술은 암호화 기술에 의존하

여 그에 대한 보호를 실행할 수 있다. 보다 구체적으로, 패스워드 기반의 보호 기술은 통상적으로 데이터의 집합을 암호화하고, 적절한 패스워드가 제공될 때에만 이러한 데이터에 대한 액세스를 제공한다. 적절한 패스워드가 제공되지 않는다면, 데이터는 암호화된 형태로 유지되고 그것에 의해 비허가 노출로부터 보호된다.

발명의 내용

해결하려는 과제

[0003] 패스워드 기반의 보호에 대한 보편성 및 사용 용이성을 이용하는 기술 중 하나로는 전체 볼륨 암호화(whole volume encryption)가 있고, 그것에 의해 주어진 볼륨에 저장된 데이터 전부 또는 거의 전부가 암호화된다. 결과적으로, 악의적인 개체가 이러한 데이터가 저장되어 있는 저장 매체에 대한 물리적 액세스를 획득한다고 해도, 이러한 데이터는 암호화된 형태로 저장되었을 것이므로 이 볼륨의 데이터는 그럼에도 불구하고 보호된 상태로 유지될 것이다. 당업자라면 알 수 있듯이, 전체 볼륨 암호화 기술은 통상적으로 효과적이고 능률적인 키 관리를 수행하기 위해 하나 이상의 계층을 갖는 키에 의존한다. 그러므로 예를 들면, "상위" 계층의 키는 "하위" 계층의 키를 복호화하는 데 이용될 수 있고, 결국 최하위 계층의 키는 저장 매체에 저장된 데이터 그 자체를 복호화하는 데 이용될 수 있다. 보호의 수단으로서, 하나 이상의 키의 계층의 복호화는 컴퓨팅 장치 자체의 상태와 결부되어, 예를 들면 저장 매체가 컴퓨팅 장치로부터 제거되었고 서로 다른 컴퓨팅 장치에 통신적으로 결합되었다면, 저장 매체가 통신적으로 결합되었던 컴퓨팅 장치의 상태가 변경되었을 것이므로 그 데이터는 복호화될 수 없다.

[0004] 컴퓨팅 장치의 작동 중에, 보안된 동작을 위해 구성된 컴퓨팅 장치라고 해도, 용이하게 액세스 가능한 형태로 중요 정보를 저장할 필요가 있는 상황 또는 경우가 존재할 수 있다. 예를 들면, 그 복호화가 통상적으로 컴퓨팅 장치의 상태와 결부되어 있는 키 등과 같이 전체 볼륨 암호화 메커니즘에서 이용되는 하나 이상의 키는, 실질적인 문제로서 컴퓨팅 장치의 상태에 영향을 줄 수 있는 컴퓨팅 장치의 업데이트 동안에 용이하게 액세스 가능한 형태로 저장되어야 할 필요가 있을 것이다. 이와 같이 용이하게 액세스 가능한 정보의 후속적인 제거는 용이하게 액세스 가능한 형태로 이러한 정보를 저장하는 것과 연관된 잠재적 보안 문제점을 개선해야 한다.

[0005] 그러나 현대의 저장 매체는 때때로 특정한 데이터 집합을 삭제되는 것으로 표시하는 한편, 저장 매체 자체에서 이러한 데이터를 실제적으로 파괴하지 않는 기법 및 기술을 이용한다. 예를 들면, 현대의 자기 기반의 저장 매체는 때때로 상당한 시간 량 동안에 삭제될 것으로 표시된 데이터가 실제적으로 덮어쓰기(overwritten)되지 않아서, 복원 불가능하게 파괴되지 않는 저장 능력을 포함한다. 그 중간 시간에, 데이터는 공지된 데이터 복원 메커니즘을 통해 액세스 가능하도록 유지될 수 있다. 유사한 방식으로, 고체 상태 저장 기술을 이용하는 현대의 저장 매체는 때때로 웨어-레벨링(wear-leveling) 기술을 실행한다. 이러한 기술의 결과로, 현대의 고체 상태 기반의 저장 매체는 데이터가 복원 불가능하게 제거될 것으로 예정된 후 상당한 시간 량이 지날 때까지 삭제되도록 표시된 데이터를 실제적으로 덮어쓰기하지 않을 것이다. 자기 기반의 저장 매체에서 그러하듯이, 고체 상태 기반의 저장 매체가 이러한 중요 정보를 적합하게 삭제하는 데 있어서의 장애는 실질적으로 더 약한 보안 상태를 초래할 수 있다.

과제의 해결 수단

[0006] 기존의 TPM(Trusted Platform Modules)은 작은 양의 보안된 저장 용량을 포함할 수 있다. 이러한 TPM 저장은 복원 불가능하게 제거될 중요 정보 집합의 일부 또는 전부를 저장하는 데 이용될 수 있다. 다른 현대의 저장 매체와는 다르게, TPM의 설계 명세는 TPM이 그 저장부에서 데이터를 제거하도록 지시받을 때, 보안되고 복원 불가능한 방식으로 그것을 실행하는 것을 명확히 요구한다.

[0007] 일실시예에서, 전체 볼륨 암호화 메커니즘은 특정 업데이트 동작 동안 등에서, 전체 볼륨 암호화 메커니즘과 연관된 하나 이상의 키의 프로텍터를 생성한 다음, TPM의 보안된 저장부 내에 이러한 프로텍터를 잠금 해제하는 키를 저장하는 동작을 위해 잠시 중단될 수 있다. 생성된 프로텍터는 프로텍터를 잠금 해제하는 키가 저장되어 있는 TPM의 보안된 저장부 내에 위치를 식별할 수 있는 메타데이터를 포함할 수 있다. 다음으로, 업데이트 동작을 완료한 후에, 프로텍터 및 TPM 내에 저장된 키는 삭제될 수 있다. 그 저장 메커니즘이 삭제되도록 요청되었던 데이터의 즉각적인 복원 불가능한 제거를 제공하지 않는 저장 매체에 저장되어 있는 경우와 같이, 생성된 프로텍터 그 자체가 복원 불가능하게 제거되지 않는다고 해도, 그 키는 복원 불가능하게 제거될 것이므로 전체

볼륨 암호화는 보안을 유지할 수 있다.

[0008] 다른 실시예에서, 암호화된 정보 등과 같이 키에 의해 보호된 정보는 보안되고 복원 불가능한 소거를 제공 또는 보장하지 않는 저장 장치에 저장될 수 있다. 이러한 정보를 보호하는 키는 TPM의 보안된 저장부 내에 저장될 수 있다. 보호된 정보가 복원 불가능하게 제거될 것이라면, 그 키는 TPM으로부터 보안되고 복원 불가능하게 제거될 수 있고, 그에 따라 보호된 정보는 그것이 저장된 저장 장치가 그 보안되고 복원 불가능한 탈착 가능성을 보장할 수 없는 경우에도 액세스 불가능하게 될 수 있다. 마찬가지로, 보호된 정보가 에일리어스(aliased), 복사 또는 그 외에 저장 장치에 의해 몇몇 다른 형태로 유지된다면, 그 복원 불가능한 제거를 포함하는 이러한 정보에 대한 제어는 여전히 TPM 내에 단독으로 유지되는 키 덕분에 달성될 수 있다.

[0009] 또 다른 실시예에서, 저장 매체가 이전에 통신적으로 결합되었었던 컴퓨팅 장치로부터 물리적으로 제거되고, 그에 따라 통신적으로 접속 해제되었다면, 저장 매체에 저장된 데이터는 보안된 상태로 유지되고, 액세스 불가능하게 될 수 있다. 적합한 컴퓨팅 장치에 의한 데이터의 견고한 액세스를 제공하기 위해서, 전체 볼륨 암호화 메커니즘은 이러한 저장 매체에 저장된 데이터를 암호화하는 데 이용될 수 있고, 전체 볼륨 암호화 메커니즘과 연관된 하나 이상의 키는 TPM 내에 저장된 키에 의해 보호될 수 있지만, 그에 대한 액세스는 예를 들면, 컴퓨팅 장치의 특정한 구성에 대해 키의 액세스를 결부시키는 것 등으로 반드시 한정되는 것은 아니다. 그러나 저장 매체가 물리적으로 도난당했고 그에 따라서 컴퓨팅 장치로부터 통신적으로 접속 해제 되었다면, 이러한 키는 해당 컴퓨팅 장치의 TPM으로부터 검색될 수 없을 것이고, 결과적으로 저장 매체에 저장된 데이터는 암호화된 상태로 유지되어 액세스 불가능할 것이다.

[0010] 다른 실시예에서, 컴퓨팅 장치에 형성된 컴퓨팅 환경의 측면은, 컴퓨팅 장치가 휴지 상태(hibernated state)인 동안에 보호될 수 있다. 컴퓨팅 장치가 휴지 상태일 때, 생성된 휴지 상태 화상은 이러한 컴퓨팅 장치에 의해 이용되거나 이용되지 않을 수 있는 임의의 다른 암호화 메커니즘과는 독립적으로 암호화될 수 있다. 이러한 암호화된 휴지 상태 화상을 복호화하기 위한 키는 TPM 내에 저장될 수 있고, TPM으로부터 다음에 요청하는 프로세스로 그것을 공개하는 것은 컴퓨팅 장치가 휴지 상태일 때 컴퓨팅 장치의 특정한 구성에 결부될 수 있다. 다음으로 컴퓨팅 장치의 동작이 휴지 상태로부터 재개될 때, 암호화된 휴지 상태 화상은 컴퓨팅 장치가 휴지 상태였던 동안에 컴퓨팅 장치의 구성이 크게 변동되지 않은 경우에만 복호화되고 액세스될 수 있다. 추가하여, 암호화된 휴지 상태 화상을 복호화하기 위한 키는 컴퓨팅 장치가 휴지 상태로부터 재개될 때 TPM으로부터 삭제되어, 그 구성이 크게 변경된 컴퓨팅 장치에서 암호화된 휴지 상태 화상을 액세스 및 복원하려는 다수의 시도를 방지할 수 있다.

[0011] 이 요약은 이하의 상세한 설명에서 추가적으로 설명되는 개념의 선택을 단순화된 형태로 도입하고자 제공된 것이다. 이 요약은 청구 대상의 액세스 제어 특징 또는 중요한 특징을 식별하도록 의도된 것이 아니고, 청구 대상의 범주를 제한하기 위해 사용되도록 의도된 것도 아니다.

[0012] 추가적인 특징 및 이점은 첨부된 도면을 참조하여 계속 서술되는 이하의 상세한 설명으로부터 명확해질 것이다.

[0013] 이하의 상세한 설명은 첨부된 도면과 함께 고려할 때 가장 잘 이해될 수 있을 것이다.

도면의 간단한 설명

[0014] 도 1은 TPM을 포함하는 예시적인 컴퓨팅 장치를 도시하는 도면.

도 2는 정의된 시간 주기 동안 저장된 중요 정보를 저장한 다음 안전하게 삭제하는 데 있어서 TPM의 예시적인 사용을 도시하는 블록도.

도 3은 저장 매체의 물리적 도난을 통한 데이터 유포를 방지하는 데 있어서 TPM의 예시적인 사용을 도시하는 블록도.

도 4는 휴지 상태 동안에 컴퓨팅 장치를 보호하는 데 있어서 TPM의 예시적인 사용을 도시하는 블록도.

도 5는 정의된 시간 주기 동안 저장된 중요 정보를 저장한 다음 안전하게 삭제하는 데 있어서 TPM의 예시적인 사용을 도시하는 흐름도.

도 6은 휴지 상태 동안에 컴퓨팅 장치를 보호하는 데 있어서 TPM의 예시적인 사용을 도시하는 흐름도.

발명을 실시하기 위한 구체적인 내용

[0015] 이하의 설명은 TPM 내에 저장된 정보를 안전하고 복원 불가능하게 삭제하는 TPM의 능력을 이용하는 것과, TPM과 연관된 컴퓨팅 장치의 특정한 구성에 대해 중요 정보를 공개하는 것과 결부하기 위해 TPM의 능력을 이용하는 것을 포함하여, 중요 정보를 저장 또는 그 외에 보유하는 데 있어서 기존의 TPM(Trusted Platform Module)을 이용하는 것에 관한 것이다. 전체 볼륨 암호화 메커니즘을 잠시 중단하는 것이 적절할 수 있는 상황에서, 전체 볼륨 암호화 메커니즘과 연관된 하나 이상의 키는 프로텍터 내에 암호화될 수 있고, 이러한 프로텍터를 잠금 해제하는 것과 연관된 키는 TPM에 저장될 수 있다. 다음으로, 전체 볼륨 암호화 메커니즘이 재활성화될 수 있을 때, 프로텍터에 대한 키는 TPM에 의해 안전하고 복원 불가능하게 삭제될 수 있다. 마찬가지로, TPM에 저장된 정보는 보안되고 복원 불가능한 소거를 보장할 수 없는 저장 장치와 연관된 저장 매체에 저장되었거나, 이러한 저장 매체가 컴퓨팅 장치로부터 통신적으로 접속 해제되는 상황에서 그 데이터가 액세스 불가능하게 할 수 있다. 추가하여, 컴퓨팅 장치에서 활성화되었던 프로세스는 컴퓨팅 장치가 휴지 상태인 동안에 보호된 상태로 유지될 수 있고 이 때 휴지 상태 화상은 암호화되고, 키는 TPM 내에 저장되며 그 키의 공개는 TPM의 하나 이상의 PCR(Platform Configuration Registers)의 값에 의해 표현될 수 있는 것 등과 같이 컴퓨팅 장치의 특정한 상태와 결부된다. 휴지 상태 이후에 활성 컴퓨팅 상태로 재개될 때, 컴퓨팅 장치의 상태가 휴지 상태 동안에 크게 변경되지 않았다면 TPM 내의 키는 휴지 상태 화상을 복호화하는 데 이용될 수 있다.

[0016] 본 명세서에 설명된 기법은 전체 볼륨 암호화 메커니즘에 중점을 두고 있지만 이것으로 한정되지는 않는다. 실제로, 이하의 설명 내용은 그 후속적인 삭제가 복원 불가능한 방식으로 실행되는 임의의 보안된 정보 또는 그 액세스가 특정한 컴퓨팅 장치에 대한 통신 접속으로 한정되는 임의의 보안된 정보에 동등하게 적용 가능하다. 결과적으로, 이하의 설명은 열거된 실시예를 참조된 특정한 예시적인 상황으로 제한하도록 의도된 것이 아니다.

[0017] 필수적인 것은 아니지만, 이하의 설명은 프로그램 모듈 등과 같이 컴퓨팅 장치에 의해 실행되는 컴퓨터 실행 가능 명령어의 일반적인 문맥에서 이루어질 것이다. 보다 구체적으로, 이 설명은 다른 방식으로 지정되지 않았다면 하나 이상의 컴퓨팅 장치 또는 주변 장치에 의해 실행되는 동작의 단계 및 기호 표시를 참조할 것이다. 이와 같이, 때때로 컴퓨터 실행형으로 지칭되는 이러한 단계 및 동작은 구조화된 형태로 데이터를 나타내는 전기 신호의 처리 장치에 의한 조작을 포함한다는 것을 이해할 것이다. 이 조작은 데이터를 변환하거나 메모리 내의 위치에 그 데이터를 유지하고, 이것은 당업자에게 잘 알려진 방식으로 컴퓨팅 장치 또는 주변 장치의 동작을 재조정하거나 변경한다. 데이터가 유지되는 데이터 구조는 데이터의 포맷에 의해 정의되는 특정한 특징을 갖는 물리적 배치이다.

[0018] 일반적으로, 프로그램 모듈은 특정한 작업을 수행하거나 특정한 추상화 데이터 종류를 구현하는 루틴, 프로그램, 객체, 구성 요소, 데이터 구조 등을 포함한다. 더욱이 당업자라면 컴퓨팅 장치가 통상적인 퍼스널 컴퓨터로 반드시 한정되는 것은 아니고, 휴대형 장치, 멀티 프로세서 시스템, 마이크로 프로세서 기반 또는 프로그래밍 가능한 소비 가전, 네트워크 PC, 미니 컴퓨터, 메인프레임 컴퓨터 등을 포함하는 다른 컴퓨팅 구성을 포함한다는 것을 이해할 것이다. 마찬가지로, 이 메커니즘이 또한 통신 네트워크를 통해 연결된 분산형 컴퓨팅 환경 내에서 실행될 수 있기 때문에 컴퓨팅 장치는 독립형 컴퓨팅 장치로 반드시 한정되는 것은 아니다. 분산형 컴퓨팅 환경에서, 프로그램 모듈은 지역 및 원격 메모리 저장 장치 모두에 위치될 수 있다.

[0019] 도 1을 참조하면, 이하에 설명되는 방법에서 추가로 참조되는 하드웨어 소자를 부분적으로 포함하는 예시적인 컴퓨팅 장치(100)가 도시되어 있다. 예시적인 컴퓨팅 장치(100)는 하나 이상의 중앙 처리 장치(CPU)(120), 시스템 메모리(130), TPM(Trusted Platform module)(150) 및 시스템 메모리를 포함하는 다양한 시스템 구성 요소를 처리 장치(120)로 결합하는 시스템 버스(121)를 포함할 수 있지만 이것으로 한정되지 않는다. 시스템 버스(121)는 메모리 버스 또는 메모리 제어기, 주변 버스 및 다양한 버스 아키텍처 중 어느 하나를 이용하는 지역 버스를 포함하는 몇몇 종류의 버스 구조 중 어느 하나일 수 있다. 특정 물리적 구현에 따라서, CPU(120), 시스템 메모리(130) 및 TPM(150) 중 하나 이상은 단일 칩 등에서 물리적으로 공동 배치될 수 있다. 이러한 경우에, 시스템 버스(121)의 일부 또는 전부는 단일 칩 구조 내의 실리콘 경로에 불과할 수 있고, 도 1에서의 그 묘사는 설명을 목적으로 한 표기법적 편의 사항에 불과할 수 있다.

[0020] TPM(150)은 자신에 제공된 정보를 암호화 및 복호화하기 위한 암호화 키(151)를 포함할 수 있다. 통상적으로, TPM(150)은 공지되고 확립된 방식으로, 일회용 공개 및 비밀 암호화 키를 획득하는 데 이용될 수 있는 불변의 공개 및 비밀 암호화 키의 초기 집합을 포함한다. 추가하여, TPM(150)은 컴퓨팅 장치(100)의 상태와 고유하게 연관된 값 또는 다른 데이터를 보안된 방식으로 저장할 수 있는 PCR(Platform Configuration Registers)(155)을 포함할 수 있다. 이러한 값은 통상적으로 시스템 버스(121)를 통해 CPU(120)에 의해 TPM(150)으로

제공된다. 몇몇 실시예에서, CPU(120)에 의해 실행된 특정 코드만이 PCR(155) 내에 저장된 값을 수정할 수 있는 TPM(150)으로 데이터를 전달하도록 허용될 수 있다. TPM(150)은 비휘발성 RAM(156) 등과 같은 비휘발성 저장 용량을 더 포함할 수 있고, 그 내부에서 TPM이 CPU(120) 등과 같은 컴퓨팅 장치의 다른 소자에 의해 시스템 버스(121)를 통해 자신에게 제공된 적어도 작은 양의 정보를 보안된 방식으로 저장할 수 있다.

[0021] 상술된 소자에 추가하여, 컴퓨팅 장치(100)는 또한 전형적으로 컴퓨팅 장치(100)에 의해 액세스될 수 있는 임의의 이용 가능한 매체를 포함할 수 있는 컴퓨터 판독 가능 매체를 포함한다. 제한 사항이 아닌 예시로서, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터 등과 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현되는 매체를 포함한다. 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 다른 광학 디스크 저장, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 다른 자기 저장 장치, 또는 원하는 정보를 저장하는 데 이용될 수 있고 컴퓨팅 장치(100)에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만 이것으로 한정되지 않는다. 통신 매체는 전형적으로 반송파(carrier wave) 또는 다른 전송 메커니즘 등과 같은 변조된 데이터 신호 내에 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터를 구현하고, 임의의 정보 전달 매체를 포함한다. 제한 사항이 아닌 예시로서, 통신 매체는 유선 네트워크 또는 직접 유선 접속 등과 같은 유선 매체와, 음향, RF, 적외선 및 다른 무선 매체 등과 같은 무선 매체를 포함한다. 상술된 것 중 임의의 것들에 대한 조합도 컴퓨터 판독 가능 매체의 범주 내에 포함되어야 할 것이다.

[0022] 통신 매체를 이용할 때, 컴퓨팅 장치(100)는 하나 이상의 원격 컴퓨터에 대한 논리적 접속을 통해 네트워크형 환경 내에서 동작할 수 있다. 도 1에 도시된 논리적 접속은 LAN(local area network), WAN(wide area network) 또는 다른 네트워크일 수 있는 네트워크(180)에 대한 범용 네트워크 접속(171)이다. 컴퓨팅 장치(100)는 시스템 버스(121)로 접속되어 있는 네트워크 인터페이스 또는 어댑터(170)를 통해 범용 네트워크 접속(171)에 접속된다. 네트워크형 환경에서, 컴퓨팅 장치(100)나 그 부분 또는 주변부와 관련하여 도시되어 있는 프로그램 모듈은 범용 네트워크 접속(171)을 통해 컴퓨팅 장치(100)에 통신적으로 결합된 하나 이상의 다른 컴퓨팅 장치의 메모리 내에 저장될 수 있다. 도시된 네트워크 접속은 예시적인 것이고, 컴퓨팅 장치 사이에 통신 링크를 형성하는 다른 수단도 이용 가능하다는 것을 이해할 것이다.

[0023] 컴퓨터 저장 매체 중에서, 시스템 메모리(130)는 ROM(Read Only Memory)(131) 및 RAM(Random Access Memory)(132)를 포함하는 휘발성 및/또는 비휘발성 메모리의 형태로 컴퓨터 저장 매체를 포함한다. 다른 것 중에서도 컴퓨팅 장치(100)를 부팅하는 코드를 포함하는 BIOS(Basic Input/Output System)(133)는 전형적으로 ROM(131) 내에 저장된다. RAM(132)은 전형적으로 처리 장치(120)에 의해 즉시 액세스 가능 및/또는 현재 작동되고 있는 데이터 및/또는 프로그램 모듈을 포함한다. 제한 사항이 아닌 예시로서, 도 1은 RAM(132) 내에 상주하는 운영 시스템(134), 다른 프로그램 모듈(135) 및 프로그램 데이터(136)를 도시한다. RAM(132)은 또한 TCG 이벤트 로그(190) 등과 같이 TPM(150)의 동작과 관련될 수 있는 데이터를 포함할 수 있다. 일실시예에서, TCG 이벤트 로그(190)는 전원이 공급된 이후 또는 마지막으로 재시동된 이후로 컴퓨팅 장치(100)에 의해 로딩 또는 실행되는 모든 모듈의 고유한 식별 정보를 포함할 수 있고, 그 동일한 모듈의 로딩 또는 실행은 하나 이상의 PCR(155) 내의 TPM(150)에 의해 현재 유지되는 값의 생성을 초래할 수 있다.

[0024] 컴퓨팅 장치(100)는 다른 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 매체를 추가로 포함할 수 있다. 오로지 예시로서, 도 1은 탈착 불가능, 비휘발성 자기 또는 고체 상태 매체에 대한 판독 또는 기록을 실행하는 하드 디스크 드라이브(141)를 도시한다. 예시적인 컴퓨팅 장치에서 이용될 수 있는 다른 탈착 가능/탈착 불가능, 휘발성/비휘발성 컴퓨터 저장 매체는 자기 테이프 카세트, 플래시 메모리 카드, DVD(digital versatile disks), 디지털 비디오 테이프, 고체 상태 RAM, 고체 상태 ROM 등을 포함하지만 이것으로 한정되지 않는다. 하드 디스크 드라이브(141)는 전형적으로 인터페이스(140) 등과 같은 탈착 불가능 메모리 인터페이스를 통해 시스템 버스(121)에 접속된다.

[0025] 상술되고 도 1에 도시된 드라이브 및 그와 연결된 컴퓨터 저장 매체는 컴퓨팅 장치(100)를 위한 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 다른 데이터의 저장을 제공한다. 도 1에서, 예를 들면 하드 디스크 드라이브(141)는 운영 시스템(144), 다른 프로그램 모듈(145) 및 프로그램 데이터(146)를 저장하는 것으로 도시되어 있다. 이러한 구성 요소는 운영 시스템(134), 다른 프로그램 모듈(135) 및 프로그램 데이터(136)와 동일하거나 상이할 수 있다는 것을 주지하라. 운영 시스템(144), 다른 프로그램 모듈(145) 및 프로그램 데이터(146)는 최소한 이들이 상이한 복사본을 가질 수 있기 때문에 본 명세서에 도시된 것과는 상이한 개수로 제공된

다.

[0026] 일실시예에서, 운영 시스템(144), 다른 프로그램 모듈(145) 및 프로그램 데이터(146)는 암호화된 형태로 하드 디스크 드라이브(141)에 저장될 수 있다. 예를 들면, 하드 디스크 드라이브(141)는 전체 볼륨 암호화 메커니즘을 구현하거나 이용할 수 있고, 그것에 의해 하드 디스크 드라이브(141)에 저장된 데이터의 전부 또는 거의 전부가 암호화된 포맷으로 저장될 수 있다. 도 2를 참조하면, 예시적인 시스템(200)에서 하드 디스크 드라이브(141)는 운영 시스템(144), 프로그램 모듈(145) 및 프로그램 데이터(146) 중 적어도 상당한 부분을 포함할 수 있는 암호화된 부분(240)을 포함하도록 도시되어 있다. 키(220)는 컴퓨팅 장치(100)에 의해서 활용되거나, 하드 디스크 드라이브(141)와 연결된 하드웨어에 의해서 활용되어, 암호화된 부분(240)으로부터 데이터를 복호화할 수 있고, 그것에 의해 컴퓨팅 장치가 운영 시스템(144), 프로그램 모듈(145) 및 프로그램 데이터(146)를 의미 있게 액세스할 수 있게 한다.

[0027] 당업자에게 알려진 바와 같이, 전체 볼륨 암호화 메커니즘은 키(220) 등과 같은 키의 다수의 레벨 및 계층을 이용할 수 있다. 예를 들면, 운영 시스템(144), 프로그램 모듈(145) 또는 프로그램 데이터(146) 등과 같은 데이터를 서로 다른 키를 가지고 재 암호화해야하는 것을 피하기 위해서, 키(220)는 다른 키에 의해 그 자체가 암호화될 수 있다. 키(220)의 암호화된 버전 및 이러한 암호화된 키와 연관된 임의의 메타데이터는, "키 프로텍터(key protector)"로 지칭될 수 있다. 또한 당업자에게 알려진 바와 같이, 단일 키에 대해 다수의 키 프로텍터가 생성될 수 있고, 각각의 키 프로텍터는 서로 다른 인증 또는 다른 보안 메커니즘과 연관된다. 따라서 예를 들면, 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 데이터를 복호화할 수 있는 키(220)는 사용자의 패스워드와 연관된 키를 이용하여 하나의 키 프로텍터로 암호화될 수 있고, PCR(155)의 특정한 값과 연관된 키를 사용하여 다른 키 프로텍터로 암호화될 수 있다. 이러한 방식으로, 암호화된 부분(240)은 인가된 사용자가 그 패스워드를 입력하는 경우 또는 PCR(155)의 값이 컴퓨팅 장치가 신뢰되는 상태라고 표시하는 경우에 컴퓨팅 장치(100)에 의해 복호화 및 액세스될 수 있다.

[0028] 다수의 계층의 키는 앞서 도시된 바와 같이 다양한 액세스 대안을 제공하는 데 활용될 수 있다. 추가하여 다수의 계층의 키는 예를 들면, 신뢰도의 증가, 보안 보증의 제공, 성능의 증가, 예를 들면, 자신의 키를 잊어버릴 수 있는 사용자를 위한 제 3 자 보조 또는 지원의 제공 또는 다른 목적을 포함하는 다른 키 관리 목적을 위해 이용될 수 있다. 그러므로 이하의 설명에서, 전체 볼륨 암호화 메커니즘과 연관된 키(220) 등과 같은 키에 대한 참조는 임의의 계층의 키를 참조하도록 의도된 것이고, 예를 들면, 암호화된 부분(240)을 직접적으로 복호화하는 특정한 키에 대해서만 배타적으로 참조하는 것으로 의도된 것이 아니다.

[0029] 특정 상황에서, 전체 볼륨 암호화 메커니즘에 의해 전형적으로 제공되는 보호가 일시적으로 중단되어야 할 필요가 있을 수 있다. 예를 들면, 컴퓨팅 장치(100)의 신뢰 상태에 영향을 줄 수 있는 업데이트 동안에, PCR(155)을 위한 적절한 값을 미리 결정하는 것이 어렵거나 불가능할 수 있고, 이러한 결정이 없으면 암호화된 부분(240) 내에 저장된 데이터에 대한 액세스를 가능하게 하는 데 필요하고 PCR의 특정한 값과 연관된 키는 액세스 불가능할 것이므로, 전체 볼륨 암호화는 중단되어야 할 필요가 있을 것이다. 이러한 문제를 피하기 위해서, 전체 볼륨 암호화 또는 다른 보안 메커니즘은 예를 들면, 키(220)의 암호화된 버전 및 키(220)의 암호화된 버전을 복호화하는 데 필요한 키를 모두 포함할 수 있는 "클리어 키(clear key)" 프로텍터(210)를 생성하는 것에 의해서 컴퓨팅 상태에 대한 변경을 기대하고 일시적으로 중단될 수 있다. 확인되는 바와 같이, 이러한 "클리어 키" 프로텍터(210)는 임의의 프로세스가 키(220) 등과 같이 보호된 키 자체를 액세스하기 위해 "클리어 키" 프로텍터에 액세스할 수 있게 하고, 이는 이러한 프로세스에게 암호화된 부분(240) 내의 모든 데이터에 대한 액세스를 제공할 수 있다. 결과적으로, 예를 들면 하드 디스크 드라이브(141)에서 "클리어 키" 프로텍터(210)의 존재는 이러한 드라이브에서 구현되는 전체 볼륨 암호화의 보안 측면을 효과적으로 중단 또는 불능화한다. 도 2의 시스템(200)의 하드 디스크 드라이브(141)에서 구현되는 것 등과 같은 전체 볼륨 암호화 메커니즘의 보안 측면을 다시 가능하게 하기 위해서, 클리어 키 프로텍터(210)는 그것이 검색될 수 없게 하는 방식으로 하드 디스크 드라이브로부터 삭제될 수 있다.

[0030] 예를 들면, 전체 볼륨 암호화 메커니즘의 보안 측면을 피할 수 있는 클리어 키 프로텍터 등과 같은 중요 정보의 복원 불가능한 삭제를 제공하기 위해서, 특정 정보는 TPM(150)의 NV RAM(230) 내에 저장될 수 있다. 그러므로 일실시예에서, 클리어 키 프로텍터(210)와 연관된 키(230)가 상술된 바와 같이 클리어 키 프로텍터와 저장되는 것 대신에, TPM(150)의 NV RAM(156) 내에 저장될 수 있다는 것 외에도 도 2의 시스템(200)에 도시된 바와 같이 운영 시스템(134) 또는 다른 프로세스는 하드 디스크 드라이브(141)에 저장될 수 있는 클리어 키 프로텍터(210)를 생성할 수 있다. 그러므로 운영 시스템(134)은 2개의 서로 다른 저장 매체에 데이터를 제공하는 것으로 도시되어 있다. 특히, 운영 시스템(134)은 하드 디스크 드라이브(141)에 클리어 키 프로텍터(210)를 저장할 수

있고, TPM(150)의 NV RAM(156) 내에 클리어 키 프로텍터(210)와 연관된 키(230)를 저장할 수 있다.

[0031] 도 2에 도시된 시스템(200)의 클리어 키 프로텍터(210)는 키(230) 자체 외에도, TPM NV RAM(156) 내에 저장되어 있는 키(230)에 대한 포인터를 포함할 수 있다. 보다 구체적으로, 일실시예에서 클리어 키 프로텍터(210)는 키(230)가 TPM(150)의 NV RAM(156) 내에 저장되어 있는 NV 인덱스를 포함할 수 있다. 당업자에게 알려진 바와 같이, 클리어 키 프로텍터(210)의 후속적인 액세스는 그와 함께 저장되어 있는 NV 인덱스를 노출시킬 것이고, 그것에 의해 TPM(150)으로부터 키(230)를 요청하는 액세스 프로세스가 가능하게 한다. 그에 응답하여, TPM(150)은 요청하는 프로세스에 키(230)를 제공할 수 있고, 요청하는 프로세스는 이러한 키(230)를 가지고 클리어 키 프로텍터(210)로부터 키(220)를 획득할 수 있고, 암호화된 부분(240) 내의 정보를 액세스할 수 있다.

[0032] 도 2의 시스템(200)에 도시된 바와 같이, 컴퓨팅 장치(100)가 업데이트되어 업데이트된 컴퓨팅 장치(201)의 형태를 갖추면, 운영 시스템(134) 또는 다른 관련 프로세스는 예를 들면, 하드 디스크 드라이브(141)에서 구현되는 전체 볼륨 암호화의 보안 측면을 피하도록 생성된 정보를 삭제할 수 있다. 그러므로 도시된 바와 같이, 클리어 키 프로텍터(210)를 삭제하는 명령어는 하드 디스크 드라이브(141)에 제공될 수 있고, 키(230)를 삭제하는 명령어는 TPM(150)에 제공될 수 있다. 상술된 바와 같이, 클리어 키 프로텍터(210)는 하드 디스크 드라이브(141)의 저장 매체로부터 복원 불가능하게 제거되지 않을 수 있다. 예를 들어, 하드 디스크 드라이브(141)가 자기 저장 매체로 이루어져 있다면, 클리어 키 프로텍터(210)는 그것이 하드 디스크 드라이브(141)에 저장을 위해 제공된 다른 데이터에 의해 덮어쓰기될 때까지 실제적으로 이 자기 저장 매체에 유지될 수 있다. 통상적인 자기 저장 매체 기반의 저장 장치는 삭제되도록 표시된 데이터를 임의로 덮어쓰기할 수 있는 보안 삭제 기능을 실행할 수 있지만, 자기 저장 매체의 본질은 그것이 몇 번 덮어쓰기되었다고 할지라도 이전에 저장된 정보의 복원이 가능하게 하는 것이다. 마찬가지로, 하드 디스크 드라이브(141)가 고체 상태 기반의 저장 매체로 이루어져 있다면, 클리어 키 프로텍터(210)는 그것이 삭제되도록 표시된 후에도 이 고체 상태 기반의 저장 매체에 유지될 수 있다. 보다 구체적으로, 고체 상태 기반의 저장 매체는 전형적으로 임의의 다른 세그먼트에서보다 특정한 세그먼트에 더 많이 기록하는 것을 피할 수 있는 웨어 레벨링(wear leveling) 기술과 함께 사용된다. 결과적으로, 세그먼트에 저장된 데이터는, 그 데이터가 삭제되었었다고 해도, 상당한 시간 주기 동안 액세스 가능한 상태로 유지될 수 있다.

[0033] 도 2의 시스템(200)에서, 클리어 키 프로텍터(250) 및 키(260)는 삭제될 것이나 복원 가능한 상태에 있는 클리어 키 프로텍터(210) 및 보호된 키(220)를 예시하도록 의도된 것이다. 그러나 도 2에서 확인되는 바와 같이, TPM NV RAM(156)으로부터 키(230)를 복원 불가능하게 제거하는 것은 하드 디스크 드라이브(141)에서 구현되는 전체 볼륨 암호화의 보안 측면을 복구할 수 있다. 보다 구체적으로, 키(230)가 클리어 키 프로텍터(210)와 함께 저장되었다면, 삭제된 후에도 클리어 키 프로텍터(250)는 하드 디스크 드라이브(141)의 저장 매체로부터 복원될 수 있고, 키(260)는 획득될 수 있었고, 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보를 액세스하는 데 이용될 수 있었다. 그러나 그와 같이 명령받았을 때 그 NV RAM(156) 내에 저장된 정보의 안전한 삭제를 요구하는 명세에 부합될 수 있는 TPM(150) 내에 키(230)가 저장되었었기 때문에, 프로텍터(250)를 액세스하기 위해서는 키(230)가 필요하고, 키(260)의 획득은 더 이상 이용 가능하거나 검색 가능하지 않을 것이므로 하드 디스크 드라이브(141)의 저장 매체로부터 클리어 키 프로텍터(250)를 복원한다고 해도 키(260)를 획득할 수 없을 것이다. 결과적으로, 암호화된 부분(240) 내에 저장된 정보는 클리어 키 프로텍터(210)의 보안되거나 복원 불가능한 삭제가 없다고 해도 보호된 상태로 유지될 것이다.

[0034] 상기 설명 및 도 2에 제공된 도면은 암호화된 부분(240)의 복호화에 직접적으로 연관되는 것으로 도시된 키(220)를 보호하는 프로텍터를 참조하였으나, 당업자라면 상기 설명 및 도면은 통상적으로 전체 볼륨 암호화 메커니즘 등과 같은 보안 메커니즘에 의해 생성되고 그와 함께 사용되는 다수 계층의 키 중 어느 것에도 동등하게 적용 가능하다는 것을 인식할 것이다. 그러므로 예를 들면, 보호된 키(220)는 암호화된 부분(240)을 직접적으로 복호화할 수 있어야만 하는 것은 아니지만, 그 대신에 암호화된 부분(240)을 복호화할 수 있는 다른 키를 대신에 복호화할 수 있는 중간 계층의 키일 수 있다.

[0035] 추가하여, 상기 설명 및 도 2에 제공된 도면은 컴퓨팅 장치(100) 등과 같은 컴퓨팅 장치의 상태에 대한 변경 동안에 일시적으로 활용될 수 있는 것 등과 같은 전체 볼륨 암호화 메커니즘과 연관된 보호되지 않았거나 "클리어 키 프로텍터"의 보안된 삭제와 명시적으로 관련되어 있으나, 상술된 원칙은 보안된 삭제를 보장할 수 없는 저장 장치와 연관된 저장 매체에 저장된 임의의 보호된 데이터의 보안된 삭제에 동등하게 적용 가능하다. 보다 구체적으로, 몇몇 다른 데이터(통상적으로 또한 본 명세서에는 "키"로 지칭됨)가 정보에 대한 액세스를 획득하기 위해 이용될 수 있는 보호된 방식으로 정보가 저장되었다면, 이러한 정보에 대한 보안되고 복원 불가능한 제거를 제공하기 위해서, 앞서 상세히 설명된 것과 같이 보호된 정보는 임의의 저장 매체에 저장될 수 있고, 키는 TPM

NV RAM(156) 내에 저장될 수 있다. 저장 매체 및 이러한 저장 매체가 연결되어 있는 저장 장치가 보호된 정보에 대한 보안되고 복원 불가능한 제거를 제공 또는 보장할 수 없다고 해도, TPM(150)에 의해 제공될 수 있는 키의 보안되고 복원 불가능한 삭제는 상술된 것과 같이 이 보호된 정보가 저장되어 있었던 저장 매체 또는 장치의 능력과 무관하게 보호된 정보의 복원 불가능한 제거를 사실상 초래할 수 있다.

[0036] 많은 경우에, 저장 매체 및 이 매체가 연관된 저장 장치는 저장 매체에 저장되어 있는 보호된 정보를 에일리어스, 복사, 복제 또는 증식할 수 있는 하드웨어 기반의 메커니즘에 기인하여 복원 불가능한 제거를 보장할 수 없으므로, 보호된 정보의 하나의 복사본 또는 측면에 대한 보안된 제거는 모든 이러한 측면 또는 복사본의 보안된 제거를 보장할 수 없을 것이다. 이러한 경우에, 보호된 정보가 저장 하드웨어 자체의 일부분으로서 증식될 수 있는 경우에, TPM NV RAM(156) 내에 단일 키의 보존은 단일성의 수단을 제공할 수 있고, 보호된 정보에 대한 제어를 제공할 수 있다. 추가하여, 필수적인 것은 아니지만, 상술된 바와 같이 보호된 정보가 복원 불가능하게 제거되어야 한다는 것은 TPM NV RAM(156)로부터 키를 보안되고 복원 불가능하게 제거하는 것을 통해 달성될 수 있다.

[0037] 또 다른 실시예에서, TPM NV RAM(156) 내에 키(230) 등과 같은 키를 저장하는 것은 하드 디스크 드라이브(141) 등과 같은 저장 장치의 물리적 도난에 대한 보호의 수단 또는 이와 다르게 유지 관리 등을 이유로 합법적으로 제어되었던 저장 장치로부터의 정보 도난에 대한 보호의 수단을 제공하기 위해 이용될 수 있다. 도 3을 참조하면 시스템(300)은 컴퓨팅 장치로부터 물리적으로 또한 통신적으로 분리될 수 있는 하드 디스크 드라이브(141)와 함께 컴퓨팅 장치(100)를 포함하는 것으로 도시되어 있다. 상술된 바와 같이, 키(220)를 보호하는 키 프로텍터(210)는 하드 디스크 드라이브(141)에서 생성 및 저장될 수 있다. 위와 마찬가지로, 키(220)는 하드 디스크 드라이브(141)의 암호화된 부분(240)에 대한 복호화 및 액세스 제공을 위해 직접 또는 간접적으로 활용될 수 있다. TPM NV RAM(156) 내에 키(230)를 저장하고, 키 프로텍터(210)와 함께 키(230)에 대한 포인터를 제공함으로써, 컴퓨팅 장치(100) 및 그곳에서 실행되는 프로세스는 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보를 액세스하기 위해 모색할 때, 키 프로텍터(210)로부터 키(230)가 저장되어 있는 TPM NV RAM(156) 내의 위치까지 포인터를 따라갈 수 있고, 그 후에 TPM(150)으로부터 이러한 키를 획득하고 그것을 활용하여 궁극적으로 하드 디스크 드라이브의 암호화된 부분을 액세스할 수 있다.

[0038] 추가하여 일실시예에서, 키(230)에 대한 액세스 또는 보다 구체적으로, 키(230)가 저장되어 있는 TPM NV RAM(156)의 특정 인덱스에 대한 액세스는, TPM(150)에 의해 자유롭게 허가받을 수 있고, PCR(155)의 특정 값 또는 컴퓨팅 장치(100)의 상태와 연관된 다른 유사 정보로 반드시 한정되지는 않을 것이다. 결과적으로, 컴퓨팅 장치(100)에서 실행되는 프로세스는 컴퓨팅 장치 또는 그것에 의해 실행되는 프로세스의 전체적 보안에 대해 중요하지 않을 수 있는 컴퓨팅 장치의 상태에 관한 측면을 고려하지 않고 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보를 자유롭게 액세스할 수 있다. 이러한 환경은 서버 컴퓨팅 장치(100)의 상태가 보안되지 않은 방식으로 변경될 기회를 최소화할 수 있지만, 작동 가능한 가동 시간(uptime)이 가능한 한 많아지도록 유지할 방법을 모색해야만 하는 제한된 액세스의 물리적 환경 등과 같이 통상적으로 하드웨어 기반의 보안을 제공받을 수 있는 서버 컴퓨팅 장치에서 특히 유용할 수 있다.

[0039] 그러나 이러한 컴퓨팅 장치 또는 보다 구체적으로 이러한 컴퓨팅 장치의 구성 요소는 도난될 가능성이 있으므로, 상술된 바와 같이 필요한 정보를 TPM NV RAM(156) 내에 저장하는 것은 도난된 하드 디스크 드라이브(141) 또는 다른 유사한 도난된 저장 매체의 암호화된 부분(240)으로부터 정보가 활용되는 것을 방지할 수 있다. 이와 다르게, 하드 디스크 드라이브(141)의 고장이 발생하여 그 하드 디스크 드라이브의 교체를 필요로 할 수 있는 상황이 되면, 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보는 하드 디스크 드라이브, 또는 임의의 다른 유사한 저장 매체가 컴퓨팅 장치(100)로부터 물리적으로 또한 통신적으로 분리될 때 액세스 불가능하게 될 수 있다. 사실상, 하드 디스크 드라이브가 컴퓨팅 장치(100)로부터 통신적으로 분리되면 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보는 충분히 액세스 불가능하게 되고, 이는 하드 디스크 드라이브 또는 그곳에 저장된 정보에 대한 비용 및 시간 소모적인 소거 또는 다른 파기를 요구하지 않고도 다양한 보안 기준을 충족시킬 수 있다.

[0040] 도 3의 시스템(300)에서 확인되는 바와 같이, 예를 들어, 하드 디스크 드라이브(141)가 서버 컴퓨팅 장치(100)로부터 물리적으로 제거되는 경우 등과 같이, 허가된 유지 관리의 일부분으로서 또는 도난에 의해서 하드 디스크 드라이브(141)가 컴퓨팅 장치(100)로부터 통신적으로 분리된 다음, 상이한 컴퓨팅 장치에 통신적으로 결합되면, 이러한 상이한 컴퓨팅 장치에서 실행되는 프로세스는 컴퓨팅 장치(100)의 TPM(150)의 NV RAM(156) 내에 저장된 키(230)를 액세스할 수 없을 것이다. 이러한 키(230)에 대한 액세스가 없으므로, 하드 디스크 드라이브(141)가 다음에 통신적으로 결합되는 서로 다른 컴퓨팅 장치에서 실행되는 프로세스는 프로텍터(210)로부터 키

(220)를 획득할 수 없을 것이고, 그러므로 하드 디스크 드라이브(141)의 암호화된 부분(240) 내에 저장된 정보를 의미 있게 액세스할 수 없을 것이다. NV RAM(156) 내에 저장된 정보는 전자 통신 메커니즘을 통하거나 TPM(150) 자체의 물리적 액세스를 통해서 컴퓨팅 장치(100)의 외부에 있는 컴퓨팅 장치에서 실행되는 프로세스에 의해 TPM(150)으로부터 쉽게 획득될 수 없기 때문에, TPM NV RAM 내에 키(230) 등과 같이 필요한 정보를 저장하는 것은 컴퓨팅 장치(100)의 작동 가능한 가동 시간에 역효과를 주지 않으면서, 도난에 대비한 보안 및 허가된 유지 관리의 일부분으로서 교체된 저장 매체의 후속적인 액세스에 대한 보안을 모두 포함하여, 컴퓨팅 장치(100)로부터 통신적으로 접속 해제될 수 있는 저장 매체에 저장된 데이터에 대한 보안 수단을 제공할 수 있다.

[0041] 앞서 상세하게 열거되어 있지는 않지만, 당업자에게 알려진 바와 같이 TPM(150)은 하나 이상의 PCR(155)의 값에 의해 통상적으로 표시되는 것 등과 같이 특정한 상태의 컴퓨팅 장치(100)에게 TPM NV RAM(156) 등과 같은 곳 내부에 저장된 정보의 공개를 제한할 수 있다. 그러므로 다른 실시예에서, 이러한 TPM(150)의 게이트키핑(gatekeeping) 기능은 예를 들면, 컴퓨팅 장치가 휴지 상태에 있거나 중단 상태에 있을 때 등과 같이 컴퓨팅 장치(100)가 취약한 상태에 있을 수 있는 동안에 정보를 보호하기 위해 활용될 수 있다.

[0042] 도 4를 참조하면, 시스템(400)은 컴퓨팅 장치(100)가 휴지 상태에 있는 동안에 휴지 상태 화상(410)이 보호될 수 있게 하는 예시적인 메커니즘을 도시한다. 먼저, 컴퓨팅 장치(100)의 휴지 상태가 개시되면, 휴지 상태 화상(410)이 생성될 수 있다. 당업자에게 알려진 바와 같이 또한 도 4의 점선으로 도시된 바와 같이, 휴지 상태 화상(410) 등과 같은 휴지 상태 화상은 휴지 상태 이전에 컴퓨팅 장치의 상태와 연관된 정보를 포함할 수 있다. 예를 들면, 휴지 상태 화상(410)은 휴지 상태인 시간에 컴퓨팅 장치(100)의 RAM(132) 내에 존재하는 운영 시스템(134), 프로그램 모듈(135) 및 프로그램 데이터(136)의 상태를 포함할 수 있어서, 휴지 상태로부터 그 실행이 재개될 때, 컴퓨팅 장치(100)는 휴지 상태 화상(410)으로부터 RAM(132)으로 정보를 로딩할 수 있고, 그것에 의해 운영 시스템 및 프로그램 모듈이 그들의 이전 동작 또는 실행을 재개할 수 있게 한다.

[0043] 휴지 상태 화상(410)이 실행 상태에서의 프로세스 및 애플리케이션과 연관된 정보를 포함할 수 있으므로, 이것은 소정의 보안 관련 동작이 이미 실행된 이후에만 이용 가능할 수 있는 정보를 포함할 수 있다. 예를 들면, 운영 시스템(134) 또는 프로그램 모듈(135)의 소정의 측면은 컴퓨팅 장치(100)가 신뢰되는 상태에 있다고 결정된 이후에만 RAM(132) 내에 로딩될 수 있다. 그러나 운영 시스템(134) 또는 프로그램 모듈(135)의 이러한 측면은 임의의 추가적인 보호가 없어도 RAM(132) 내에 상주할 수 있다. 이러한 정보가 휴지 상태 화상(410)의 일부분으로서 수집 및 저장되었으므로, 예를 들면, 컴퓨팅 장치(100)가 휴지 상태에 있는 동안에 휴지 상태 화상에 대한 후속적인 액세스는 허가되지 않은 액세스로부터 이러한 정보를 보호하도록 의도된 통상의 보안 제약없이 이러한 정보에 대한 액세스를 제공할 수 있다.

[0044] 그러므로 일실시예에서, 휴지 상태 화상(410)의 무결성 및 컴퓨팅 장치(100)의 상태를 유지하기 위해서, 휴지 상태 화상은 도 4의 시스템(400)에 도시된 바와 같이 암호화되어 암호화된 휴지 상태 화상(415)으로 저장될 수 있다. 도 4의 시스템(400)은 운영 시스템(134)에 의해 실행되는 휴지 상태 화상(410)의 암호화를 도시하고 있으나, 당업자라면 이러한 암호화가 예를 들면, 프로그램 모듈(135)의 일부분으로서 실행되는 프로세스를 포함하는 다른 프로세스에 의해서도 동등하게 실행될 수 있다는 것을 인식할 것이다. 휴지 상태 화상(410)의 암호화 및 저장 장치에 그것을 암호화된 휴지 상태 화상(415)을 저장하는 것에 추가하여, 예를 들면, 하드 디스크 드라이브(141), 운영 시스템(134) 또는 다른 관련 프로세스 등은 암호화된 휴지 상태 화상(415)을 잠금 해제할 수 있거나 휴지 상태 화상(410)에 대한 액세스를 제공할 수 있는 키(430)를 TPM NV RAM(156) 내에 더 저장할 수 있다.

[0045] 일실시예에서, 키(430)에 대한 요청이 이루어질 때, PCR(155)의 하나 이상의 값이 컴퓨팅 장치(100)가 휴지 상태였던 시간에서와 동일하지 않다면 TPM이 키(430)를 공개 또는 제공하지 않게 하는 TPM(150)에 대한 명령어와 함께 TPM NV RAM(156) 내에 키(430)가 저장될 수 있다. 보다 구체적으로, 상술된 바와 같이 하나 이상의 PCR(155)의 값은 컴퓨팅 장치(100)의 상태와 고유하게 연관될 수 있다. 결과적으로, 컴퓨팅 장치(100)가 휴지 상태일 때, 하나 이상의 PCR(155)의 값은, 휴지 상태일 때 컴퓨팅 장치(100)의 상태 및 컴퓨팅 장치가 휴지 상태로부터 재개될 때 가져야 하는 컴퓨팅 장치의 상태를 반영할 수 있다. 그러므로 하나 이상의 PCR(155)의 값은 컴퓨팅 장치(100)의 상태가 휴지 상태였던 때부터 다음에 재개될 때까지 크게 변경되지 않은 것을 보장하도록 참조될 수 있고, 이와 같이 상술된 바와 같이 휴지 상태 화상(410)에 대한 액세스를 제공할 수 있는 키(430)의 공개는 컴퓨팅 장치가 휴지 상태일 때 하나 이상의 PCR(155)의 값에 결부될 수 있다.

[0046] 다음으로, 컴퓨팅 장치(100)가 휴지 상태로부터 재개될 때, 당업자에게 잘 알려진 바와 같이 운영 시스템(134)

의 구성 요소일 수 있는 부트 로더(434)는 휴지 상태 화상(410)에 대한 액세스 및 그것을 RAM(132)에 로딩하도록 시도할 수 있다. 그러나 그와 같이 할 수 있게 되기 전에, 부트 로더(434)는 먼저 TPM NV RAM(156)로부터 키(430)를 획득할 수 있다. 상술된 방식에서, 암호화된 휴지 상태 화상(415)은 예를 들면, TPM NV RAM(156) 내에서 키(430)의 위치에 대한 NV 인덱스에 대한 참조를 포함할 수 있다. 이러한 참조는 예를 들면, 부트 로더(434)가 TPM(150)으로부터 키(430)를 검색하도록 시도할 때 부트 로더(434)에 의해 이용될 수 있다.

[0047] 그러나 TPM(150)에 의한 키(430)의 공개는 하나 이상의 PCR(155)의 값에 결부될 수 있으므로, TPM은 먼저 컴퓨팅 장치가 휴지 상태로부터 재개되고 키(430)가 요청될 때에 PCR(155)의 값을 키(430)가 TPM NV RAM(156) 내에 저장될 때 지정되었던 PCR의 값에 대해 비교할 수 있다. 컴퓨팅 장치(100)의 상태에 대한 하나 이상의 중요한 측면이 컴퓨팅 장치가 휴지 상태였던 때부터 변경되었다면, 키(430)의 공개와 결부된 하나 이상의 PCR(155)의 값은 키(430)가 TPM NV RAM(156) 내에 저장되었던 때에 그 값과 동등하지 않을 것이고, TPM(150)은 키를 제공하지 않을 것이다. 그러므로 예를 들면, 악의적이거나 불분명 또는 신뢰되지 않는 컴퓨터 실행 가능 명령어 또는 다른 프로세스가 컴퓨팅 장치가 휴지 상태인 동안에 컴퓨팅 장치(100)에 비밀리에 삽입되었거나 실행을 준비하였다면, 이러한 컴퓨터 실행 가능 명령어 또는 프로세스의 실행 또는 활성화는 TCG 이벤트 로그(490) 내에 기록될 수 있고, PCR(155)의 값에 반영될 수 있다. 보다 구체적으로, 이러한 프로세스 또는 명령어의 비밀스런 삽입은 PCR(155)의 값이, 휴지 상태 이전에 TPM NV RAM(156) 내에 키(430)가 저장될 때 키(430)의 공개가 결부된 값과 상이해지게 할 것이고, 결과적으로 TPM(150)이 예를 들면, 부트 로더(434) 등과 같은 요청 프로세스에 대해 키(430)를 제공하는 것을 거부하게 할 것이다.

[0048] 결과적으로, 암호화된 휴지 상태 화상(415)은 복호화될 수 없을 것이고, 컴퓨팅 장치(100)는 새롭게 비밀리에 삽입된 명령어 또는 프로세스에 의해 휴지 상태로부터 그 동작을 재개할 수 없을 것이다. 그 대신에 당업자라면 인식할 수 있는 바와 같이, 컴퓨팅 장치(100)는 완전히 재시작되어, 임의의 비밀리에 삽입된 명령어 또는 프로세스의 효과를 제거 또는 중성화할 수 있고, 결과적으로 컴퓨팅 장치(100)를 보호하고 보다 구체적으로 예를 들면, 운영 시스템(134) 또는 프로그램 모듈(135)에 의해 로딩되고 활용되었을 수 있는 중요 정보가 노출되지 않게 할 수 있다.

[0049] 상술된 메커니즘의 동작은 도 5 및 도 6의 흐름도에 의해 보다 세부적으로 제시된다. 도 5를 참조하면, 흐름도(500)는 예를 들면, 업데이트 프로세스 동안 등에서 저장 매체에 일시적으로 저장될 필요가 있을 수 있는 중요 정보의 보안되고 복원 불가능한 삭제를 제공하도록 실행될 수 있는 예시적인 일련의 단계를 도시한다. 흐름도(500)에 도시된 단계는 또한 적어도 부분적으로, 이러한 정보가 컴퓨팅 장치에 대해 밀접하게 결부되는 방식으로 정보를 저장하고, 그 정보를 활용하여 이러한 저장 매체가 컴퓨팅 장치로부터 통신적으로 접속 해제될 때 저장 매체에 저장된 다른 정보를 보호하는 데 적용될 수 있다.

[0050] 먼저 단계(510)에서, 예를 들면, 컴퓨팅 장치의 부팅 프로세스에 영향을 줄 수 있거나, 컴퓨팅 장치의 작동 상태를 크게 변경시킬 수 있는 컴퓨팅 장치의 업데이트 또는 다른 변경이 개시될 수 있다. 다음으로, 단계(515)에서 예를 들면, 전체 볼륨 암호화 메커니즘과 연관된 키에 대하여 클리어 키 프로텍터가 생성될 수 있다. 단계(515)에서 생성된 클리어 키 프로텍터에 액세스할 수 있는 "클리어 키"는 단계(520)에서 TPM NV RAM 내에 저장될 수 있다. 예를 들면, 키가 저장되어 있는 TPM NV RAM 내에서의 위치와 연관된 NV 인덱스 등과 같이 TPM NV RAM 내에 저장된 키에 대한 포인터는, 단계(525)에서 클리어 키 프로텍터와 함께 저장되거나 클리어 키 프로텍터와 연관될 수 있다. 단계(530)에서, 컴퓨팅 장치의 상태에 크게 영향을 줄 수 있는 업데이트 또는 다른 변경의 실행과 연관된 하나 이상의 단계가 실행될 수 있다. 또한 단계(530)의 일부분으로서, 컴퓨팅 장치는 재부팅되거나 재시작될 수 있다.

[0051] 다음으로, 단계(535)에서는 예를 들면, 전체 볼륨 암호화 메커니즘의 부분으로서 보호된 정보 등과 같이 보호된 정보를 복호화하거나 액세스하려는 노력의 부분으로서 단계(515)에서 생성된 클리어 키 프로텍터가 액세스될 수 있다. 단계(540)에서는 단계(535)에서 액세스된 클리어 키 프로텍터로부터, NV 인덱스 등과 같은 포인터를 획득 및 활용하여 클리어 키 프로텍터에 의해 보호된 키를 복호화하거나 액세스하기 위한 키를 획득할 수 있다. 그 키가 단계(540)에서 성공적으로 획득되었다면, 단계(535)에서 획득된 클리어 키 프로텍터는 액세스될 수 있고, 결과적인 키를 활용하여 단계(545)에서 그 볼륨을 잠금 해제할 수 있다.

[0052] 상술된 바와 같이, 단계(530)에서 실행된 업데이트 또는 다른 변경은 예를 들면, 전체 볼륨 암호화 메커니즘과 연관된 키를 컴퓨팅 장치의 상태에 결부시키는 기존의 메커니즘에 영향을 줄 수 있다. 결과적으로, 단계(545)에서 전체 볼륨 암호화 서비스에 의해 보호된 볼륨이 잠금 해제된 후, 암호화된 볼륨을 액세스할 수 있는 키에 대한 하나 이상의 새로운 프로텍터는 단계(550)에서 선택적으로 생성될 수 있다. 추가하여, 단계(515)에서 생

성된 클리어 키 프로텍터는 단계(555)에서 저장되었던 저장 매체로부터 삭제될 수 있고, 단계(560)에서 TPM은 TPM NV RAM으로부터 그 키를 삭제하도록 명령받을 수 있다. 앞서 상세히 설명된 바와 같이, 단계(555)에서 삭제될 것으로 간주된 클리어 키 프로텍터가 사실상 복원 불가능하게 제거되지 않았다고 해도, 단계(560)에서 TPM NV RAM으로부터 키를 삭제하게 하는 TPM에 대한 명령어는 TPM이 부합되는 명세에 따라서 그 키가 안전하고 복원 불가능하게 삭제되도록 할 수 있다. 당업자라면 인식할 수 있는 바와 같이, 단계(555)에서 클리어 키 프로텍터의 삭제 및 단계(560)에서 TPM의 NV RAM으로부터 키를 삭제하게 하는 TPM에 대한 명령어는 반드시 도 5의 흐름도(500)에 도시된 순서와 정확히 동일하게 발생해야 하는 것은 아니고, 그 대신에 단계(545)에서 볼륨의 잠금 해제 동안 또는 잠금 해제 이후의 임의의 시간에 발생할 수 있다. 다음으로, 단계(565)에서 관련 프로세싱이 종료될 수 있다.

[0053] 앞서 상세히 설명된 바와 같이, 도난 또는 다른 통신적 분리로부터 다른 저장 매체에 있는 정보의 보안을 유지하기 위한 목적으로 정보의 중대한 부분이 TPM NV RAM 내에 저장되어 있는 경우 등과 같이 도 5의 흐름도(500)에 도시된 단계가 반드시 모두 실행되어야 하는 것은 아니다. 예를 들면, 단계(530)에서 컴퓨팅 시스템의 업데이트 또는 다른 변경 및 단계(550)에서 새로운 프로텍터의 대응하는 생성과, 단계(555) 및 단계(560)에서 각각 저장 매체로부터 클리어 키 프로텍터의 후속적인 삭제 및 TPM NV RAM으로부터 키의 삭제는 오로지 특정 실시예에만 적용 가능할 수 있고, 컴퓨팅 장치로부터 저장 매체의 도난 또는 다른 통신 분리의 경우에 저장 매체에 있는 정보를 보호하기 위한 방법을 단지 모색할 때 반드시 실행되어야 하는 것은 아니다.

[0054] 도 6을 참조하면, 흐름도(600)는 휴지 상태 또는 다른 중지 상태인 동안에 컴퓨팅 장치를 보호하기 위해 실행될 수 있는 예시적인 일련의 단계를 나타낸다. 먼저 흐름도(600)에서 확인되는 바와 같이, 단계(610)에서 사용자 또는 다른 프로세스는 컴퓨팅 장치의 휴지 상태 또는 정지 상태를 개시할 수 있다. 다음으로, 단계(615)에서 통상적인 휴지 상태 메커니즘에 따르면, 예를 들면 컴퓨팅 장치의 RAM으로부터의 관련 정보를 포함하는 휴지 상태 화상이 생성될 수 있다. 단계(620)에서 이 휴지 상태 화상은 컴퓨팅 장치가 휴지 상태에 있거나 그 외의 중지 상태에 있는 동안에 그에 대한 액세스 또는 수정으로부터 보호하기 위해 암호화될 수 있다. 암호화된 휴지 상태 화상과 연관되고, 암호화된 휴지 상태 화상을 복호화하는 데 이용될 수 있는 키는 단계(625)에서 TPM NV RAM 내에 저장될 수 있다.

[0055] 상술된 바와 같이, 단계(625)에서 TPM NV RAM에 키를 제공하는 데 있어서, TPM은 키에 대한 요청이 이루어질 때 TPM의 PCR의 하나 이상의 값이, 컴퓨팅 장치가 휴지 상태가 되었던 단계(625)의 시점에서의 값과 동일하지 않으면 요청하는 프로세스에게 그 키를 공개하지 않도록 명령받을 수 있다. 단계(620)에서 휴지 상태 화상이 암호화되고, 단계(625)에서 TPM NV RAM 내에 키가 저장되었다면, 단계(630)에서 컴퓨팅 장치는 휴지 상태의 요건을 갖추고 휴지 상태로 진입한다. 그 후의 소정의 시점에서, 단계(630)에 또한 포함되어 있듯이, 컴퓨팅 장치는 활성 동작을 재개하도록 명령받을 수 있다. 예를 들면, 부트 로더 또는 휴지 상태 관리자 등과 같이 이러한 시간에 컴퓨팅 장치에서 실행되는 관련 프로세스는 TPM으로부터 TPM NV RAM 내에 저장된 키를 획득하고, 단계(620)에서 암호화되었던 휴지 상태 화상의 복호화 및 액세스를 위하여 키를 이용함으로써 휴지 상태 바로 직전에 실행되었던 실행 내역으로 컴퓨팅 장치를 복원하기 위한 방법을 모색할 수 있다.

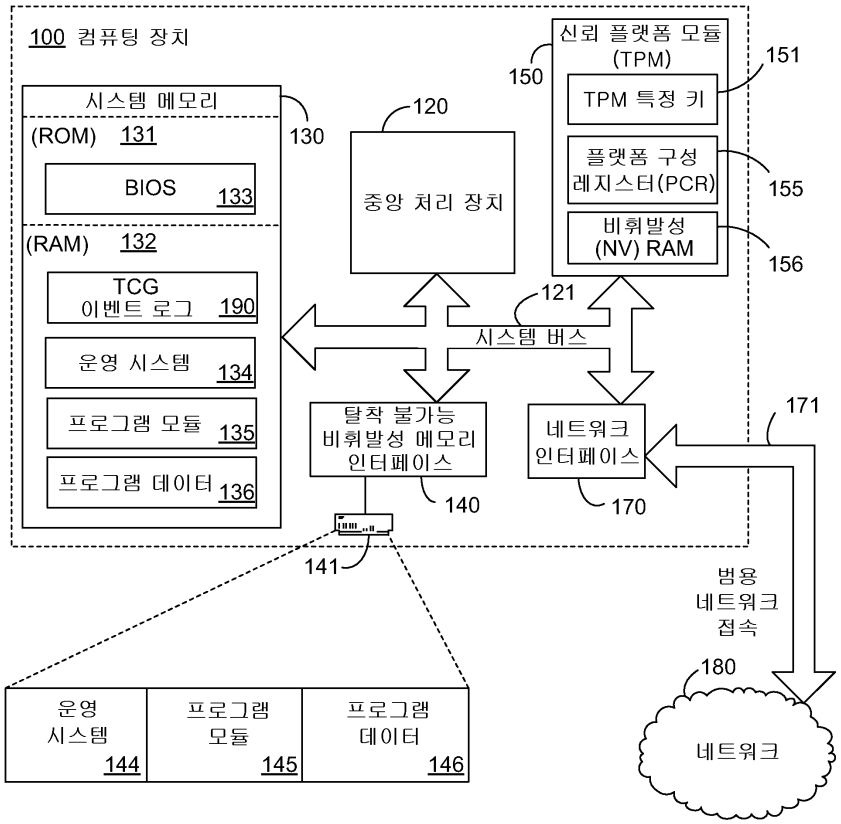
[0056] 그러므로 단계(635)에서, TPM은 하나 이상의 PCR의 현재의 값을 키의 공개를 위해 지정된 값에 대해 검사할 수 있다. 단계(635)에서 관련 PCR 값이 키의 공개를 위해 지정된 값과 동일하다면, 프로세스는 단계(640)로 진행될 수 있고 TPM에 의해 키가 요청하는 프로세스로 제공된다. 그러면 단계(645)에서 요청 프로세스는 단계(615) 및 단계(620)에서 생성되었던 암호화된 휴지 상태 화상을 잠금 해제하고, 활성 컴퓨팅 상태를 복구하기 위해 키를 활용한다. 다음에 관련 프로세스는 단계(660)에서 종료될 수 있다.

[0057] 그러나 단계(635)에서 관련 PCR 값이 키의 공개를 위해 지정된 값과 동일하지 않다면, 프로세스는 단계(650)로 진행될 수 있고 여기에서 TPM은 요청 프로세스에 키를 제공하는 것을 거부할 수 있다. 이러한 경우에 암호화된 휴지 상태 화상은 복호화될 수 없으므로, 컴퓨팅 장치는 활성 프로세싱을 재개할 수 없을 것이고, 단계(655)에서 전체 재시동 또는 운전 중지를 실행하고, 후속 시점에서 부팅 프로세스를 실행한다. 그러므로 예를 들면, 컴퓨팅 장치가 휴지 상태에 잇는 동안에 악의적이거나 미확인된 컴퓨터 실행 가능 명령어 또는 컴퓨팅 장치에 대한 다른 변경이 활성 프로세싱의 재개 시에 실행되도록 비밀리에 삽입되었거나 설정되는 경우 등과 같이 컴퓨팅 장치의 상태가 크게 변경되었다면, 단계(650) 등에서와 같이 TPM은 그 키의 제공을 거부할 수 있고, 단계(655)에서 전체 재시동 또는 재부팅의 실행은 컴퓨팅 장치가 휴지 상태였던 동안에 컴퓨팅 장치에 대해 비밀리에 실행된 임의의 변경을 소거 또는 무효화할 수 있다. 다음에 관련 프로세스는 단계(660)에서 종료될 수 있다.

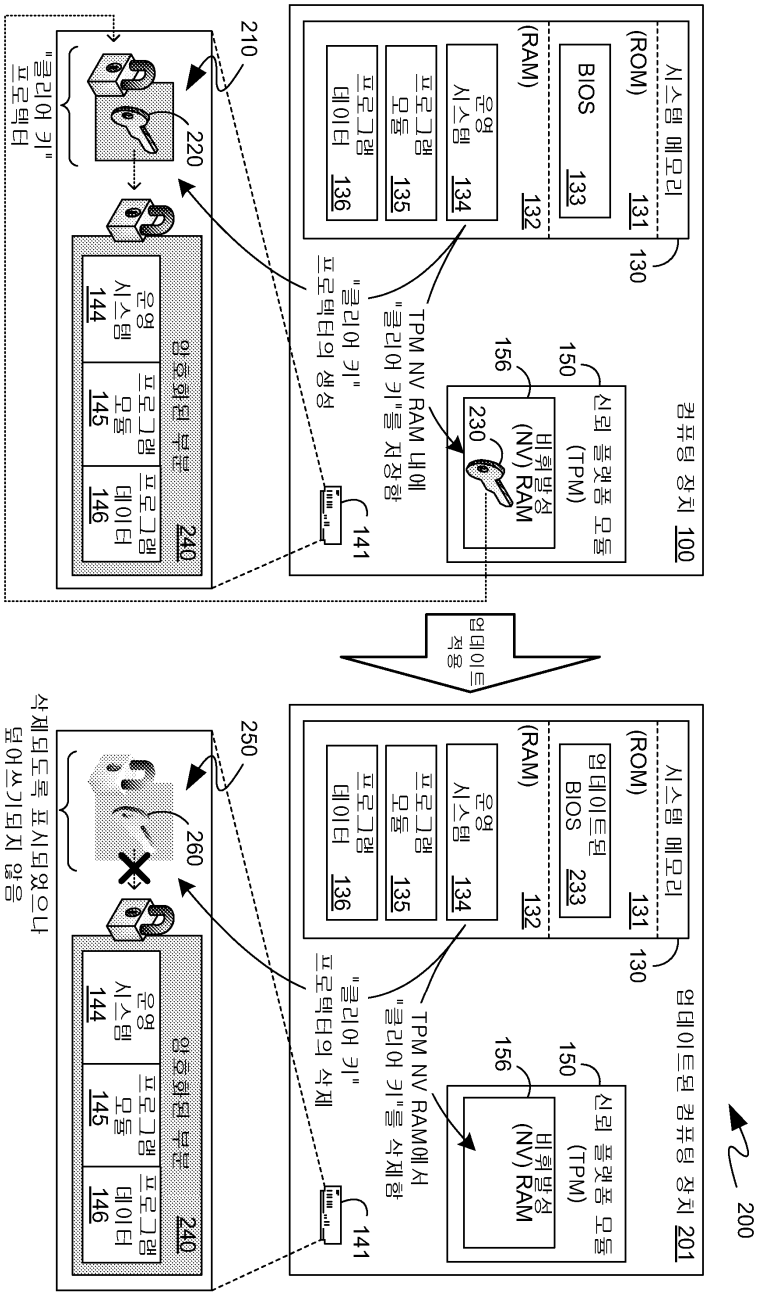
[0058] 상술된 내용으로부터 확인되는 바와 같이, TPM의 저장 능력을 활용함으로써 중요 정보를 보안된 방식으로 저장하고 복원 불가능하게 소거하는 메커니즘에 관해 개시하였다. 본 명세서에 설명된 청구 대상의 많은 가능한 변형을 고려할 때, 본 발명은 이러한 모든 실시예가 이하의 청구항 및 그 등가물의 범주에 속하는 것으로 주장하고자 한다.

도면

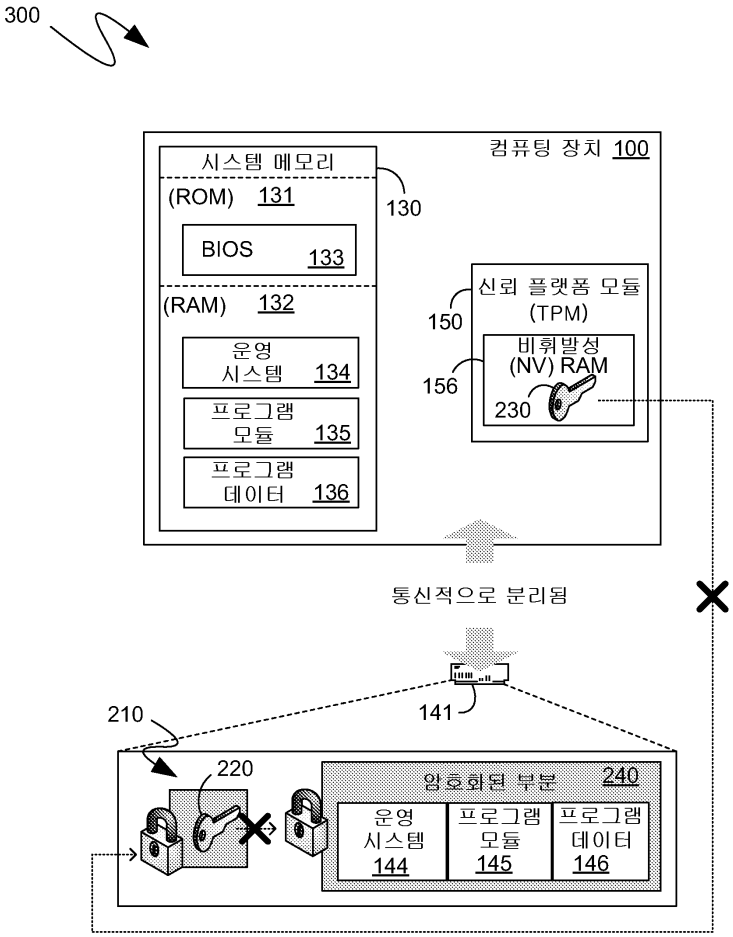
도면1



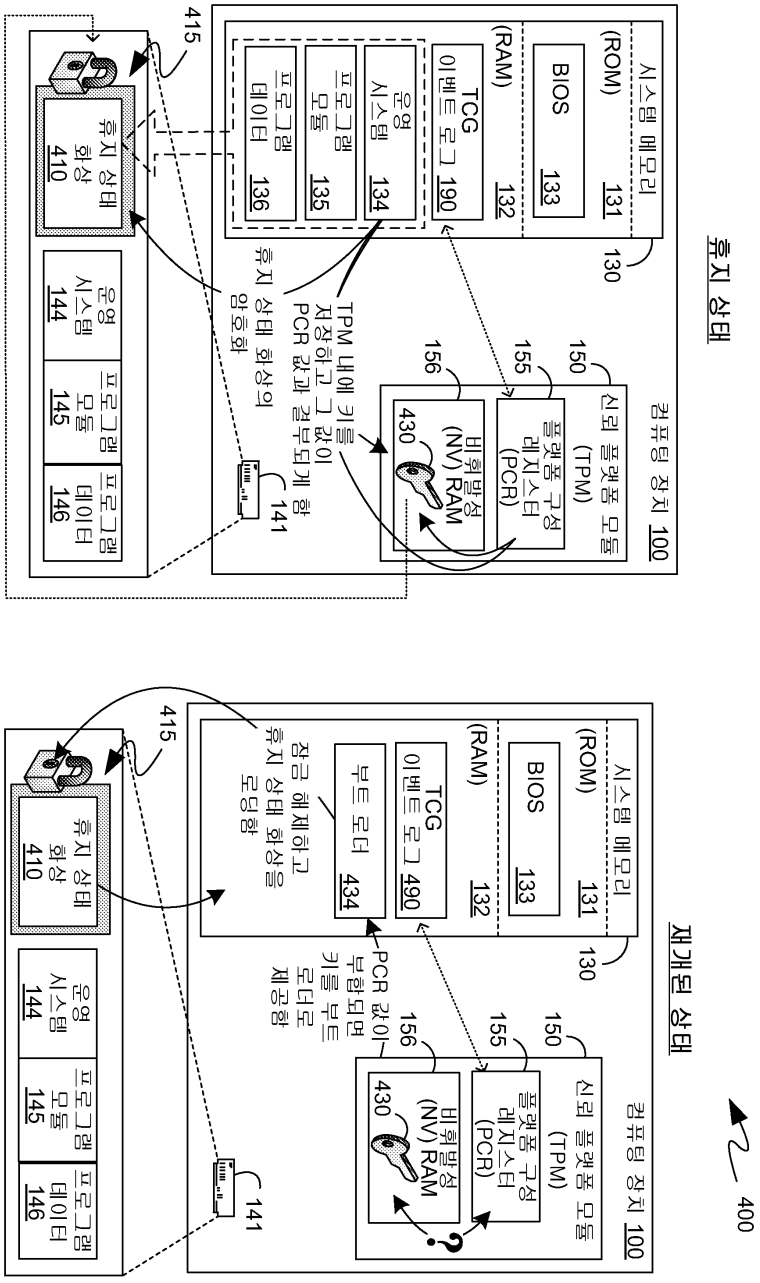
도면2


컴퓨팅 장치 100
시스템 메모리 131
(ROM) 131
BIOS 133
(RAM) 132
운영 시스템 134
프로그램 모듈 135
프로그램 데이터 136
130
신뢰 플랫폼 모듈 (TPM) 150
비휘발성 (NV) RAM 156
230
TPM NV RAM 내에 "클리어 키"를 저장함
"클리어 키" 프로텍터의 생성
141
210
220
"클리어 키" 프로텍터
암호화된 부분 240
운영 시스템 144
프로그램 모듈 145
프로그램 데이터 146
업데이트 적용
업데이트된 컴퓨팅 장치 201
업데이트된 BIOS 233
TPM NV RAM에서 "클리어 키"를 삭제함
"클리어 키" 프로텍터의 삭제
250
260
삭제되도록 표시되었으나 덮어쓰기되지 않음
200

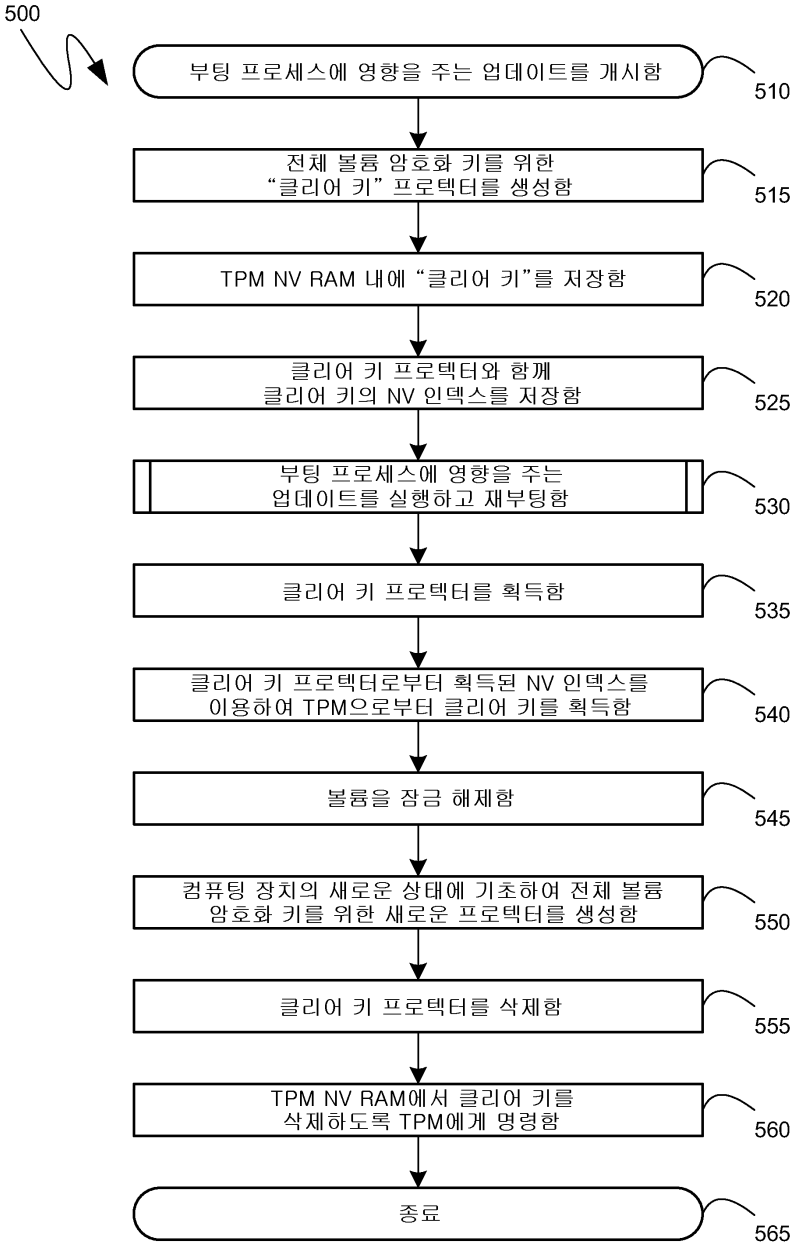
도면3


300
컴퓨팅 장치 100
시스템 메모리
(ROM) 131
130
BIOS 133
(RAM) 132
운영 시스템 134
프로그램 모듈 135
프로그램 데이터 136
신뢰 플랫폼 모듈 (TPM)
150
비휘발성 (NV) RAM
156
230
통신적으로 분리됨
141
210
220
암호화된 부분 240
운영 시스템 144
프로그램 모듈 145
프로그램 데이터 146

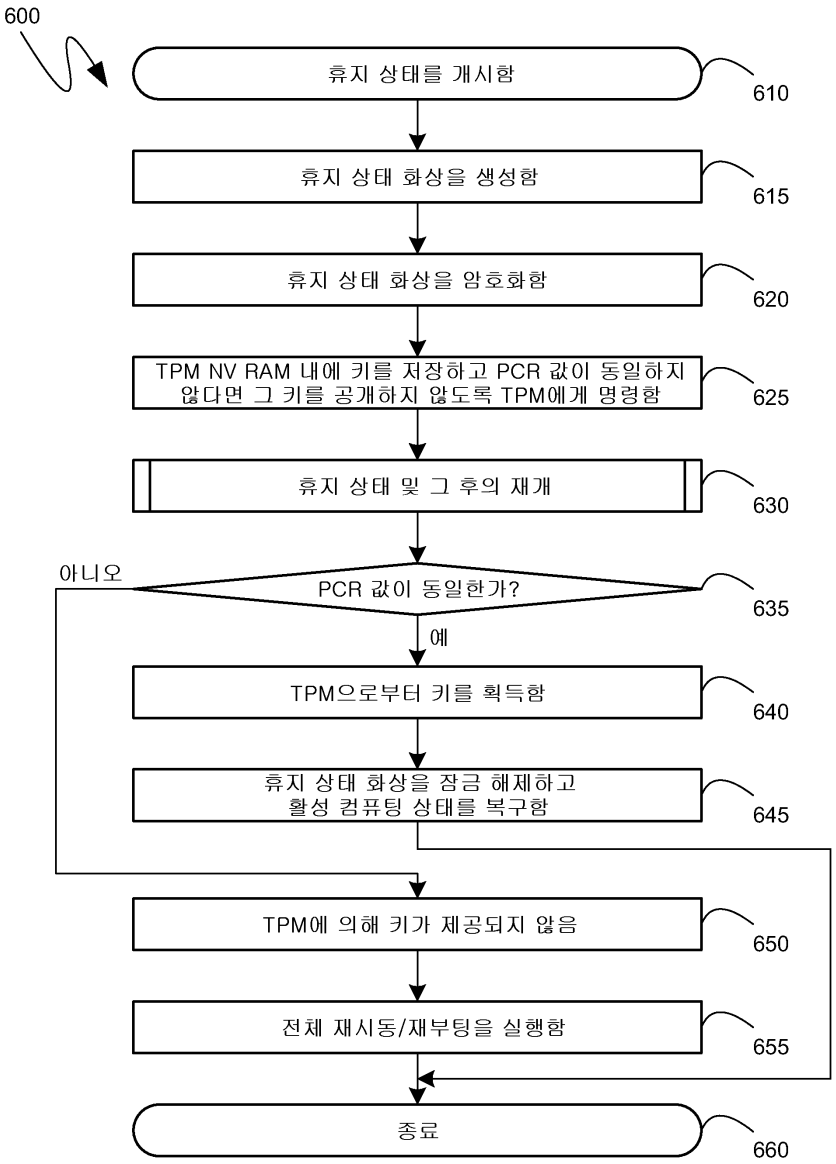
도면4


휴지 상태
시스템 메모리 (ROM) 131
BIOS 133
(RAM) 132
운영 시스템 134
프로그램 모듈 135
프로그램 데이터 136
TCG 이벤트 로그 190
130
신뢰 플랫폼 모듈 (TPM)
플랫폼 구성 레지스터 (PCR) 155
비휘발성 (NV) RAM 430 156
150
컴퓨팅 장치 100
TPM 내에 키를 저장하고 그 값이 PCR 값과 같부되게 함
휴지 상태 화상의 암호화
141
415
휴지 상태 화상 410
운영 시스템 144
프로그램 모듈 145
프로그램 데이터 146
재개된 상태
시스템 메모리 (ROM) 131
BIOS 133
(RAM) 132
TCG 이벤트 로그 490
부트 로더 434
잠금 해제하고 휴지 상태 화상을 로딩함
130
신뢰 플랫폼 모듈 (TPM)
플랫폼 구성 레지스터 (PCR) 155
비휘발성 (NV) RAM 430 156
150
컴퓨팅 장치 100
PCR 값이 부합되면 키를 부트 로더로 제공함
141
415
휴지 상태 화상 410
운영 시스템 144
프로그램 모듈 145
프로그램 데이터 146
400

도면5


500
부팅 프로세스에 영향을 주는 업데이트를 개시함
510
전체 볼륨 암호화 키를 위한
“클리어 키” 프로텍터를 생성함
515
TPM NV RAM 내에 “클리어 키”를 저장함
520
클리어 키 프로텍터와 함께
클리어 키의 NV 인덱스를 저장함
525
부팅 프로세스에 영향을 주는
업데이트를 실행하고 재부팅함
530
클리어 키 프로텍터를 획득함
535
클리어 키 프로텍터로부터 획득된 NV 인덱스를
이용하여 TPM으로부터 클리어 키를 획득함
540
볼륨을 잠금 해제함
545
컴퓨팅 장치의 새로운 상태에 기초하여 전체 볼륨
암호화 키를 위한 새로운 프로텍터를 생성함
550
클리어 키 프로텍터를 삭제함
555
TPM NV RAM에서 클리어 키를
삭제하도록 TPM에게 명령함
560
종료
565

도면6


600
휴지 상태를 개시함
610
휴지 상태 화상을 생성함
615
휴지 상태 화상을 암호화함
620
TPM NV RAM 내에 키를 저장하고 PCR 값이 동일하지 않다면 그 키를 공개하지 않도록 TPM에게 명령함
625
휴지 상태 및 그 후의 재개
630
아니오
PCR 값이 동일한가?
635
예
TPM으로부터 키를 획득함
640
휴지 상태 화상을 잠금 해제하고 활성 컴퓨팅 상태를 복구함
645
TPM에 의해 키가 제공되지 않음
650
전체 재시동/재부팅을 실행함
655
종료
660