(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0051181
(43) 공개일자 2011년05월17일

(51) Int. Cl.
G06F 21/20 (2006.01) *G06F 21/24* (2006.01)
(21) 출원번호 10-2011-7000361
(22) 출원일자(국제출원일자) 2008년07월07일
심사청구일자 없음
(85) 번역문제출일자 2011년01월06일
(86) 국제출원번호 PCT/US2008/069334
(87) 국제공개번호 WO 2010/005425
국제공개일자 2010년01월14일

(71) 출원인
휴렛-팩커드 디벨롭먼트 컴퍼니, 엘.피.
미국 텍사스주 77070 휴스턴 콤파크 센터 드라이브 웨스트 11445
(72) 발명자
왕 란
미국 텍사스주 77070 휴스턴 톰볼 파크웨이 20555
알리 발리우딘 와이
미국 텍사스주 77070 휴스턴 톰볼 파크웨이 20555
(뒷면에 계속)
(74) 대리인
제일광장특허법인

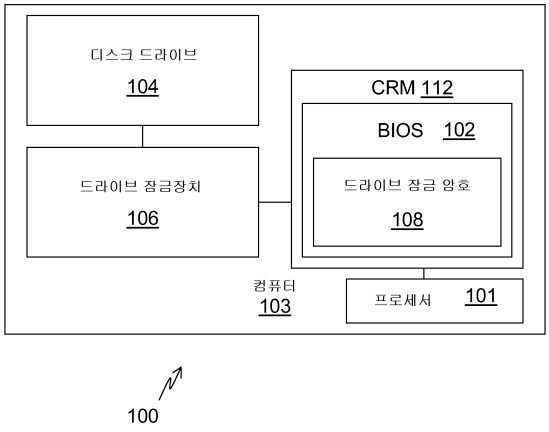
전체 청구항 수 : 총 15 항

(54) 데이터 보안 시스템, 방법 및 컴퓨터 판독가능 매체

(57) 요 약

시스템은 기본 입력 출력 시스템("BIOS")과, 디스크 드라이브와, 디스크 드라이브에 대한 인증되지 않은 액세스를 방지하도록 구성된 보안 시스템을 포함한다. 복수의 사용자 중 적어도 2 명의 사용자의 각각에 대해, BIOS는 사용자의 토큰에 기초하여 사용자를 인증한다. BIOS는 또한 인증에 기초하여 보안된 데이터에 액세스하고, 사용자로부터의 입력 없이 보안 시스템에 보안된 데이터를 제공한다.

대 표 도 - 도1a



(72) 발명자

노보아 마누엘

미국 텍사스주 77070 휴스턴 콤파크 센터 드라이브 웨스트 11445

리오스 제니퍼 이

미국 텍사스주 77070 휴스턴 톰볼 파크웨이 20555

특허청구의 범위

청구항 1

기본 입력 출력 시스템("BIOS";bios-input-output-system)과,

디스크 드라이브와,

상기 디스크 드라이브에 대한 인증되지 않은 액세스를 방지하도록 구성된 보안 시스템을 포함하되,

복수의 사용자 중 적어도 2 명의 사용자의 각각에 대해, 상기 BIOS는,

복수의 토큰 중 하나의 토큰에 기초하여 사용자를 인증하고 -상기 적어도 2 명의 사용자의 각각은 상기 복수의 토큰 중 서로 다른 토큰과 연관됨- ,

상기 인증에 기초하여 보안된 데이터에 액세스하며,

상기 사용자로부터의 입력 없이 상기 보안 시스템에 상기 보안된 데이터를 제공하는

시스템.

청구항 2

제 1 항에 있어서,

상기 보안 시스템은 드라이브 잠금 시스템(drive-lock system)이고,

상기 보안된 데이터는 드라이브 잠금 암호(drive-lock password)인

시스템.

청구항 3

제 1 항에 있어서,

상기 토큰은 암호, 스마트 카드 및 지문으로 이루어진 그룹으로부터 선택되는

시스템.

청구항 4

제 1 항에 있어서,

상기 보안된 데이터는 신뢰 플랫폼 모듈("TPM";Trusted Platform Module)에 의해 암호화되는

시스템.

청구항 5

제 1 항에 있어서,

상기 인증은 사용자가 BIOS 암호, 파워 온(power-on) 암호, 드라이브 잠금 암호 및 운영 시스템 암호로 이루어진 그룹으로부터 선택된 암호를 제공하지 못하게 하는

시스템.

청구항 6

제 1 항에 있어서,

상기 인증은 상기 사용자가 BIOS 암호, 파워 온 암호, 드라이브 잠금 암호 및 운영 시스템 암호를 제공하지 못하게 하는

시스템.

청구항 7

제 1 항에 있어서,

상기 사용자를 인증하는 것, 상기 보안된 데이터에 액세스하는 것 및 상기 보안된 데이터를 제공하는 것은 파워 온 셀프 테스트("POST";power-on self-test) 동안에 발생하는

시스템.

청구항 8

제 1 항에 있어서,

상기 보안된 데이터에 액세스하는 것은 상기 토큰의 해시에 기초하여 상기 보안된 데이터를 복호화하는 것을 더 포함하는

시스템.

청구항 9

제 1 항에 있어서,

상기 BIOS는 상기 복수의 토큰에 기초하여 상기 드라이브 잠금 암호를 생성하는

시스템.

청구항 10

제 1 항에 있어서,

상기 보안 시스템은 상기 보안된 데이터에 기초하여 상기 디스크 드라이브에 대한 액세스를 허용하는

시스템.

청구항 11

복수의 토큰 중 하나의 토큰에 기초하여 복수의 사용자 중 적어도 2 명의 사용자의 각각을(동시 아님) 인증하는 단계 -상기 적어도 2 명의 사용자의 각각은 상기 복수의 토큰 중 서로 다른 토큰과 연관됨- 와,

상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 인증에 기초하여 보안된 데이터에 액세스하는 단계와,

상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 사용자로부터의 입력 없이 보안 시스템에 상기 보안된 데이터를 제공하는 단계를 포함하는

방법.

청구항 12

제 11 항에 있어서,

상기 보안된 데이터를 제공하는 단계는 상기 사용자로부터의 입력 없이 드라이브 잠금 시스템에 드라이브 잠금 암호를 제공하는 단계를 포함하는

방법.

청구항 13

제 11 항에 있어서,

상기 보안된 데이터에 액세스하는 단계는 상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 인증에 기초하여 상기 보안된 데이터에 액세스하는 단계를 포함하되,

상기 보안된 데이터는 신뢰 플랫폼 모듈("TPM")에 의해 암호화되는

방법.

청구항 14

소프트웨어를 저장하는 컴퓨터 판독가능 매체에 있어서,

상기 소프트웨어는, 프로세서에 의해 실행되는 경우에, 상기 프로세서가,

복수의 토큰 중 하나의 토큰에 기초하여 복수의 사용자 중 적어도 2 명의 사용자의 각각을(동시 아님) 인증하게 하고 -상기 적어도 2 명의 사용자의 각각은 상기 복수의 토큰 중 서로 다른 토큰과 연관됨- ,

상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 인증에 기초하여 보안된 데이터에 액세스하게 하며,

상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 사용자로부터의 입력 없이 보안 시스템에 상기 보안된 데이터를 제공하게 하는

컴퓨터 판독가능 매체.

청구항 15

제 14 항에 있어서,

상기 보안된 데이터에 액세스하는 것은 상기 적어도 2 명의 사용자의 각각에 대해(동시 아님) 상기 인증에 기초하여 상기 보안된 데이터에 액세스하는 것을 포함하되,

상기 보안된 데이터는 신뢰 플랫폼 모듈("TPM")에 의해 암호화되는

컴퓨터 판독가능 매체.

명 세 서

배 경 기 술

[0001] 다수의 컴퓨터는 특히 상업적 설정에서 다수의 사용자를 갖는다. 그러나, 컴퓨터에 대한 다수의 보안 시스템은 단일 사용자용으로만 설계되었다. 예컨대, 보안을 강화하기 위해 사용자가 유효 암호를 제시하지 않으면 컴퓨터는 디스크 드라이브가 작동하지 못하게 할 것이다. 그러한 암호는 "드라이브 잠금 암호"로 지칭된다. 다수

의 사용자 사이에서 동일한 드라이브 잠금 암호를 공유하는 것은 보안의 강도를 감소시키지만, 다수의 드라이브 잠금 암호의 사용은 하드 드라이브에 의해 지원되지 않는다.

[0002] 문제점을 증가시키는 것으로서, 사용자에게 기본 입력 출력 시스템("BIOS") 암호, 파워 온 암호, 드라이브 잠금 암호, 운영 시스템 암호 등의 증가하는 암호의 수를 기억하도록 요구된다. 이와 같이, 사용자는 기억가능한 암호를 선택하거나, 각각의 목적마다 동일한 암호를 선택하거나, 양자 모두를 선택하려는 경향이 있다. 이 경향은 보안의 강도를 더욱 약화시킨다.

발명의 내용

과제의 해결 수단

[0003] 본 발명의 실시예의 상세한 설명에 있어서, 이제 첨부 도면을 참조할 것이다.

도면의 간단한 설명

[0004] 도 1a는 본 발명의 적어도 하나의 실시예에 따른 데이터 보안 시스템을 도시한다.

도 1b는 본 발명의 적어도 하나의 실시예에 따른 TPM을 사용하는 데이터 보안 시스템을 도시한다.

도 2는 본 발명의 적어도 하나의 실시예에 따른 데이터 보안 방법을 도시한다.

발명을 실시하기 위한 구체적인 내용

[0005] 표기법 및 명명법

[0006] 후속하는 특허청구범위 및 설명 전체에서 특정 시스템 구성요소를 지칭하는 데 특정 용어가 사용된다. 당업자가 알고 있듯이, 컴퓨터 회사는 구성요소를 상이한 이름에 의해 지칭할 수 있다. 이 문서는 이름은 상이하지만 기능은 상이하지 않은 구성요소를 구별하도록 의도하지 않는다. 후속하는 설명 및 특허청구범위에서, "포함하는"이라는 용어는 제한을 두지 않는 방식으로 사용되므로, "포함하지만, ...로 제한되지 않음"을 의미하도록 의도된다. 또한, "연결하다"라는 용어는 간접적이거나 직접적인 전기적 또는 광학적 접속을 의미하도록 의도된다. 따라서, 제 1 장치가 제 2 장치에 연결되면, 그 접속은 다른 장치 및 접속부를 통한 간접적인 전기적 접속, 직접적인 광학적 접속 등을 통해서일 수 있다.

[0007] "토큰"이라는 용어는 "고유한 식별자"를 의미하도록 의도된다. 그러므로, 토큰은 번호, 스트링, 암호, 사용자 이름과 암호의 조합, 스마트 카드, 스마트 카드와 핀 번호의 조합, 지문, 지문의 조합 등을 포함할 수 있지만, 이들로 제한되지 않는다.

[0008] "보안 시스템"이라는 용어는 "액세스를 제한하는 방식"을 의미하도록 의도된다. 설명을 위해, 보안 시스템은 디스크 드라이브에 대한 액세스를 제한하는 것에 관하여 설명된다. 이와 같이, 보안 시스템은 드라이브 잠금장치이다. 그러나, 액세스가 제한될 수 있는 임의의 및 모든 대상은 본 발명의 범위 내에 있다.

[0009] 후속하는 논의는 본 발명의 다양한 실시예에 관한 것이다. 하나 이상의 실시예가 선호될 수 있지만, 개시된 실시예는 이와 다르게 지정되지 않는 한, 특허청구범위를 포함하는 본 발명의 범위를 제한하는 것으로서 해석되거나 사용되어서는 안 된다. 또한, 당업자는 후속 설명이 광범위한 응용을 가짐을 알 것이며, 임의의 실시예의 논의는 예시적인 실시예만을 의미하고, 특허청구범위를 포함하는 본 발명의 범위가 그 실시예로 제한됨을 암시하도록 의도되지 않는다.

[0010] 앞서 개설된 장애를 고려하여, 데이터 보안에 대한 시스템 및 방법이 개시된다. 도 1a는 적어도 하나의 실시예에 따라 데이터 보안의 시스템(100)을 도시한다. 시스템(100)은 컴퓨터(103)를 포함하고, 컴퓨터(103)는 컴퓨터 판독가능 매체(112)에 연결된 프로세서(101)를 포함한다. 다양한 실시예에서, 컴퓨터 판독가능 매체(112)는 휘발성 메모리(예컨대, RAM 등), 비휘발성 메모리(예컨대, ROM, 플래시 메모리, CD ROM 등) 및 이들의 조합을 포함한다. 컴퓨터 판독가능 매체(112)는 프로세서(101)에 의해 실행되는 소프트웨어 또는 펌웨어를 포함한다. 본 명세서에 설명된 동작 중 하나 이상은 소프트웨어 또는 펌웨어의 실행 동안에 프로세서(101)에 의해 수행된다.

[0011] 바람직하게, 컴퓨터 판독가능 매체(112)는 기본 입력 출력 시스템("BIOS")(102)을 포함한다. 그러나, 소프트웨어 또는 펌웨어의 임의의 유형은 본 발명의 범위 내에 있다. 바람직하게, 컴퓨터(103)는 또한 디스크 드라이브(104) 및 디스크 드라이브(104)에 대한 인증되지 않은 액세스를 방지하도록 구성된 보안 시스템을 포함한다. 도시된 바와 같이, 보안 시스템은 드라이브 잠금장치(106)이다. 디스크 드라이브(104)는 데이터를 저장하는 하드웨어인 것이 바람직하다. 적어도 하나의 실시예에서, 디스크 드라이브(104)는 자기 표면 상에 디지털 인코딩된 데이터를 저장하는 비휘발성 저장 장치이다. BIOS(102)는 컴퓨터(103)가 파워 온될 때 활성화되는 펌웨어인 것이 바람직하다. 적어도 하나의 실시예에서, BIOS(102)는 구성요소 하드웨어, 예컨대, 디스크 드라이브(104)를 식별하고 개시하며, 컴퓨터(103)가 운영 시스템에 의해 제어되도록 준비한다.

[0012] 도시된 바와 같이, 보안 시스템은 디스크 드라이브(104)에 대한 인증되지 않은 액세스를 방지하는 드라이브 잠금장치(106)이다. 그러나, 임의의 대상에 대한 액세스를 제한하는 임의의 방식은 본 발명의 범위 내에 있다. 드라이브 잠금장치(106)는 하드웨어, 소프트웨어 또는 펌웨어일 수 있다. 적어도 하나의 실시예에서, 드라이브 잠금장치(106)는 적당한 데이터가 제공될 때에만 디스크 드라이브에 대한 액세스를 허용하는데, 도시된 바와 같이, 데이터는 BIOS(102)에 저장된 드라이브 잠금 암호(108)이다. 예컨대, 드라이브 잠금장치(106)는 디스크 드라이브(104) 내의 디스크가 스피닝(spinning)하지 못하게 하므로, 드라이브 잠금 암호(108)가 제공될 때까지, 판독되거나 기록되지 못하게 한다. 바람직하게, 디스크 드라이브(104) 상의 데이터의 민감한 특성 때문에, 인증되지 않은 사용자에 의한 액세스로부터 드라이브 잠금 암호(108)를 보호하기 위해 보안 방책이 취해진다.

[0013] 보안은 토큰 사용에 의해 강화될 수 있다. 토큰은 번호, 스트링, 암호, 사용자 이름과 암호의 조합, 스마트 카드, 스마트 카드와 핀 번호의 조합, 지문, 지문의 조합 등과 같은 고유한 식별자인 것이 바람직하다. 각각의 사용자는 상이한 토큰을 갖는다. 지문에 사용되는 사람 손가락의 경우에, 데이터의 페이로드는 물리적 토큰과 연관된다. 스마트 카드의 경우에, 데이터의 페이로드는 스마트 카드 그 자체로부터 판독된다. 암호의 경우에, 데이터의 페이로드는 암호 그 자체이거나 정확한 암호를 제시함으로써 릴리스된다. 적어도 하나의 실시예에서, 데이터의 페이로드는 드라이브 잠금 암호(108)에 액세스하는 데 필요한 키를 복호화하는 데 사용된다. 이와 같이, 드라이브 잠금 암호(108)는 각각의 사용자마다 한번 씩, 다수 회 별도로 암호화된다. 컴퓨터 관리자가 컴퓨터(103)를 사용할 사용자를 등록할 때, 토큰이 선택되고 데이터의 페이로드가 알려진다. 만일 사용자가 등록되는 첫 번째 사용자이면, 즉, BIOS(102)에 의해 처음으로 인증되면, BIOS(102)는 드라이브 잠금 암호(108)를 생성한다. 바람직하게, BIOS(102)는 알고 있듯이, 사용자가 드라이브 잠금 암호(108)를 기억할 필요가 없으므로, 강력 암호, 예컨대, 길고 랜덤한 암호를 생성한다.

[0014] 이어서 토큰의 해시가 생성되며, 특히 데이터의 페이로드의 해시가 생성된다. 해시는 해시 함수의 출력이다. 해시 함수는 입력으로서 임의의 길이의 스트링에 대해 출력으로서 고정된 길이의 스트링을 생성하는 "단방향" 변환이다. "단방향"이라는 용어는 주어진 세트의 입력에 대해, 출력이 매우 고유하고(어떤 다른 입력의 조합도 동일한 출력을 초래하지 않음), 출력이 주어지면, 입력이 유도가능해서는 안 된다. 여기서, 해시 함수에 대한 입력은 데이터의 페이로드이다. 해시 함수의 2 가지 예는 "MD5" 및 "SHA" 해시 함수이다. MD5 또는 메시지 다이제스트 알고리즘 5, 해시 함수는 전형적으로 16 진수의 32 문자열로 표현되는 128 비트 해시를 출력한다. SHA, 또는 안전 해시 함수, 해시 함수는 5 개의 변이를 갖는다. 각각의 변이는 원하는 보안의 강도에 따라 상이한 크기의 해시를 출력한다. 그러나, 임의의 해시 함수는 본 발명의 범위 내에 있다.

[0015] 바람직하게, 해시 함수의 출력은 드라이브 잠금 암호를 암호화하도록 암호화 키로서 사용하는 데 적합하다. 암호화의 2 가지 예는 "AES" 및 "트리플 DES"이다. AES 또는 고급 암호 표준, 암호화 알고리즘은 128 비트의 블록 및 128, 192 또는 256 비트의 키를 사용하는 블록 암호이다. 트리플 DES 또는 트리플 데이터 암호화 표준은 168 비트의 키를 사용하는 블록 암호이다. 그러나, 임의의 암호화 유형은 본 발명의 범위 내에 있다. 바람직하게, BIOS(102)는 토큰의 해시를 사용하여 유도된 시크릿(secret) 또는 암호화 키로서 토큰의 해시를 사용하여 드라이브 잠금 암호(108)를 암호화하도록 대칭 암호화를 사용한다. 추가적인 데이터를 키에 추가하고 키를 추측하려는 시도를 보다 어렵게 만드는 솔팅(salting)으로 지칭되는 기술을 사용하여 추가적인 보안도 가능하다. 대칭 암호화의 특성은 복호화 키가 암호화 키와 동일하거나 이와 평범하게 관련된다는 것이다. 이와 같이, 암호화 또는 복호화 키를 아는 것은 드라이브 잠금 암호를 알게 할 것이다. 설명을 위해, 암호화 및 복호화 키는 동일한 것으로 간주할 것이다.

[0016] 따라서, 키의 생성 후에, 적어도 하나의 실시예에서, 키는 불명료해지고 암호화된 드라이브 잠금 암호(108)와 함께 BIOS(102)에 저장된다. 불명료화는 키를 판독 또는 획득하기 어렵게 하고, 불명료화의 임의의 방법은 본 발명의 범위 내에 있다. 이와 같이, 만일 사용자가 디스크 드라이브(104)에 액세스하기를 원하면, BIOS(102)는 사용자의 토큰을 요청하고 그 토큰을 알려져 있거나 저장된 데이터 및/또는 값과 비교하고/비교하거나 상관시켜

서 사용자를 인증한다. 성공적인 인증 후에, 예컨대, 데이터의 페이로드는 데이터베이스 내의 엔트리와 일치하고, BIOS는 불명료화 프로세스를 반전시킴으로써 키를 명료하게 하고, 드라이브 잠금 암호(108)를 복호화하는데 키를 사용한다. 마지막으로, 드라이브 잠금장치(106)는 드라이브 잠금 암호(108)를 제공받고, 디스크 드라이브(104)는 액세스 가능하다.

[0017] 다른 실시예에서, 키가 삭제되는 동안에 암호화된 드라이브 잠금 암호(108)만이 저장된다. 등록 후에, 만일 사용자가 디스크 드라이브(104)에 액세스하기를 원하면, BIOS(102)는 사용자의 토큰을 요청하는 것이 바람직하다. 이어서 BIOS는 토큰의 해시를 계산하는데, 특히 데이터의 페이로드의 해시가 생성된다. 그 다음에 BIOS(102)는 드라이브 잠금 암호(108)를 복호화하도록 해시를 키로서 사용함으로써 사용자를 인증한다. 키가 토큰으로부터 유도되므로, 적당한 토큰 없이는 드라이브 잠금 암호(108)가 사용자에게 액세스 가능하지 않을 것이다. 일단 복호화되면, 디스크 드라이브(104)에 대한 액세스가능성을 얻기 위해 드라이브 잠금장치(106)에 드라이브 잠금 암호(108)가 제공된다. 이와 같이, 키 및 복호화된 드라이브 잠금 암호(108)가 컴퓨터(103) 상의 어디에도 저장되지 않고 일시적으로만 이용가능하므로 보안은 더 강화된다.

[0018] 다른 실시예에서, 암호화되거나 소거 상태에 있는 키는 그 자체가 결코 저장되지 않지만, 추가적인 보호 방안(예컨대, 스마트 카드, USB 디스크, 암호 토큰 등)을 가진 외부 토큰 또는 플랫폼에 저장된다. 이와 같이, 사용자가 키를 복호화하도록 "시크릿을 아는 것"을 필요로 할 뿐만 아니라 소거 또는 암호화된 키를 보유하는 매체(토큰)를 소유해야 하므로 보안이 강화된다. 특히, 특정 지식의 소유뿐만 아니라 특정 항목의 소유를 필요로 하는 것은 전자만을 또는 후자만을 필요로 하는 것에 비해 보안을 강화시킨다.

[0019] 제 2 사용자가 등록되게 하도록, 컴퓨터 관리자인 것이 바람직한 제 1 사용자는 제 1 사용자의 토큰으로부터 생성된 키를 사용하여 드라이브 잠금 암호(108)를 복호화한다. 그 다음에, BIOS(102)는 제 2 사용자의 토큰에 기초하여 제 2 키를 사용하여 드라이브 잠금 암호(108)를 암호화한다. 이와 같이, 임의의 수의 사용자는 동일한 드라이브 잠금 암호(108)를 사용하지만 상이한 토큰을 이용하는 컴퓨터(103)를 사용할 수 있다.

[0020] 보안을 강화하기 위해, 암호화된 드라이브 잠금 암호(108) 및/또는 키는 BIOS(102)에 저장되기 전에 압축될 수 있다. 보안을 더 강화하기 위해, BIOS(102)에 저장되기 전에 랜덤하거나 특히 알려져 있는 비트가 암호화된 드라이브 잠금 암호(108) 및/또는 키에 삽입될 수 있다. 이들 추가적인 랜덤하거나 특히 알려져 있는 비트는 때때로 "솔트(salt)"로 지칭된다.

[0021] 바람직하게, 드라이브 잠금 암호(108)는 사용자로부터의 입력 없이 드라이브 잠금장치(106)에 제공된다. 이와 같이, 사용자는 사용자의 토큰을 제공한 후에 디스크 드라이브(104)를 액세스 가능하게 하도록 어떠한 액션도 취할 필요가 없다. 바람직하게, 사용자를 인증하는 것, 보안된 데이터에 액세스하는 것 및 보안된 데이터를 드라이브 잠금장치(106)에 제공하는 것은 컴퓨터 동작의 파워 온 셀프 테스트("POST") 단계 동안에 발생한다. 이와 같이, 사용자는 운영 시스템에 액세스할 수 있기 전에 BIOS 암호, 파워 온 암호, 드라이브 잠금 암호, 운영 시스템 암호 또는 임의의 다른 기능을 위한 임의의 다른 토큰을 공급하도록 요구되지 않을 것이다. 그러나, 만일 원한다면, 단 하나 또는 특정 조합의 토큰이 제거될 수 있다.

[0022] 만일 드라이브 잠금 암호(108)가 전술한 바와 같이 사용자의 토큰에 기초하여 각각의 사용자마다 암호화되면, 몇몇 측면에서 보안이 강화된다. 첫째로, 사용자가 드라이브 잠금 암호(108)를 기억할 필요가 없으므로 BIOS(102)에 의해 강력 드라이브 잠금 암호(108)가 생성될 수 있다. 둘째로, 단 하나의 드라이브 잠금 암호만 존재하더라도, 다수의 사용자를 수용하는 컴퓨터의 경우에, 다수의 사용자는 그들의 토큰이 공통 드라이브 잠금 암호일 것이므로 서로 그들의 토큰을 공유할 필요도 통신할 필요도 없다. 세번째로, 다수의 사용자는 드라이브 잠금 암호(108)의 존재를 알 필요가 없다. 네번째로, 적어도 하나의 실시예에서, BIOS(102)가 암호화된 키를 저장하므로, 컴퓨터(103)로부터 도난된 디스크 드라이브(104)는 다른 컴퓨터에 의해 액세스될 수 없다.

[0023] 도 1b는 본 발명의 적어도 하나의 실시예에 따른 TPM을 사용하는 데이터 보안 시스템을 도시한다. TPM(110)은 암호법에 전용인 신뢰 컴퓨팅 그룹에 의해 설계된 마이크로프로세서이다. TPM(110)은 의사 난수 발생기를 사용하여 암호 키를 생성한다. 적어도 하나의 실시예에서, 드라이브 잠금 암호(108)는 추가 보안을 위해 그러한 키를 사용하여 TPM(110)에 의해 요청된 바와 같이 암호화되고 복호화된다. 키는 불투명 BLOB(binary large object)와 같은, TPM(110)에 의해 생성되고 해석가능한 정보를 포함한다.

[0024] 바람직하게, 키는 대칭이고 TPM(110)의 키와 레지스터 사이에서 "배타적 논리합" 함수("XOR")를 실행함으로써 BIOS(102)에 저장되기 전에 보호된다. 도시된 바와 같이, 레지스터는 플랫폼 구성 레지스터 7("PCR7")(114)이다. 보호를 제거하기 위해, 보호된 키는 제 2 XOR 함수의 출력이 원시 키가 되도록 PCR7 내의 값과 함께 다른

XOR 함수의 입력으로서 사용될 수 있다. 바람직하게, 보안을 강화하기 위해 운영 시스템이 PCR7에 액세스하기 전에 BIOS(102)는 PCR7(114)에 배치된 값이 변경되게 할 것이다.

[0025] 적어도 하나의 실시예에서, 드라이브 잠금 암호(108)는 구성 시간에 PCR7을 가진 TPM(110)에 봉인된다(sealed). 봉인 동작의 시간에 PCR7 값은 사용자 인증의 성공을 나타내는 값을 반영해야 한다. 등록 후에, 만일 사용자가 디스크 드라이브(104)에 액세스하기를 원하면, BIOS(102)는 사용자의 토큰을 요청하는 것이 바람직하다. 만일 사용자 인증이 성공적이면, BIOS(102)는 PCR7(114)로 하나의 값을 확장한다. 만일 사용자 인증이 성공하지 못하면, BIOS(102)는 PCR7(114)로 상이한 값을 확장한다. 그 다음에, BIOS(102)는 TPM(110)이 드라이브 잠금 암호(108)를 봉인해제하도록 요청한다. PCR7(114)이 인증이 성공적이었음을 나타내는 값을 갖는 경우에만, TPM(110)이 드라이브 잠금 암호(108)를 봉인해제하고 릴리스할 것이다. 일단 TPM(110)에 의해 봉인해제되면, 드라이브 잠금 암호(108)는 디스크 드라이브(104)에 대한 액세스가능성을 허용하도록 드라이브 잠금장치(106)에 제공된다. 그 다음에, BIOS(102)는 TPM(110)이 드라이브 잠금 암호(108)에 액세스하기 위해 임의의 봉인해제 동작을 수행하지 못하도록 난수를 PCR7(114)로 확장한다. 따라서, BIOS(102)에서 드라이브 잠금 암호가 부트 프로세스에서 특정 단계에서만 액세스가능하므로 보안이 더 강화된다.

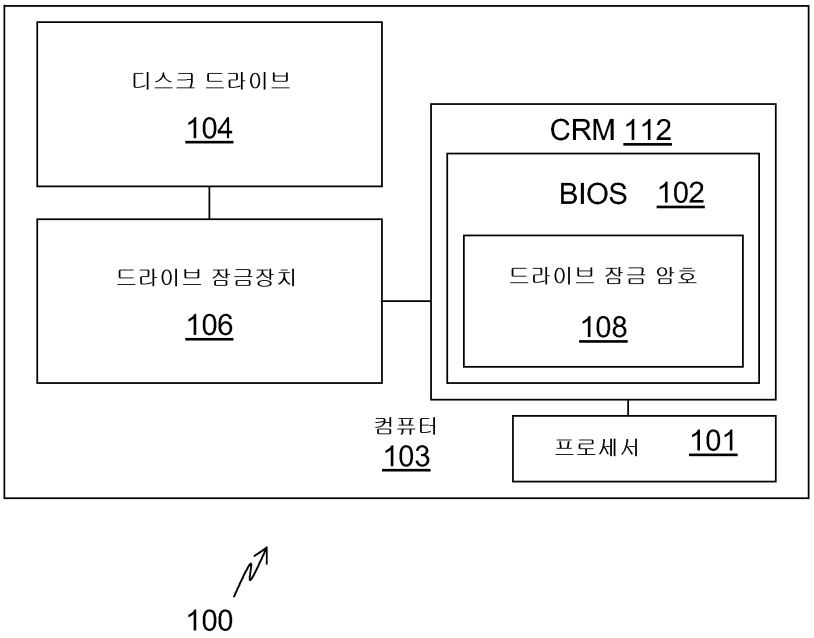
[0026] 도 2는 본 발명의 적어도 하나의 실시예에 따른 데이터 보안 방법(200)을 도시한다. 단계(202)에서 시작되고 단계(212)에서 종료되며, 방법은 사용자로부터 토큰을 수신하는 단계를 포함한다(단계 204). 각각의 사용자는 상이한 토큰을 갖는다. 단계(206)에서, 사용자는 사용자의 토큰에 기초하여 인증된다. 단계(208)에서, 보안된 데이터가 인증에 기초하여 액세스되고, 보안된 데이터는 각각의 인증된 사용자마다 액세스가능하다. 단계(210)에서, 보안된 데이터는 사용자로부터의 입력 없이 보안 시스템에 제공된다. 바람직하게, 보안된 데이터를 제공하는 것은 사용자로부터의 입력 없이 드라이브 잠금 시스템에 드라이브 잠금 암호를 제공하는 것을 포함한다. 또한, 보안된 데이터에 액세스하는 것은 적어도 하나의 실시예에서 인증에 기초하여 TPM에 의해 암호화된 보안된 데이터에 액세스하는 것을 포함한다. 바람직하게, 보안된 데이터는 복수의 사용자 중에서 각각의 인증된 사용자마다 액세스가능하다. 적어도 하나의 실시예에서, 보안된 데이터에 액세스하는 것은 토큰의 해시에 기초하여 보안된 데이터를 복호화하는 것을 더 포함한다.

[0027] 다양한 실시예에서, 마스터 드라이브 잠금 암호는 관리자의 운영 시스템 암호와 사용자의 운영 시스템 암호 사이의 관계와 유사한, 사용자 드라이브 잠금 암호보다 더 큰 범위의 함수에 대한 액세스를 허용한다. 그러나, 본 개시는 드라이브 잠금 암호의 유형과 컴퓨터(103)의 사용자 양자 모두 조합된 이용가능한 마스터 및 사용자 드라이브 잠금 암호보다 수가 더 많으므로, 설명을 위해 단일 드라이브 잠금 암호를 참조하였다. 추가적으로, 당업자는 사용자 잠금 암호뿐만 아니라 마스터 드라이브 잠금 암호도 수용하도록 본 개시의 교시를 구현할 수 있다.

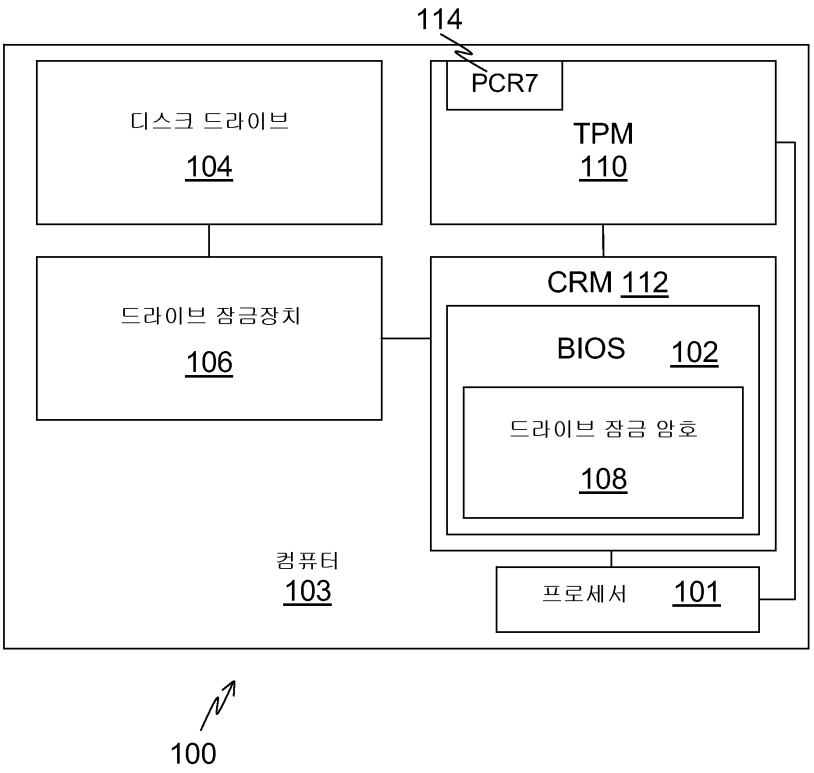
[0028] 이상의 논의는 본 발명의 원리 및 다양한 실시예를 예시하는 것으로 여겨진다. 일단 이상의 논의가 완전히 인식되면 다수의 변형 및 변경이 당업자에게 자명해질 것이다. 후속하는 특허청구범위가 그러한 모든 변형 및 변경을 포함하는 것으로 해석되도록 의도된다.

도면

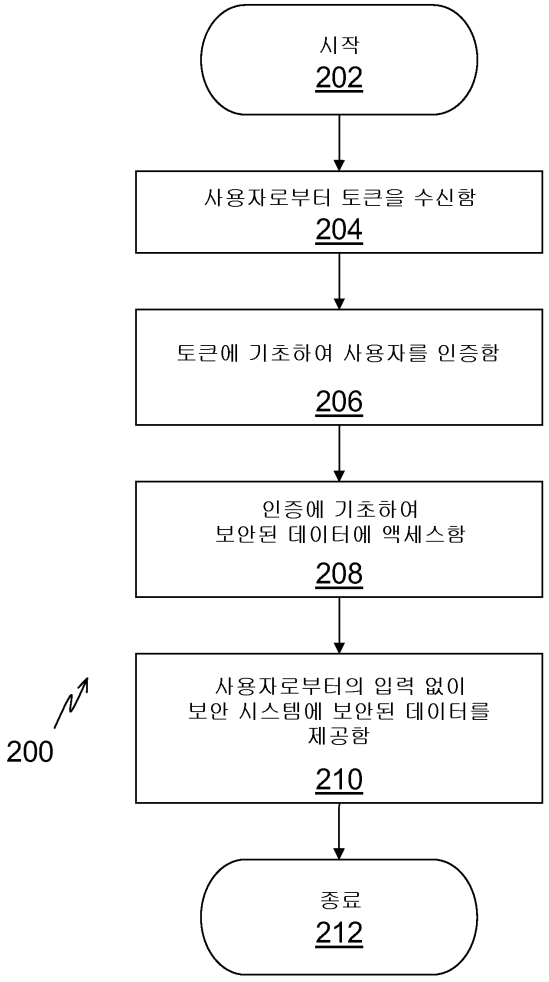
도면1a


디스크 드라이브
104
CRM 112
BIOS 102
드라이브 잠금장치
106
드라이브 잠금 암호
108
컴퓨터
103
프로세서 101
100

도면1b


114
PCR7
디스크 드라이브
104
TPM
110
CRM 112
드라이브 잠금장치
106
BIOS 102
드라이브 잠금 암호
108
컴퓨터
103
프로세서 101
100

도면2


시작
202
사용자로부터 토큰을 수신함
204
토큰에 기초하여 사용자를 인증함
206
인증에 기초하여
보안된 데이터에 액세스함
208
사용자로부터의 입력 없이
보안 시스템에 보안된 데이터를
제공함
210
종료
212
200