(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0071528
(43) 공개일자 2008년08월04일

(51) Int. Cl.
G06F 21/00 (2006.01)
(21) 출원번호 10-2008-0009832
(22) 출원일자 2008년01월30일
심사청구일자 없음
(30) 우선권주장
11/668,892 2007년01월30일 미국(US)

(71) 출원인
테크날러지 프라퍼티즈 리미티드
미국 캘리포니아 95014 쿠페르티노 피프쓰 플로어 스티븐즈 크리크 블러버드 20400
(72) 발명자
아이에르 스리 엠
미국 캘리포니아 95135 산호세 피노트 그리스 웨이 4167
안토노풀로스 니콜라스
미국 캘리포니아 95118 산호세 몬트모렌시 코트 4355
(74) 대리인
박장원

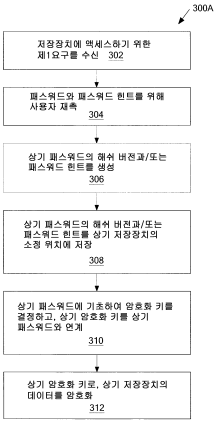
전체 청구항 수 : 총 39 항

(54) 저장 장치 데이터 암호화와 데이터 액세스를 위한 방법 및시스템

(57) 요 약

저장장치 데이터 암호화와 데이터 액세스를 위한 방법 및 시스템에 관해 아래, 기술한다. 본 발명의 일부 실시예들을 요약하여 기술하면 다음과 같다. 본 발명의 일 실시예에 따른 방법은 저장부에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 과정과, 상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 과정과, 소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터의 해독을 위해 상기 암호화 키를 액세스하는 과정을 포함한다. 여기서, 상기 저장부에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화되는 것을 특징으로 한다. 일 실시예에서, 상기 요구를 수신하는 과정은 파워-업, 타임아웃의 완료, 그리고 상기 시스템의 재시작 중 적어도 어느 하나에 대응하여 초기화되는 세션의 제1요구를 수신하는 과정을 포함하는 것을 특징으로 한다.

대표도 - 도3a



특허청구의 범위

청구항 1

저장부에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 과정과;

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 과정과;

소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터를 풀기 위해 암호화 키에 액세스하는 과정으로 이루어지며,

여기서, 상기 저장부에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화되는 것을 특징으로 하는 방법.

청구항 2

제1항에 있어서, 상기 저장부는

디스크 드라이브인 것을 특징으로 하는 방법.

청구항 3

제1항에 있어서, 상기 저장부는

시스템 주변의 저장부인 것을 특징으로 하는 방법.

청구항 4

제3항에 있어서, 상기 과정들은

상기 시스템과 저장부 사이에 연결된 인터셉터에 의해 수행되고, 상기 인터셉터는 적어도 하나의 컨트롤러와 메모리를 포함하는 것을 특징으로 하는 방법.

청구항 5

제4항에 있어서, 상기 암호화 키는

상기 인터셉터, 시스템, 그리고 저장부 중의 하나로부터 액세스되는 것을 특징으로 하는 방법.

청구항 6

제5항에 있어서,

상기 저장부의 숨겨진 위치에서 상기 암호화 키를 찾아내는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 7

제1항 내지 제6항의 어느 한 항에 있어서,

파워-업, 타임 아웃의 완료, 그리고 상기 시스템의 재시작 중 적어도 어느 하나에 대응하여, 상기 요구를 제안하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 8

제1항 내지 제7항의 어느 한 항에 있어서, 상기 암호화 키에 액세스 하는 과정은

상기 암호화 키를 해독하기 위해 제2의 암호화 키에 액세스하는 과정을 포함하는 것을 특징으로 하는 방법.

청구항 9

제1항 내지 제8항의 어느 한 항에 있어서,

상기 암호화 키를 이용하는 상기 요구된 데이터를 해독하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 10

제9항에 있어서,

상기 복호화된 데이터를 상기 저장부의 제1저장위치로부터 적어도 제2저장위치 이동시키는 과정과;

상기 암호화 키로서 상기 데이터를 재 암호화하는 과정을 포함하는 것을 특징으로 하는 방법.

청구항 11

제10항에 있어서,

상기 암호화된 데이터를 다시 상기 제1저장 위치로 이동시키는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 12

제1항 내지 제11항의 어느 한 항에 있어서,

상기 소정 패스워드에 매칭되지 않는 상기 적어도 하나의 패스워드 입력에 대응하여,

상기 저장장치의 위치를 확인하기 위해, 기 확인된 수신측으로 상기 시스템과 관련된 네트워크 주소를 송신하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 13

제12항에 있어서, 상기 수신측은

기 확인된 웹 사이트인 것을 특징으로 하는 방법.

청구항 14

저장부에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 과정과;

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 과정과;

소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터를 풀기 위해 암호화 키에 액세스하는 과정으로 이루어지며,

여기서, 상기 저장부에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화되는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 15

제14항에 있어서, 상기 저장부는

시스템 주변의 저장부인 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 16

제15항에 있어서, 상기 과정들은

상기 시스템과 저장부 사이에 연결된 인터셉터에 의해 수행되고, 상기 인터셉터는 적어도 하나 이상의 컨트롤러와 메모리를 포함하는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 17

제16항에 있어서, 상기 암호화 키는

상기 인터셉터, 시스템, 그리고 저장부 중의 하나로부터 액세스되는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 18

제17항에 있어서, 상기 암호화 키는

상기 저장부로부터 액세스 될 때, 숨겨진 트랙들에 저장되는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 19

제17항에 있어서, 상기 요구를 수신하는 과정은

파워-업, 타임아웃의 완료, 그리고 상기 시스템의 재시작 중 적어도 어느 하나에 대응하여 초기화되는 세션의 제1요구를 수신하는 과정을 포함하는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행 방법.

청구항 20

제14항에 있어서, 상기 소정 패스워드에 매칭되는 상기 적어도 하나의 대표 패스워드에 대응하여,

데이터를 상기 저장부의 제1저장위치로부터 적어도 제2저장위치 이동시키는 과정과;

상기 암호화 키로서 상기 데이터를 암호화하는 과정을 포함하는 것을 특징으로 하는 명령들의 집합을 저장한 독출 가능 기기 매체의 수행방법.

청구항 21

제1항 내지 제13항 중의 어느 한 항의 방법을 실행하는 것을 특징으로 하는 시스템의 컴퓨터 프로그램.

청구항 22

저장부에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 수단과;

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 수단과;

소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터를 풀기 위해 암호화 키에 액세스하는 수단을 포함하여 구성되며,

여기서, 상기 저장부에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화되는 것을 특징으로 하는 시스템.

청구항 23

호스트 시스템과 적어도 하나의 암호화 키를 이용하여 데이터를 암호화하는 저장부 사이에 연결되며, 적어도 프로세서와 메모리를 포함하는 인터셉터 장치에 있어서,

상기 저장부에 저장된 데이터로 액세스할 것에 관한 요구를 상기 호스트 시스템으로부터 수신하고,

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받고,

소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터를 풀기 위해 상기 암호화 키에 액세스하는 것을 특징으로 하는 인터셉터 장치.

청구항 24

제23항에 있어서, 상기 장치는

상기 호스트 시스템, 상기 저장부, 그리고 상기 장치 중의 어느 하나로부터 상기 암호화 키를 액세스하는 것을 특징으로 하는 인터셉터 장치.

청구항 25

제24항에 있어서, 상기 장치는

상기 저장부의 숨겨진 위치로부터 상기 암호화 키를 액세스하는 것을 특징으로 하는 인터셉터 장치.

청구항 26

제23항 내지 제25항의 어느 한 항에 있어서, 상기 장치는

상기 암호화 키에 액세스하기 위해 상기 암호화 키의 암호화된 버전을 복호화하는 것을 특징으로 하는 인터셉터 장치.

청구항 27

제26항에 있어서, 상기 장치는

상기 액세스된 암호화 키를 이용하는 상기 요구된 데이터를 복호화하는 것을 특징으로 하는 인터셉터 장치.

청구항 28

제27항에 있어서, 상기 장치는

상기 호스트 시스템에 상기 복호화된 데이터를 제공하는 것을 특징으로 하는 인터셉터 장치.

청구항 29

저장부에 액세스하기 위한 요구를 수신하는 과정과;

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 과정과;

상기 패스워드 입력에 대응하여 암호화 키를 생성하는 과정과;

상기 암호화 키를 상기 패스워드와 연계하는 과정과;

상기 암호화 키로서 데이터를 암호화하는 과정과;

상기 암호화된 데이터를 상기 저장부에 저장하는 과정으로 이루어진 것을 특징으로 하는 방법.

청구항 30

제29항에 있어서,

상기 패스워드의 마스크 버전을 생성하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 31

제30항에 있어서,

상기 저장부의 소정 위치에, 상기 패스워드의 마스크 버전을 저장하는 것을 특징으로 하는 방법.

청구항 32

제29항 내지 제31항의 어느 한 항에 있어서,

상기 패스워드로부터 상기 암호화 키를 생성하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 33

제29항 내지 제31항의 어느 한 항에 있어서,

상기 암호화 키의 마스크 버전을 생성하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 34

제29항 내지 제33항의 어느 한 항에 있어서,

상기 암호화 키나 상기 암호화 키의 마스크 버전을 저장하는 과정을 더 포함하는 것을 특징으로 하는 방법.

청구항 35

제29항에 있어서,

암호화된 데이터를 선택하는 과정과;

상기 데이터가 소스 위치에 있을 때 상기 데이터를 목적 위치로 이동시키는 과정과;

상기 암호화 키를 사용하는 상기 목적 위치에 있는 데이터를 암호화하는 과정으로 이루어진 것을 특징으로 하는 방법.

청구항 36

저장부에 액세스하기 위한 요구를 수신하는 수단과;

상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 수단과;

상기 패스워드 입력에 대응하여 암호화 키를 생성하는 수단과;

상기 암호화 키를 상기 패스워드와 연계하는 수단과;

상기 암호화 키로서 데이터를 암호화하는 수단과;

상기 암호화된 데이터를 상기 저장부에 저장하는 수단으로 이루어진 것을 특징으로 하는 방법.

청구항 37

적절한 시스템에서 구동될 때 제29항 내지 제35항 중 어느 한 항의 방법을 실행하는 컴퓨터 프로그램.

청구항 38

제37항의 컴퓨터 프로그램을 운반하는 캐리어.

청구항 39

제38항에 있어서, 상기 캐리어는 독출 가능 기기 매체인 것을 특징으로 하는 캐리어.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 저장 장치 데이터 암호화와 데이터 액세스를 위한 방법 및 시스템에 관한 것이다.

배 경 기 술

<2> 개인적 일이나 비즈니스 업무를 처리하는데 있어서, 휴대용 전자장치에 대한 신뢰성이 증대되면서,

<3> 전통적으로 물리적인 형태로 수행되던 문서와 미디어는 전자적 수단을 경유한 전송과 액세스를 위해 디지털화되고 있다. 휴대용 전자장치(예: 플레쉬 메모리 장치, 랩탑, 노트북, PDA, 모바일 폰, 그리고/혹은 블랙베리 등)는 테스크 관리를 용이하게 하기 위해, 대체로 멀티미디어와 문서 액세스 소프트웨어와 함께 장착된다.

<4> 이러한 상기 휴대용 전자장치의 저장장치들은 사진, 비디오 파일, 오디오 파일, 금융정보, 영수증 의료기록, 보험정보, 비즈니스 관련 문서(예: 사업계획, 재무 대차대조표, 법률 서류) 등과 같은 대용량의 파일이나 문서들을 저장할 수 있다. 또한, 임시 인터넷 파일과 쿠키(cookies)는 금융문서나(또는) 의료기록과 같은 신용정보에 접근할 수 있는 사용자 정보(예: 웹 사이트의 패스워드 등)를 저장할 수 있다.

<5> 개인의 프라이버시와 비밀은 전자장치의 인증되지 않은 접근에 의해 위태로워질 수 있기 때문에, 휴대용 전자장치의 사용이 증가함에 따라 저장장치에 저장된 데이터의 보안은 필수적인 것이 되었다.

<6> 반면, 패스워드(예: 운영시스템 로그온 패스워드, 바이오스 (BIOS) 패드워드 등)는 인증되지 않은 사용자가 호스트 장치(예: 랩탑 컴퓨터)에 로그온 하는 것을 막기 때문에 장치의 제거에 따라 저장장치의 컨텐츠는 호스트 시스템으로부터 손상될 수 있다.

<7> 예를 들어, 데이터 해커가 상기 저장장치를 물리적으로 제거하고, 데이터 해커의 접근을 인증하는 다른 호스트 장치로 옮겨 놓을 수 있다.

<8> 그러므로, 비록 호스트 장치의 운영 시스템이 활성화되지 않아도, 저장장치의 데이터 보호에 사용되도록 저장장치의 데이터를 암호화하는 보안 기술이 필요하다. 예를 들어, 상기 호스트 시스템이 상기 저장장치의 데이터에 액세스할 수 있게 데이터가 상기 저장장치로부터 직접 읽혀진다면, 상기 액세스 요구는 상기 저장장치 데이터의 복호화 이전에 인정된다.

발명의 내용

해결 하고자하는 과제

<9> 본 발명은 저장장치 데이터 암호화와 데이터 액세스를 위한 방법 및 시스템을 제공하는 데 그 목적이 있다.

과제 해결수단

<10> 본 발명의 일 실시예에 따른 방법은 저장부에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 과정과, 상기 요구에 대응하여, 사용자로부터 패스워드의 입력받는 과정과, 소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터의 해독을 위해 상기 암호화 키를 액세스하는 과정을 포함한다. 여기서, 상기 저장부에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화되는 것을 특징으로 한다. 일 실시예에서, 상기 요구를 수신하는 과정은 파워-업, 타임아웃의 완료, 그리고 상기 시스템의 재시작 중 적어도 어느 하나에 대응하여 초기화되는 세션의 제1요구를 수신하는 과정을 포함하는 것을 특징으로 한다.

<11> 또한, 일 실시예에서, 상기 소정 패스워드에 매칭되지 않는 패스워드에 대응하여, 상기 저장장치의 위치를 확인하기 위해, 기 확인된 수신측으로 상기 시스템과 관련된 IP주소를 송신하는 과정을 포함하는 것을 특징으로 한다.

<12> 본 발명은 이러한 방법들을 수행하는 장치와 방법들을 포함하며, 이러한 방법들을 수행하는 처리 시스템과 컴퓨터 독출 매체를 포함한다.

<13> 본 발명의 부가적인 특성 및 이점들은 아래의 설명에 기재될 것이며, 부분적으로는 상기 설명에 의해 명백해지거나 본 발명의 실행을 통해 숙지 될 것이다. 본 발명의 목표 및 다른 이점들은 특히 아래 기재된 설명 및 부가된 도면뿐만 아니라 청구항에서 지적한 구조에 의해 구현될 것이다.

효 과

<14> 본 발명은 호스트 장치의 운영 시스템이 활성화되지 않는 경우에도 저장장치의 데이터 보호에 사용되도록 저장장치의 데이터를 암호화함으로써 데이터의 보안을 강화할 수 있다.

발명의 실시를 위한 구체적인 내용

<15> 다음의 설명과 도면들은 예시적인 것이고 한정적으로 해석되지 않아야 한다. 여러 특정 세부사항들은 개시된 기술 대한 완전한 이해를 돕기 위해 기술된 것이다. 그러나, 일 예로서, 잘 알려져 있거나 종래의 세부사항들은 설명의 모호함을 피하기 위해 기술되지 않을 것이다.

<16> 본 상세설명에 기술된 내용은 본 발명과 동일한 실시예일 수도 있고 적어도 하나의 참고 수단이 될 수는 있으나, 반드시 필수적인 사항은 아니다.

<17> '일 실시예' 혹은 '실시예'에 관한 본 명세서의 참조는 본 상세설명의 적어도 한 실시예에 포함되는 실시예와 관련하여 기술된 특징이나 구조, 특성을 의미하는 것이다.

<18> 본 명세서의 여러 곳에서 쓰이고 있는 문구 '일 실시예에서'의 외형이 동일한 실시예와 관련된 모든 것일 필요는 없다. 그리고 분리된 것이거나 다른 실시예와 상호 배타적인 양자 택일의 실시예일 필요도 없다. 또한, 다양한 특징들이 어떤 실시예에서는 공개되어 기술될 수 있고, 다른 실시예들에서는 공개되지 않을 수도 있다. 유사하게, 다양한 요구가 어떤 실시예에서는 요구될 수 있지만, 다른 실시예에서는 그렇지 않을 수도 있다.

<19> 본 발명의 실시예들은 저장장치 데이터 암호화와 데이터 액세스를 위한 방법 및 시스템을 포함한다.

<20> 하드웨어 모듈들을 경유한 저장장치의 데이터 암호화는 저장장치의 데이터 암호화를 통해, 프라이버시와 기밀성을 보증하는 보호방법을 제공한다. 디스크 드라이버와 같은 저장장치 상에 존재하는 데이터는 상기 디스크 드라이버 상에 저장된 데이터 암호화 처리를 통해 보호된다. 저장장치를 보호하라는 명령이 수신되면, 일 실시예에 따라 패스워드 설정 프로세스가 개시(initiated)된다.

<21> 상기 개시(initiatial) 설정 프로세스는, 상기 저장장치의 데이터에 액세스(예: 암호화, 해독, 삭제, 백업 등)할 수 있도록 하는 하나 혹은 그 이상의 패스워드를 사용자가 설정할 수 있도록 해 준다. 각기 다른 액세스 레벨들(예: 읽기/쓰기/삭제에 관한 특별 권한)이 일 실시예에 따라, 사용자들에게 각기 다르게 설정될 수 있다. 예를 들면, 상기 시스템 관리자(system administrator)는 상기 저장장치의 데이터를 암호화할 수 있는 권한과

해독할 수 있는 권한을 인증받을 수 있다. 상기 시스템 관리자는 또한, 다른 암호화 키를 가지고 재 암호화를 개시(initiate)할 수 있는 특별한 권한을 소유할 수 있다. 인증된 사용자는 암호화된 드라이브의 데이터를 읽을 수 있는(해독할 수 있는) 특별권한을 소유할 수 있다.

<22> 일단, 상기 개시(initiatial) 설정 프로세스가 완료되고 상기 미리 설정된(이하, '소정'이라 한다) 패스워드가 제공되면, 저장장치에 쓰여질 새로운 데이터는 본 발명의 일 실시예에 따라 상기 저장장치에 저장되기 전에, 암호화될 수 있다. 추가적으로, 만일, 사용자가 사용자 디스크 드라이브를 암호화하고자 하는 경우, 이미 상기 디스크 드라이브에 저장된 데이터는 제2의 저장위치(예: 동일 디스크 드라이브 상의 다른 저장위치, 다른 저장장치, 시스템 메모리, 메모리 장치 등)로 이동되고 암호화될 수 있다. 그런 다음, 상기 원래의 저장위치로 다시 이동시킬 수 있다.

<23> 본 발명의 일 실시예에 따르면, 보호된 저장장치의 데이터를 암호화하기 위한 액세스는 소정 패스워드와 매칭되는 패스워드를 제공함으로써 이루어질 수 있다. 상기 소정 패스워드를 제공함으로써, 상기 보호된 저장장치의 암호화 데이터에 사용되는 암호화 키는 상기 암호화된 데이터를 해독하여 액세스할 수 있다. 일 실시예에서, 상기 암호화 키 혹은 상기 암호화 키의 마스크 버전은 상기 저장장치의 소정 저장위치에 있는 상기 호스트 시스템의 하나 혹은 그 이상의 저장장치에 저장된다. 상기 저장장치의 소정 저장 위치는 상기 저장된 암호화 키로 액세스될 수 있는 것으로, 오퍼레이팅 시스템에 로그-온하기 전, 부팅(boot-up)시간 동안 접근 가능하다.

<24> 본 발명의 일 실시예에 따른 방법은, 저장장치에 저장된 데이터로 액세스할 것에 관한 요구를 수신하는 과정을 포함하고, 상기 저장장치에 저장된 데이터는 적어도 하나의 암호화 키를 사용하여 암호화된다.

<25> 저장장치로의 액세스를 위한 상기 요구는, 상기 저장장치에 인스톨 (installed)된 호스트 오퍼레이팅 시스템에 로그-온하기 전의 부팅시간(boot-up)동안 사용자에 의해 생성된 것이다. 상기 요구는 또한, 상기 저장장치의 두 번째 파티션(partition)에 인스톨된 제2의 오퍼레이팅 시스템을 구동하고자, 사용자에 의해 생성될 것이다. 특정 파일이나 폴더에 액세스하기 위한 시도들은 또한, 저장장치에 저장된 암호화된 데이터로의 액세스를 위해 생성되어야 하는 요구를 촉발시킬 것이다. 또한, 어떤 요구는, 상기 시스템이나 오퍼레이팅 시스템이 슬립모드(sleep mode), 파워 세이브 모드(power save mode), 혹은 타임아웃(time out) 상태에 존재할 때, 자동적으로 혹은 수동적으로 생성된다. 상기 요구는 일반적으로, 시스템이 다시 시작되거나 부팅(boot-up)되는 동안 자동적으로 생성될 것이다.

<26> 본 발명의 일 실시예에 따른 상기 호스트 시스템 상의 각 파일은 서로 다른 암호화 키를 갖는다. 각각의 폴더는 서로 다른 암호화 키를 갖는다. 다른 실시예에 따르면, 상기 저장장치에 놓인 모든 데이터는 하나의 암호화 키에 의해 암호화된다. 암호화 키들을 특정하는 파일, 암호화 키들을 특정하는 폴더, 그리고/혹은 암호화 키들을 특정하는 파티션의 조합은 상기 저장장치 상에서 구현되거나 호스트 시스템의 다수 저장장치들에서 구현될 수 있다. 파일들, 폴더들, 파티션들, 그리고/혹은 저장장치들에 대한 암호화 키의 할당은 사용자의 지정에 의해 혹은 자동적으로 이루어질 수 있다.

<27> 덧붙여, 데이터 암호화에 사용되는 상기 암호화 키는 사용자의 요구에 따라 혹은 자동적인 유발에 의해 바뀔 수 있다. 다른 암호화 키를 적용하기 전에, 상기 다른 암호화 키로 동일한 데이터를 암호화하기 전의 상기 오리지널 키로서 상기 암호화된 데이터는 복호화될 수 있다. 예를 들어, 상기 자동적 유발(trigger)은, 성공적 시도에 뒤따르는 여러 차례 실패한 로그-온 시도와 같이 이벤트에 기인하는 것일 수 있다. 상기 자동적 유발은 또한, 암호화 키가 소정 횟수 동안 사용되었을 때와 같이, 횟수에 기반한 것일 수 있다.

<28> 본 발명의 일 실시예에 따른 상기 방법은 상기 요구에 대응하여, 패스워드의 입력을 사용자에게 촉구(prompt)하는 과정과, 소정 패스워드에 매칭되는 적어도 하나의 패스워드 입력에 대응하여, 상기 요구된 데이터를 해독하기 위해 상기 암호화 키에 액세스하는 과정을 포함한다.

<29> 예를 들어, 호스트 시스템에 슬립모드 상태로 존재할 때, 사용자는 상기 호스트 시스템이 더 이용되기 전에 맞는 패스워드를 입력하도록 재촉(prompt)을 받을 수 있다. 상기 사용자로부터 제공된 패스워드는, 시스템 로그-온 전에 액세스 가능한 소정의 패스워드와 비교된다. 일 실시예에서, 상기 소정의 패스워드는 상기 저장장치의 소정 위치에 저장되고, 액세스 된다. 예를 들어, 상기 소정의 패스워드는 부팅 가능한 저장장치의 마스터 부트 레코드(master boot record)에 저장될 수 있다. 일 실시예에서, 하나의 저장 장치를 위한 상기 소정의 패스워드는 또 다른 저장 장치에 저장될 수 있다. 예를 들어, 다수의 저장장치를 갖는 시스템에서, 상기 슬레이브(slave) 저장장치들을 위한 상기 소정의 패스워드는 마스터(master) 저장장치에 저장될 수 있다.

<30> 본 발명의 일 실시예에 따르면, 옳바른 패스워드는 상기 저장장치의 데이터 암호화에 사용된 하나 혹은 여러 암

호화 키들의 액세스를 허용한다. 양자 택일로서, 하나의 패스워드가 상기 오퍼레이팅 시스템으로의 시스템 부팅을 돕는 반면, 부가적인 패스워드는, 일단, 사용자가 상기 시스템에 로그-인하면, 다른 파티션들, 파일들, 혹은 폴더들로의 액세스를 가능하게 한다. 일 실시예에서, 옳바른 패스워드는 상기 요구된 데이터를 해독하는 암호화 키와 연계된다.

<31> 양자 택일로서, 상기 옳바른 패스워드는 상기 암호화 키의 마스크(masked) 버전(예: 암호화 버전)과 연계되고, 상기 옳바른 패스워드는 상기 암호화 키의 마스크 버전을 언 마스크(un-mask)하는데 사용될 것이다. 일 실시예에서, 상기 옳바른 패스워드는 상기 암호화 키의 마스크 버전을 언마스크하기 위한 추가적인 키를 구별하는데 사용된다. 또한, 암호화 키의 전송이 어떤 방해를 받아, 암호화 키의 기밀성을 손상시키는 것을 방지하기 위해, 상기 암호화 키는 마스크 형태(예: 암호화된, 마스크된, 개인/공용 키 롤링 교환(private/public key rolling exchange) 등)로 장치로부터 장치로 전송된다.

<32> 상기 저장장치에 저장된 상기 요구된 데이터는 어떠한 적절한 암호화 알고리즘에 의해 암호화될 수 있다. 예를 들어, 사용 가능한 암호화 알고리즘들은 RSA, 데이터 암호화 표준(DES/3DES), Blowfish, 인터내셔널 데이터 암호화 알고리즘(IDEA), 최적의 소프트웨어 암호화 알고리즘(SEAL), RC4, 어드밴스 암호화 표준(AES), 등과 같은 알고리즘들만을 포함하는 것으로 한정하지 않는다.

<33> 도 1은 본 발명의 일 실시예에 따른 저장장치102를 도시한 것으로, 상기 저장장치 102는, 모듈 104와 관련된 인터셉터(interceptor)를 통해, 호스트 시스템 106과 통신한다.

<34> 상기 저장장치 102는 하드 디스크 드라이브, 병렬포트를 갖는 하드 디스크 드라이브(PATA), 시리얼 포트를 갖는 하드 드라이브(SATA), 스카시(SCSI) 드라이브, 광(optical) 드라이브, 미그네틱 드라이브, 외부 저장장치, 플레쉬 장치와 같은 반도체 저장장치, 혹은 마그네틱-광(magnetic-optical) 저장장치 중 적어도 하나로서, 호스트 시스템 106의 주변에 연결된다. 상기 인터셉터 모듈 104는 도 9를 참조하여 기술되며, 제어기, 메모리, 프로세싱 유닛, 그리고 암호화를 목적으로 하는 소프트 웨어 모듈을 포함하게 될 것이다. 본 발명의 일 실시예에 따른 상기 인터셉터 모듈 104는 상기 저장장치 102와 호스트 시스템 106간에 연결된다.

<35> 상기 호스트 시스템 106은 저장장치 103를 지원하는 어떠한 타입의 시스템도 될 수 있다. 예를 들어, 상기 호스트 시스템은 데스크 탑 컴퓨터, 노트북, 랩탑 컴퓨터, 휴대용 컴퓨터, 모바일 폰, 스마트 폰, PDA 등의 어떠한 것에도 한정하지 않고 포함한다. 일 실시예에서, 상기 호스트 시스템 106과 인터셉터 모듈 104는 네트워크 108로 연결될 수 있다.

<36> 도 2는 본 발명의 일 실시예에 따라, 인터셉터 104를 경유하여 저장장치 102와 통신하는 호스트 시스템 106의 개략적인 구성의 일 예를 나타낸 것이다.

<37> 본 발명의 일 실시예에 따른 상기 호스트 시스템 106은 프로세싱 유닛 202, 칩셋 204, 메모리 206, 그리고 I/O 장치의 배열(키보드, 포인팅 장치, 사운드 시스템, 그리고/혹은 비디오 시스템 등을 포함)을 포함한다. 상기 도시된 호스트 시스템 106은 본 발명의 사상과 크게 다름없이, 본 시스템의 많은 변화와 수정을 이룰 수 있는 간략한 예시도이다. 예를 들어, 상기 메모리는 종래에 알려진 바와 같이, '북측' 브릿지에 위치할 수 있다. 상기 비디오 시스템은 그 자신을 북측 브릿지 액세스로 나눌 수 있다. 그리고 상기 I/O는 상기 '남측' 브릿지를 통해 연결될 수 있다.

<38> 본 발명의 일 실시예에 따른 상기 인터셉터 모듈 104는 상기 칩셋 204을 경유하여 상기 호스트 시스템 106과 연결된다. 상기 인터셉터 모듈 104과 저장장치 106은, 시리얼 ATA(SATA) 인터페이스, 병렬 ATA(PATA) 인터페이스, 파이어 와이어(FireWire), 스카시(SCSI), 혹은 유에스비(USB)와 같은 인터페이스 중의 하나에 의해 연결될 수 있다. 상기 저장장치 104와 인터페이스로 접속된 인터셉터 모듈 104는 다른 전송장치들의 스펙(Specification)에 의존하여 각기 다른 데이터 전송율을 지원한다. 예를 들어, 상기 SATA인터페이스는 1.5, 3, 그리고 6 Gbits/s의 데이터율을 지원한다. 상기 파이어 와이어 800과 파이어 와이어 400은 서로 각기 다른 데이터 전송율을 사용한다.

<39> 도 3A는 본 발명의 일 실시예에 따른, 저장장치 데이터 암호화와 데이터 액세스를 위한 패스워드 설정을 도시한 흐름도 300A이다.

<40> 프로세스 302에서, 저장장치에 액세스하기 위한 제1요구가 수신된다. 예를 들어, 사용자가 새로 구입한 랩탑(예: 호스트 시스템)에 로그-온을 시도할 때, 상기 사용자는 새로 구입한 랩탑의 상기 저장장치에 액세스하기 위한 제1요구를 생성한다. 또한, 사용자가 새로 인스톨된 미사용 저장장치를 사용하고자 할 때, 상기 저장장치에 액세스하기 위한 상기 제1요구는 사용자에 의해 생성된다. 일 실시예에서, 상기 사용된 저장장치에 접속하

기 위한 제1요구는 또한, 상기 사용자가 저장장치 데이터 암호화 능력을 가지고 있는 시스템에 인스톨된 저장 데이터를 갖는 저장장치의 데이터를 보호하고자 할 때, 생성된다.

<41> 프로세스 304에서, 상기 사용자는 하나 혹은 그 이상의 패스워드를 설정할 것을 재촉받는다. 그리고 도 5의 스크린 샷에 도시된 바와 같은 패스워드 힌트를 설정할 것을 재촉받는다. 일 실시예에서, 상기 하나 혹은 그 이상의 패스워드는, 호스트 시스템의 하나 혹은 그 이상의 저장장치들의 데이터를 암호화하기 위해, 하나 혹은 그 이상의 암호화 키들을 생성하는데 사용된다. 일 실시예에서, 하나 혹은 그 이상의 패스워드가 상기 요구에 대응하여 사용자에 의해 일단 설정되면, 상기 암호화 키는 미리 설정되고 상기 하나 혹은 그 이상의 패스워드와 연계된다. 또한, 상기 소정의 암호화 키는 상기 사용자에 의해 설정된 하나 혹은 그 이상의 패스워드들에 기초하여, 마스크(예: 암호화 혹은 해쉬(hashed))될 수 있다. 본 발명의 일 실시예에 따르면, 도 8의 스크린 샷의 예에서 나타난 바와 같이 상기 패스워드 힌트는 부정확한 패스워드로 인한 로그-온 시도의 실패에 의해 사용자에게 제공된다.

<42> 프로세스 306에서, 상기 패스워드의 해쉬 버전과 상기 패스워드 힌트가 생성된다. 상기 패드워드의 해쉬(혹은 마스크)버전과 상기 패스워드 힌트는 상기 패스워드와 패스워드 힌트를 보호하기 위해 생성될 수 있다. 예를 들어, 만일 데이터가 상기 저장장치로부터 직접 읽혀지면, 상기 패스워드는 위장된 형태로 나타날 것이다. 다양한 해싱 알고리즘들이 사용될 수 있다. 본 발명의 일 실시예에 따라, 암호화 알고리즘은 상기 패스워드를 마스크(mask)하는데 사용될 수 있다.

<43> 프로세스 308에서, 상기 패스워드의 해쉬(혹은 어떤 알고리즘에 의해 위장된)버전과(혹은) 패스워드 힌트는 상기 저장장치의 소정 위치에 저장된다. 본 발명의 일 실시예에 따르면, 상기 패스워드들의 해쉬 버전과(혹은) 패스워드 힌트들은, 상기 호스트의 오퍼레이팅 시스템에 액세스할 수 없는 저장장치의 섹터들에 저장된다. 그러므로, 암호화된 데이터의 액세스는, 옳바른 패스워드를 먼저 제공하지 않는 오퍼레이팅 시스템에 의해서는 통과될 수 없다. 일 실시예에서, 상기 패스워드의 해쉬 버전과(혹은) 패스워드 힌트는 동일한 호스트 시스템의 다른 저장장치에 저장된다. 예를 들어, 슬레이브(slave) 장치들에 대한 상기 패스워드들은 마스터(master) 장치에 저장될 수 있다.

<44> 프로세스 310에서, 상기 저장장치에 저장된 데이터를 암호화하는 암호화 키는 상기 패스워드에 기초하여 결정되고, 상기 암호화 키는 앞으로의 액세스를 위해 상기 패스워드와 연계된다. 일 실시예에서, 상기 암호화 키는 미리 설정된다. 그리고 보안의 추가적 계층을 생성하는 패스워드로서의 동작에 기초하여 한층 더 변형(예: 암호화 or 해쉬)될 수 있다. 예를 들어, 만일 상기 패스워드가 손상되었다면, 상기 특정 알고리즘은 해커(hacker)에게 알려지지 않았기 때문에 상기 암호화 키는 보안을 유지하게 된다.

<45> 동작 312에서, 상기 저장장치의 데이터는 상기 암호화 키에 의해 암호화된다. 예를 들어, 도 6의 스크린 샷의 예에 도시된 바와 같이, 보호되어야 하는 소스 드라이브는 윈도우 602에 도시된 '소스(Source) 드라이브'의 리스트 하에서 선택될 수 있다. 일 실시예에서, '목적(Destination) 드라이브'(예: 도 6의 윈도우 604에 도시된 '목적 드라이브'로부터)는 상기 소스 드라이브로부터 데이터를 이동시키기 위해 선택될 것이다. 상기 데이터는 상기 소스 드라이브로부터 이동될 수 있고 상기 목적 드라이브에서 암호화될 수 있다. 상기 암호화된 데이터는 상기 소스 드라이브로 되돌려지거나 상기 목적 드라이브에 저장된다. 일 실시예에서, 목적 드라이브는 선택될 필요가 없다. 예를 들어, 상기 소스 드라이브에서 암호화된 상기 데이터는 상기 소스 드라이브의 제2저장위치로 이동되고 암호화된다. 이와 비슷하게, 상기 암호화된 데이터는 상기 원래의 저장 위치로 되돌려지거나 상기 소스 드라이브의 제2저장 위치에 저장된다.

<46> 본 발명의 일 실시예에서, 만일, 상기 호스트 시스템이 상기 저장장치에 데이터를 쓰도록 하는 요구를 생성한다면, 상기 데이터는, 상기 저장장치로 이동되기 전, 상기 암호화 키에 의해 암호화된다. 또한, 상기 데이터는 암호화되기 이전에 상기 저장장치에 쓰여질 수 있고, 그런 다음 자동적 유발(automatic triggers) 혹은 수동적 유발(manual triggers)에 기초하여 나중에 암호화된다. 예를 들어, 소정의 시간 간격을 두고 쓰여진 데이터는 암호화된다. 이와 유사하게, 쓰여진 데이터의 소정 분량(예: 5Kb)이 동시에 암호화될 수 있다.

<47> 도 3B는 본 발명의 일 실시예에 따른, 저장장치 데이터 암호화와 데이터 액세스를 인증하는 프로세스를 도시한 흐름도 300B이다.

<48> 프로세스 322에서, 저장장치에 액세스하기 위한 요구가 수신된다. 예를 들어, 상기 요구에 의해, 세션(Session)의 초기화(initiation)가 수신될 수 있다. 상기 세션은 파워-업(power-up), 타임 아웃(time-out)의 완료, 혹은 시스템의 재시작(restart) 중에 적어도 하나에 대응하여 초기화(initiated)될 수 있다. 상기 세션은 또한,

슬립모드(sleep mode) 또는 파워 세이브 모드(power save mode)의 존재 이후에, 유발될 수 있다. 일 실시예에서, 상기 요구는, 상기 저장장치의 특정 파티션들, 폴더들, 혹은 파일들이 액세스되는 때에 생성된다. 더욱이, 어떤 요구는 또한, 상기 저장장치의 다른 파티션에 주재하는 어떤 다른 오퍼레이팅 시스템이 액세스될 때, 생성된다.

<49> 프로세스 324에서, 상기 사용자는 도 7의 스크린 샷에 도시된 패스워드에 대해 재촉 받는다. 상기 패스워드는 상기 저장장치의 데이터에 대한 액세스를 인증하기 위해 사용된다. 예를 들어, 상기 패스워드는, 룩업 테이블(look-up table)을 통해 상기 저장장치의 데이터를 암호화하는 암호화 키를 식별하는데, 사용될 수 있다. 또한, 이전에 논의되었던 것처럼, 상기 패스워드는 상기 암호화 키를 언-마스크(un-mask)하는데 사용될 수 있다. 본 발명의 일 실시예에 따른 다중 패스워드는, 하나의 저장장치에서 각기 다른 파일들(files), 폴더들(folders), 오퍼레이팅 시스템들(operating system), 혹은 파티션들(partitions) 을 사용할 수 있다.

<50> 프로세스 326에서, 사용자가 입력한 패스워드의 해쉬 버전은 소정의 알고리즘에 기초하여 계산된다. 본 발명의 일 실시예에 따라, 암호화 알고리즘이 사용될 수 있다. 프로세스 328에서, 상기 저장장치의 소정 위치에 저장된 상기 소정 패스워드의 해쉬 버전은 식별(identified)된다. 프로세스 330에서, 상기 소정의 패스워드의 해쉬 버전은 상기 사용자가 입력한 패스워드의 해쉬 버전과 비교된다. 프로세스 332에서, 만일, 동일한 것(match)으로 결정되면, 상기 암호화 키로의 액세스는 허용(enabled)된다. 프로세스 334에서, 상기 호스트 시스템의 사용자에 의해 액세스되는 저장장치로부터 요구된 데이터는 복호화 된다.

<51> 본 발명의 일 실시예에 따른 상기 암호화 키는 상기 인터셉터 모듈, 상기 호스트 시스템, 그리고/혹은 상기 저장장치 중의 하나로부터 액세스된다. 예를 들어, 상기 암호화 키는 상기 저장장치로부터 액세스될 때, 숨겨진 위치(들)나 트랙(들)에 저장된다. 본 발명의 일 실시예에 따른, 상기 암호화 키를 액세스하는 과정은 상기 암호화 키를 해독하는 제2암호화 키를 액세스하는 과정을 포함한다. 예를 들어, 상기 암호화 키는 위장된(예: 암호화, 마스크) 폼으로 저장되고, 옳바른 패스코드(passcode 혹은 패스워드)가 상기 접속 요구로서 제공될 때 해독될 것이다.

<52> 도 3C는 본 발명의 일 실시예에 따라, 유실되거나 도난당한 휴대용 장치를 식별하는 프로세스를 도시한 흐름도 300C이다.

<53> 프로세스 330에서, 상기 소정 패스워드의 해쉬 버전은 상기 사용자가 입력한 패스워드의 해쉬 버전과 비교된다. 만일, 일치하지 않는 것으로 식별되면, 상기 소정 패스워드와 입력된 패스워드간의 발생하는 불일치의 횟수를 체크한다. 만일, 상기 횟수가 소정 한계 값(threshold)을 초과하지 않으면 상기 동작 342에서 사용자는 다시 패스워드 그리고/혹은 패스워드 힌트에 대해 재촉한다. 예를 들어, 도 7C의 스크린 샷 700C에 도시된 바와 같이 무효한 키가 입력되고 사용자는 재시도하거나 혹은 종료하는 옵션을 갖는다.

<54> 만일, 상기 횟수가 상기 소정의 한계값을 초과하면, 그리고 프로세스 344에서 만일, 상기 시스템이 네크워크에 연결되어 있다면, 상기 호스트 시스템의 IP주소는 네트워크 서버로 보고된다. 일 실시예에서, MAC주소, 사용자 이름, 워크 그룹 이름과 같이, 상기 호스트의 유일한(unique) 식별자는 또한, 방송(Broadcast)될 것이고 IP주소와 연계될 것이다. 전자장치를 잃어버린 사람들이 자신의 잃어버린 전자장치에 액세스하기 위해 어떠한 시도가 이루어지고 있는지 볼 수 있게 하기 위해, 상기 호스트 시스템 식별자와 IP주소는 상기 전자장치를 잃어버린 사람들을 위한 웹 사이트에 공개될 수 있다. 만일, 잃어버린 전자장치에 액세스하기 위한 어떠한 시도가 이루어지고 있다면, 상기 공개된 IP주소는 상기 잃어버린 전자장치들이 어디쯤에 있는지에 대한 단서가 될 것이다.

<55> 본 발명의 일 실시예에서, 상기 로그-온 시도의 실패 시에, 만일, 상기 호스트 시스템이 네트워크에 연결되지 않은 경우, 상기 실패한 시도에 관한 지시자는 저장될 것이고 상기 시스템이 네트워크와 연결된 다음에 방송될 것이다. IP주소를 웹사이트에 보고하는 것과 더불어, 만일, 로그-온의 시도가 실패한 경우, 통지(notification)는 사용자에 의해 특정된 e-메일 주소로 전송된다. 상기 e-메일은 실패한 로그-온 시도의 횟수, 로그-온을 시도하는데 사용된 패스워드, 시스템의 상태, 상기 시스템의 IP주소가 현재 이용가능 한지 등과 같은 정보들을 보고할 수 있다. 일 실시예에서, e-메일 통지는 어떤 액세스 요구가 실패했을 때 전송될 수 있다. 예를 들어, 만일, 특정 파일이나 폴더에 액세스하려는 시도가 실패했을 때 e-메일은 사용자에 의해 특정된 e-메일 주소로 전송될 수 있다.

<56> 도 4A는 본 발명의 일 실시예에 따라 저장장치 데이터 암호화와 데이터 액세스에 대한 패스워드 인증을 위해, 저장장치, 인터셉터 모듈, 그리고 호스트 시스템 간의 상호작용을 도시한 도 3B의 프로세스의 일 예를 묘사한 상호작용 다이어그램 400A이다.

<57> 프로세스 402에서, 사용자는 세션의 제1액세스를 초기화(initiate) 하고 상기 호스트 시스템은 인터셉터 모듈로 어떤 요구를 전달한다. 상기 인터셉터 모듈은 상기 세션의 제1요구로서 상기 요구를 확인한다. 본 발명의 일 실시예에 따른 세션은 파워-업, 타임-아웃, 재시작, 혹은 이전 세션을 종료하기 위한 어떤 다른 유발(trigger) 이후에 시작될 수 있다. 프로세스 404에서, 상기 인터셉터 모듈은 상기 저장장치의 상기 숨겨진 위치(들)나 트랙(들)으로부터 상기 키의 암호화 버전을 검색한다. 프로세스 406에서, 상기 숨겨진 트랙들에서의 상기 키의 위치가 파악되고, 상기 파악된 위치의 암호화 키는 상기 인터셉터 모듈로 보내진다.

<58> 프로세스 408에서, 드라이버 로드(driver load)는 플러그-앤-플레이(Plug-and-Play) 특성을 갖는 USB같은 장치를 이용하여 상기 호스트 시스템에서 초기화(initiate) 된다. 프로세스 410에서, 상기 인터셉터 모듈은 패스워드를 위해 사용자를 재촉하도록 상기 호스트 시스템으로 전송할 요구(예: 요구신호 혹은 명령)를 생성한다. 프로세스 412에서, 상기 사용자에게 패스워드의 입력을 재촉한다. 프로세스 414에서, 사용자가 상기 패스워드를 입력한 후, 상기 시스템은 상기 패스워드가 예상했던 것(옳바른 패스워드)과 일치하는 지 판단한다. 프로세스 406에서, 상기 저장장치의 숨겨진 트랙으로부터 검색된 상기 암호화 키는 또한, 암호화 알고리즘(예: DES/3DES, BlowFish, AES or 다른 적당한 암호화 방법들)이나 상기 암호화 키를 위장할 수 있는 다른 방법을 이용하여 암호화될 수 있다. 만일, 상기 패스워드가 일치하면, AES나 다른 적당한 프로토콜과 같은 암호화 알고리즘을 이용하여 상기 시스템은 상기 데이터를 암호화하거나 해독하는 상기 키를 열게(unlocked) 된다.

<59> 본 발명의 일 실시예에 따르면, 만일, 상기 패스워드가 일치하지 않으면, 상기 프로세스는 프로세스 410으로 루프-백(loop back)하여, 다시 상기 패스워드를 입력하도록 사용자를 재촉한다. 상기 패스워드 일치에 실패한 시도가 소정 횟수에 이르면, 상기 호스트 시스템은 상기 세션을 종료(예: 타임-아웃이나 시스템 재부팅에 의해)하게 될 것이다. 일 실시예에서, 힌트 또는 힌트 질문은 상기 패스워드를 기억해 내는 것을 돕거나 언락 오버라이드(Unlock override)를 허용하기 위해 사용자에게 제공된다. 일 실시예에서, 마스터 암호화 키는 이용가능(available)하고 암호화된 드라이브에 액세스하기 위한 마스터 패스워드에 액세스된다.

<60> 도 4B는 본 발명의 일 실시예에 따라 저장장치 데이터 액세스를 위해, 저장장치, 인터셉터 모듈, 그리고 호스트 시스템 간의 상호작용을 도시한 도 3B의 프로세스의 일 예를 다르게 묘사한 상호작용 다이어그램 400B이다.

<61> 프로세스 452에서, 상기 호스트 시스템은 ''Get Data''명령을 발행한다. 프로세스 454에서, 상기 ''Get Data'' 명령은 상기 인터셉터에 의해 수신되어 식별된다. 프로세스 456에서, 상기 ''Get Data''명령은 상기 인터셉터 모듈에 의해 해석된다. 프로세스 458에서, 상기 ''Get Data''명령은 상기 저장장치로 보내진다.

<62> 프로세스 460에서, 상기 저장장치는 상기 명령을 수신하고 해석한다. 프로세스 462는 상기 요구된 데이터는 상기 ''Get Data''명령에 대응하여, 검색(retrieve)된다. 프로세스 464에서, 상기 요구된 데이터를 갖는 응답을 상기 호스트로 되돌려 보낸다.

<63> 프로세스 466에서, 상기 검색된 데이터는 적절한 알고리즘(예: DES/3DES, Blowfish, AES 등과 같은 암호화 알고리즘)에 의한 복호화를 통해 해독된다 상기 알고리즘에 의존하여, 암호화 키는 상기 검색된 데이터(예: 위에서 기술된 바와 같이 이전에 검색된 상기 키)를 해독하는데 사용될 수 있다.

<64> 어떤 경우에는, 상기 키는 하드 디스크 드라이브에 의해서는 해석될 수 없지만 상기 인터셉터에 의해서는 해석되는 파라미터들을 포함하는 모의 (simulated) 명령들(미도시)을 전송함으로써 호스트 컴퓨터로부터 전송될 수 있으며, 따라서 예를 들면 키의 수신을 위한 명령으로 해석될 수 있다.

<65> 프로세스 468에서, 상기 저장장치로부터 검색된 상기 요청 데이터의 복호화 버전이 상기 호스트 시스템으로 전송된다. 프로세스 470에서, 상기 저장장치로부터 검색된 상기 요청 데이터의 복호화 버전이 획득된다. 일 실시예에서, 자동 백업 소프트웨어는 암호화 기능(예: AES)을 통하여 저장장치의 데이터를 백업할 수 있다. 예를 들면, 상기 저장장치의 저장위치에 있는 비암호화 데이터(un-encrypted)는 암호화될 제2저장 위치로 일시적으로 옮겨질 수 있으며 이후 원래의 저장위치로 다시 옮겨질 수 있다. 일 실시예에서, 상기 제2저장위치는 동일한 저장장치의 다른 저장 위치이다. 일 실시예에서, 상기 제2저장위치는 다른 저장장치이다.

<66> 일 실시예에서, 상기 저장장치의 데이터가 암호화되도록, 상기 원래의 오리지날(예: 비암호화) 데이터는 암호화되지 않은 데이타를 삭제하는 멀티플 랜덤 오버라이트(overwrite)에 의해, 제거될 수 있다.

<67> 도 5는 본 발명의 일 실시예에 따라, 패스워드의 생성 혹은 변경을 위한 인터페이스을 나타낸 스크린 샷 500을 도시한 것이다.

<68> 상기 스크린 샷 500은 패스워드 유지에 사용되는 보안 액세스 스크린을 보여준다. 일 실시예에서, 상기 보안 액

세스 스크린은 상기 저장장치의 데이터에 액세스하기 전이나, 상기 오퍼레이팅 시스템으로의 로그온을 위해 저장장치의 데이터에 액세스하기 전에 패드워드 인증을 디스에이블하는 '디스에이블 패스워드 보안' 체크박스를 포함한다. 예를 들면, 만일 상기 '디스에이블 패스워드 보안' 박스가 선택되면, 상기 패스워드 필드와 상기 힌트 필드는 상기 호스트 시스템을 설정하기 전이나 로그온하기 전에 채워질 필요가 없다. 이 경우, 상기 저장장치에 저장된 데이터는 암호화되지 않는다. 또한, 상기 암호화 키가 데이터 액세스 이전에 제공해야 하는 패스워드없이 복호화에 이용 가능한 경우를 제외하면, 상기 저장장치에 저장된 데이터는 암호화될 수 있다.

<69> 일 실시예에서 새로운 패드워드는, 상기 '새로운 패스워드'와 '새로운 패스워드 확인' 필드에 요구되는 패드워드를 입력함으로써, 상기 저장장치를 보호하도록 설정된다. 이 경우, 상기 '현재 패스워드' 필드는 블랭크(빈상태)로 남겨둘 수 있다. 일 실시예에서, 상기 '현재 패스워드' 필드에 상기 보정된 패스워드를 제공하는 것과 상기 '새로운 패스워드'와 '새로운 패스워드 확인' 필드에 요구되는 패드워드를 입력하는 것으로, 존재하는 패스워드는 바뀌게 된다.

<70> 상기 '힌트'필드는 오직 사용자만이 정답을 알 수 있는 질문을 입력하도록 사용될 수 있다. 부정확한 패스워드가 소정 횟수 입력되었을 때와 같이, 상기 질문은 사용자가 패스워드를 잊었을 때 묻게 될 것이다. 상기 '힌트' 필드는 또한, '상기 패드워드는 순이 고모의 생일과 관련된 것이다'와 같이, 사용자의 패스워드를 연상할 수 있도록 하여 패스워드 힌트의 입력에 사용될 수 있다. 일 실시예에서, 상기 사용자는 자신의 패드워드를 기억하지 못하고 있음을 알리고, 소정 횟수의 부정확한 패스워드를 입력하기 전에 패스워드 힌트를 보여줄 것을 요구하게 될 것이다.

<71> 도 6은 본 발명의 일 실시예에 따라, 저장장치를 보호하는 인터페이스를 나타낸 스크린 샷 600을 도시한 것이다.

<72> 상기 스크린 샷 600은 패스워드 유지에 사용되는 보안 액세스 스크린을 보여준다. 일 실시예에서, 소스 드라이브(예: 데이터 암호화에 의해 보호되는 저장장치)는 서브 윈도우 602의 아래 리스트에 실린 저장장치들의 리스트로부터 선택된다. 그리고 목적 드라이브는 서브 윈도우 604의 아래 리스트에 실린 저장장치들의 리스트로부터 선택된다. 예를 들어, 상기 소스 드라이브는 보호받는 데이터들을 갖는 저장장치이다. 상기 소스 드라이브의 데이터는 암호화된 후, 상기 목적 드라이브로 이동되어 저장된다. 일 실시예에서, 상시 소스 드라이브의 데이터는 암호화를 위해, 상기 목적 드라이브로 이동되고, 상기 소스 드라이브에서는 삭제될 것이다. 그런 다음, 상기 암호화된 데이터는 상기 소스 드라이브로 다시 이동되어 저장된다.

<73> 일 실시예에서, 하나의 저장장치(예: 소스 드라이브)는 상기 프로세스와 관계를 맺게 된다. 예를 들어, 상기 소스 드라이브에서 암호화된 데이터는 다른 저장 위치로 이동되어 암호화 된다. 상기 비보호 데이터는 상기 원래의 저장 위치에서 삭제되고, 상기 다른 저장위치의 암호화된 데이터는 일 실시예에 따라, 상기 원래의 저장 위치로 다시 이동시켜 저장될 수 있다.

<74> 도 7A는 본 발명의 일 실시예에 따라, 보호된 저장장치에 액세스하기 위한 로그인 스크린의 인터페이스를 나타낸 스크린 샷 700A을 도시한 것이다.

<75> 상기 스크린 샷 700A은 저장장치의 데이터에 액세스하기 위한 인증에 대한 두 레벨의 보안 액세스의 예를 보인다. 일 실시예에서, 저장장치로의 액세스가 인정되기 전에 상기 소정의 패스워드는 패스워드 필드에 입력되어야 할 것이다. 일 실시예에서, 저장장치로의 액세스가 인정되기 전에, 비트맵 윈도에 나타난 텍스트가 정확한 패스워드로서 추가적으로 '비트맵 윈도' 필드에 입력될 것이다. 일단, 상기 '패스워드' 필드가 채워지면, 상기 '로그인' 아이콘이 액세스를 확인하기 위해 클릭될 수 있고, 검증이 성공하면 액세스가 허가된다.

<76> 도 7B는 본 발명의 일 실시예에 따라, 패스워드 프롬프트를 가지고 있는 로그인 스크린의 인터페이스를 나타낸 스크린 샷 700B를 도시한 것이다.

<77> 일 실시예에 따라, 상기 소정의 패스워드는 필드'Please Enter Password'에 시스템(예를 들면, 로그온 하기 위한 하나 이상의 운영체계 혹은 액세스하기 위한 하나 이상의 저장장치)에 액세스하기 위해 입력된다.

<78> 도 7C는 본 발명의 일 실시예에 따라, 도 7B에 입력된 무효한(invalid) 패스워드로 인해 로그온에 실패한 스크린 샷 700C를 도시한 것이다.

<79> 본 발명에 따른 로그온 실패에서, 사용자는 종료나 재시도의 옵션을 갖는다. 사용자는 소정 횟수의 무효한 패스워드를 입력할 수 있다. 상기 무효한 패스워드의 입력이 상기 소정 횟수에 도달했을 때, 상기 시스템은 종료하거나 도 8의 실시예에 도시된 바와 같이 사용자에게 패스워드 힌트를 제공할 수 있다.

<80> 상기 스크린 샷 800은 사용자에게 패스워드 힌트를 보이기 위한 프롬프트의 예를 보인 것이다. 상기 패스워드 힌트 프롬프트는 만일 사용자가 패스워드를 잊었을 경우 사용자에 의해 요청될 수 있다. 일 실시예에서, 상기 패스워드 힌트 프롬프트는 부정확한 패스워드의 입력이 소정 횟수 발생했을 때 유발된다. 예를 들어, 만일 사용자가 부정확한 패스워드를 3차례 입력하면, 상기 시스템은 패스워드 설정 시 지정된 패스워드 힌트를 제공할 수 있다.

<81> 도 9는 본 발명의 일 실시예에 따라, 프로세싱 유닛 902, 제어기, 메모리 모듈, 소프트웨어 모듈 그리고/혹은 무선 모듈을 갖는 인터셉터 모듈 104의 개략적인 구성의 일 예를 나타낸 것이다.

<82> 상기 프로세싱 유닛 902는 상기 암호화 모듈과 같은 다양한 소프트웨어 인스턴스와/혹은 상기 오퍼레이팅 시스템을 포함할 수 있다. 본 발명의 일 실시예에 따른 암호화 모듈은 저장장치에 저장된 데이터를 해독하고 보호하는 하나 혹은 다수의 암호화 알고리즘을 수행하는 코드를 포함한다. 일 실시예에서, 각기 다른 암호화 알고리즘들이 각각의 저장장치들에 사용될 수 있고, 상기 제어기와/혹은 메모리는 관련된 암호화 알고리즘과 상기 암호화 알고리즘으로 암호화된 상기 저장장치를 연계시킬 수 있다. 일 실시예에서 상기 암호화 모듈은 하나 혹은 그 이상의 저장장치를 보호하기 위해, 하나 혹은 그 이상의 암호화 알고리즘을 이용하여 하나 혹은 그 이상의 암호화 키를 저장하는 메모리를 포함한다. 상기 인터셉터 모듈 104이 암호화/복호화를 처리하는 동안, 상기 암호화 키는, 양자 택일적 사항으로써 선택적 장치에 의해 상기 인터셉터 모듈 104로 제공된다. 예를 들어, 상기 하나 혹은 그 이상의 암호화 키는 인증을 위해 상기 인터셉터 모듈 104로 전송될 수 있다. 본 발명의 일 실시예에 따른 상기 인증은 많은 형태들 중의 하나, 예를 들면, 상기 호스트 시스템의 사용자 아이덴티티를 식별하는 패스워드 인증을 택할 수 있다.

<83> 도 10은 상술한 하나 이상의 방법들을 수행하기 위한 기계 장치와 명령 세트를 갖는 전형적인 형태의 컴퓨터 시스템 1000에 대한 개략의 구성을 보인다. 다른 실시예로서, 상기 장치는 독립형 디바이스로서 작동하거나, 다른 기계 장치에 액세스할 수 있다(예를 들면, 네트워크). 네트워크 되는 배치에서, 상기 기계장치는 클라이언트-서버 네트워크 환경에서 서버 또는 클라이언트 장치의 자격으로 작동하거나, 피어투피어(peer to peer) 네트워크 환경에서 동등한 자격의 피어 머신(peer machine)으로 작동할 수 있다. 상기 기계 장치는 서버 컴퓨터, 클라이언트 컴퓨터, 개인 컴퓨터(PC), 태블릿 PC, 셋톱 박스(STB), 개인 휴대 정보 단말기(PDA), 셀룰러 폰, 웹 어플라이언스, 네트워크 라우터, 스위치 또는 브리지 또는 그 기계장치에 의해 취해진 특정 동작을 지정하는 한 세트의 명령들(순차적인 명령 또는 비순차적인 명령)의 실행이 가능한 임의의 기계 장치일 수 있다. 상기 기계 판독 가능 매체 1022가 단일 매체인 실시예를 보이고 있지만, 상기 기계 판독 가능 매체란, 단일 매체 또는 다중 매체를 포함할 수 있다. (예를 들면, 집중화되거나 분할된 데이터베이스, 또는 캐시와 서버에 관련된 데이터베이스) 상기 "기계 판독 가능 매체"는 또한 기계 장치에 의해 실행하기 위해 명령들 세트를 부호화하거나 수행하거나, 또는 저장할 수 있는 매체들을 포함할 수 있다. 상기 매체는 본 발명의 어느 하나 이상의 방법들이 기계 장치에서 실행될 수 있도록 한다. 더욱이, 단일 기계장치만이 도시되어 있지만, 상기 용어 '기계장치'는, 여기서 논의된 어느 하나 혹은 그 이상의 방법론들을 행하는 명령의 집합을 개인적으로 혹은 공동으로 수행하는 기계들의 수집(collection)에 포함된다.

<84> 상기 기기 판독 가능 매체(1022)가 단일 매체가 되도록 예시적인 실시예에서 도시된다 하더라도, 상기 용어 ''기기 판독 가능 매체''는 하나 이상의 명령 셋을 저장하는 단일 매체 또는 다수의 미디어(예: 집중 또는 분산된 데이터 베이스, 및/또는 관련 캐쉬 및 서버)를 포함하도록 되어야 한다. 또한 상기 용어 ''기기 판독 가능 매체''는 저장, 인코딩 또는 기기가 실행하기 위한 명령을 운반(carrying)할 수 있으며, 기기로 하여금 본 발명의 어떤 하나 이상의 방법론들을 수행하도록 하는 어떤 매체를 포함하도록 되어야 한다. 일반적으로, 명세서의 실시예들을 구현하기 위하여 실행된 루틴(routines)들은, 운영 시스템, 또는 특정 어플리케이션, 구성소자, 프로그램, 객체(object), 모듈 또는 ''컴퓨터 프로그램''으로 부르는 명령 시퀀스(sequence of instruction)의 일부분으로 구현될 수 있다. 상기 컴퓨터 프로그램은 전형적으로 컴퓨터에서 다양한 메모리와 저장장치에 다양한 시간에 설정되는 하나 이상의 명령 셋으로 구성되며, 상기 하나 이상의 명령 셋은, 컴퓨터에서 하나 이상의 프로세서에 의해 리드되고 실행되며, 상기 컴퓨터로 하여금 명세서의 다양한 양상(aspect)을 포함하는 엘리먼트를 실행하기 위한 동작(operations)들을 수행하도록 한다.

<85> 게다가, 실시예들은 전적으로 펑처링 (functioning) 컴퓨터 및 컴퓨터 시스템의 컨텍스트(context)에서 기술되었다 해도 이 분야에서 통상의 지식을 가진 자는 다양한 실시예가 다양한 형태로 프로그램 제품으로 유통될 수 있으며, 명세서는 실제로 유통에 영향을 미치기 위해 사용되는 특정 타입의 기기 또는 컴퓨터 판독가능 매체에 관계없이 동일하게 적용한 다는 것을 인식할 수 있을 것이다. 컴퓨터 판독가능 매체의 예들은, 휘발성 및 비휘발성 메모리 장치, 플로피 및 다른 삭제 가능 디스크, 하드 디스크 드라이브, 광 디스크(예: CD-ROM, DVD), 그

중 하나로서 디지털 및 아날로그 링크와 같은 전송형 미디어등과 같은 기록 가능형 미디어를 포함하며, 그러나 이에 한정되는 것은 아니다.

<86> 본 발명의 실시예들은 예시적인 특정 실시예들을 참조하여 기술되었지만, 상기 실시예들에 다양한 수정과 변형이 이루어질 수 있다는 것은 자명할 것이다. 따라서, 상기 명세서와 도면은 제한적이기 보다는 예시적인 것으로 간주되어야 한다. 전술한 명세서는 예시적인 특정 실시예들을 참조하여 기술하였다. 후술하는 청구항에 나타난 것처럼 다양한 수정이 더 넓은 정신 및 범위를 벗어나지 않는 한 상기 실시예들에 적용될 수 있다. 따라서, 상기 명세서와 도면은 제한적이기 보다는 예시적인 것으로 여겨져야 한다.

도면의 간단한 설명

<87> 도 1은 본 발명의 일 실시예에 따라, 인터셉터 모듈을 통해, 호스트 시스템과 통신하는 저장장치의 일 예를 도시한 것이다.

<88> 도 2는 본 발명의 일 실시예에 따라, 인터셉터 모듈을 경유하여 저장장치와 통신하는 호스트 시스템의 개략적인 구성의 일 예를 나타낸 것이다.

<89> 도 3A는 본 발명의 일 실시예에 따른, 저장장치 데이터 암호화와 데이터 액세스를 위한 패스워드 설정을 도시한 흐름도이다.

<90> 도 3B는 본 발명의 일 실시예에 따른, 저장장치 데이터 암호화와 데이터 액세스를 인증하는 프로세스를 도시한 흐름도이다.

<91> 도 3C는 본 발명의 일 실시예에 따라, 유실되거나 도난당한 휴대용 장치를 식별하는 프로세스를 도시한 흐름도이다.

<92> 도 4A는 본 발명의 일 실시예에 따라 저장장치 데이터 암호화와 데이터 액세스에 대한 패스워드 인증을 위해, 저장장치, 인터셉터 모듈, 그리고 호스트 시스템 간의 상호작용을 도시한 도 3B의 프로세스의 일 예를 묘사한 상호작용 다이어그램이다.

<93> 도 4B는 본 발명의 일 실시예에 따라 저장장치 데이터 액세스를 위해, 저장장치, 인터셉터 모듈, 그리고 호스트 시스템 간의 상호작용을 도시한 도 3B의 프로세스의 일 예를 다르게 묘사한 상호작용 다이어그램이다.

<94> 도 5는 본 발명의 일 실시예에 따라, 패스워드의 생성 혹은 변경을 위한 인터페이스을 나타낸 스크린 샷을 도시한 것이다.

<95> 도 6은 본 발명의 일 실시예에 따라, 저장장치를 보호하는 인터페이스를 나타낸 스크린 샷을 도시한 것이다.

<96> 도 7A는 본 발명의 일 실시예에 따라, 보호된 저장장치에 액세스하기 위한 로그인 스크린의 인터페이스를 나타낸 스크린 샷을 도시한 것이다.

<97> 도 7B는 본 발명의 일 실시예에 따라, 패스워드 프롬프트를 가지고 있는 로그인 스크린의 인터페이스를 나타낸 스크린 샷을 도시한 것이다.

<98> 도 7C는 본 발명의 일 실시예에 따라, 도 7B에 입력된 무효한 패스워드로 인해 로그온에 실패한 스크린 샷을 도시한 것이다.

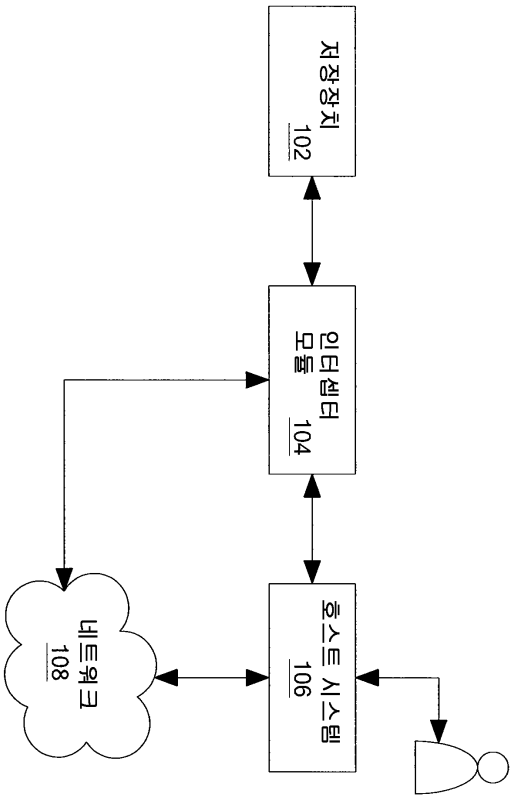
<99> 도 8의 본 발명의 일 실시예에 따라, 패스워드 힌트를 디스플레이 하는 스크린의 인터페이스를 나타낸 스크린 샷을 도시한 것이다.

<100> 도 9는 본 발명의 일 실시예에 따라, 프로세싱 유닛, 제어기, 메모리 모듈, 소프트웨어 모듈 그리고/혹은 무선 모듈을 갖는 인터셉터 모듈의 개략적인 구성의 일 예를 나타낸 것이다.

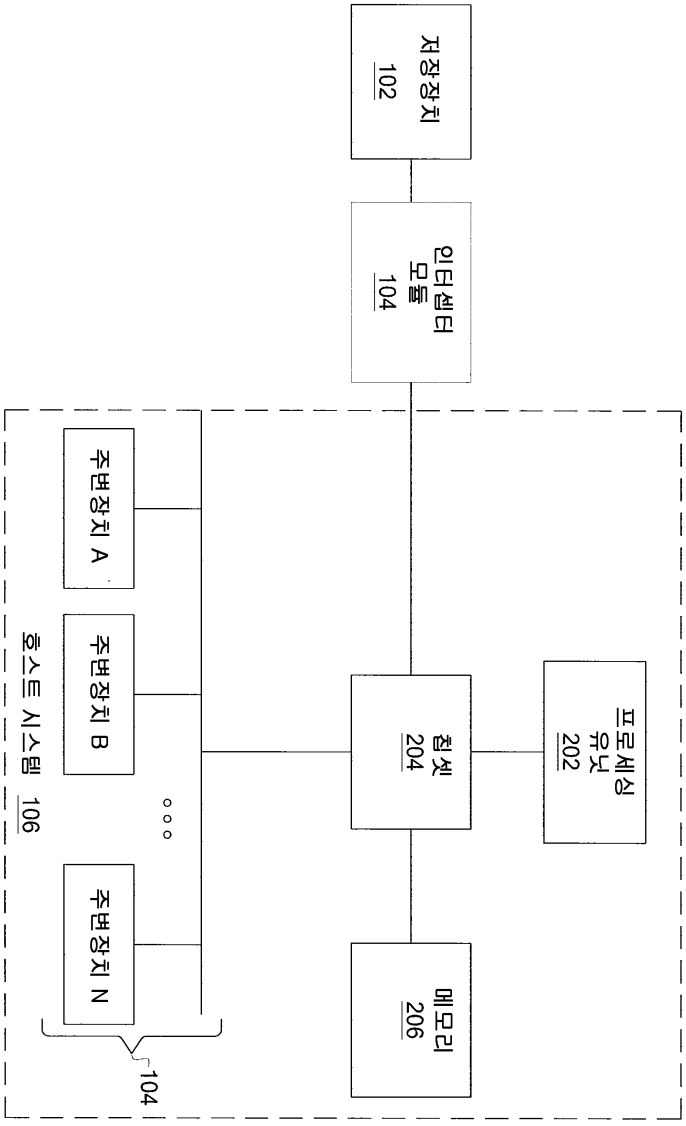
<101> 도 10은 본 발명의 일 실시예에 따라, 명령 세트에 대한 소스를 갖는 블록 다이어그램을 도시한 것이다.

도면

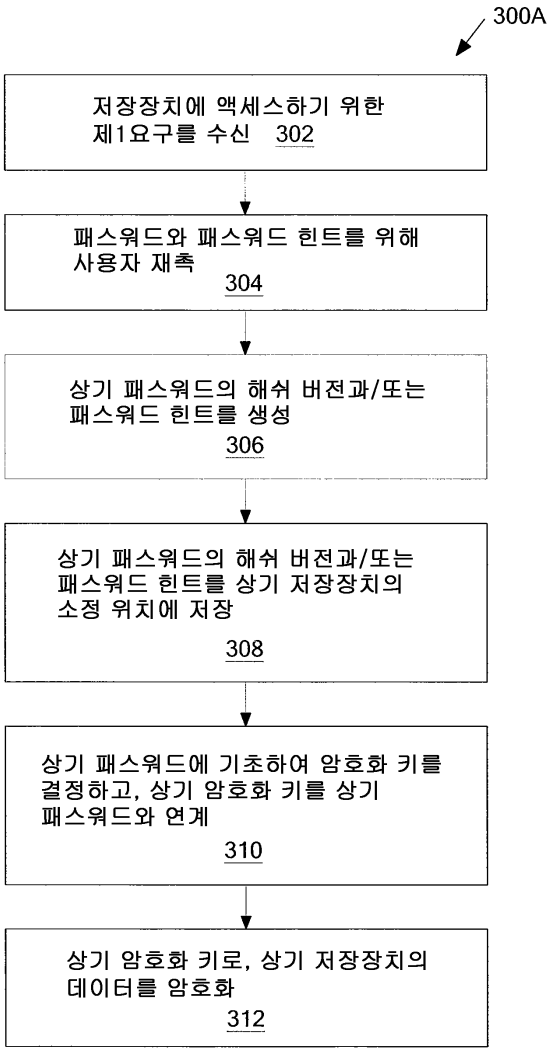
도면1



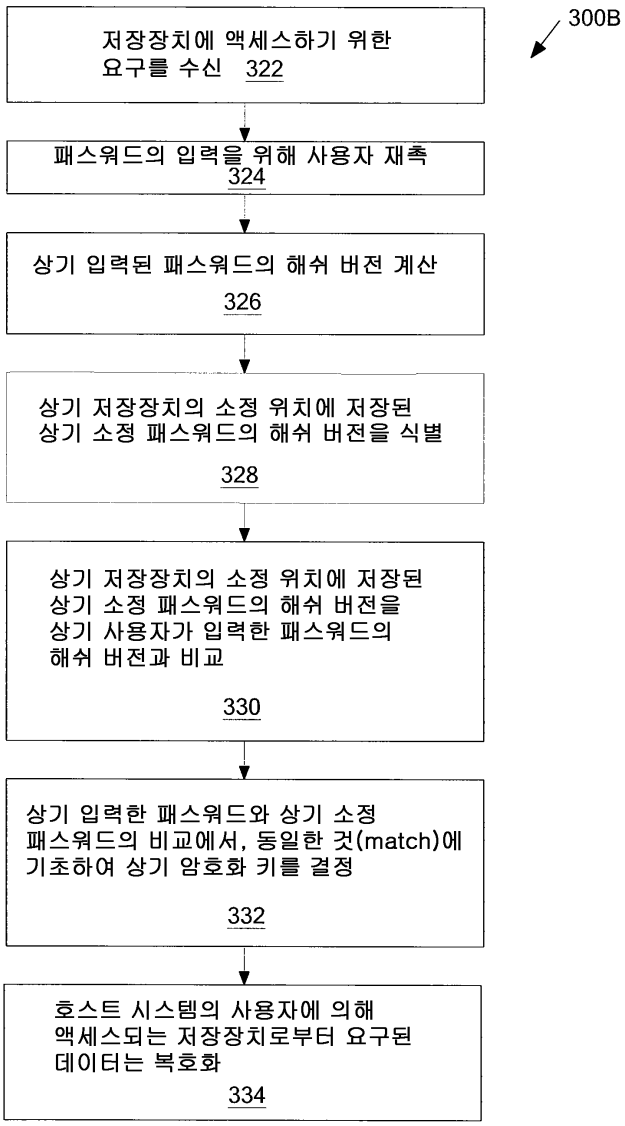
도면2


저장장치
102
인터셉터
모듈
104
프로세싱
유닛
202
칩셋
204
메모리
206
주변장치 A
주변장치 B
주변장치 N
호스트 시스템 106
104

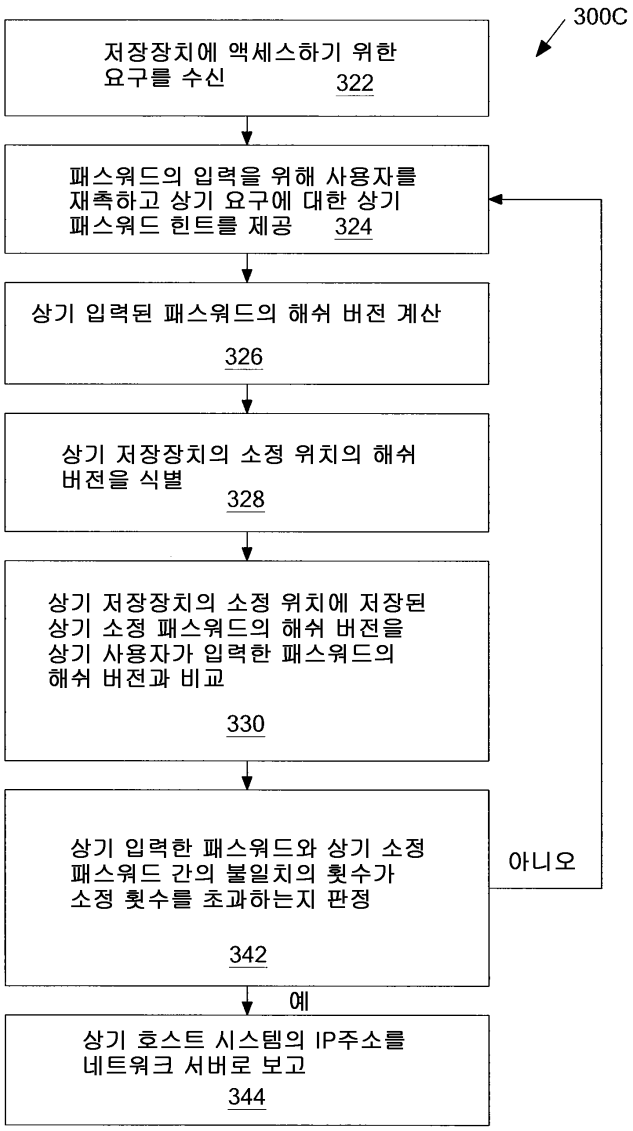
도면3a


300A
저장장치에 액세스하기 위한 제1요구를 수신 302
패스워드와 패스워드 힌트를 위해 사용자 재촉 304
상기 패스워드의 해쉬 버전과/또는 패스워드 힌트를 생성 306
상기 패스워드의 해쉬 버전과/또는 패스워드 힌트를 상기 저장장치의 소정 위치에 저장 308
상기 패스워드에 기초하여 암호화 키를 결정하고, 상기 암호화 키를 상기 패스워드와 연계 310
상기 암호화 키로, 상기 저장장치의 데이터를 암호화 312

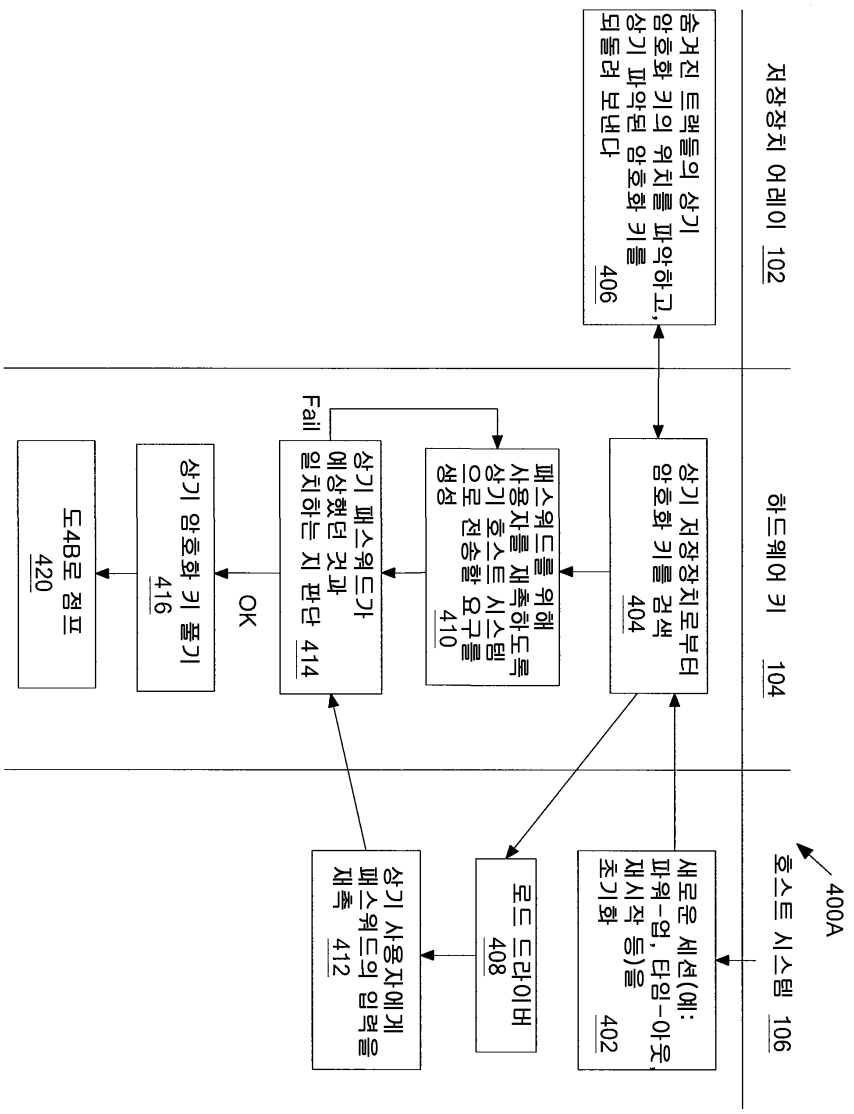
도면3b


300B
저장장치에 액세스하기 위한 요구를 수신 322
패스워드의 입력을 위해 사용자 재촉 324
상기 입력된 패스워드의 해쉬 버전 계산 326
상기 저장장치의 소정 위치에 저장된 상기 소정 패스워드의 해쉬 버전을 식별 328
상기 저장장치의 소정 위치에 저장된 상기 소정 패스워드의 해쉬 버전을 상기 사용자가 입력한 패스워드의 해쉬 버전과 비교 330
상기 입력한 패스워드와 상기 소정 패스워드의 비교에서, 동일한 것(match)에 기초하여 상기 암호화 키를 결정 332
호스트 시스템의 사용자에 의해 액세스되는 저장장치로부터 요구된 데이터는 복호화 334

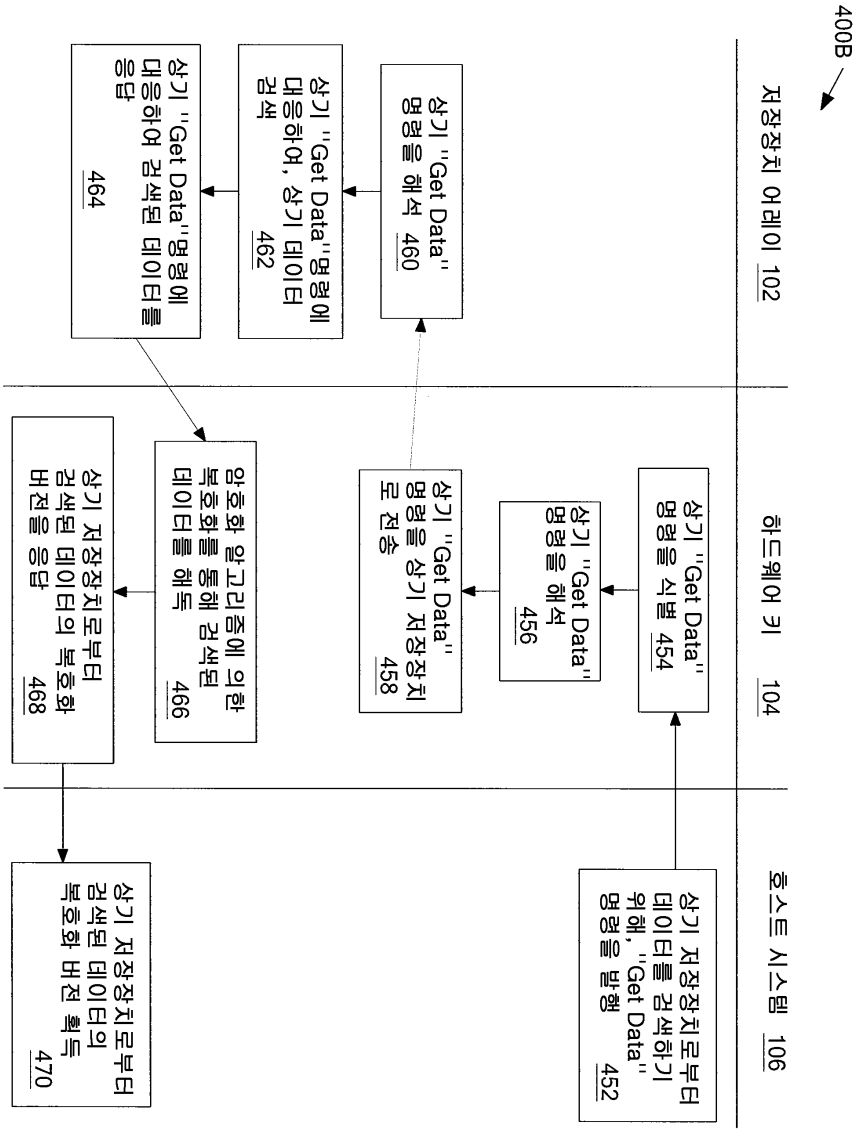
도면3c


300C
저장장치에 액세스하기 위한 요구를 수신 322
패스워드의 입력을 위해 사용자를 재촉하고 상기 요구에 대한 상기 패스워드 힌트를 제공 324
상기 입력된 패스워드의 해쉬 버전 계산 326
상기 저장장치의 소정 위치의 해쉬 버전을 식별 328
상기 저장장치의 소정 위치에 저장된 상기 소정 패스워드의 해쉬 버전을 상기 사용자가 입력한 패스워드의 해쉬 버전과 비교 330
상기 입력한 패스워드와 상기 소정 패스워드 간의 불일치의 횟수가 소정 횟수를 초과하는지 판정 342
아니오
예
상기 호스트 시스템의 IP주소를 네트워크 서버로 보고 344

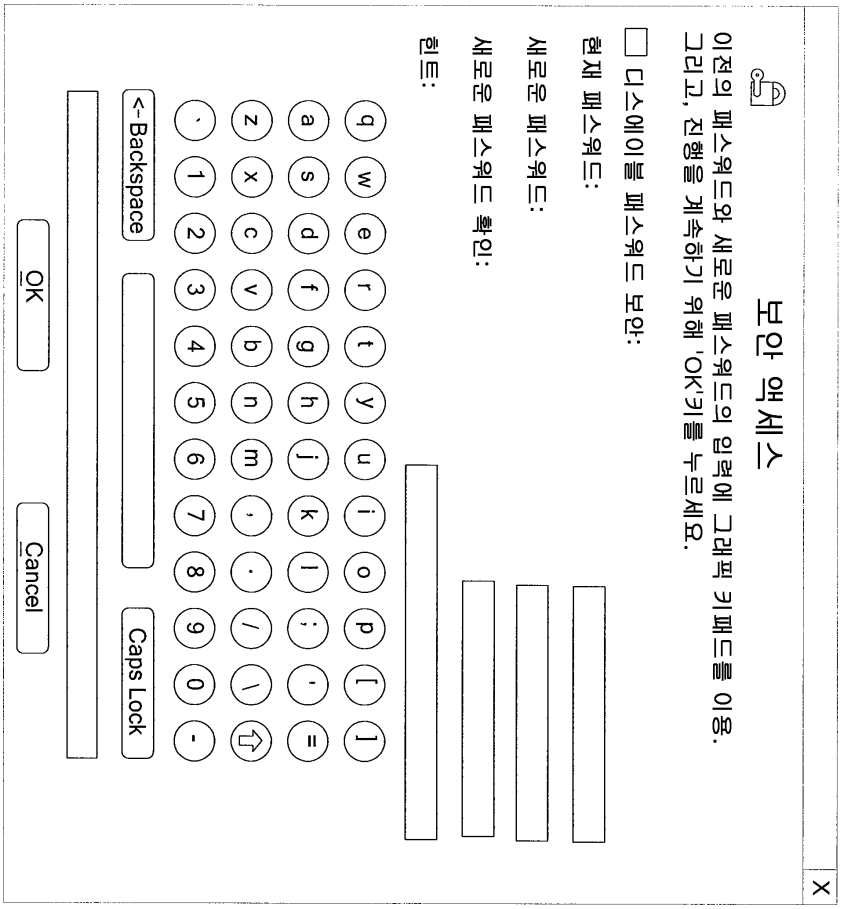
도면4a


400A
호스트 시스템 106
하드웨어 키 104
저장장치 어레이 102
새로운 세션(예: 파워-업, 타임-아웃, 재시작 등)을 초기화 402
상기 저장장치로부터 암호화 키를 검색 404
숨겨진 트랙들의 상기 암호화 키의 위치를 파악하고, 상기 파악된 암호화 키를 되돌려 보낸다 406
로드 드라이버 408
패스워드를 위해 사용자를 재촉하도록 상기 호스트 시스템으로 전송할 요구를 생성 410
상기 사용자에게 패스워드의 입력을 재촉 412
상기 패스워드가 예상했던 것과 일치하는 지 판단 414
Fail
OK
상기 암호화 키 풀기 416
도4B로 점프 420

도면4b

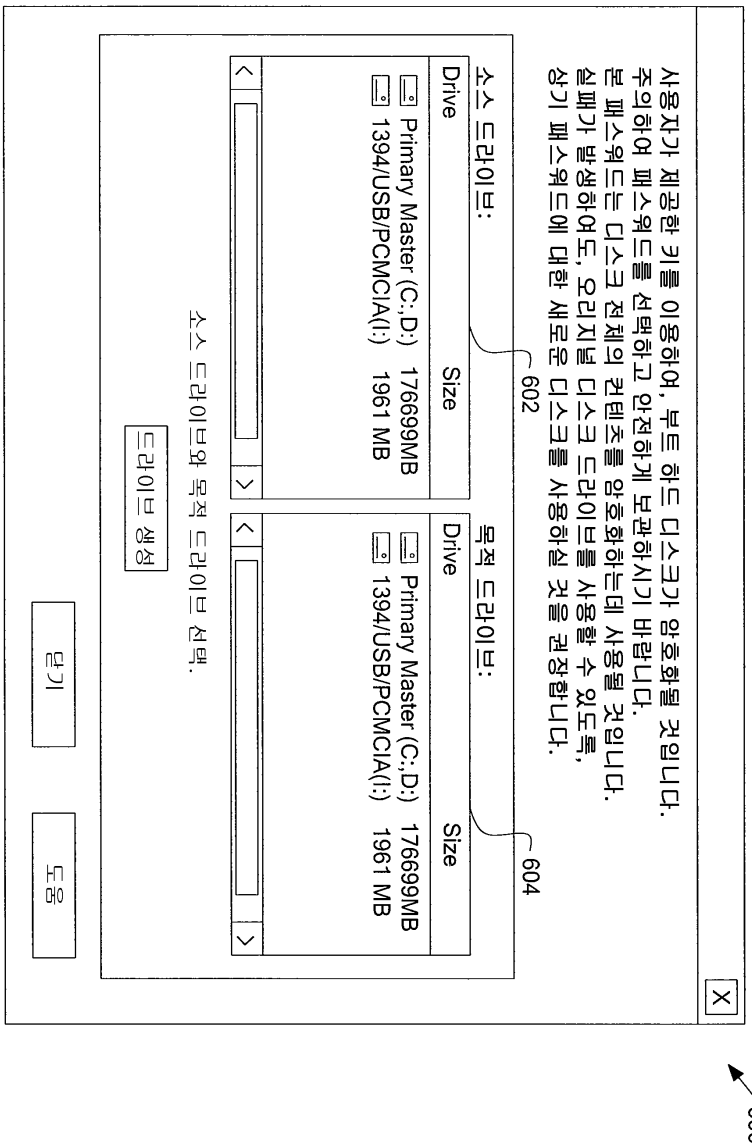

400B
저장장치 어레이 102
하드웨어 키 104
호스트 시스템 106
상기 저장장치로부터 데이터를 검색하기 위해, "Get Data" 명령을 발행 452
상기 "Get Data" 명령을 식별 454
상기 "Get Data" 명령을 해석 456
상기 "Get Data" 명령을 상기 저장장치로 전송 458
상기 "Get Data" 명령을 해석 460
상기 "Get Data"명령에 대응하여, 상기 데이터 검색 462
상기 "Get Data"명령에 대응하여 검색된 데이터를 응답 464
암호화 알고리즘에 의한 복호화를 통해 검색된 데이터를 해독 466
상기 저장장치로부터 검색된 데이터의 복호화 버전을 응답 468
상기 저장장치로부터 검색된 데이터의 복호화 버전 획득 470

도면5

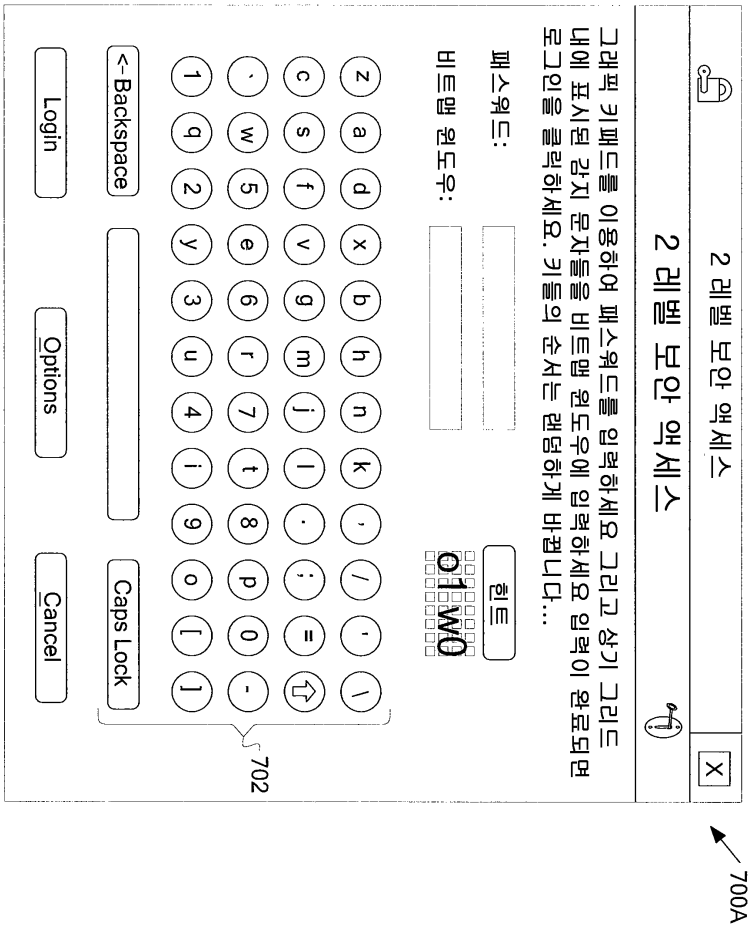

보안 액세스
이전의 패스워드와 새로운 패스워드의 입력에 그래픽 키패드를 이용.
그리고, 진행을 계속하기 위해 'OK'키를 누르세요.
디스에이블 패스워드 보안:
현재 패스워드:
새로운 패스워드:
새로운 패스워드 확인:
힌트:
q w e r t y u i o p [ ]
a s d f g h j k l ; ' =
z x c v b n m , . / \
` 1 2 3 4 5 6 7 8 9 0 -
<-Backspace
Caps Lock
OK
Cancel

500

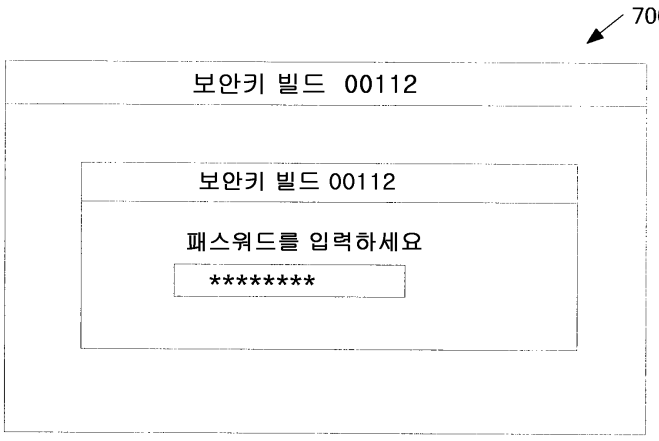
도면6


600
X
사용자가 제공한 키를 이용하여, 부트 하드 디스크가 암호화될 것입니다.
주의하여 패스워드를 선택하고 안전하게 보관하시기 바랍니다.
본 패스워드는 디스크 전체의 컨텐츠를 암호화하는데 사용될 것입니다.
실패가 발생하여도, 오리지널 디스크 드라이브를 사용할 수 있도록,
상기 패스워드에 대한 새로운 디스크를 사용하실 것을 권장합니다.
602
604
소스 드라이브:
목적 드라이브:
Drive
Size
Primary Master (C:,D:) 176699MB
1394/USB/PCMCIA(I:) 1961 MB
소스 드라이브와 목적 드라이브 선택.
드라이브 생성
닫기
도움

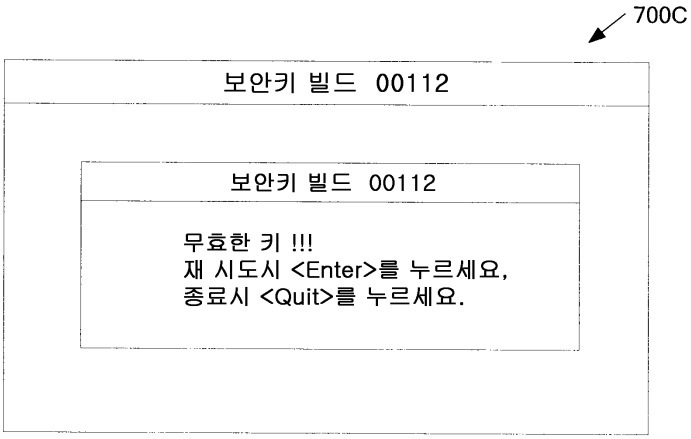
도면7a


2 레벨 보안 액세스
2 레벨 보안 액세스
그래픽 키패드를 이용하여 패스워드를 입력하세요 그리고 상기 그리드 내에 표시된 감지 문자들을 비트맵 윈도우에 입력하세요 입력이 완료되면 로그인을 클릭하세요. 키들의 순서는 랜덤하게 바뀝니다....
패스워드:
비트맵 윈도우:
힌트
Caps Lock
<- Backspace
Login
Options
Cancel
702
700A

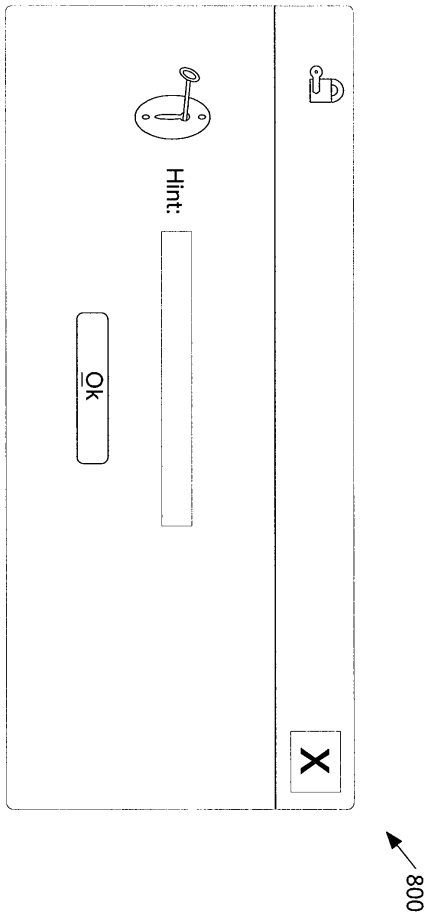
도면7b


700B
보안키 빌드 00112
보안키 빌드 00112
패스워드를 입력하세요
****

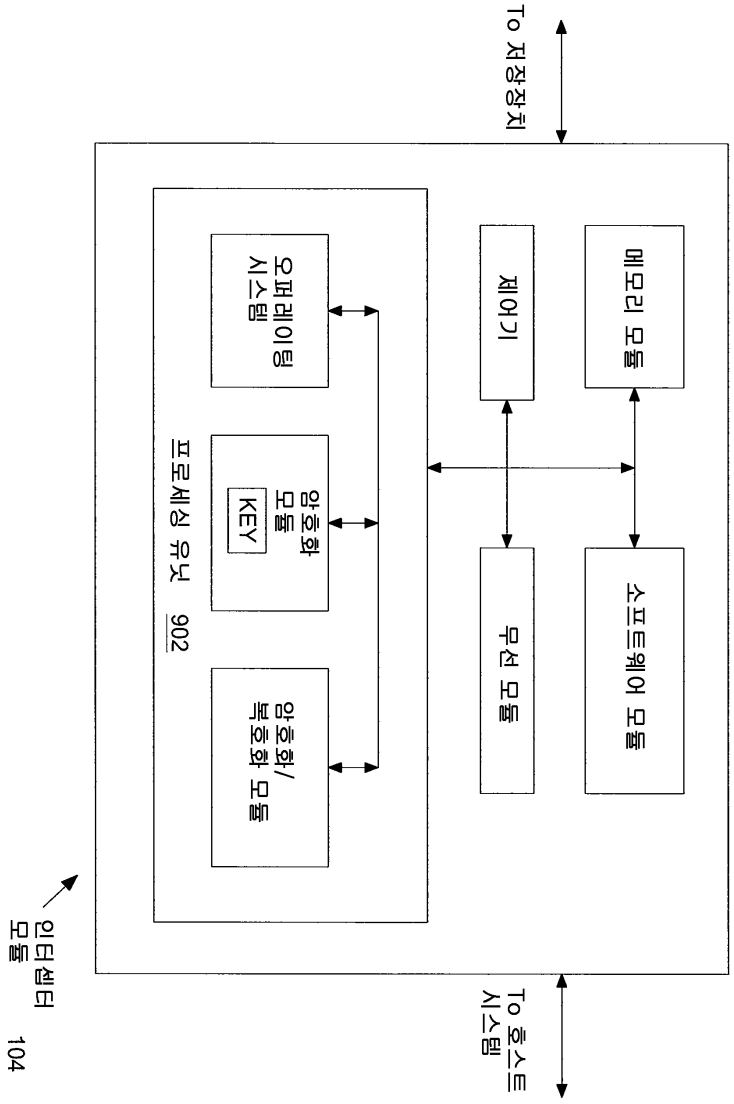
도면7c


700C
보안키 빌드 00112
보안키 빌드 00112
무효한 키 !!!
재 시도시 <Enter>를 누르세요,
종료시 <Quit>를 누르세요.

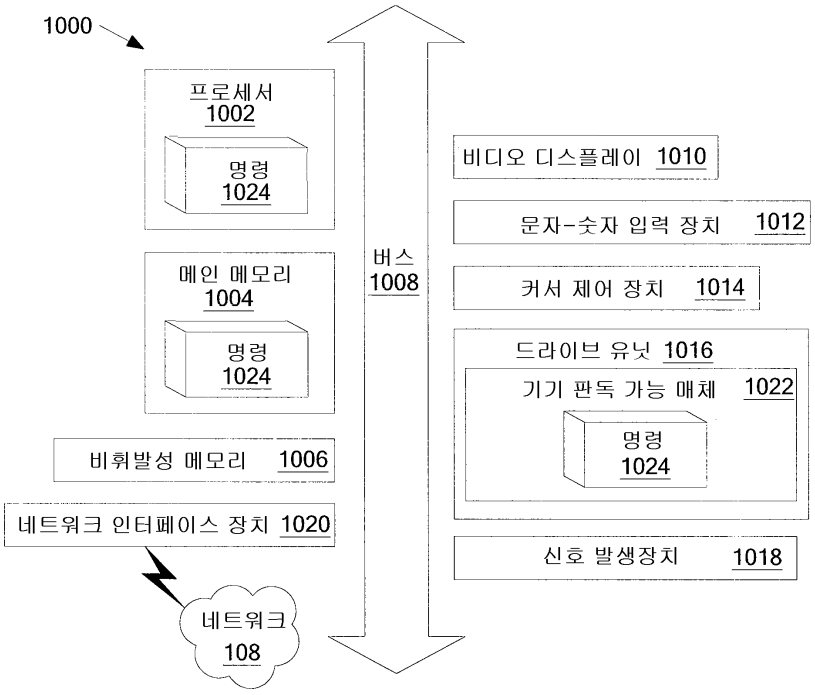
도면8


Hint:
Ok
800

도면9


To 저장장치
메모리 모듈
제어기
오퍼레이팅 시스템
암호화 모듈
KEY
프로세싱 유닛 902
암호화/복호화 모듈
무선 모듈
소프트웨어 모듈
To 호스트 시스템
인터셉터 모듈 104

도면10


1000
프로세서
1002
명령
1024
메인 메모리
1004
명령
1024
비휘발성 메모리 1006
네트워크 인터페이스 장치 1020
네트워크
108
버스
1008
비디오 디스플레이 1010
문자-숫자 입력 장치 1012
커서 제어 장치 1014
드라이브 유닛 1016
기기 판독 가능 매체 1022
명령
1024
신호 발생장치 1018