(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월18일
(11) 등록번호 10-1213807
(24) 등록일자 2012년12월12일

(51) 국제특허분류(Int. Cl.)
G06F 21/04 (2006.01) *G06F 11/30* (2006.01)
(21) 출원번호 10-2007-7012294
(22) 출원일자(국제) 2005년12월20일
심사청구일자 2010년12월13일
(85) 번역문제출일자 2007년05월31일
(65) 공개번호 10-2007-0097031
(43) 공개일자 2007년10월02일
(86) 국제출원번호 PCT/US2005/046091
(87) 국제공개번호 WO 2006/071630
국제공개일자 2006년07월06일
(30) 우선권주장
11/021,021 2004년12월23일 미국(US)
(56) 선행기술조사문헌
US20020184482 A1*
WO2003030434 A2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
프랭크, 알렉산더
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
잉글랜드, 파울
미국 98052-6399 워싱턴주 레드몬드 원 마이크로소프트 웨이
(74) 대리인
제일특허법인

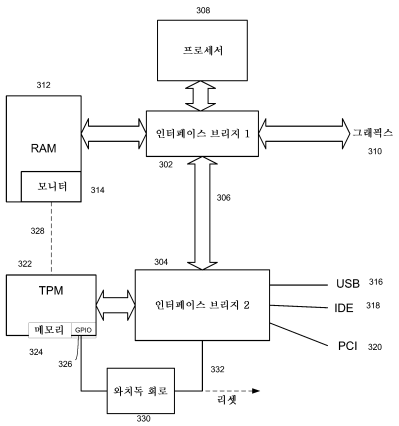
전체 청구항 수 : 총 9 항 심사관 : 신상길

(54) 발명의 명칭 **컴퓨터, 컴퓨터에 공지된 동작 상태를 행하게 하는 방법 및와치독 회로**

(57) 요 약

공지의 모니터를 검증하는 데에 이용되는 신뢰 환경을 포함함으로써 컴퓨터가 공격으로부터 안전할 수 있다. 이 모니터는 소정의 상태 집합으로의 부합을 위해 컴퓨터의 상태를 판정하는 데에 이용될 수 있다. 이 상태들은 PPU를 위해 이용가능한 신용장과 같은 사용을 의미하는 용어에 관련될 수 있으며, 혹은 컴퓨터가 바이러스 보호 프로그램과 같은 특정 소프트웨어를 실행시키는 상태, 또는 인증되지 않은 주변장치가 공격받지 않는 상태 또는 요구된 토큰이 존재하는 상태와 관련될 수 있다. 모니터는 신뢰 환경을 통하거나 혹은 직접 와치독 회로에 신호를 전송할 수 있다. 와치독 회로는, 소정의 타임아웃 기간 내에 이 신호를 수신받지 못할 경우 컴퓨터의 사용을 중단시킨다.

대 표 도 - 도4



특허청구의 범위

청구항 1

모니터의 동작을 강제하기(enforcing) 위한 신뢰 컴퓨팅 기반(trusted computing base)을 구현하는 컴퓨터로서,

상기 모니터를 실행시키는 프로세서;

상기 모니터를 검증하기 위해 상기 프로세서에 연결되는 신뢰 환경 - 상기 신뢰 환경은 상기 모니터로부터 메시지를 수신하도록 구성됨 - ; 및

상기 신뢰 환경에 연결되며, 기간을 결정하기 위한 타이머를 포함하는 와치독 회로 - 상기 와치독 회로는 상기 신뢰 환경이 상기 기간 내에 상기 메시지를 수신하지 않을 경우 상기 기간 후에 상기 컴퓨터의 동작을 중단시키고, 상기 신뢰 환경에 의해 서명된 재시작 신호가 검증되는 경우 상기 와치독 회로는 상기 서명된 재시작 신호를 수신하여 상기 타이머를 재시작시킴 -

를 포함하는, 컴퓨터.

청구항 2

제1항에 있어서,

상기 신뢰 환경은 상기 모니터를 암호화 방식으로(cryptographically) 식별하는, 컴퓨터.

청구항 3

제1항에 있어서,

상기 신뢰 환경은 범용 입/출력 포트를 더 포함하며, 상기 모니터는 암호화 방식으로 식별된 후에 상기 범용 입/출력 포트에 액세스할 수 있는, 컴퓨터.

청구항 4

제1항에 있어서,

상기 신뢰 환경은 전용 통신 링크를 통해 상기 와치독 회로에 결합되는, 컴퓨터.

청구항 5

제1항에 있어서,

상기 와치독 회로는, 상기 컴퓨터의 동작을 중단시킬 때 상기 컴퓨터로 하여금 재부팅하게 하는, 컴퓨터.

청구항 6

제5항에 있어서,

상기 컴퓨터로 하여금 재부팅하게 하는 신호는 전도체 상에서 전달되며, 상기 전도체는 탬퍼링(tampering)을 방지하도록 구성되는 컴퓨터.

청구항 7

제1항에 있어서,

상기 모니터는 상기 메시지 전송과 함께 적어도 한번 토큰을 검증하는, 컴퓨터.

청구항 8

제7항에 있어서,

상기 토큰은, 상기 모니터가 현재 버전인지 여부를 판단함에 있어 상기 모니터에 의해 사용되는 버전 번호를 포함하는, 컴퓨터.

청구항 9

컴퓨터에 이미 알려진 동작 상태를 행하게 하는 방법으로서,

이미 알려진 모니터의 신뢰성을 검증하는 단계;

상기 이미 알려진 모니터를 실행시키는 단계;

상기 이미 알려진 모니터로부터의 신호를 와치독 회로로 전송하기 전에 상기 신호를 신뢰 환경으로 전송하는 단계; 및

상기 신호에 응답하여 상기 와치독 회로가 상기 컴퓨터의 동작을 중단시키는 것을 방지하는 단계

를 포함하는, 컴퓨터에 이미 알려진 동작 상태를 행하게 하는 방법.

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

명 세 서

배 경 기 술

[0001] 퍼스널 컴퓨터와 같은 컴퓨팅하 장치에서 사용하기 위한 신뢰 플랫폼 모듈(trusted platform module; TPM)이 공지되어 있다. TPM의 목적은, 거래, 애플리케이션 및 매체의 라이센싱, 사용자 데이터 보호, 및 특수 기능과 관련된 보안 서비스 및 컴퓨터 아이덴티티를 제공하는 것이다.

[0002] 신뢰 플랫폼 모듈은 상업적으로 이용가능하며, 예를 들어 TPM은 STM Microelectronics의 ST19WP18 모듈로부터 입수가능하다. TPM은 키들을 저장하며 후속하여 이 키들을 이용하여 애플리케이션 프로그램, BIOS 정보, 또는 아이덴티티를 인증한다. 그러나, TPM의 사용은 자발적인 것이며, 현재의 규격 및 구현예와 예측되는 규격 및 구현예에 따르면 TPM은 컴퓨팅 장치에 대해 소정의 상태가 되도록 명령하는(mandate) 데에 이용될 수 없다. 몇몇 비즈니스 모델에서는, 컴퓨터가 컴퓨터 소유자/제공자의 직접적인 제어에서 벗어나 있는 방식을 취하는데, 예로서 사용량별 요금 지불 방식(pay-per-use; PPU) 비즈니스 모델을 들 수 있다. 이러한 예에서, TPM 서비스의 서컴벤션(circumvention)이 발생할 가능성이 있으며, 서컴벤션이 발생한 경우 그 비즈니스에 바람직하지 못한 악영향을 미칠 수 있다.

발명의 상세한 설명

[0003] 컴퓨팅 장치에 대해 강제로 소정의 상태들이 되게 하는 모니터 프로그램을 인증하는 데에 신뢰 플랫폼 모듈(TPM)이 이용될 수 있다. TPM에 주입되거나 기입된 소유자 키들이 그 소유자에 의해 승인된 모니터가 동작할 것을 요청하는 데에 이용될 수 있다. 그 후, 승인된 모니터는 모니터의 승인된 상태에 의해 TPM의 자원에 액세스할 수 있다. 이러한 TPM의 보안 자원은, 예를 들면 범용 입/출력(general purpose input/output; GPIO) 포트일 수 있다. 설정된 기간 내에 GPIO를 이용하여 수신된 신호에 의해 와치독 타이머가 재시작하지 않으면, 상기 설정된 기간이 만료되는 순간 컴퓨터를 리셋하도록 하는 간단한 와치독 타이머가 구성될 수 있다.

[0004] 컴퓨터를 이러한 방식으로 구성함으로써, TPM은 알려진 모니터가 가동되고 있음을 보장하는 것을 돕는 데에 이용될 수 있으며, 와치독 타이머는 모니터와 TPM 양쪽 모두가 디스에이블되거나 탬퍼링(tampering)되지 않도록 보장하는 것을 돕는 데에 이용될 수 있다.

실 시 예

[0012] 다음 본문은 다수의 서로 다른 실시예의 상세한 설명을 개시하지만, 상세한 설명의 법적 범위는 본 개시 내용의 끝에 개시되는 청구항의 표현에 의해 정의된다는 것을 이해해야 한다. 모든 가능한 실시예를 설명하는 것이 불가능한 것은 아니지만 무익할 것이므로, 상세한 설명은 단지 예시적인 것으로서 해석되어야 하고, 모든 가능한 실시예를 설명하지는 않는다. 다수의 다른 실시예는 본 발명의 청구의 범위와 여전히 부합하게 될 본 특허 출원의 출원일 이후에 개발될 기술이나 현재 기술을 이용하여 구현될 수 있다.

[0013] 또한, "본원에서 개시된, 용어 '___'는 여기서 ...를 의미하도록 정의된다"라는 문장이나 유사한 문장을 이용하여 본 특허 출원에서 소정의 용어를 명백히 정의하지 않는 한, 그 용어의 의미를 자신의 평이한 또는 통상의 의미를 넘어 명백히 또는 암시적으로 제한하려는 의도는 아니고, 이와 같은 용어는 (본 발명의 청구항의 표현을 제외한) 본 특허 출원의 임의 섹션에서 이루어진 임의의 서술에 기초하여 범위를 제한하려는 것으로 해석되지 않아야 함을 이해해야 한다. 본 특허 출원에서 단일 의미와 양립 가능하도록 본 특허 출원의 말미에 있는 청구항에서 인용되는 임의의 용어를 지칭하는 범위까지는, 단지 독자가 혼동하지 않도록 명확히 하기 위해 행해지지만, 이와 같은 청구항 용어는 그 단일 의미에 암시나 다른 방법에 의해 제한되지 않는 것으로 의도된다. 결국, 어떤 구조도 인용함 없이 기능 및 "수단"이란 단어를 인용함으로써 청구항 요소를 정의하지 않는 한, 임의의 청구항 요소의 범위는 미국 특허법 제112조 제6항을 적용하여 해석되어야 하는 것으로 의도되지 않는다.

[0014] 본 발명의 기능 중 대부분과 본 발명의 원리 중 대다수는 주문형 집적 회로(IC)와 같은 집적 회로와 소프트웨어 프로그램이나 명령어에서 가장 잘 구현되거나 이를 이용하여 가장 잘 구현된다. 당업자는, 예를 들어, 가용 시간, 현재 기술 및 경제적 고려에 의해 영향을 받아 상당한 노력과 다수의 설계 선택이 필요하더라도, 본원에서 개시된 개념과 원리에 의해 도움을 받을 때, 이와 같은 소프트웨어 명령어와 프로그램 및 IC를 최소의 실험으로 쉽게 생성할 수 있을 것이다. 따라서, 본 발명에 따른 원리와 개념을 불명료하게 할 위험의 최소화와 간결을 위해, 만약 있더라도, 이와 같은 소프트웨어와 IC의 추가 설명은 본 발명의 바람직한 실시예의 원리와 개념과 관련하여 필수적인 것으로 한정될 것이다.

[0015] 도 1은 동적 소프트웨어 프로비저닝 시스템을 구현하는데 이용될 수 있는 네트워크(10)를 도시한다. 네트워크(10)로는 인터넷, 가상 사설 네트워크(virtual private network; VPN), 또는 하나 이상의 컴퓨터, 통신 장치, 데이터베이스 등을 서로 통신 가능하게 접속하는 임의의 다른 네트워크가 있다. 네트워크(10)는 이더넷(16), 라우터(18) 및 지상선(20)을 통해 퍼스널 컴퓨터(12)와 컴퓨터 단말기(14)에 접속될 수 있다. 한편, 네트워크(10)는 무선 통신국(26)과 무선 링크(28)를 통해 랩톱 컴퓨터(22)와 PDA(24)에 무선으로 접속될 수 있다. 이와 유사하게, 서버(30)는 통신 링크(32)를 이용하여 네트워크(10)에 접속될 수 있고, 메인프레임(34)은 다른 통신

링크(36)를 이용하여 네트워크(10)에 접속될 수 있다.

[0016] 도 2는 컴퓨터(110)의 형태인 컴퓨팅 장치를 도시한다. 컴퓨터(110)의 구성 요소는 처리 장치(120), 시스템 메모리(130), 및 시스템 메모리를 포함한 여러 시스템 구성 요소를 처리 장치(120)에 연결하는 시스템 버스(121)를 포함할 수 있지만, 이에 한정되지는 않는다. 시스템 버스(121)는 다양한 버스 아키텍처 중 임의의 버스 아키텍처를 이용하는 메모리 버스 또는 메모리 제어기, 주변장치 버스, 및 로컬 버스를 포함한 여러 타입의 버스 구조 중 임의의 버스 구조일 수 있다. 일 례로서, 이와 같은 아키텍처는 산업 표준 아키텍처(Industry Standard Architecture; ISA) 버스, 마이크로 채널 아키텍처(Micro Channel Architecture; MCA) 버스, 확장 ISA(Enhanced ISA; EISA) 버스, 비디오 전자공학 협회(Video Electronics Standards Association; VESA) 로컬 버스, 및 메자닌(mezzanine) 버스로도 공지되어 있는 주변장치 구성요소 상호접속(Peripheral Component Interconnect; PCI) 버스를 포함하지만, 이에 한정되지는 않는다.

[0017] 통상, 컴퓨터(110)는 다양한 컴퓨터 판독 가능 매체를 포함한다. 컴퓨터 판독 가능 매체는 컴퓨터(110)에 의해 액세스될 수 있는 임의의 이용 가능한 매체일 수 있으며, 휘발성 및 비휘발성 매체, 이동식 및 고정식 매체를 포함한다. 일 예로서, 컴퓨터 판독 가능 매체는 컴퓨터 기억 매체 및 통신 매체를 포함할 수 있지만, 이에 한정되는 것은 아니다. 컴퓨터 기억 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 기억하기 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 이동식 및 고정식 매체를 포함한다. 컴퓨터 기억 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital versatile disks) 또는 기타 광 디스크 기억장치, 자기 카세트, 자기 테이프, 자기 디스크 기억장치 또는 기타 자기 기억장치, 또는 원하는 정보를 기억하는데 이용될 수 있으며 컴퓨터(110)에 의해 액세스될 수 있는 임의의 다른 매체를 포함하지만, 이에 한정되지는 않는다. 통상, 통신 매체는 반송파 또는 기타 전송 메커니즘과 같은 변조된 데이터 신호로 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터를 구현하며, 임의의 정보 전달 매체를 포함한다. "변조된 데이터 신호"란 용어는 신호 내의 정보가 인코드되도록 그 신호의 하나 이상의 특성을 설정 또는 변경시킨 신호를 의미한다. 일 예로서, 통신 매체는 유선 네트워크 또는 직접 유선(direct-wired) 접속과 같은 유선 매체와, 음향, 무선 주파수, 적외선 및 기타 무선 매체와 같은 무선 매체를 포함하지만, 이에 한정되지는 않는다. 또한, 상기 매체의 임의의 조합도 컴퓨터 판독 가능 매체의 범위 내에 포함된다.

[0018] 시스템 메모리(130)는 ROM(131) 및 RAM(132)과 같은 휘발성 및/또는 비휘발성 메모리의 형태인 컴퓨터 기억 매체를 포함한다. 통상, 예를 들어, 시동 동안, 컴퓨터(110) 내의 요소 간의 정보 전달을 돕는 기본 루틴을 포함하는, 기본 입출력 시스템(133; BIOS)이 ROM(131)에 기억된다. 통상, RAM(132)은 처리 장치(120)에 의해 현재 동작 상태에 있고/있거나 즉시 액세스할 수 있는 데이터 및/또는 프로그램 모듈을 포함한다. 일 예로서, 도 2는 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136), 및 프로그램 데이터(137)를 포함하지만, 이에 한정되지는 않는다.

[0019] 또한, 컴퓨터(110)는 다른 이동식/고정식, 휘발성/비휘발성 컴퓨터 기억 매체를 포함할 수도 있다. 일 예로서, 도 2는 고정식, 비휘발성 자기 매체로부터 판독하거나 이에 기입하는 하드 디스크 드라이브(141), 이동식, 비휘발성 자기 디스크(152)로부터 판독하거나 이에 기입하는 자기 디스크 드라이브(151), 및 CD ROM 또는 다른 광 매체와 같은 이동식, 비휘발성 광 디스크(156)로부터 판독하거나 이에 기입하는 광 디스크 드라이브(155)를 도시한다. 예시적인 운영 환경에서 이용될 수 있는 다른 이동식/고정식, 휘발성/비휘발성 컴퓨터 기억 매체는 자기 테이프 카세트, 플래시 메모리 카드, DVD, 디지털 비디오 테이프, 고체 상태 RAM, 고체 상태 ROM 등을 포함하지만, 이에 한정되지는 않는다. 통상, 하드 디스크 드라이브(141)는 인터페이스(140)와 같은 고정식 메모리 인터페이스를 통해 시스템 버스(121)에 접속되고, 통상, 자기 디스크 드라이브(151)와 광 디스크 드라이브(155)는 인터페이스(150)와 같은 이동식 메모리 인터페이스에 의해 시스템 버스(121)에 접속된다.

[0020] 상술한 도 2에 도시되어 있는 드라이브와 그 연관된 컴퓨터 기억 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 기타 데이터의 기억을 컴퓨터(110)에 제공한다. 도 2에서, 예를 들어, 하드 디스크 드라이브(141)는 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146), 및 프로그램 데이터(147)를 기억하는 것으로서 도시되어 있다. 이들 구성 요소는 운영 체제(134), 애플리케이션 프로그램(135), 기타 프로그램 모듈(136), 및 프로그램 데이터(137)와 동일하거나 다를 수 있다는 것에 주목하자. 본원에서, 운영 체제(144), 애플리케이션 프로그램(145), 기타 프로그램 모듈(146), 및 프로그램 데이터(147)에는 서로 다른 번호가 주어져서, 적어도, 이들이 서로 다른 사본임을 나타낸다. 사용자는 통상, 마우스, 트랙볼 또는 터치 패드로 지칭되는 포인팅 장치(161) 및 키보드(162)와 같은 입력 장치를 통해 컴퓨터(110) 내에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시안함)는 마이크, 조이스틱, 게임 패드, 위성 방송 수신용 안테나, 스캐너

등을 포함할 수 있다. 이들 및 기타 입력 장치는 시스템 버스에 연결되는 사용자 입력 인터페이스(160)를 통해 처리 장치(120)에 종종 접속되지만, 병렬 포트, 게임 포트 또는 범용 직렬 버스(USB)와 같은 기타 인터페이스 및 버스 구조에 의해 접속될 수 있다. 또한, CRT(191) 또는 다른 타입의 디스플레이 장치가 비디오 인터페이스(190)와 같은 인터페이스를 통해 시스템 버스(121)에 접속된다. 모니터에 외에도, 컴퓨터는 출력 주변장치 인터페이스(190)를 통해 접속될 수 있는 스피커(197) 및 프린터(196)와 같은 기타 출력 장치를 포함할 수 있다.

[0021] 컴퓨터(110)는 원격 컴퓨터(180)와 같은 하나 이상의 원격 컴퓨터와의 논리 접속을 이용하여 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(180)로는 개인용 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치 또는 기타 공통 네트워크 노드가 있고, 통상, 컴퓨터(110)와 관련하여 상술한 요소 중 대부분 또는 모든 요소를 포함하지만, 도 2에는 메모리 기억 장치(181)만을 도시하였다. 도 2에 도시된 논리 접속은 LAN(171) 및 WAN(173)을 포함하지만, 다른 네트워크를 포함할 수도 있다. 이와 같은 네트워킹 환경은 사무실, 기업 규모 컴퓨터 네트워크, 인트라넷 및 인터넷에서 일반적이다.

[0022] LAN 네트워킹 환경에서 이용되는 경우, 컴퓨터(110)는 네트워크 인터페이스 또는 어댑터(170)를 통해 LAN(171)에 접속된다. WAN 네트워킹 환경에서 이용되는 경우, 통상, 컴퓨터(110)는 모뎀(172) 또는 인터넷과 같은 WAN(173)을 통해 통신을 확립하기 위한 다른 수단을 포함한다. 내장형 또는 외장형일 수 있는 모뎀(172)은 사용자 입력 인터페이스(160), 또는 다른 적당한 메커니즘을 통해 시스템 버스(121)에 접속될 수 있다. 네트워크 환경에서, 컴퓨터(110), 또는 그 일부와 관련하여 도시된 프로그램 모듈은 원격 메모리 기억 장치에 기억될 수 있다. 일 예로서, 도 2는 원격 애플리케이션 프로그램(185)이 메모리 장치(181) 상에 상주하는 것으로 도시하지만, 이에 한정되지는 않는다.

[0023] 통신 접속 장치(170, 172)를 이용하여 장치들 간에 통신을 행할 수 있다. 통신 접속 장치(170, 172)는 통신 매체의 일례이다. 통상, 통신 매체는 반송파 또는 기타 전송 메커니즘과 같은 변조된 데이터 신호로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터를 구현하며, 임의의 정보 전달 매체를 포함한다. "변조된 데이터 신호"는 신호 내의 정보가 인코드되도록 그 신호의 하나 이상의 특성을 설정 또는 변경시킨 신호일 수 있다. 일 예로서, 통신 매체는 유선 네트워크 또는 직접 유선(direct-wired) 접속과 같은 유선 매체와, 음향, 무선 주파수, 적외선 및 기타 무선 매체와 같은 무선 매체를 포함하지만, 이에 한정되지는 않는다. 컴퓨터 판독가능 매체는 저장 매체 및 통신 매체 양쪽 모두를 포함할 수 있다.

[0024] 이하에서 상세히 설명되는 신뢰 플랫폼 모듈(125) 또는 그 밖의 다른 신뢰 환경은 데이터 및 키를 저장하고 실행가능 코드 및 데이터를 검증할 수 있다. 신뢰 플랫폼 모듈 사양은, 섹션 4.5.2.1에 기술되어 있다. 여기서, 시스템 초기화의 일부로서, 플랫폼 콤포넌트 및 구성의 평가가 행해질 것이다. 평가를 행하는 것은, 안전하지 않은 구성을 검출하지도 못하고, 초기화 프로세스가 계속되는 것을 방지하기 위한 조치도 취하지 못할 것이다. 이를 행하는 책임은 운영 체제와 같은 적절한 기준 모니터에 부과되어 있다. TPM은 강제 시행 툴로서 정의되지 않기 때문에, 이하에서 설명되는 또다른 개선 사항이 통상의 TPM을 보충한다.

[0025] 와치독 회로(126)는 소정의 기간을 정하여, 그 기간이 경과되면 컴퓨터(110)의 동작을 중단시키도록 하는 신호(127)를 트리거한다. 이 중단은 컴퓨터(110)가 재부팅하도록 하는 시스템 리셋일 수 있다. 이 중단은 시스템 버스(121) 또는 주변 장치 버스 상의 데이터를 인터럽트할 수 있다. 와치독 회로(126)가 컴퓨터(110)의 동작을 중단시키는 것을 방지하기 위해, 상기 기간을 리셋하고 타이밍 프로세스를 다시 시작하도록 하기 위한, 통신 접속(128)을 통한 신호가 요구될 수 있다. 도 2에 도시된 바와 같이, 와치독 타이머 리셋 신호가 통신 접속(128)을 통해 전달될 수 있다. 이하에서 보다 상세히 설명하는 바와 같이, TPM(125)은 모니터 프로그램으로부터의 신호에 응답하여 와치독 타이머를 리셋하여 초기화시킬 수 있다. 이하에서 기술되는 단계들은, 특정의 원하는 모니터가 존재하고 TPM(125)과 와치독 회로(126)의 결합을 이용하여 동작하는 것을 보장하는 것을 돕는데에 이용될 수 있다.

[0026] 도 2와 같은 대표적인 컴퓨터 내의 기능 층들을 계층적 표현으로 간략하게 나타낸 블럭도인 도 3에 대해 설명한다. 신뢰 플랫폼 모듈(202)은 BIOS(204) 아래에 존재하는 하드웨어일 수 있다. TPM(202)은 컴퓨터, 및 BIOS(204)와 같은 더 높은 수준의 동작에 대한 자원으로서 작동할 수 있다. BIOS는 모니터(206)를 활성화시킬 수 있다. 모니터(206)는 운영 체제(208) 아래에 모니터 레벨(210)에 존재한다. 모니터(206)는 TPM(202)의 자원에 액세스하여 이를 이용하여 더 높은 레벨의 엔티티의 동작과 연관된 정책들을 수행할 수 있다. 운영 체제(208)는 컴퓨터(110)의 주요 기능들을 지원하고, (초기 부트스트랩이 핸드오버 제어를 수행한 후에는) 통신, 사용자 입출력, 디스크 및 그 밖의 다른 메모리 액세스, 애플리케이션 론치 등을 담당할 수 있다. 운영 체제는 또한 TPM(202)에 직접 액세스하여 이를 이용할 수 있다. 도시된 바와 같이, 제1 및 제2 애플리케이션(212,

214)은 운영 체제(208) 상에서 실행될 수 있다. 몇몇 경우에, 모니터는 운영 체제(208) 및 애플리케이션(212, 214) 양쪽 모두에 관련된 정책들을 강제 시행할 수 있다. 예를 들면, 애플리케이션(214)이 디스크(216)로부터 론칭되기 전에, 운영 체제는 라인(218)을 통해 표시되는 라이센싱 상태를 체크하여, 애플리케이션(214)이 소정의 론칭 기준을 만족시키는지 여부를 판별할 수 있다. 론칭 기준, 및 모니터 기능을 이용한 애플리케이션의 후속 계측은, 2004년 12월 8일자로 출원된, 제목이 "Method for Pay-As-You-Go Computer and Dynamic Differential Pricing"인 미국 특허 출원(대리인 정리 번호 30835/40476)에 보다 상세히 기술되어 있다. 요약하면, 모니터(206)는, 예를 들어 PPU(pay-per-use) 또는 선불제 시나리오로 애플리케이션 프로그램, 유틸리티 및 컴퓨터 자원을 평가하고 계측하는 데에 이용될 수 있다.

[0027] 도 6을 간단히 참조하여, TPM(202)에 대해 보다 상세히 기술한다. TPM(202)은, 휘발성 메모리 및 비휘발성 메모리 양쪽 모두를 포함하는 내부 메모리(502)를 구비할 수 있으며, 이들의 적어도 일부는 탬퍼링 또는 승인되지 않은 기록 동작으로부터 보안될 수 있다. 메모리는, TPM(202)을 구성하기 위해 소유자와의 제휴(affiliation)를 청구하는 엔티티들을 입증하는 데에 이용되며 외부 엔티티와의 신뢰를 확립하기 위한 소유자 키(504)를 기억할 수 있다. 메모리는 또한 무엇보다도, 플랫폼 구성 레지스터(platform configuration register; PCR)(506)를 포함할 수 있다. PCR(506)은 해시, 또는 모니터(206)와 연관된 그 밖의 다른 강한(strong) 식별자를 저장하는 데에 이용될 수 있다. TPM(202)은 또한 시계(508) 및 암호 서비스(510)를 포함할 수 있다. 이들 둘 모두는 이하에서 보다 상세히 설명되는 인증 및 승인 프로세스에서 이용될 수 있다. TPM(202)은 또한, 종종 싱글-핀 버스(Single-pin Bus) 또는 범용 입출력(GPIO)로 칭해지는 버스(512)를 포함할 수 있다. 일실시예에서, GPIO(512)는, 다른 경우에서도 설명된 바와 마찬가지로 와치독 회로에 연결될 수 있다.

[0028] TPM(202)은 또한 컴퓨터 내에서의 데이터 통신, 예를 들면 모니터(206)를 가동시키는 프로세스를 위한 범용 버스(514)에 결합될 수 있다. 버스(514)를 이용하여, 또는 몇몇 경우 다른 메카니즘(516)을 이용하여 TPM(202)은 모니터를 평가할 수 있다. 모니터의 평가에는, 모니터의 암호화 해시의 체크, 즉 모니터가 차지하는 메모리 범위 내의 해시 체크가 포함될 수 있다. PCR은 평가 데이터(506)를 저장하는 데에 이용될 수 있다. 소유자 키(504)는, 예를 들어 확인을 위해 소유자 키(504)를 요구하는 모니터의 디지털 서명된 해시에 의해 모니터(506)의 해시와 제휴할 수 있다. 소유자 키(504)는 제조시에, 또는 후에(예를 들면 고객에게 전달할 때) TPM(202)에 기입되거나 또는 주입될 수 있다. 그 후, 소유자 키(504)는 모니터(206)의 인증에 이용된다.

[0029] 예시적인 실시예에서, 모니터(206)는 예를 들어 BIOS(204)에 의한 부팅 시퀀스에서 이에 선행하는 신뢰 모듈에 의해 평가된다. BIOS(204)에 의해 산출된 해시 등의 모니터 평가가 버스(514)를 통해 TPM의 PCR(506) 내에 저장될 수 있다. TPM(202)이 그 평가(해시)의 정당성을 입증하면, TPM(202)은 모니터(206)로의 액세스를 허용하여 고유 키 및/또는 그 밖의 비밀물(secrets)이 모니터(206)에 할당되고 TPM(202)에 저장된다. TPM(202)은, 모니터의 평가가 일치하는 모든 모니터에 대응 키 및 비밀물을 할당할 것이다.

[0030] TPM은 소유자 키(504) 및 대응 모니터 측정치(506), 즉 공지된 모니터(206)의 해시로 프로그래밍될 수 있다. 소유자 키는 모니터 측정치(506)를 프로그래밍하거나 갱신하는 데에 이용되어 소유자 키(504)를 소유한 엔티티만 공지된 모니터(206)에 대한 PCR 레지스터(506)를 설정할 수 있다. 표준 TPM(202)은, 소정의 평가(506)에 대하여 검증된 모니터(206)만 GPIO(512)를 제어할 수 있게 하는 특징을 갖고 있다. GPIO(512)가 탬퍼 방지(tamper-resistant) 방식으로 와치독 회로(126)에 접속되어 있는 경우, 신뢰 사슬이 완성될 수 있다. 즉, 검증된 모니터(206)만이 GPIO(512)를 제어할 수 있으며, GPIO(512)만이 와치독 회로(126)를 재시작시키는 데에 이용될 수 있다. 따라서, 모니터(206)가 교체되거나 변경될 때, 소유자 키(504)에 의해 설정된 PCR(506)에 의해 검증된 모니터(206)만이 와치독 회로(126)의 타이머를 재시작시키는 데에 이용될 수 있다. 따라서, 예를 들어 컴퓨터(110)를 리셋시켜 와치독 회로가 컴퓨터(110)를 중단시키는 것을 방지하는 데에는 인증된 모니터만이 이용될 수 있다. 와치독 회로(126)의 타이머는, 오류가 있거나 탬퍼링된 컴퓨터(110)의 복원을 허용하면서 중요한 유용한 작업이 컴퓨터(110) 상에서 행해지는 것을 방지하기에 충분히 짧도록 선택된 기간으로 설정될 수 있다. 예를 들면, 검증된 모니터(206)에 의해 재시작되지 않는 한, 와치독 회로는 컴퓨터(110)의 동작을 10-20초마다 중단시키도록 설정될 수 있다.

[0031] 소유자 비밀물(504) 및 모니터 평가(506)는 안전한 제조 환경에서 프로그래밍될 수 있거나, 혹은 소유자 키(504)를 프로그래밍하는 엔티티에 알려진 전송 키를 이용하여 필드 프로그래밍될 수 있다. 소유자 키(504)가 일단 알려지면, 프로그래밍 엔티티, 예를 들면 서비스 제공자는, 어떤 모니터에 GPIO 버스에 대한 액세스 권한이 부여되는지를 판정할 모니터 평가를 설정할 수 있다. 소유자 키(504)는 소유자 키를 재프로그래밍하도록 요구될 수 있다. 로컬 소유자 키(504)가 타협되는 경우, 도출된 키를 이용하여 키 배포, 스케일링 및 확산 손

실로부터의 보호를 용이하게 행할 수 있다. 키 관리 기술은 데이터 보안 업계에 공지되어 있다.

[0032] 도 4는 컴퓨터(110)와 동일하거나 유사한 컴퓨터(300)의 대표적인 아키텍처를 블럭도로 나타낸 도면이다. 컴퓨터는 제1 및 제2 인터페이스 브리지(302, 304)를 가질 수 있다. 인터페이스 브리지(302, 304)는 고속 버스(306)에 의해 접속될 수 있다. 제1 인터페이스 브리지(302)는 프로세서(308), 그래픽 제어기(310) 및 메모리(312)에 접속될 수 있다. 메모리(312)는 모니터 프로그램(314)을 호스팅할 수 있으며, 또한 그 밖의 다른 범용 메모리가 이용될 수도 있다.

[0033] 제2 인터페이스 브리지(304)는 주변 버스 및 컴포넌트, 예를 들면 USB(universal serial bus)(316), IDE(Integrated Drive Electronics)(318), 또는 디스크 드라이브, 프린터, 또는 스캐너 등을 접속하는 데에 이용되는 PCI(Peripheral Component Interconnect)(320)에 접속될 수 있다. 제2 인터페이스 브리지는 또한 TPM(322)에 접속될 수 있다. 전술한 바와 같이, TPM(322)은 키 및 해시 데이터를 위한 보안 메모리(324), 및 범용 입출력(GPIO)(326)을 구비할 수 있다. TPM(322)은 접속(328)에 의해 물리적 또는 논리적으로 모니터에 접속될 수 있다. 전술한 바와 같이, BIOS(204)는 모니터(206)를 평가하고 이 평가를 TPM(322)에 저장할 수 있으며, TPM(322)은 제공된 평가에 대응하는 키 및 비밀물을 모니터(314)에 할당한다. 이에 따라, 모니터(314)에는, 이들 키 및 비밀물로 잠금된 데이터 및 자원에 대한 액세스 권한이 주어진다. 접속(328)은 또한, 신호를 와치독 회로(330)에 전송하기 위해 모니터가 GPIO(326)를 제어하는 데에 이용될 수 있다. 이 신호는 와치독 회로를 리셋시킬 수 있다. 이 신호가 와치독 회로(330) 내의 설정에 의해 금지된 기간 내에 와치독 회로(330)에 수신되지 않는 경우, 리셋 또는 그 밖의 동작 중단 신호가 접속(332)을 통해 전송될 수 있다. 탬퍼링을 억제하기 위해, GPIO(326)와 와치독 회로(330) 간의 접속이, 예를 들면 회로 기판 레이어들 간의 포팅 또는 라우팅에 의해 보호되어 와치독 회로(330)가 수동으로 재시작되는 것을 방지할 수 있다. 컴퓨터 리셋 신호 접속(332), 또는 와치독 회로(330)와 메인 프로세서 컴퓨터 리셋 포인트(도시하지 않음) 사이의 컴퓨터 리셋 신호 접속(332)의 적어도 일부가 마찬가지로 탬퍼링으로부터 보호될 수 있다.

[0034] 도 5는 도 2의 컴퓨터의 다른 아키텍처의 대표적인 블럭도이다. 도 4의 설명과 비교하여 동일한 참조 부호는 동일한 컴포넌트를 나타낸다. 와치독 회로(330)가 제2 인터페이스 브리지(304) 내로 이동하여서, 와치독 회로(330)가 다른 회로에 결합되어 탬퍼링 방지를 향상시키는 방법을 대표예로서 나타낸다. 와치독 회로(330)의 제2 인터페이스 브리지 칩(304)으로의 통합은 그 자체로 적절하지만 단지 일례일 뿐이다. 제2 인터페이스 브리지(304)는 컴퓨터 아키텍처의 주 컴포넌트이기 때문에, 제2 인터페이스 브리지(304) 내에서 원하는 레벨의 동작 중단이 실행될 수 있다. 따라서, 접속(332)과 같은, 제2 인터페이스 브리지(304)의 외부의 와치독 회로가 요구되지 않을 수 있다.

[0035] 이 다른 아키텍처에서, GPIO(326)는 와치독 회로(330)에 리셋을 신호하는 데에 이용되지 않을 수도 있다. 대신에, 논리 접속(334)을 통해 모니터(314)로부터 와치독 회로(330)에 직접 메시지가 전송될 수 있다.

[0036] 두 개의 엔티티들(314, 330) 간에 충분한 레벨의 신뢰가 존재하지 않을 수 있기 때문에, TPM(322)에 유지된 키들을 이용하여 메시지가 서명될 수 있다. 예를 들면, (예를 들면, 제조 라인 상에서, 신뢰성을 위해) 이들 키들은 제1 부팅 동안 모니터(314)와 연관될 수 있다. 키들은 임의적으로 할당될 수 있으며, 혹은 전술한 바와 같이, 키들은 루트 증명서, 일련 번호 또는 제조 시퀀스 번호 등과 같은 공지의 데이터 및 마스터 키로부터 계층적으로 도출될 수 있다. 와치독 타이머(330)는 예를 들면, 어셈블리 라인 상에서 컴퓨터(110)의 제1 부팅 동안, 이들 키들을 이용하여 서명된 메시지들만을 고려하도록 구성될 수 있다. 또한, 모니터는 이들 키들을 TPM(322)으로 잠궈서, 동일한 것으로 평가된 모니터(314)만이 이들 키들에 액세스하게 한다. 이 아키텍처의 변형예는, 모니터가 TPM(322)에 의지하여 이들 키들을 고유하고 개별적으로 그 평가에 할당하는 것이다.

[0037] 통상 동작 동안, 모니터(314)는 와치독 타이머(330)에게 보내질 메시지를 대신에 서명하도록 TPM(322)에게 요청할 수 있다. TPM(322)은 (각 부팅 동안 BIOS에 의해 TPM(322)에 저장된 그 평가마다) 모니터(314)에 대응하는 키들로 메시지를 서명한다. 모니터(314)는 논리 접속, 예를 들면 접속(328)을 통해 TPM(322)으로부터 서명된 메시지를 수신한 후, 이를 논리 접속(334)을 통해 와치독 회로(330)에 제공할 수 있다.

[0038] 와치독 회로(330)가 이 메시지를 수신하면, 와치독 회로(330)는 (제조 중에 설정된) 키들을 이용하여 이 메시지를 인증할 수 있다. 이와 다르게는, 논리 접속(336)을 이용하여 TPM(322) 내의 키 또는 비밀물을 이용하여 검증을 요구할 수 있다. 다른 모니터가 실행되고 있는 경우, 이 다른 모니터는 다르게 평가하여 서로 다른 키들 및 비밀물이 TPM에 의해 할당될 것이다. 따라서, 다른 모니터는 이 메시지를 적절하게 서명할 수 없어서 이는 와치독 회로(330)에 의해 증명될 것이다. 결국, 와치독 회로(330)는 그 타이밍 기간이 경과한 후에 컴퓨터 리셋의 발화와 같은 제재(sanction)를 개시할 것이다. 서명되거나 암호화된 메시지를 이용하면, 논리 접속(328,

334)에 대한 공격 위험을 감소시킬 수 있다.

[0039] 모니터를 이용하여 신뢰 플랫폼 모듈(TPM)을 항상 "온(on)"으로 잠그기 위한 방법을 플로우차트로 예시하는 도 7에 대해 설명하기로 한다. 전형적인 TPM, 예를 들면 TPM(125)은 사용자에 의해 선택적으로 인에이블될 수 있다. 후술하는 바와 같이, 이 방법은, 컴퓨터(110)의 중단과 같은 제재의 위험을 무릅쓰고 TPM(125)이 인에이블된 채로 남아 있게 하고, 비즈니스 소유자에 의해 선택된 모니터(206)가 실행되게 하는 양쪽 모두를 보장하는 것을 도울 것이다.

[0040] 개시 단계 402에서 전원의 투입으로 시작되어, 컴퓨터(110)가 통상의 부팅 메카니즘으로 여러 하드웨어 컴포넌트들을 초기화할 수 있다. 이는 TPM(322)에도 마찬가지로 적용된다. 부팅 시퀀스는 TCPA(Trusted Computing Platform Alliance) 방법을 따를 수 있다. 단계 403에서는, CRTM(Core Root of Trust for Measurements)(도시하지 않음)이 BIOS(133)를 평가하고 그 평가를 TPM(322)에 저장한다. 그 후, CRTM은 BIOS(133)를 로드 및 실행한다(이상적으로는 CRTM은, 공격에 거의 노출당하지 않는, 컴퓨터(110) 내의 신뢰할만한 장소에 저장될 수 있다).

[0041] BIOS(133)는, 각 소프트웨어 모듈을 로딩 및 실행하기 전에 평가할 수도 있다는 점을 제외하고는, 통상의 방식으로 실행되어 각종 컴퓨터 컴포넌트들을 초기화하고 열거(enumerating)한다. 또한, BIOS(133)는 이들 평가를 TPM(322)에 저장할 수 있다. 특히, 단계 405에서, BIOS(133)는 모니터(314)를 평가하고 모니터 평가를 TPM(322)에 저장한다.

[0042] 단계 408에서, TPM(322)은 키 및 비밀물을 고유하고 개별적으로 모니터 평가에 할당한다. 단계 408에서 TPM(322)은, 주어진 평가에 대응하는 고유한 키&비밀물을 일관성있게 할당하는 것이 필수 사항이다. 따라서, 모니터(314)에 이용가능한 비밀물은 고유하고, 일관성있으며 개별적이다. 이에 따라, 어떠한 모니터라도 자원을 잠글 수 있어서 그 특정 모니터만이 그 자원을 독점적으로 이용가능하게 될 것이다. 예를 들면, 이로 인해 와치독 회로(330)에 접속된 GPIO(326)를 프로그래밍하여 진정한(genuine) 모니터(314)와 연관된 평가만이 존중됨으로써 진정한 모니터(314)를 와치독 회로(330)에 연결시키는 것이 가능하게 된다. 그 후, 진정한 모니터(314)와 동일하게 평가된 모니터만이 GPIO(326)를 이용할 수 있게 된다.

[0043] 로딩된 모니터가 진정한지 여부에 관계없이, 단계 410에서 부팅 시퀀스는 모니터를 로딩 및 실행한다. 단계 411에서 통상의 부팅 프로세스가 계속되며, 부팅이 성공한 것으로 간주되면, 단계 412에서 컴퓨터(110)의 통상적인 동작이 이어진다.

[0044] 단계 410에서 모니터(314)가 로딩 및 실행되는 즉시, 그 루프(단계 413-419)를 시작한다. 우선, 단계 413에서 모니터(314)는 TPM의 GPIO(326)를 통해 와치독 회로(330)에 메시지를 전송한다. 이 메시지는 TPM(322)에게 GPIO(326)를 이용할 것을 신호하여서 와치독 회로(330)에게 그 타이머(도시하지 않음)를 재시작하도록 신호할 수 있다.

[0045] 메시지를 TPM(322)에 전송한 후, 단계 414에서 모니터는 테스팅 상태로 되돌아간다. 단계 414에서 모니터는, 컴퓨터(110)의 상태가 현재의 정책과 부합되는지를 테스트한다. 현재의 정책에는 공지된 프로그램, 유틸리티 또는 주변 장치들이 분명하게 존재하는지 여부가 포함될 수 있다. 테스트는 계측 또는 그 밖의 다른 PPU 계량과 또한 관련될 수 있다. 예를 들면, 특정 애플리케이션 프로그램 동작에 따른, 소비를 위한 이용가능한 프로비저닝 패킷에 대해 테스트시 체크될 수 있다. 다른 실시예에서, 이 테스트는, 특정 기간(예를 들면 월 단위) 동안의 동작과 관련될 수 있다.

[0046] 단계 414의 테스트가 실패로 되면, 단계 416(아니오 브랜치)으로 진행되며, 여기서 정책에 따라 모니터가 동작한다. 이 액션은 단지 운영 체제에 전송되는 경고 코드 또는 사용자에게 제시되는 경고 메시지일 수 있다. 이 액션은 운영 체체 및 사용자에게 부과되는 소정의 제재, 예를 들면 컴퓨터의 특정 기능을 제한하거나 삭제하는 제재일 수 있다. 이는 하드웨어 및/또는 소프트웨어 기능에 적용할 수도 있다. 예를 들면, 컴퓨터의 속도가 느려지거나, 특정 소프트웨어가 기능하지 못하게 되거나, 또는 특정 장치(예를 들면 웹캠)가 기능하지 못하게 될 수 있다. OS에 이용될 수 있는 RAM의 용량을 제한하거나, 또는 운영 체제에 이용될 수 있는 명령어 집합 아키텍처(Instruction-Set-Architecture)를 감소시키는 더 혹독한 제재가 있을 수 있다. 일실시예에서, 허용되지 않는 상태가 발견되는 경우 모니터(314)가 이용할 수 있는 하나의 액션 과정은 와치독 회로(330)의 타이머를 재시작시키지 않고 와치독 회로(330)가 제재를 가하게 하는 것일 수 있다.

[0047] 테스트가 성공하는 경우, 단계 414로부터 예(YES) 브랜치로 진행될 수 있다. 어느 경우에나, 단계 413으로 리턴하기 전의 기간 동안 단계 419에서 실행을 대기한다. 이 대기 기간으로 인해 모니터(314)를 반복적으로 가동

시킴으로써 컴퓨터의 자원이 소모되는 것이 방지된다. 단계 419에서 이 대기 기간은 와치독 타이머 카운팅 기간에 비해 매우 짧은 기간이어야 함은 명백하다. 이용가능한 짧은 기간의 결정은, 컴퓨터의 통상 동작이 루프의 실행 완료를 지연시킬 수 있을 가능성이 있는 정도일 수 있다. 그 후, 이 루프는 전술한 단계 413으로 리턴한다. 이 루프를 반복하는 기간은 와치독 회로 타임아웃 기간보다 짧은 임의의 기간이 되도록 설정될 수 있으며, 그렇지 않을 경우에는 부당한 동작 중단이 발생할 수 있다.

[0048] 단계 420에서, TPM(322)이 메시지를 수신하면, TPM(322)은 모니터 평가 결과에 따라 행동한다. 단계 420에서 평가 결과에서 진짜가 아닌 것으로 간주되어 실패하면 아무 조치도 취하지 않는(즉, 와치독 회로(330)에 신호가 전송되지 않는) 박스(422)로 진행한다(아니오 브랜치). 와치독 회로(330)는, 단계들이 이를 중단하도록 취해지지 않는 한 컴퓨터(110)의 동작을 중단시킬 것이기 때문에, TPM(322)에 의한 더 이상의 액션은 요구되지 않을 수 있다. 선택적으로, 단계 422에서 TPM(322)은 경고/에러 코드를 생성하여 운영 체제에 통지하기 위한 로깅 에러를 생성할 수도 있으며 메시지를 사용자에게 디스플레이할 수도 있다.

[0049] TPM(322)이 모니터 평가 결과 진짜인 것으로 검증하는 경우, 단계 424에서 GPIO(326)는 와치독 회로(330)에게 타이머를 재시작할 것을 신호하도록 활성화될 수 있다. 전술한 바와 같이, 와치독 회로 타이머를 재시작시킴으로써 와치독 회로(330)가 컴퓨터(110)의 리셋과 같은 중단 액션을 개시하는 것을 방지하게 된다. 그 후 단계 426에서 와치독 회로(330)는 타이머를 그 초기 값에서 재시작시킬 수 있다. 그 후 단계 428에서 타이머는 카운트를 시작할 것이며 단계 430에서 소정의 시간이 경과되었는지에 대한 테스트가 행해진다. 타이머 기간은 설정 가능할 수 있다. 타이머 구현은 공지되어 있으며 타이머가 소정의 수까지 카운트되거나 제로까지 다운되거나 설정된 클럭 횟수로 카운트되거나 그 밖의 다른 메카니즘를 이용할지의 여부는 설계 선택에 달려 있다.

[0050] 타이머가 만료되지 않은 경우, 단계 430으로부터의 아니오(no) 브랜치는 도로 단계 428로 진행될 수 있으며 단계 428에서는 타이머로부터 다른 카운트를 시작할 것이다. 기간이 만료되면, 단계 430으로부터 예(yes) 브랜치가 취해질 수 있으며 단계 432에서 와치독 회로는 컴퓨터의 동작을 중단시킴으로써 제재를 가할 수 있다. 이 중단은 재부팅을 유발하는 시스템 리셋일 수 있으며, 이로 인해 주변 장치 등이 디스에이블링된다. 단계 432에서 중단으로의 카운트 다운을 위한 와치독 회로 타이머의 기간은, 사용자가 컴퓨터(110) 상의 허용되지 않는 상태를 정정하기에 충분하고, 컴퓨터(110)에 대한 신뢰성있거나 유용한 작업을 금지시키기에 충분히 짧아야 한다.

[0051] 단계 432로부터 단계 426으로의 링크는 개념적일 수 있다. 전체 컴퓨터의 리셋에 의해 동작 중단이 실시되는 경우, 이 링크는 실제적 의미가 없다. 보다 미세한 중단이 발생하는 경우, 예를 들면 컴퓨터의 속도가 느려지는 경우, 이 링크는 카운트 다운을 재시작하는 데에 이용되며, 보다 기능을 억제하는 중단, 예를 들면 리셋을 유발하게 될 수 있다.

[0052] PPU로 컴퓨터를 공급하는 것과 연관된 비즈니스 소유자 또는 그 밖의 출자자(underwriter)의 두 가지 목적이 상술한 방법에 의해 달성될 수 있음을 알 수 있다. 우선, 사용자가 TPM(322)을 이용하는 것으로부터 벗어나거나 혹은 컴퓨터가 해킹당해서 TPM(322)이 디스에이블되는 경우, 와치독 회로(330)로의 메시지가 생성되지 않을 것이며 컴퓨터(110)의 동작은 중단될 것이다.

[0053] 마찬가지로, TPM(322)이 인에이블되어 동작가능하게 되지만, 모니터가 변경되거나 교체되어 실제로 정책(예를 들면 사용 정책)이 변경되거나 무시될 가능성이 있게 되는 경우, TPM은 모니터 요구를 이행하지 않을 것이다. 실제적으로는, 변경된 모니터 평가는 진짜의 모니터의 평가와 다르다. 따라서, 모니터 평가가 TPM(322)에 저장되면, 변경된 모니터에 대해 개별적이고 고유하며 GPIO(326)의 동작에 필요한 것과 다른 키 및 비밀물 세트를 할당할 것이다. 이에 따라, 변경된 모니터로부터 TPM으로의, GPIO(326)에게 신호하기 위한 메시지가 이행되지 않을 것이다. 따라서, 와치독 회로(330)는 재시작 신호를 수신하지 않을 것이며 컴퓨터(110)의 동작은 중단될 것이다.

[0054] 양쪽 모두의 경우에, TPM(322)은 인에이블되어야 하며 진짜의 모니터(314)는 적절하게 컴퓨터(110)의 올바른 동작을 위해 동작가능하여야 한다.

[0055] 전술한 방법 및 장치들에 대한 그 밖의 다른 사용이 계획될 수 있다. 예를 들면, 부팅 프로세스의 일부는 인증된 사용자에 의한 자격 증명의 제시를 요구할 수 있다. 올바른 자격 증명이 제시되지 않을 경우, 부팅 프로세스는 진짜 모니터를 로딩하지 않을 수 있으며, 이는 최종적으로 컴퓨터(110)의 동작을 중단시킬 수 있다.

도면의 간단한 설명

[0005] 도 1은 복수의 컴퓨팅 자원을 상호접속시키는 네트워크의 블럭도.

[0006] 도 2는 본 발명의 실시예에 따른 컴퓨터를 나타내는 간략하고 대표적인 블럭도.

[0007] 도 3은 도 2의 컴퓨터 내의 기능 층들을 계층적으로 표현한 간략하고 대표적인 블럭도.

[0008] 도 4는 도 2의 컴퓨터의 컴퓨터 아키텍처의 간략하고 대표적인 블럭도.

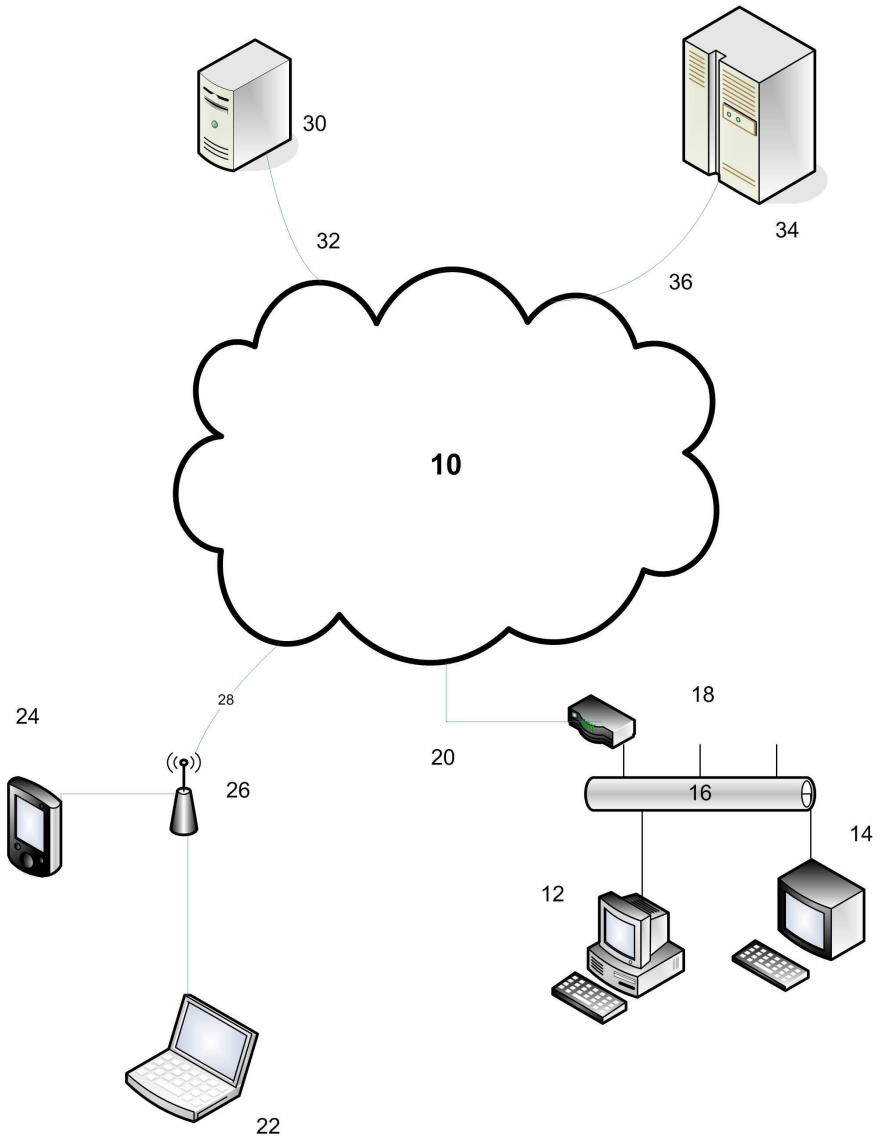
[0009] 도 5는 도 2의 컴퓨터의 다른 컴퓨터 아키텍처의 간략하고 대표적인 블럭도.

[0010] 도 6은 TPM의 간략하고 대표적인 블럭도.

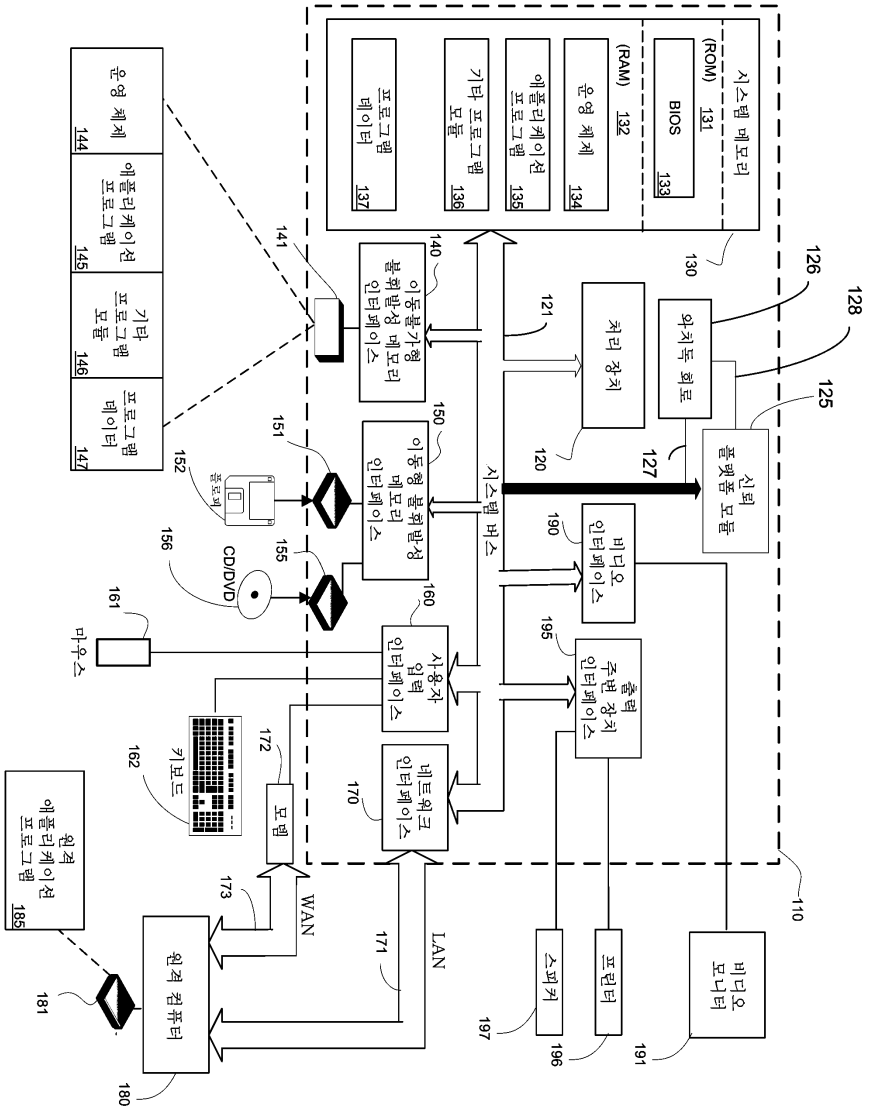
[0011] 도 7은 모니터를 이용하여 TPM을 "온"으로 잠그는(locking-on) 방법을 나타낸 흐름도.

도면

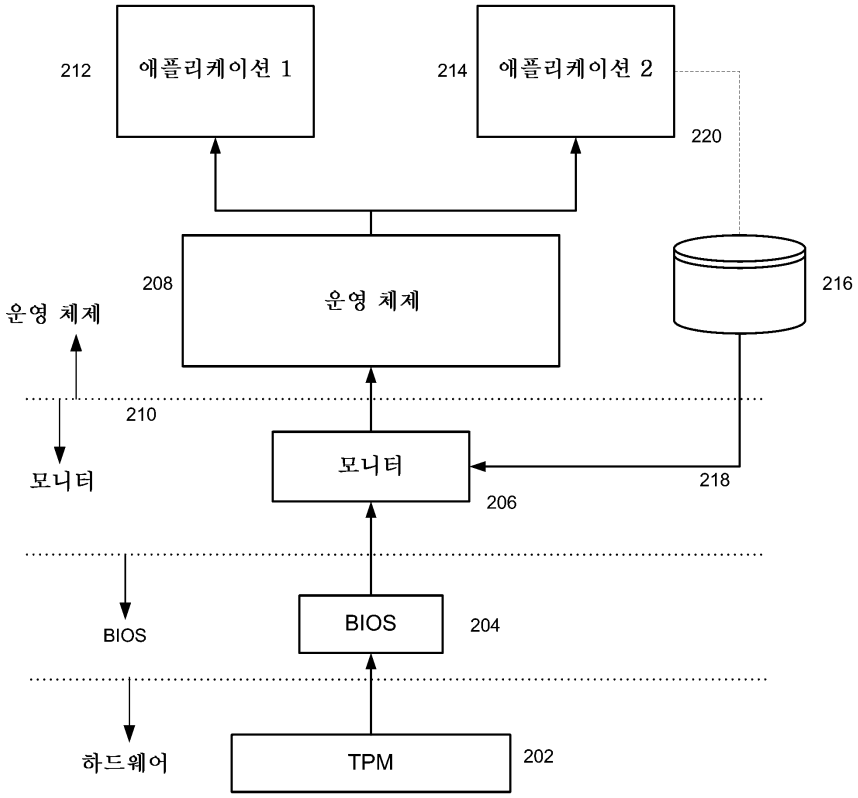
도면1



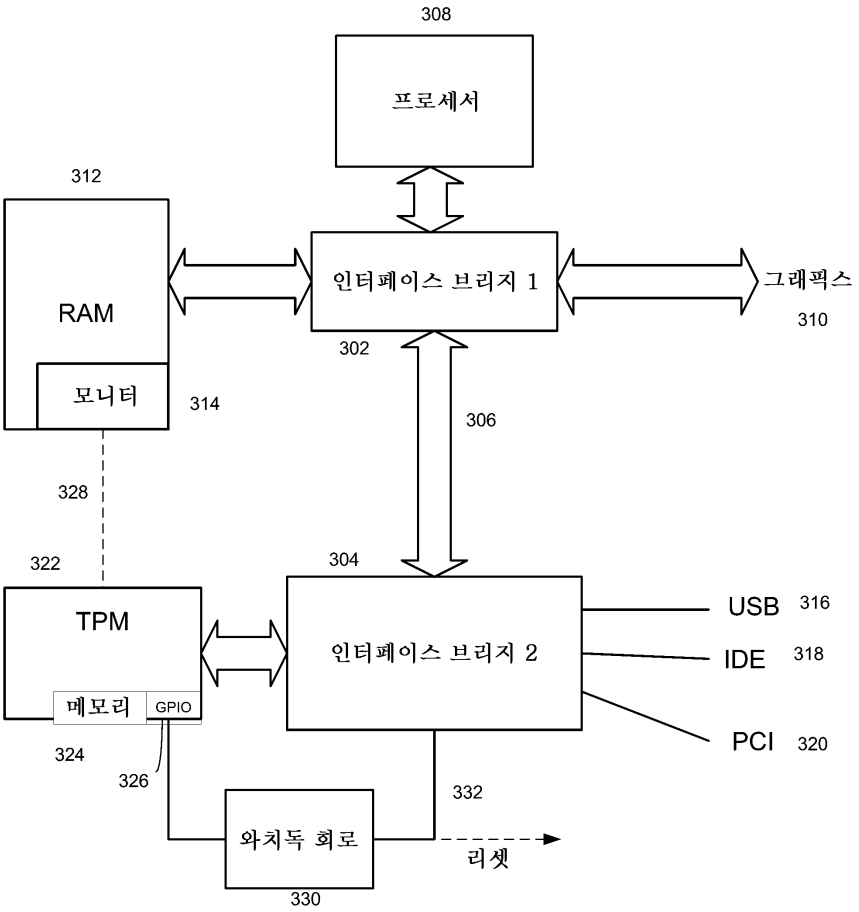
도면2


시스템 메모리
(ROM) 131
BIOS 133
(RAM) 132
운영 체제 134
응용 프로그램 135
기타 프로그램 모듈 136
프로그램 데이터 137
130
126
128
125
121
처리 장치
와치독 회로
120
127
시스템 버스
플랫폼 모듈
140
이동불가형 불휘발성 메모리 인터페이스
141
150
이동형 불휘발성 메모리 인터페이스
151
152
플로피
155
156
CD/DVD
160
161
마우스
사용자 입력 인터페이스
162
키보드
172
모뎀
170
네트워크 인터페이스
173
WAN
171
LAN
190
비디오 인터페이스
195
출력 주변 장치 인터페이스
스피커
197
196
프린터
191
비디오 모니터
110
운영 체제 144
응용 프로그램 145
기타 프로그램 모듈 146
프로그램 데이터 147
원격 응용 프로그램 185
181
원격 컴퓨터
180

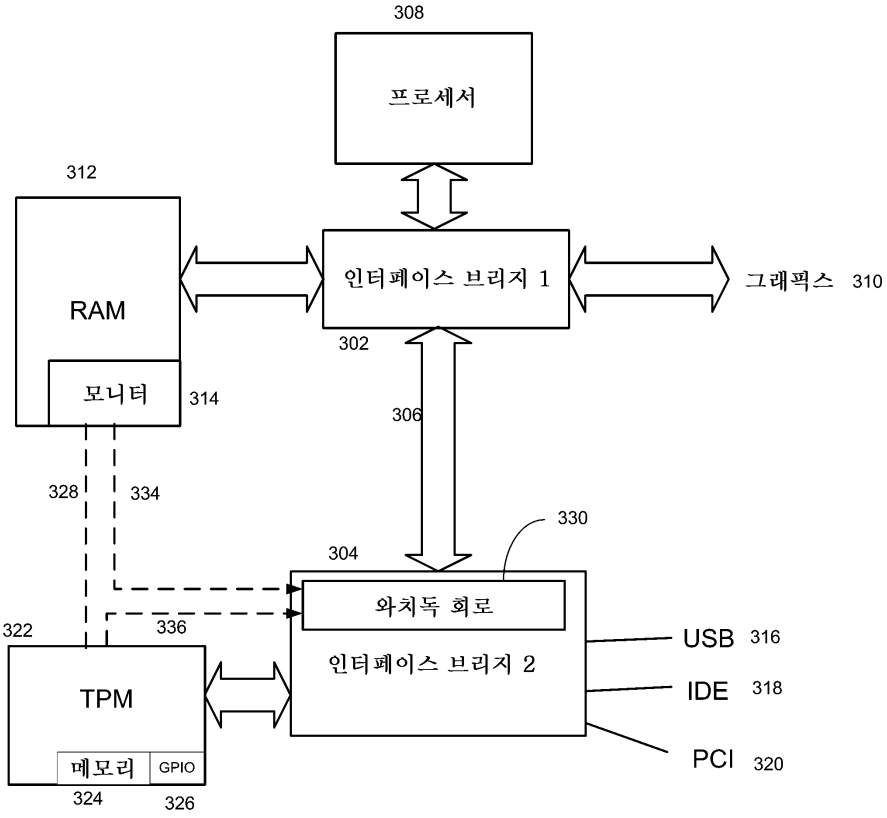
도면3


212
애플리케이션 1
214
애플리케이션 2
220
208
운영 체제
운영 체제
216
210
모니터
모니터
218
206
BIOS
BIOS
204
하드웨어
TPM
202

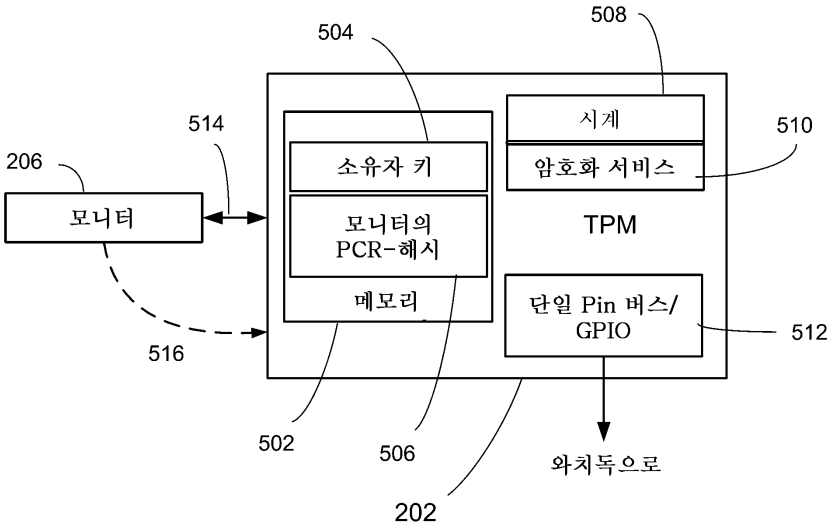
도면4


308
프로세서
312
RAM
모니터
314
인터페이스 브리지 1
그래픽스
310
302
306
328
322
304
TPM
메모리
GPIO
인터페이스 브리지 2
USB
316
IDE
318
PCI
320
324
326
332
와치독 회로
리셋
330

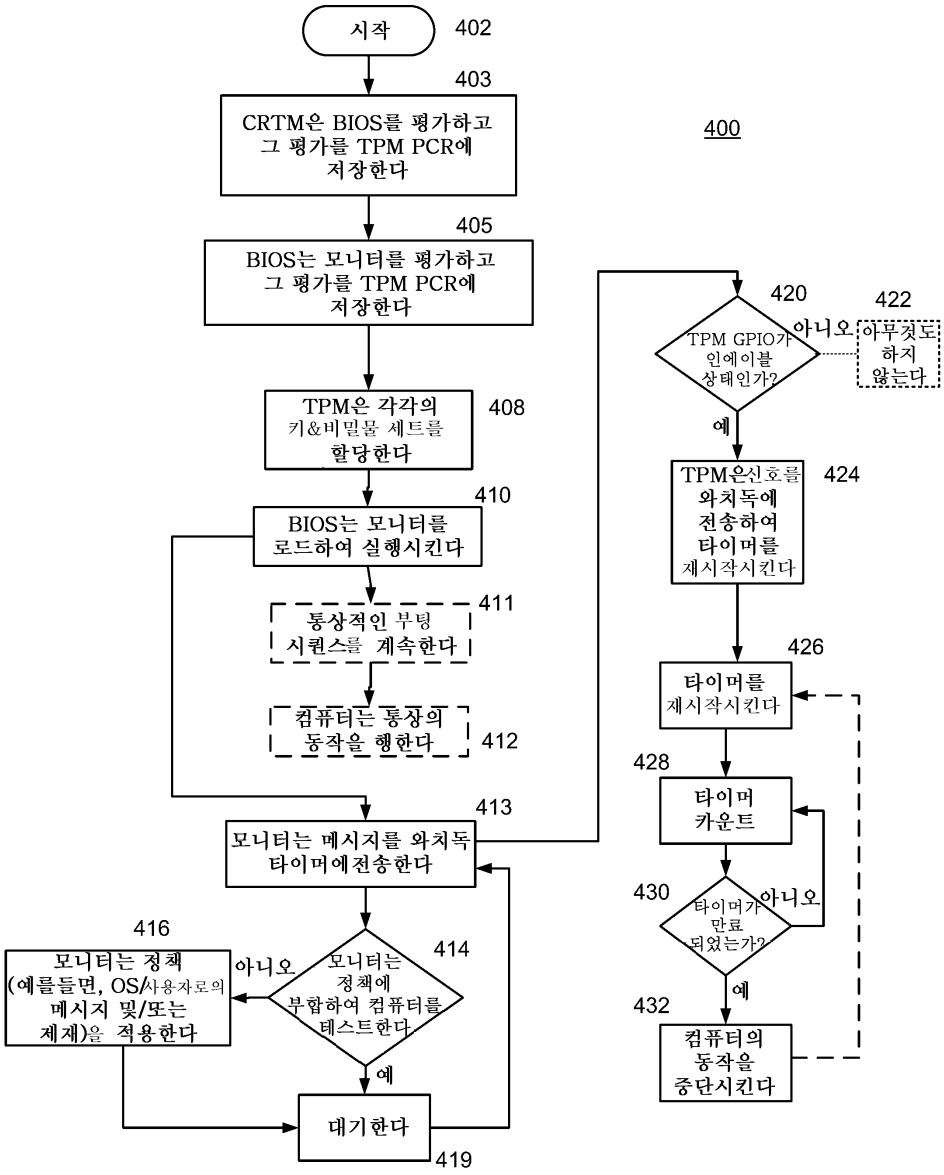
도면5


308
프로세서
312
RAM
모니터
314
인터페이스 브리지 1
그래픽스 310
302
306
328
334
330
304
와치독 회로
322
336
TPM
인터페이스 브리지 2
USB 316
IDE 318
PCI 320
메모리
GPIO
324
326

도면6


504
508
514
시계
510
206
소유자 키
암호화 서비스
모니터
모니터의
PCR-해시
TPM
메모리
단일 Pin 버스/
GPIO
512
516
502
506
와치독으로
202

도면7


시작
402
403
CRTM은 BIOS를 평가하고 그 평가를 TPM PCR에 저장한다
400
405
BIOS는 모니터를 평가하고 그 평가를 TPM PCR에 저장한다
TPM은 각각의 키&비밀물 세트를 할당한다
408
410
BIOS는 모니터를 로드하여 실행시킨다
411
통상적인 부팅 시퀀스를 계속한다
컴퓨터는 통상의 동작을 행한다
412
413
모니터는 메시지를 와치독 타이머에전송한다
416
모니터는 정책 (예를들면, OS/사용자로의 메시지 및/또는 제재)을 적용한다
아니오
414
모니터는 정책에 부합하여 컴퓨터를 테스트한다
예
대기한다
419
420
TPM GPIO가 인에이블 상태인가?
422
아니오
아무것도 하지 않는다
예
TPM은신호를 와치독에 전송하여 타이머를 재시작시킨다
424
426
타이머를 재시작시킨다
428
타이머 카운트
430
타이머가 만료 되었는가?
아니오
예
432
컴퓨터의 동작을 중단시킨다