(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0006033
(43) 공개일자 2019년01월16일

(51) 국제특허분류(Int. Cl.)
G06Q 20/38 (2012.01) *G06Q 20/40* (2012.01)
(52) CPC특허분류
G06Q 20/382 (2013.01)
G06Q 20/4016 (2013.01)
(21) 출원번호 10-2018-7038093(분할)
(22) 출원일자(국제) 2012년04월17일
심사청구일자 2018년12월28일
(62) 원출원 특허 10-2014-7026849
원출원일자(국제) 2012년04월17일
심사청구일자 2014년09월25일
(85) 번역문제출일자 2018년12월28일
(86) 국제출원번호 PCT/US2012/033907
(87) 국제공개번호 WO 2013/158075
국제공개일자 2013년10월24일

(71) 출원인
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
폐가드 비나이
미국 오레곤주 97006 비버톤 노스웨스트 아본데일 드라이브 16675
카힐 코노르
미국 버지니아주 20197 워터포드 데이몬트 레인 38580
바크쉬 산자이
미국 오레곤주 97231 포틀랜드 노스웨스트 레드시더 코트 15222
(74) 대리인
제일특허법인(유)

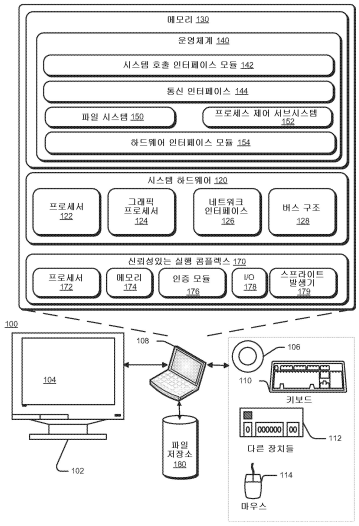
전체 청구항 수 : 총 17 항

(54) 발명의 명칭 **신뢰성 있는 서비스 상호작용**

(57) 요 약

일 실시예로, 콘트롤러는 전자 장치의 신뢰성없는 실행 콤플렉스(untrusted execution complex)상에서 실행되는 애플리케이션으로부터 원격 서비스와의 보안 통신 세션(secure communication session)에 대한 요구를 수신하고, 원격 서비스로부터 수신된 보안 크리덴셜(security credentials)을 검증하고, 보안 콘트롤러와 원격 서비스 사이에 보안 통신 연결을 수립하고, 보안 사용자 인터페이스를 수립하고, 보안 사용자 인터페이스를 통해 사용자로부터 하나 이상의 인증 크리덴셜(athentication credentials)을 수집하고, 하나 이상의 인증 크리덴셜을 원격 서비스로 전송하며, 원격 서비스와 보안 통신 세션을 수행하도록 구성된다. 다른 실시예들도 설명된다.

대 표 도 - 도1



(52) CPC특허분류
G06Q 20/405 (2013.01)

명 세 서

청구범위

청구항 1

전자 장치로서,

운영 체계를 포함하는 표준(normal) 실행 환경과,

보안 처리 요소를 포함하는 신뢰성 있는 실행 환경을 포함하되,

상기 보안 처리 요소는

상기 보안 처리 요소에 통신 가능하게 연결된 디스플레이의 영역 상에 하나 이상의 사용자 크리덴셜(user credentials)을 수신하기 위한 사용자 인터페이스를 제공하고,

상기 사용자 인터페이스에서 수행되는 입출력 동작들이 상기 신뢰성 있는 실행 환경에는 가시적이며 상기 표준 실행 환경에는 가시적이지 않도록 상기 사용자 인터페이스를 상기 표준 실행 환경으로부터 격리시키며,

상기 사용자 인터페이스에 대한 사용자 입력에 기초하여 하나 이상의 인증 크리덴셜을 수신하고,

상기 하나 이상의 인증 크리덴셜을 원격 서비스에 전송하여 상기 원격 서비스와의 보안 거래를 가능하게 하는

전자 장치.

청구항 2

제1항에 있어서,

상기 보안 처리 요소는,

상기 하나 이상의 인증 크리덴셜을 사용하여 상기 원격 서비스와의 인증된 통신 연결을 가능하게 하는

전자 장치.

청구항 3

제2항에 있어서,

상기 보안 처리 요소는,

상기 원격 서비스와 암호화 키를 교환하는

전자 장치.

청구항 4

제1항에 있어서,

상기 보안 처리 요소는,

상기 원격 서비스로부터 보안 인증서를 수신하고,

상기 보안 인증서를 확인하는

전자 장치.

청구항 5

제1항에 있어서,

상기 보안 처리 요소는,

상기 표준 실행 환경의 상기 운영 체계에서 실행되는 애플리케이션으로부터 신뢰성 있는 사용자 입력에 대한 요청을 수신하고,

상기 요청은 상기 애플리케이션 및 상기 요청을 고유하게 식별하는 식별자를 포함하는

전자 장치.

청구항 6

제5항에 있어서,

상기 보안 처리 요소는,

상기 보안 처리 요소와 상기 표준 실행 환경의 상기 운영 체계에서 실행되는 상기 애플리케이션 사이에 보안 채널을 수립하고,

상기 보안 처리 요소로부터의 상기 신뢰성 있는 사용자 입력을 상기 보안 채널을 통해 상기 애플리케이션으로 전달하는

전자 장치.

청구항 7

제1항에 있어서,

상기 전자 장치는 PDA(personal digital assistant), 모바일 전화기, 또는 엔터테인먼트 장치(entertainment device) 중 적어도 하나를 포함하는

전자 장치.

청구항 8

운영 체계를 포함하는 표준 실행 환경 및 보안 처리 요소를 포함하는 신뢰성 있는 실행 환경을 포함하는 전자 장치를 사용하여 보안 거래를 가능하게 하는 방법으로서,

상기 보안 처리 요소를 사용하여,

상기 보안 처리 요소에 통신 가능하게 연결된 디스플레이의 영역 상에 하나 이상의 사용자 크리덴셜을 수신하기 위한 사용자 인터페이스를 제공하는 단계와,

상기 사용자 인터페이스에서 수행되는 입출력 동작들이 상기 신뢰성 있는 실행 환경에는 가시적이며 상기 표준 실행 환경에는 가시적이지 않도록 상기 사용자 인터페이스를 상기 표준 실행 환경으로부터 격리시키는 단계와,

상기 사용자 인터페이스에 대한 사용자 입력에 기초하여 하나 이상의 인증 크리덴셜을 수신하는 단계와,

상기 하나 이상의 인증 크리덴셜을 원격 서비스에 전송하여 상기 원격 서비스와의 보안 거래를 가능하게 하는 단계를 포함하는

보안 거래를 가능하게 하는 방법.

청구항 9

제8항에 있어서,

상기 보안 처리 요소를 사용하여,

상기 하나 이상의 인증 크리덴셜을 사용하여 상기 원격 서비스와의 인증된 통신 연결을 가능하게 하는 단계를 더 포함하는

보안 거래를 가능하게 하는 방법.

청구항 10

제9항에 있어서,

상기 보안 처리 요소를 사용하여,

상기 원격 서비스와 암호화 키를 교환하는 단계를 더 포함하는

보안 거래를 가능하게 하는 방법.

청구항 11

제8항에 있어서,

상기 보안 처리 요소를 사용하여,

상기 원격 서비스로부터 보안 인증서를 수신하는 단계와,

상기 보안 인증서를 확인하는 단계

를 더 포함하는

보안 거래를 가능하게 하는 방법.

청구항 12

제8항에 있어서,

상기 보안 처리 요소를 사용하여,

상기 표준 실행 환경의 상기 운영 체계에서 실행되는 애플리케이션으로부터 신뢰성 있는 사용자 입력에 대한 요청을 수신하는 단계를 더 포함하되,

상기 요청은 상기 애플리케이션 및 상기 요청을 고유하게 식별하는 식별자를 포함하는

보안 거래를 가능하게 하는 방법.

청구항 13

제12항에 있어서,

상기 보안 처리 요소를 사용하여,

상기 보안 처리 요소와 상기 표준 실행 환경의 상기 운영 체계에서 실행되는 상기 애플리케이션 사이에 보안 채널을 수립하는 단계와,

상기 보안 처리 요소로부터의 상기 신뢰성 있는 사용자 입력을 상기 보안 채널을 통해 상기 애플리케이션으로 전달하는 단계

를 더 포함하는

보안 거래를 가능하게 하는 방법.

청구항 14

제8항에 있어서,

상기 전자 장치는 PDA, 모바일 전화기, 또는 엔터테인먼트 장치 중 적어도 하나를 포함하는

보안 거래를 가능하게 하는 방법.

청구항 15

제8항 내지 제14항 중 어느 한 항에 기재된 방법을 수행하는 수단을 포함하는 장치.

청구항 16

제8항 내지 제14항 중 어느 한 항에 기재된 방법을 구현하거나 수행하는 메커니즘을 포함하는 시스템.

청구항 17

컴퓨팅 장치에 의해 실행되는 경우, 제8항 내지 제14항 중 어느 한 항에 기재된 방법을 수행하는 복수의 명령어를 포함하는 적어도 하나의 머신 판독가능 저장 매체.

발명의 설명

기 술 분 야

배 경 기 술

[0001] 본원에 설명된 주제는 전반적으로 전자 장치의 분야에 관한 것으로, 더 구체적으로는 전자 장치를 이용하여 신뢰성 있는 서비스 상호작용(interaction)을 구현하는 시스템 및 방법에 관한 것이다.

[0002] 악성 소프트웨어(멀웨어(malware))는 비인가된 사람이 결제 크리덴셜(payment credentials)을 포함한 개인 정보를 훔치는데 이용될 수 있다. 예로서, 멀웨어는 디스플레이를 스푸핑(spoofing)하거나 또는 디스플레이 모듈로의 입력을 스누핑(snooping)함으로써 사용자의 기밀 입력을 훔칠 수 있다. 일단 결제 크리덴셜을 차지하면, 멀웨어 또는 멀웨어의 사용자는 사용자를 대신해 사기성 거래를 실행할 수 있다. 이러한 위협은 자신의 정보가 유출될까봐 두려워해서 온라인 활동을 하지 않는 인구 비율에 영향을 미친다. 이것은 온라인 상거래(online commerce)를 통해 얻을 수 있는 효율성을 감소시키고, 관련자에 의해 구매되는 상품과 서비스의 양을 제한하여, 온라인 상거래의 성장을 제한한다.

[0003] 이러한 문제에 대한 기존의 솔루션은 이들이 전자 장치의 운영 체계안에 관리된다는 사실(이것은 늘 취약점으로 인식된다)이나 또는 외부적으로 연결된 하드웨어 장치를 필요로 한다는 사실(이것은 소비자 사용 편이성 지수를 제한한다)로 인해 그 유용성 및/또는 보안성이 제한된다. 따라서, 전자 상거래를 위한 보안 컴퓨팅 환경을 제공하는 시스템 및 기술이 유용할 수 있을 것이다. 한편, 본 발명의 배경이 되는 기술은 발명의 명칭이 "Assignment and Distribution of Access Credentials to Mobile Communication Devices"인 미국 공개특허공보 US 2011/0271331호(2011.11.3)에 개시되어 있다.

도면의 간단한 설명

[0004] 상세한 설명은 첨부된 도면을 참조하여 설명된다.

도 1은 일부 실시예에 따라 신뢰성 있는 서비스 상호작용을 위한 인프라스트럭처(infrastructure)를 포함하도록

될 수 있는 예시적인 전자 장치의 개략적 예시도이다.

도 2는 일부 실시예에 따른 신뢰성 있는 서비스 상호작용을 위한 예시적인 아키텍처의 고수준의 개략적 예시도이다.

도 3은 일부 실시예에 따라 신뢰성 있는 서비스 상호작용을 구현하는 방법의 동작들을 예시하는 흐름도이다.

도 4는 일부 실시예에 따라 신뢰성 있는 서비스 상호작용을 구현하도록 되어 있는 전자 장치의 개략적인 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0005] 본원에는 전자 장치에서 신뢰성 있는 서비스 상호작용을 구현하기 위한 시스템 및 방법이 설명된다. 다음의 설명에서, 다양한 구체적인 세부사항들은 다양한 실시예의 완전한 이해를 제공하기 위해 설정된다. 그러나 당업자라면 이러한 다양한 실시예가 이러한 구체적인 세부사항들 없이도 실시될 수 있음을 이해할 것이다. 다른 사례로서, 특정 실시예를 모호하게 하지 않도록 하기 위해 공지의 방법, 프로시저, 구성 요소들 및 회로들은 상세히 예시 또는 설명되지 않았다.

[0006] 도 1은 일부 실시예에 따라 신뢰성 있는 서비스 상호작용을 구현하도록 될 수 있는 예시적인 시스템(100)의 개략적 예시도이다. 일 실시예에서, 시스템(100)은 전자 장치(108)와, 스크린(104), 하나 이상의 스피커(106), 키보드(110), 하나 이상의 다른 I/O 장치(112) 및 마우스(114)를 갖는 디스플레이(102)를 포함하는 하나 이상의 동반 입력/출력 장치를 포함한다. 다른 I/O 장치(112)는 터치 스크린, 음성 활성화 입력 장치(voice-activated input device), 트랙볼, 지오로케이션 장치(geolocation device), 가속도계/자이로스코프(gyroscope)를 포함할 수 있고, 그리고 시스템으로 하여금 사용자로부터 입력을 수신하게 하는 임의의 다른 장치도 포함할 수 있다.

[0007] 다양한 실시예에서, 전자 장치(108)는 개인용 컴퓨터, 랩탑 컴퓨터, PDA, 모바일 전화기, 엔터테인먼트 장치(entertainment device) 또는 다른 컴퓨팅 장치로서 구현될 수 있다. 전자 장치(108)는 시스템 하드웨어(120)와 메모리(130)를 포함하고, 메모리는 RAM 및/또는 ROM으로 구현될 수 있다. 파일 저장소(file store)(180)는 컴퓨팅 장치(108)에 통신할 수 있게 접속될 수 있다. 파일 저장소(180)는 예를 들면 하나 이상의 하드 드라이브, CD-ROM 드라이브, DVD-ROM 드라이브 또는 다른 유형의 저장 장치처럼 컴퓨팅 장치(108)에 대해 내부적일 수도 있다. 파일 저장소(180)는 또한 예를 들면 하나 이상의 외부 하드 드라이브, 네트워크 부착 저장장치 또는 클라우드 저장 네트워크같은 독립적인 저장장치 네트워크처럼 컴퓨터(108)에 대해 외부적일 수도 있다.

[0008] 시스템 하드웨어(120)는 하나 이상의 프로세서(122), 그래픽 프로세서(124), 네트워크 인터페이스(126) 및 버스 구조(128)를 포함할 수 있다. 일 실시예로, 프로세서(122)는 미국 캘리포니아주 산타클라라 소재의 인텔사로부터 입수할 수 있는 Intel®Core2 Duo® 프로세서로서 구현될 수도 있다. 본원에서 이용되는 것처럼, "프로세서"라는 용어는 임의의 유형의 연산적 요소를 의미하는데, 제한하려는 것은 아니지만 예를 들면 마이크로프로세서, 마이크로콘트롤러, 복합 명령어 집합 컴퓨팅(CISC;complex instruction set computing) 마이크로프로세서, 축소 명령어 집합(RISC;reduced instruction set) 마이크로프로셋, 매우 긴 명령어 워드(VLIW;very long instruction word) 또는 임의의 유형의 프로세서 또는 프로세싱 회로가 있다.

[0009] 그래픽 프로세서(124)는 그래픽 및/또는 비디오 동작을 관리하는 부속 프로세서로서 기능할 수 있다. 그래픽 프로세서(124)는 컴퓨팅 시스템(100)의 머더보드상에서 프로세서의 패키징에 통합될 수 있거나 또는 머더보드상에 확장 슬롯을 통해 접속될 수도 있다.

[0010] 일 실시예로, 네트워크 인터페이스(126)는 예를 들면 이더넷 인터페이스(예컨대, IEEE 802.3-2002 참조)같은 유선 인터페이스일 수도 있고, 또는 예를 들면 IEEE 802.11a, b 혹은 g-순응 인터페이스(예컨대, IT-Telecommunications and information exchange between systems LAN/MAN--Part Ⅱ: Wireless LAN Medium Access Control(MAC)와 Physical Layer(PHY) specificatiom Amendment 4: Further Higher Data Rate Extension in the 2.4GHz Band, 802.11G-2003 참조)같은 무선인터페이스일 수도 있다. 무선 인터페이스의 다른 예는 GPRS(general packet radio service) 인터페이스를 들 수 있다(예컨대, Guidelines on GPRS Handset Requirements, Global System for Mobile Communications?GSM Association, Ver.3.0.1, 2002년 12월을 참조).

[0011] 버스 구조(128)는 시스템 하드웨어(128)의 여러 성분들을 연결한다. 일 실시예로, 버스 구조(128)는 몇가지 유형의 버스 구조 중 하나 이상일 수도 있는데, 이러한 몇가지 유형으로는 메모리 버스, 주변 버스나 외부 버스 및/또는 제한하려는 것은 아니지만 11비트 버스, ISA(Industrial Standard Architecture), MSA(Micro-Channel Architecture), EISA(Extended ISA), IDE(Intelligent Drive Electronics), VLB(VESA Local Bus),

PCI)Peripheral Component Interconnect), USB(Universal Serial Bus), AGP(Advanced Graphics Port), PCMCIA(Personal Computer Memory Card International Association bus) 및 SCSI(Small Computer Systems Interface)를 포함한 임의의 다양한 이용가능한 버스 아키텍처를 이용하는 국소 버스를 들 수 있다.

[0012] 메모리(130)는 컴퓨팅 장치(108)의 동작을 관리하는 운영 체계를 포함할 수 있다. 일 실시예로, 운영 체계(140)는 시스템 하드웨어(120)에 대해 인터페이스를 재공하는 하드웨어 인터페이스 모듈(154)을 포함한다. 또한, 운영 체계(140)는 컴퓨팅 장치(108)의 동작시에 이용되는 파일을 관리하는 파일 저장소(150)와, 컴퓨팅 장치(108)상에서 실행되는 프로세스를 관리하는 프로세스 제어 서브시스템(152)을 포함할 수 있다.

[0013] 운영 체계(140)는 원격 공급원으로부터 데이터 패킷 및/또는 데이터 스트림을 송수신하기 위해 시스템 하드웨어(120)와 연계하여 동작할 수 있는 하나 이상의 통신 인터페이스를 포함(또는 관리)할 수도 있다. 운영 체계(140)는 메모리(130)내에 상주하는 하나 이상의 애플리케이션 모듈과 운영 체계(140) 사이에 인터페이스를 제공하는 시스템 호출 인터페이스 모듈(142)을 더 포함할 수도 있다. 운영 체계(140)는 UNIX 운영 체계나 그 파생 운영 체계(예컨대, Linux, Solaris 등등)로서 구현될 수도 있고, 또는 Window® 브랜드 운영 체계나 다른 운영 체계로서 구현될 수도 있다.

[0014] 일부 실시예에서, 시스템(100)은 본원에서 신뢰성 있는 실행 콤플렉스(trusted execution complex)(170)로 지칭되는 저 전력 임베디드 프로세서(low-power embedded processor)를 포함할 수도 있다. 신뢰성 있는 실행 콤플렉스(170)는 시스템(100)의 머더보드상에 위치된 독립적인 집적 회로로서 구현될 수 있다. 도 1에 도시된 실시예에서, 신뢰성 있는 실행 콤플렉스(170)는 프로세서(172), 메모리 모듈(174), 인증 모듈(176), I/O 모듈(178) 및 보안 스프라이트 발생기(secure sprite generator)(179)를 포함한다. 일부 실시예에서, 메모리 모듈(164)은 지속성 플래시 메모리 모듈을 포함할 수 있고, 인증 모듈(174)은 지속성 메모리 모듈에 엔코드된 로직 명령어, 예컨대 펌웨어 또는 소프트웨어로서 구현될 수 있다. I/O 모듈(178)은 직렬 I/O 모듈 또는 병렬 I/O 모듈을 포함할 수 있다. 신뢰성 있는 실행 콤플렉스(170)는 물리적으로 메인 프로세서(122) 및 운영 체계(140)와 분리되어 있으므로, 신뢰성 있는 실행 콤플렉스(170)는 해커의 공격에 대항하여 안전할 수 있고, 따라서 해커가 함부로 조작할 수 없다.

[0015] 일부 실시예에서, 신뢰성 있는 실행 콤플렉스는 예컨대 온라인 상거래 사이트나 그와 같은 부류처럼 호스트 전자 장치와 원격 컴퓨팅 장치 사이의 하나 이상의 거래를 위해 신뢰성 있는 서비스 상호작용을 보증하는데 이용될 수도 있다. 도 2는 일부 실시예에 따른 신뢰성 있는 서비스 상호작용을 위한 예시적인 아키텍처의 고수준의 개략적 예시도이다. 도 2를 참조하면, 호스트 장치(210)는 신뢰성 없는 실행 콤플렉스와 신뢰성 있는 실행 콤플렉스를 갖는 것으로 특성화될 수 있다. 호스트 장치(210)가 시스템(100)으로서 구현될 때, 신뢰성 있는 실행 콤플렉스는 신뢰성 있는 실행 콤플렉스(170)에 의해 구현될 수 있는 반면, 신뢰성 없는 실행 콤플렉스는 시스템(100)의 메인 프로세서(122)와 운영 체계(140)에 의해 구현될 수 있다. 일부 실시예에서는, 신뢰성 있는 실행 콤플렉스가 메인 프로세서(122)의 안전한 부분에 구현될 수도 있다.

[0016] 도 2에 예시된 것처럼, 거래를 개시하는 원격 엔티티(이것은 도 2에서 거래 시스템으로서 식별됨)는 전자 상거래 웹사이트 또는 그런 부류로서 구현될 수 있고, 통신 네트워크(240)를 통해 호스트 장치로 접속될 수 있다. 사용시, 전자 장치(108)의 소유주 또는 운용자는 시스템(250)상에서 안전한 거래를 개시하기 위해 네트워크를 통해 브라우저(220)나 다른 애플리케이션 소프트웨어를 이용해 거래 시스템(250)에 액세스할 수 있다.

[0017] 인증 모듈(176)은 단독으로 또는 인증 플로그-인(222), 입력/출력 모듈(178) 및 보안 스프라이트 발생기(179)와 조합하여 대화 상자(dialog box)(280)를 통해 신뢰성 있는 서비스 상호작용을 보증하는 프로시저를 구현할 수 있다.

[0018] 신뢰성 있는 서비스 상호작용을 구현하는 시스템의 다양한 구조들이 설명되면서 시스템의 동작 양상들이 도 3을 참조하여 설명될 것인데, 여기서 도 3은 일부 실시예에 따라 신뢰성 있는 서비스 상호작용을 구현하는 방법의 동작들을 예시하는 흐름도이다. 일부 실시예에서, 도 3의 흐름도에 도시된 동작들은 신뢰성 있는 실행 콤플렉스(170)의 인증 모듈(176) 단독으로 구현할 수도 있고 또는 다른 모듈과 조합하여 구현할 수도 있다.

[0019] 개론적으로, 일부 실시예에서 전자 장치는 신뢰성 없는 실행 콤플렉스에서 실행되는 예컨대 브라우저같은 애플리케이션으로부터 인터넷 상거래 서비스같은 원격 서비스에 대해 서비스 요청을 개시할 수 있다. 서비스 요청에 대한 응답으로, 원격 서비스는 전자 장치로 크리덴셜을 제공할 수 있다. 원격 서비스로부터의 크리덴셜의 수신에 응답하여, 플러그-인 모듈(222)은 신뢰성 있는 실행 콤플렉스내의 인증 모듈(176)로부터 인증 서비스를 호출할 수 있다. 일부 실시예에서, 인증 서비스는 원격 서비스와의 통신 세션(communication session)을 관리

하는 동작을 구현할 수도 있다.

[0020] 도 3을 참조하면, 동작(305)에서 전자 장치상에서 실행되는 브라우저는 원격 서비스에 대한 요청을 개시한다. 다시 한 번 더, 예로서, 원격 서비스는 전자 상거래 사이트 또는 그런 부류일 수 있으며, 요청은 그 사이트에 의해 제공되는 보안 서비스에 액세스하기 위한 요청일 수 있다. 동작(310)에서, 요청은 전자 장치의 사용자로부터 원격 서비스에 수신된다. 일부 실시예에서, 요청은 요청 장치 및/또는 애플리케이션을 고유하게 식별하는 식별자를 포함할 수도 있고, 요청을 고유하게 식별하는 식별자를 포함할 수도 있다. 예를 들어, 식별자는 요청이 발생된 시간을 식별하는 타임스탬프(timestamp)를 포함할 수도 있다.

[0021] 요청에 대한 응답으로서, 동작(315)에서 원격 서비스는 서비스 요청에 대한 응답에 예컨대 비밀 키(private key), 인프라스트럭처 키 또는 그런 부류같은 인증서(certificate)를 첨부하고, 동작(320)에서 원격 서비스는 이 응답을 요청을 개시한 브라우저로 전송한다. 동작(325)에서, 브라우저는 응답을 수신한다. 인증 플러그인(222)은 응답이 인증서를 포함함을 검출하고, 그에 대한 응답으로서, 원격 서비스와의 보안 통신 세션을 개시 및 관리하기 위해 인증 모듈(176)에 대한 요청을 개시하고, 이 요청과 함께 상기 응답(동작(320))을 전송한다.

[0022] 동작(330)에서, 보안 콘트롤러내의 인증 모듈(176)은 원격 서비스로부터 요청 및 연관 인증서를 수신하고, 동작(335)에서 보안 콘트롤러내의 인증 모듈(176)은 인증서를 인증한다. 일부 실시예에서, 인증 모듈(176)은 원격 검증 시스템(remote validation system)(260)으로 인증서를 인증할 수 있다.

[0023] 일단 인증서가 검증되면, 동작(340)에서 보안 스프라이트 발생기(179)는 전자 장치의 디스플레이상에 보안 대화 상자(280)를 발생한다. 동작(345)에서, 입력/출력 모듈(178)은 대화 상자(280)를 잠궈두어, 대화 상자(280)의 비트맵(bitmap)에 구현된 입력/출력 동작이 오로지 신뢰성 있는 실행 콤플렉스에만 가시적이게 한다. 일단 대화 상자(280)가 잠궈지면, 대화 상자(280)에 구현된 입력/출력 동작은 신뢰성 없는 실행 콤플렉스에 대해서는 가시적이지 않다.

[0024] 도 2를 잠시 참고하면, 일부 실시예에서, 대화 상자(280)는 사용자 이름을 입력하기 위한 제 1 윈도우(282)와, 패스워드를 입력하기 위한 데 2 윈도우(284)를 포함할 수도 있다. 또한, 대화 상자(280)는 예컨대 디스플레이상에 키보드(286)같은 입력 메커니즘을 포함할 수도 있다. 사용자는 키보드(286)를 이용해 자신의 사용자 이름 및/또는 패스워드를 입력할 수 있다.

[0025] 도 3을 다시 참조하면, 동작(350)에서 보안 콘트롤러내의 인증 모듈(176)은 대화 상자(280)를 통해 사용자로부터 인증 입력을 수신한다. 동작(355) 및 동작(360)에서, 보안 콘트롤러의 인증 모듈(176)과 원격 서비스 사이에 보안 통신 연결이 수립된다. 일부 실시예에서, 보안 연결을 수립하는 것은 암호화 키를 교환하는 핸드세이크 프로시저(handshake procedure)를 수반할 수도 있다. 선택적으로, 원격 서비스와 인증 모듈(716) 사이에 가상 사설 네트워크(VPN; virtual private network) 터널이 수립될 수도 있다.

[0026] 동작(365)에서, 인증 모듈(176)은 대화 상자(280)를 통해 수신한 크리덴셜(즉, 사용자 이름 및 패스워드 조합)을 원격 서비스로 전송하고, 원격 서비스는 동작(370)에서 이 크리덴셜을 인증한다.

[0027] 동작(375) 및 동작(380)에서, 보안 콘트롤러 및 원격 서비스는 보안 통신 세션을 실행한다. 일부 실시예에서, 보안 통신 세션은 보안 스프라이트 발생기(179)에 의해 발생된 대화 상자(280)를 통해 실시될 수도 있고, 이로써 보안 통신 세션내의 입력 및 출력은 오로지 신뢰성 있는 실행 콤플렉스에게만 가시적이 되며, 따라서 신뢰성 없는 실행 콤플렉스에서 실행되는 다른 애플리케이션이나 멀웨어에 의해 스눕핑되지 않을 수 있다.

[0028] 통신 세션이 종료되면, 보안 콘트롤러내의 인증 모듈(176)은 해제되어 대화 상자(280)를 닫고(동작(385)), 신뢰성 없는 실행 콤플렉스에 대한 디스플레이의 제어로 복귀한다.

[0029] 전술한 것처럼, 일부 실시에에서, 전자 장치는 컴퓨터 시스템으로서 구현될 수 있다. 도 4는 일부 실시예에 따른 컴퓨터 시스템(400)의 개략적인 예시도이다. 컴퓨터 시스템(400)은 컴퓨팅 장치(402) 및 전력 어댑터(404)(예를 들면, 이것은 컴퓨팅 장치(402)에 전력을 공급하기 위한 것임)를 포함한다. 컴퓨팅 장치(402)는 예를 들면 랩탑(혹은 노트북) 컴퓨터, PDA, 데스크탑 컴퓨팅 장치(예컨대, 워크스테이션 또는 데스크탑 컴퓨터), 랙-장착 컴퓨팅 장치(rack-mounted computing device) 등등처럼 임의의 적당한 컴퓨팅 장치일 수 있다.

[0030] 전력은 다음의 공급원, 즉, 하나 이상의 배터리 팩, AC 아웃렛(outlet)(예컨대, 변압기 및/또는 전력 어댑터(404)같은 어댑터를 통해), 자동차용 전원장치, 비행기용 전원장치 등등의 공급원 중 하나 이상으로부터 컴퓨팅 장치(402)의 다양한 성분들로 제공될 수 있다(예컨대, 컴퓨팅 장치 전력 공급 장치(406)를 통해). 일부 실시에에서, 전력 어댑터(404)는 전력 공급원 출력(예컨대, 약 110VAC 내지 240VAC의 AC 아웃렛 전압)을 약 7VDC 내지

12.6VDC 범위의 직류(DC) 전압으로 변활할 수 있다. 따라서, 전력 어댑터(404)는 AC/DC 어댑터일 수 있다.

[0031] 컴퓨팅 장치(402)는 또한 하나 이상의 중앙 처리 장치(CPU)를 포함할 수 있다. 일부 실시예에서, CPU(408)는 캘리포니아주, 산타 클라라소재의 인텔사로부터 입수할 수 있는 Pentium® Ⅱ 프로세서 계열, Pentium® Ⅲ 프로세서, Pentium® Ⅳ, CORE2 Duo 프로세서 또는 Atom 프로세서를 포함한 Pentium® 계열의 프로세서 중 하나 이상의 프로세서일 수 있다. 선택적으로, 다른 CPU도 이용될 수 있는데, 예를 들면 인텔사의 Itanium®, XEON™ 및 Celeron® 프로세서가 이용될 수도 있다. 또한, 다른 제조사의 하나 이상의 프로세서가 활용될 수도 있다. 더욱이, 프로세서는 단일 또는 다중 코어 디자인을 가질 수도 있다.

[0032] 칩셋(412)은 CPU(408)에 접속되거나 CPU(408)와 통합될 수 있다. 칩셋(412)은 메모리 제어 허브(MCH;memory control hub)(414)를 포함할 수 있다. MCH(414)는 메인 시스템 메모리(418)에 접속된 메모리 콘트롤러(416)를 포함할 수 있다. 메인 시스템 메모리(418)는 CPU(408) 또는 시스템(400)에 포함된 임의의 다른 장치에 의해 실행되는 명령어의 시퀀스와 데이터를 저장한다. 일부 실시예에서, 메인 시스템 메모리(418)는 RAM을 포함할 수 있지만, 이 메인 시스템 메모리(418)는 예컨대 DRAM, SDRAM 등처럼 다른 메모리 유형을 이용하여 구현될 수도 있다. 예컨대 다중 CPU 및/또는 다중 시스템 메모리처럼 추가적인 장치들은 버스(410)에 접속될 수 있다.

[0033] MCH(414)는 그래픽 가속기(422)에 접속된 그래픽 인터페이스(420)를 포함할 수 있다. 일부 실시예에서, 그래픽 인터페이스(420)는 초고속 그래픽 포트(AGP;accelerated graphics port)를 통해 그래픽 가속기(422)에 접속된다. 일부 실시예에서, 디스플레이(예컨대, 평면 패널 디스플레이)(440)는 예를 들어 비디오 메모리 또는 시스템 메모리같은 저장 장치에 저장된 이미지의 디지털 표현을 디스플레이에 의해 해석 및 디스플레이되는 디스플레이 신호로 변환하는 신호 변환기를 통해 그래픽 인터페이스(420)에 접속될 수 있다. 디스플레이 장치에 의해 발생된 디스플레이(440) 신호는 다양한 제어 장치를 거쳐서 디스플레이에 의해 해석된 후에 디스플레이상에 표시될 것이다.

[0034] 허브 인터페이스(hub interface)(424)는 MCH(414)를 플랫폼 제어 허브(PCH;platform control hub)(426)로 접속한다. PCH(426)는 컴퓨터 시스템(400)에 접속된 입력/출력(I/O) 장치에 대한 인터페이스를 제공한다. PCH(426)는 주변 장치 상호연결(PCI;peripheral component interconnect) 버스에 접속될 수도 있다. 그러므로 PCH(426)는 PCI 버스(430)에 대한 인터페이스를 제공하는 PCI 브릿지(428)를 포함한다. PCI 브릿지(428)는 CPU(408)와 주변 장치 사이에 데이터 경로를 제공한다. 추가적으로, 예컨대 캘리포니아주, 산타 클라라 소재의 인텔사로부터 입수할 수 있는 PCI Express™ 아키텍처처럼 다른 유형의 I/O 상호연결 토폴로지가 활용될 수도 있다.

[0035] PCI 버스(430)는 오디오 장치(432) 및 하나 이상의 디스크 드라이브(434)에 접속된다. 다른 장치들이 PCI 버스(430)에 접속될 수도 있다. 또한, CPU(408) 및 MCH(414)는 단일 칩을 형성하도록 결합될 수도 있다. 더 나아가, 그래픽 가속기(422)는 다른 실시에에서 MCH(414) 내부에 포함될 수도 있다.

[0036] 추가적으로, PCH(426)에 접속된 다른 주변 장치들은 다양한 실시예로 IDE(integrated drive electonics) 또는 소형 컴퓨터 시스템 인터페이스(SCSI) 라드 드라이브, USB 포트, 키보드, 마우스, 병렬 포트, 직렬 포트, 플로피 디스크 드라이브, 디지털 출력 지원기기(예컨대, 디지털 비디오 인터페이스(DVI)) 등등을 포함할 수 있다. 그러므로, 컴퓨팅 장치(402)는 휘발성 및/또는 비휘발성 메모리를 포함할 수도 있다.

[0037] 따라서, 본원에는 전자 장치에서 신뢰성 있는 상호작용을 구현하는 아키텍처 및 그 연관 방법이 설명된다. 일부 실시예에서, 이 아키텍처는 원격 서비스와 신뢰성 있는 실행 콤플렉스 사이에 보안 통신을 수립하기 위해 전자 장치 플랫폼에 매립된 하드웨어 성능을 이용한다. 실행 콤플렉스는 보안 통신 세션의 적어도 일부분이 실행되는 보안 대화 상자를 제시하는 신뢰성 있는 실행 콤플렉스로 구현될 수 있다. 일부 실시예에서, 신뢰성 있는 실행 콤플렉스는 예컨대 동글(dongle)처럼 원격 장치에 구현될 수도 있다.

[0038] 본원에서 언급되는 "로직 명령어"라는 용어는 하나 이상의 논리적 동작을 수행하는 하나 이상의 머신에 의해 이해될 수 있는 표현에 관한 것이다. 예를 들어, 로직 명령어는 하나 이상의 데이터 객체를 실행하는 프로세서 컴파일러에 의해 해석 가능한 명령어를 포함할 수 있다. 그러나, 이것은 단순히 머신-판독가능 명령어의 일 예일 뿐이며, 실시예들은 이와 관련하여 제한되지 않는다.

[0039] 본원에서 언급되는 "컴퓨터 판독가능 매체"라는 용어는 하나 이상의 머신에 의해 인지가능한 표현들을 보유할 수 있는 매체에 관한 것이다. 예를 들어, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 명령어 또는 데이터를 저장하는 하나 이상의 저장 장치를 포함할 수 있다. 이러한 저장 장치는 예컨대 광학적 저장 매체, 자기적 저장 매체 또는 반도체 저장 매체같은 저장 매체를 포함할 수 있다. 그러나 이것은 단순히 컴퓨터 판독가능 매체의 일

예일 뿐이며, 실시예들은 이와 관련하여 제한되지 않는다.

[0040] 본원에서 언급되는 "로직"이라는 용어는 하나 이상의 논리적 동작을 수행하는 구조에 관한 것이다. 예를 들어, 로직은 하나 이상의 입력 신호에 기반하여 하나 이상의 출력 신호를 제공하는 회로를 포함할 수 있다. 이러한 회로는 디지털 입력을 수신하고 디지털 출력을 제공하는 유한 상태 머신이나 또는 하나 이상의 아날로그 립력 신호에 응답하여 하나 이상의 아날로그 출력 신호를 제공하는 회로를 포함할 수 있다. 이러한 회로는 ASIC(application specific integrated circuit) 또는 FPGA(field-programmable gate array)에 제공될 수 있다. 또한 로직은 머신 판독가능 명령어를 실행하는 처리 회로와 결합하여 메모리에 저장된 머신 판독가능 명령어를 포함할 수도 있다. 그러나 이것은 단순히 로직을 제공하는 구조의 일 예일 뿐이며, 실시예들은 이와 관련하여 제한되지 않는다.

[0041] 본원에 설명된 방법 중 일부는 컴퓨터 판독가능 매체상에 로직 명령어로서 구현될 수도 있다. 프로세서상에서 실행될 때, 이러한 로직 명령어는 프로세서로 하여금 전술한 방법을 구현하는 전용 머신으로서 프로그램되도록 한다. 프로세서는 본원에 설명된 방법을 실행하는 로직 명령어로 구성될 때 전술한 방법을 수행하는 구조를 구성한다. 선택적으로, 본원에 설명된 방법은 예컨대 PFGA, ASIC 또는 그런 부류상에서 로직을 줄여줄 수 있다.

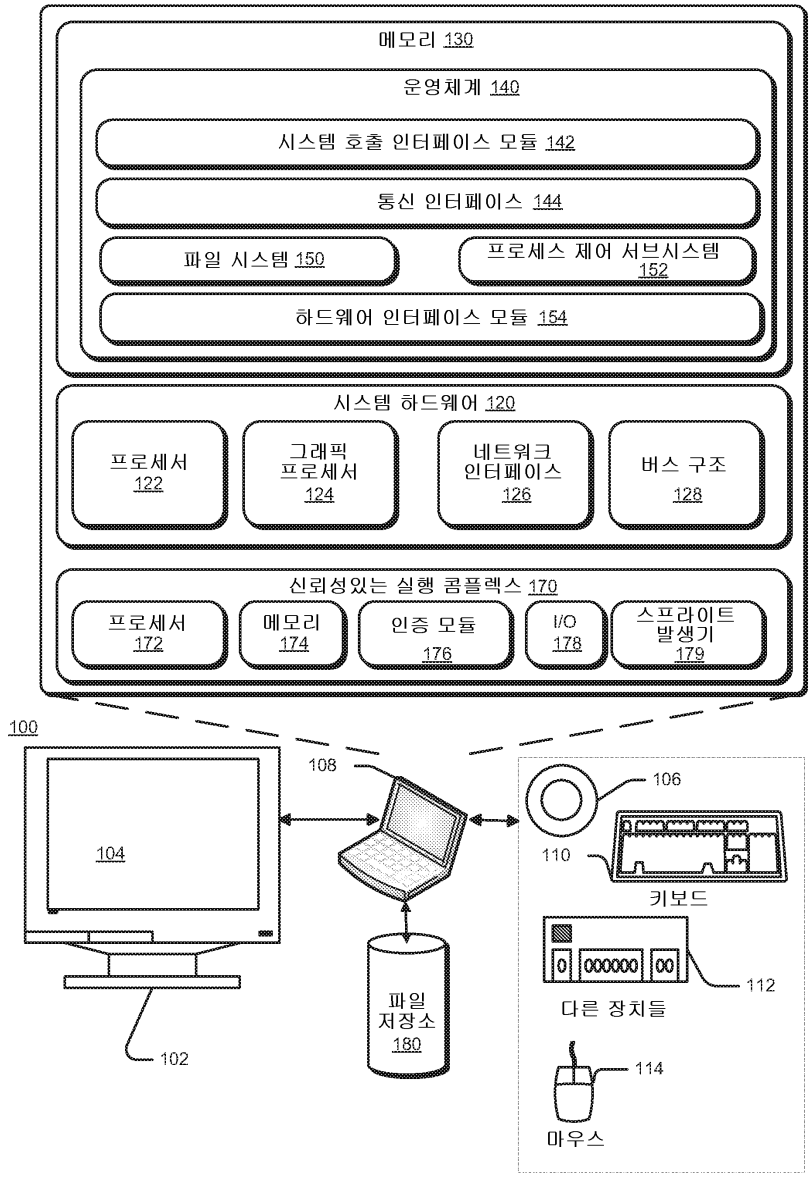
[0042] 설명 및 특허청구범위에서, 접속 및 연결된 용어들과 그 파생어들이 이용될 수도 있다. 특정 실시예에서, '연결된'이라는 용어는 두 개 이상의 요소가 서로 직접적인 물리적 또는 전기적 접촉 상태임을 나타내는데 이용될 수 있다. '접속된'이라는 용어는 두 개 이상의 요소가 직접적인 물리적 또는 전기적 접촉 상태임을 의미한다. 그러나 '접속된'이라는 용어는 두 개 이상의 요소가 서로 직접적인 접촉 상태이지 않으면서도 여전히 서로 협력 또는 상호작용할 수도 있음을 의미하기도 한다.

[0043] 명세서에서 언급하는 "일 실시예" 또는 "일부 실시예"는 실시예와 함께 설명된 특정 특징, 구조 또는 특성이 적어도 하나의 구현에 포함됨을 의미한다. 명세서의 여러 곳에서 "일 실시예로"라는 구절이 나타나는데, 이것은 모두 동일한 실시예를 지칭하는 것일 수도 있고 모두 동일한 실시예를 지칭하는 것이 아닐 수도 있다.

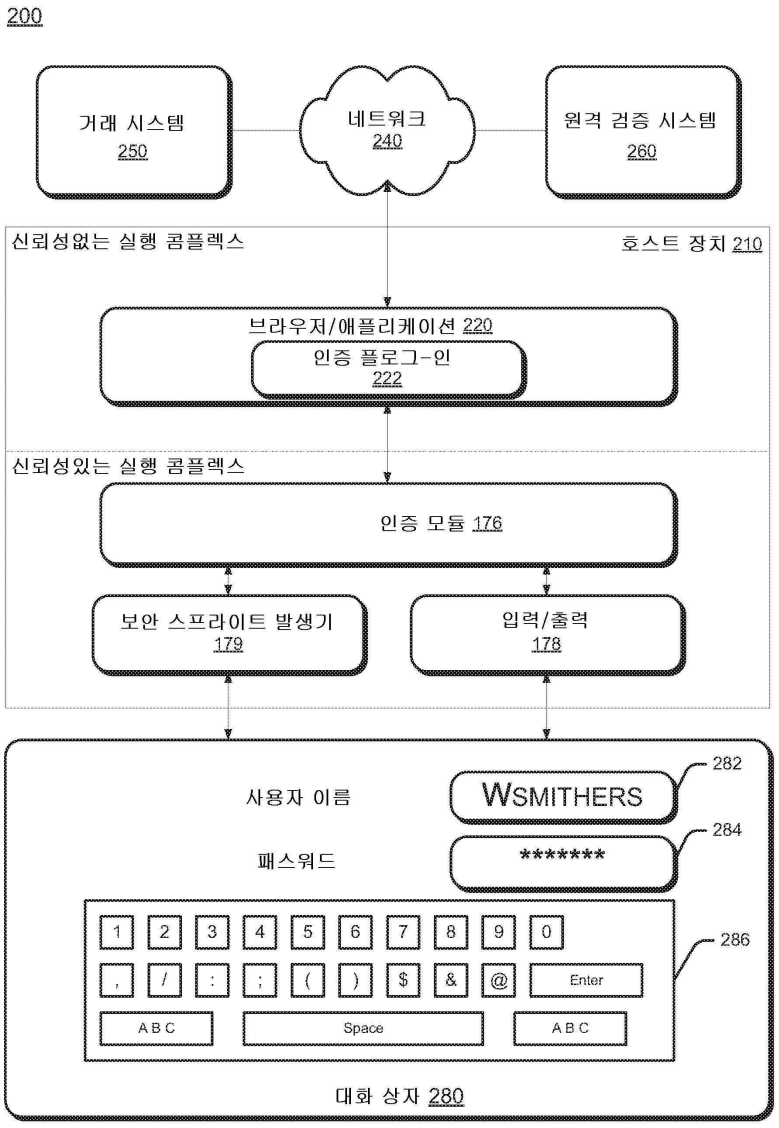
[0044] 비록 실시예들이 구조적 특징 및/또는 방법론적 행위에 특정한 표현으로 설명되었지만, 청구된 주제는 이러한 설명된 특정한 특징들 또는 행위들로 한정될 수 없음을 이해해야 한다. 오히려, 이러한 특정한 특징들 및 행위들은 청구된 주제를 구현하는 표본 형태로서 개시된다.

도면

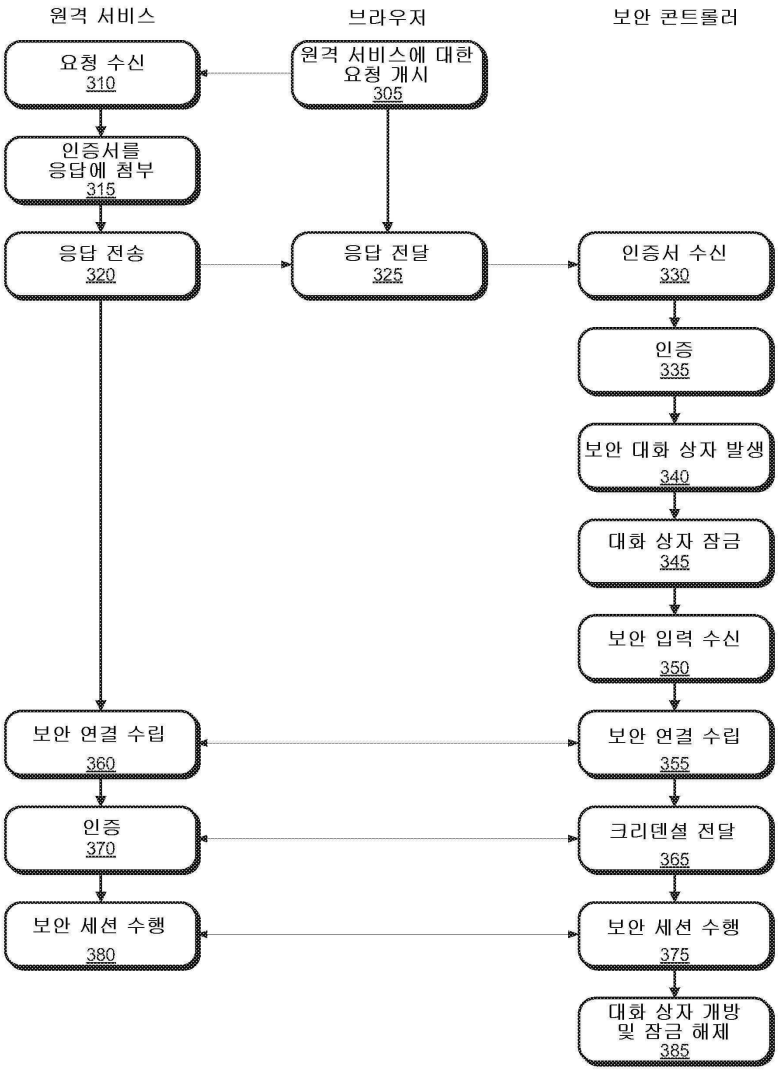
도면1


메모리 130
운영체계 140
시스템 호출 인터페이스 모듈 142
통신 인터페이스 144
파일 시스템 150
프로세스 제어 서브시스템 152
하드웨어 인터페이스 모듈 154
시스템 하드웨어 120
프로세서 122
그래픽 프로세서 124
네트워크 인터페이스 126
버스 구조 128
신뢰성있는 실행 콤플렉스 170
프로세서 172
메모리 174
인증 모듈 176
I/O 178
스프라이트 발생기 179
100
104
102
108
파일 저장소 180
106
110
키보드
112
다른 장치들
114
마우스

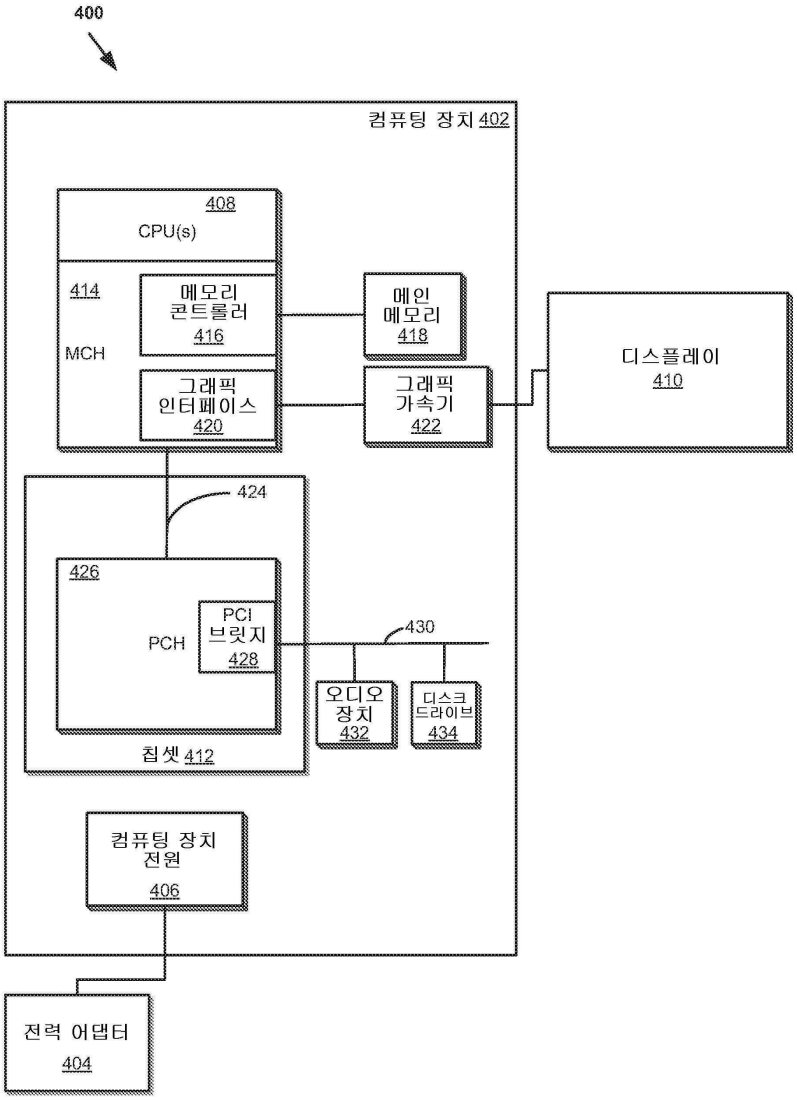
도면2


200
거래 시스템
250
네트워크
240
원격 검증 시스템
260
신뢰성없는 실행 콤플렉스
호스트 장치 210
브라우저/애플리케이션 220
인증 플로그-인
222
신뢰성있는 실행 콤플렉스
인증 모듈 176
보안 스프라이트 발생기
179
입력/출력
178
사용자 이름
WSMITHERS
282
패스워드
****
284
1 2 3 4 5 6 7 8 9 0
, / : ; ( ) $ & @ Enter
ABC Space ABC
286
대화 상자 280

도면3


원격 서비스
브라우저
보안 콘트롤러
요청 수신
310
원격 서비스에 대한
요청 개시
305
인증서를
응답에 첨부
315
응답 전송
320
응답 전달
325
인증서 수신
330
인증
335
보안 대화 상자 발생
340
대화 상자 잠금
345
보안 입력 수신
350
보안 연결 수립
360
보안 연결 수립
355
인증
370
크리덴셜 전달
365
보안 세션 수행
380
보안 세션 수행
375
대화 상자 개방
및 잠금 해제
385

도면4


400
컴퓨팅 장치 402
408
CPU(s)
414
MCH
메모리
콘트롤러
416
그래픽
인터페이스
420
메인
메모리
418
그래픽
가속기
422
디스플레이
410
424
426
PCH
PCI
브릿지
428
430
오디오
장치
432
디스크
드라이브
434
칩셋 412
컴퓨팅 장치
전원
406
전력 어댑터
404