(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0136006
(43) 공개일자 2014년11월27일

(51) 국제특허분류(Int. Cl.)
H04W 12/08 (2009.01) *H04W 12/06* (2009.01)
H04W 88/02 (2009.01) *H04W 92/18* (2009.01)
(21) 출원번호 10-2014-7026704
(22) 출원일자(국제) 2012년04월16일
심사청구일자 2014년09월24일
(85) 번역문제출일자 2014년09월24일
(86) 국제출원번호 PCT/US2012/033748
(87) 국제공개번호 WO 2013/158060
국제공개일자 2013년10월24일

(71) 출원인
인텔 코오퍼레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
페가데, 비나이
미국 97006 오레곤주 비버톤 노쓰웨스트 아본데일 디알. 16675
바크시, 산자이
미국 97231 오레곤주 포틀랜드 노쓰웨스트 레드세달 씨티. 15222
(74) 대리인
양영준, 백만기

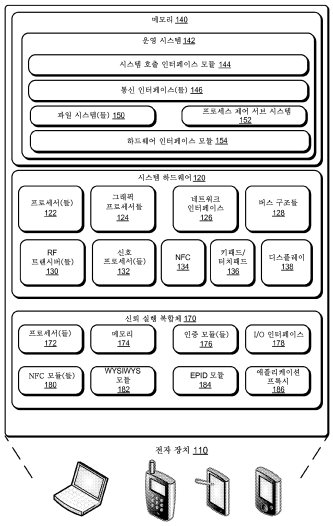
전체 청구항 수 : 총 22 항

(54) 발명의 명칭 **확장성 보안 실행**

(57) 요 약

한 실시 형태에서, 제어기는, 제2 전자 장치 내의 원격 프로세서와의 페어링을 확립하고, 원격 프로세서와의 제1 보안 통신 채널을 생성하고, 제1 보안 채널을 통해 처리 태스크의 제1 부분을 원격 프로세서에 송신하고, 제2 통신 채널을 통해 처리 태스크의 제1 부분으로부터의 입력을 수신하고, 상기 입력을 이용하여 처리 태스크의 적어도 제2 부분을 완료하도록 구성된 로직을 포함한다. 다른 실시 형태가 기술될 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

제1 전자 장치용의 제어기로서,

제2 전자 장치 내의 원격 프로세서와의 페어링을 확립하고;

상기 원격 프로세서와의 제1 보안 통신 채널을 생성하고;

상기 제1 보안 채널을 통해 처리 태스크의 제1 부분을 상기 원격 프로세서에 송신하고;

상기 처리 태스크의 상기 제1 부분으로부터의 입력을, 제2 통신 채널을 통해 수신하고;

상기 입력을 이용하여 상기 처리 태스크의 적어도 제2 부분을 완료하도록 구성된 로직을 포함하는 제어기.

청구항 2

제1항에 있어서,

상기 로직은, 상기 원격 프로세서와 통신하기 위해 근거리 무선 통신 인터페이스를 포함하는 제어기.

청구항 3

제1항에 있어서,

상기 처리 태스크의 상기 제1 부분에 확인 코드를 추가하도록 구성된 로직을 더 포함하는 제어기.

청구항 4

제1항에 있어서,

상기 제어기에 결합된 로컬 프로세서를 더 포함하고,

상기 로컬 프로세서는,

상기 원격 프로세서로부터, 상기 처리 태스크의 상기 제1 부분의 출력을 수신하고;

상기 로컬 제어기에 결합된 디스플레이에 상기 출력을 제시하도록 구성된 로직을 포함하는 제어기.

청구항 5

제4항에 있어서,

상기 로컬 프로세서는,

입력 장치로부터 입력을 수신하고;

상기 입력을 상기 제어기에 전달하도록 구성된 로직을 더 포함하는 제어기.

청구항 6

제4항에 있어서,

상기 원격 프로세서로부터 수신된 비트 맵을 렌더링하고;

상기 비트 맵 내의 입력을 수신하도록 구성된 로직을 더 포함하는 제어기.

청구항 7

제6항에 있어서, 상기 입력을 검증하도록 구성된 로직을 더 포함하는 제어기.

청구항 8

전자 장치로서,

비신뢰 컴퓨팅 환경을 구현하는 프로세서; 및

제어기를 포함하고,

상기 제어기는,

제2 전자 장치 내의 원격 프로세서와의 페어링을 확립하고;

상기 원격 프로세서와의 제1 보안 통신 채널을 생성하고;

상기 제1 보안 채널을 통해 처리 태스크의 제1 부분을 상기 원격 프로세서에 송신하고;

상기 처리 태스크의 상기 제1 부분으로부터의 입력을, 제2 통신 채널을 통해 수신하고;

상기 입력을 이용하여 상기 처리 태스크의 적어도 제2 부분을 완료하도록 구성된 로직을 포함하는 전자 장치.

청구항 9

제8항에 있어서,

상기 로직은, 상기 원격 프로세서와 통신하기 위해 근거리 무선 통신 인터페이스를 포함하는 전자 장치.

청구항 10

제8항에 있어서,

상기 처리 태스크의 상기 제1 부분에 확인 코드를 추가하도록 구성된 로직을 더 포함하는 전자 장치.

청구항 11

제10항에 있어서,

상기 제어기에 결합된 로컬 프로세서를 더 포함하고,

상기 로컬 프로세서는,

상기 원격 프로세서로부터, 상기 처리 태스크의 상기 제1 부분의 출력을 수신하고;

상기 로컬 제어기에 결합된 디스플레이에 상기 출력을 제시하도록 구성된 로직을 포함하는 전자 장치.

청구항 12

제11항에 있어서,

상기 로컬 프로세서는,

입력 장치로부터 입력을 수신하고;

상기 입력을 상기 제어기에 전달하도록 구성된 로직을 더 포함하는 전자 장치.

청구항 13

제11항에 있어서,

상기 원격 프로세서로부터 수신된 비트 맵을 렌더링하고;

상기 비트 맵 내의 입력을 수신하도록 구성된 로직을 더 포함하는 전자 장치.

청구항 14

제13항에 있어서, 상기 입력을 검증하도록 구성된 로직을 더 포함하는 전자 장치.

청구항 15

제1 전자 장치 내의 제어기와 제2 전자 장치 내의 원격 프로세서 사이의 페어링을 확립하는 단계;

상기 제어기와 상기 원격 프로세서 사이에 제1 통신 채널을 생성하는 단계;

상기 제1 보안 채널을 통해 상기 제어기로부터 상기 원격 프로세서에 처리 태스크의 제1 부분을 송신하는 단계;

상기 제어기 내에서, 제2 통신 채널을 통해, 상기 처리 태스크의 상기 제1 부분으로부터의 입력을 수신하는 단계; 및

상기 제어기 내에서, 상기 입력을 사용하여 상기 처리 태스크의 적어도 제2 부분을 완료하는 단계를 포함하는 방법.

청구항 16

제15항에 있어서, 상기 처리 태스크의 상기 제1 부분에 확인 코드를 추가하는 단계를 더 포함하는 방법.

청구항 17

제16항에 있어서,

로컬 프로세서 내에서, 상기 처리 태스크의 상기 제1 부분의 출력을 상기 원격 프로세서로부터 수신하는 단계; 및

상기 로컬 프로세서에 결합된 디스플레이 모듈에 상기 출력을 제시하는 단계를 더 포함하는 방법.

청구항 18

제17항에 있어서,

상기 로컬 프로세서 내에서, 입력 장치로부터의 입력을 수신하는 단계; 및

상기 입력을 상기 로컬 프로세서로부터 상기 제어기에 전달하는 단계를 더 포함하는 방법.

청구항 19

제15항에 있어서, 상기 입력을 검증하는 단계를 더 포함하는 방법.

청구항 20

비 일시적인 컴퓨터 판독 가능 매체에 저장된 로직 명령어를 포함하는 컴퓨터 프로그램 제품으로서,

상기 로직 명령어는, 제어기에 의해 실행되는 경우에, 상기 제어기로 하여금,

제2 전자 장치 내의 원격 프로세서와의 페어링을 확립하고;

상기 원격 프로세서와의 제1 보안 통신 채널을 생성하고;

상기 제1 보안 채널을 통해 처리 태스크의 제1 부분을 상기 원격 프로세서에 송신하고;

상기 처리 태스크의 상기 제1 부분으로부터의 입력을, 제2 통신 채널을 통해 수신하고;

상기 입력을 이용하여 상기 처리 태스크의 적어도 제2 부분을 완료하도록 구성하게 하는, 컴퓨터 프로그램 제품.

청구항 21

제20항에 있어서,

로직은, 상기 원격 프로세서와 통신하기 위해 근거리 무선 통신 인터페이스를 포함하는, 컴퓨터 프로그램 제품.

청구항 22

제21항에 있어서,

상기 처리 태스크의 상기 제1 부분에 확인 코드를 추가하는 로직을 더 포함하는, 컴퓨터 프로그램 제품.

명 세 서

기 술 분 야

[0001] 본 명세서에 기재된 주제는 일반적으로 컴퓨팅 분야에 관한 것이고, 특히 전자 장치가 원격 전자 장치에서의 처리 능력을 이용할 수 있게 하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 일반적인 전자 상거래에 있어서, 상인(및 기본 생태계)은, 거래를 행하는 개인이 인가된 사람임을 확신하지 못한다. 사기 거래가 온라인 생태계에서 허용되면, 일반적으로 신뢰 당사자, 이 예에서는 상인, 또는 사기당한 개인이 기본 사기 비용을 부담해야 한다.

발명의 내용

해결하려는 과제

[0003] 온라인 공간에서의 또 다른 단점은, 인가받지 않은 개인이 사용하기 위해, 지불 자격 증명을 포함하는, 개인 정보를 도용하는 데 종종 사용되는 시스템 멀웨어의 위협이 항상 존재한다는 것이다. 이러한 위협은, 자신의 정보가 위태롭다는 두려움으로 인해 온라인 활동을 행하지 않는 인구의 일정 비율에 영향을 미친다. 이것은 온라인 상거래를 통해 얻을 수 있는 효율성을 감소시키고, 관련 개인들에 의해 구매되는 상품과 서비스의 양을 제한하여, 온라인 상거래의 성장을 제한한다.

과제의 해결 수단

[0004] 일부 컴퓨팅 시스템은, 인증 프로세스를 관리하기 위해 신뢰 실행 복합체(trusted execution complex) 내에 매립된, 메인 프로세서로부터 분리된 보안 제어기를 이용할 수 있다. 보안 제어기는 계산 및 메모리 자원이 제한될 수 있어, 많은 계산 작업을 보안 제어기가 구현하기에는 어려울 수 있다.

발명의 효과

[0005] 따라서, 많은 계산 작업이 원격 프로세서에 대해 오프로드될 수 있게 하는 보안 실행을 제공하는 시스템과 기술이 유용성을 찾을 수 있다.

도면의 간단한 설명

[0006] 상세한 설명은 첨부된 도면을 참조하여 설명한다.

도 1은 일부 실시 형태에 따른 확장성 보안 실행을 구현하기 위해 기반 구조를 포함하도록 구성될 수 있는 예시적인 전자 장치의 개략도이다.

도 2는 일부 실시 형태에 따른 확장성 보안 실행을 위한 예시적인 네트워크 아키텍처의 하이-레벨 개략도이다.

도 3은 일부 실시 형태에 따른 확장성 보안 실행을 위한 예시적인 아키텍처의 개략도이다.

도 4는 일부 실시 형태에 따른 확장성 보안 실행을 구현하는 방법에서의 동작을 나타내는 흐름도이다.

도 5는 일부 실시 형태에 따른, 확장성 보안 실행을 위한 예시적인 시스템의 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0007] 전자 장치의 확장성 보안 실행을 구현하기 위한 예시적인 시스템 및 방법이 본원에서 설명된다. 본원에 기재된 시스템 및 방법의 일부 실시 형태는, 네트워크 보안의 콘텍스트에서, 특히 전자 상거래 설정에 있어서 유용성을 발견할 수 있다. 본원에 기술된 일부 실시 형태는, 보안 프로세서 또는 관리능력 엔진이라고도 종종 불리는 신뢰 실행 엔진이, 별도의 처리 장치에 위치할 수 있는 원격 프로세서에 처리 태스크 중 하나 이상의 부분을 오프로드할 수 있게 한다. 예로서, 전자 상거래 애플리케이션의 콘텍스트에서, 제1 컴퓨팅 장치에서의 신뢰 실행 엔진은, 별도의 컴퓨팅 장치에 위치한 원격 프로세서에, 비트 맵 생성과 같은 그래픽 집중 동작을 오프로드할 수 있다. 원격 프로세서는 디스플레이에 비트 맵을 제시하고 디스플레이로부터의 입력을 수집할 수 있는, 상기 제1 장치의 비신뢰 실행 복합체 상에서 실행되는 애플리케이션에 비트 맵을 전달할 수 있다. 원격 프로세서에의 비트 맵 생성의 오프로딩은, 상기 제1 장치에서의 멀웨어가, 비트 맵 영역으로부터의 사용자 입력 또는 출력을 방해하거나 스누핑(snooping)하는 것을 억제한다.

[0008] 본 문서는, 확장성 보안 실행이 구현될 수 있고, 확장성 보안 실행을 구현하기 위한 예시적인 동작의 하드웨어

및 소프트웨어 환경에 대한 설명을 제공한다. 다음의 설명에서, 다수의 특정 세부 사항은, 다양한 실시 형태에 대한 철저한 이해를 제공하기 위해 제시된다. 그러나, 다양한 실시 형태는 특정 세부 사항 없이도 실시될 수 있음을 당업자는 이해할 것이다. 다른 경우에 있어서, 잘 알려진 방법, 절차, 구성 요소 및 회로는, 특정한 실시 형태를 모호하게 하지 않도록 상세히 도시 또는 설명되지는 않는다.

[0009] 도 1은 일부 실시 형태에 따른 확장성 보안 실행을 구현하기 위해 구성될 수 있는 예시적인 전자 장치(110)의 개략도이다. 도 1에 도시된 바와 같이, 전자 장치(110)는, 모바일 전화, 태블릿 컴퓨터 휴대용 컴퓨터, 또는 개인 휴대 정보 단말기(PDA)와 같은 종래의 모바일 장치로서 구체화될 수 있다.

[0010] 일부 실시 형태에서, 전자 장치는, 신뢰 실행 엔진으로서 또는 보안 요소 또는 관리능력 엔진으로서 종종 지칭될 수도 있는, 신뢰 실행 복합체를 포함할 수 있다. 신뢰 실행 복합체는, 비신뢰 실행 복합체라고도 종종 지칭되는, 1차 실행 복합체와는 별도인 하나 이상의 제어기를 포함할 수 있다. 분리는, 신뢰 실행 복합체가, 비신뢰 실행 복합체로부터 물리적으로 분리될 수 있다는 의미에서 물리적일 수 있다. 대안적으로는, 신뢰 실행 복합체는, 신뢰 실행 복합체가, 비신뢰 실행 복합체를 호스팅하는 동일한 칩 또는 칩셋 상에서 호스팅되지만, 신뢰 실행 복합체가 보안되도록 실리콘 레벨에서 분리될 수 있다는 의미에서 논리적일 수 있다.

[0011] 다양한 실시 형태에서, 전자 장치(110)는 디스플레이, 하나 이상의 스피커, 키보드, 하나 이상의 다른 I/O 장치(들), 마우스 등을 포함하는 하나 이상의 첨부 입/출력 장치를 포함하거나 이에 결합될 수 있다. 예시적인 I/O 장치(들)은, 터치 스크린, 음성 활성화된 입력 장치, 트랙볼, 위치 측정 장치, 가속도 센서/자이로 스코프, 생체 특징 입력 장치, 및 전자 장치(110)가 사용자로부터의 입력을 수신할 수 있게 허용하는 임의의 다른 장치를 포함할 수 있다.

[0012] 전자 장치(110)는, 랜덤 액세스 메모리 및/또는 판독 전용 메모리로서 구현될 수 있는, 시스템 하드웨어(120) 및 메모리(140)를 포함한다. 파일 스토어는, 컴퓨팅 장치(110)에 통신적으로 결합될 수 있다. 파일 스토어는, 예를 들어, eMMC, SSD, 하나 이상의 하드 드라이브, 또는 다른 종류의 스토리지 장치 등의 컴퓨팅 장치(110)의 내부일 수 있다. 파일 스토어(180)는 예를 들어, 하나 이상의 외부 하드 드라이브, 네트워크 부착 스토리지, 또는 별도의 스토리지 네트워크 등의 컴퓨터(110) 외부에 있을 수도 있다.

[0013] 시스템 하드웨어(120)는, 하나 이상의 프로세서(122), 그래픽 프로세서(124), 네트워크 인터페이스(126) 및 버스 구조(128)를 포함할 수 있다. 한 실시 형태에서, 프로세서(122)는, 미국 캘리포니아주 산타 클라라에 소재하는 인텔사에서 제공하는, 인텔® 아톰™ 프로세서, 인텔® 아톰™ 기반 시스템-온-칩(SOC) 또는 인텔® 코어2 듀오® 프로세서로서 구체화될 수 있다. 본원에서 사용되는 용어 "프로세서"는 마이크로프로세서, 마이크로 제어기, 복합 명령어 세트 컴퓨팅(CISC) 마이크로프로세서, 축소 명령 세트(RISC) 마이크로프로세서, 매우 긴 명령 워드(VLIW) 마이크로프로세서, 또는 임의의 다른 유형의 프로세서 또는 프로세싱 회로와 같지만 이에 한정되지는 않는, 임의의 유형의 계산적 요소를 의미한다.

[0014] 그래픽 프로세서(들)(124)는 그래픽 및/또는 비디오 동작을 관리하는 부 프로세서로서 기능할 수 있다. 그래픽 프로세서(124)는 전자 장치(110)의 마더 보드에 통합되거나, 마더 보드에 확장 슬롯을 통해 결합될 수 있다.

[0015] 한 실시 형태에서, 네트워크 인터페이스(126)는, 이더넷 인터페이스(예를 들면, 전기 전자 학회/IEEE 802.3-2002 참조) 등의 유선 인터페이스, 또는 IEEE 802.11a, b 또는 g-호환 인터페이스(예를 들면, IT-통신 및 시스템들 LAN/MAN--파트 II 간의 정보 교환을 위한 IEEE 표준: 무선 LAN 매체 액세스 제어(MAC) 및 물리 계층(PHY) 명세 개정 4: 2.4 GHz 대역에서의 더 높은 데이터 속도 확장, 802.11G-2003 참조) 등의 무선 인터페이스일 수 있다. 무선 인터페이스의 또 다른 예는, 일반적인 패킷 무선 서비스(GPRS) 인터페이스(예를 들면, GPRS 핸드셋 요구 사항에 대한 가이드 라인, 이동 통신/GSM 협회의 글로벌 시스템, 버전 3.0.1, 2002년 12월 참조)일 수 있다.

[0016] 버스 구조(128)는 시스템 하드웨어(128)의 다양한 구성 요소를 연결한다. 한 실시 형태에서, 버스 구조(128)는, 메모리 버스, 주변 버스 또는 외부 버스, 및/또는 11-비트 버스, 산업 표준 아키텍처(ISA), 마이크로-채널 아키텍처(MSA), 확장 ISA(EISA), 지능형 드라이브 전자 장치(IDE), VESA 로컬 버스(VLB), 주변 구성 요소 상호 접속(PCI), 범용 직렬 버스(USB), 고급 그래픽 포트(AGP), 개인용 컴퓨터 메모리 카드 국제 협회 버스(PCMCIA), 및 소형 컴퓨터 시스템 인터페이스(SCSI), 고속 동기식 직렬 인터페이스(HSI), 직렬 저전력 칩간 미디어 버스(SLIMbus®) 등을 포함하나 이에 한정되지 않는, 임의의 다양한 사용 가능 버스 아키텍처를 사용하는 로컬 버스를 포함하는 몇몇 유형의 버스 구조(들) 중 하나 이상일 수 있다.

[0017] 전자 장치(110)는, RF 신호를 송수신하는 RF 트랜시버(130), 근거리 통신(NFC) 라디오(134), 및 RF 트랜시버

(130)에 의해 수신된 신호를 처리하는 신호 처리 모듈(132)을 포함할 수 있다. RF 트랜시버는, 예를 들어, 블루투스 또는 802.11X. IEEE 802.11a, b 또는 g-호환 인터페이스(예를 들면, IT-통신 및 시스템들 LAN/MAN--파트 II 간의 정보 교환을 위한 IEEE 표준: 무선 LAN 매체 액세스 제어(MAC) 및 물리 계층(PHY) 명세 개정 4: 2.4 GHz 대역에서의 더 높은 데이터 속도 확장, 802.11G-2003 참조) 등의 프로토콜을 통해 로컬 무선 연결을 구현할 수 있다. 무선 인터페이스의 또 다른 예는, WCDMA, LTE, 일반 패킷 무선 서비스(GPRS) 인터페이스(예를 들면, GPRS 핸드셋 요구 사항에 대한 가이드 라인, 이동 통신/GSM 협회의 글로벌 시스템, 버전 3.0.1, 2002년 12월 참조)일 수 있다.

[0018] 전자 장치(110)는, 예를 들어, 키패드(136) 및 디스플레이(138) 등의 하나 이상의 입/출력 인터페이스를 더 포함할 수 있다. 일부 실시 형태에서, 전자 장치 (110)는 키패드를 가지 않을 수 있고 입력용 터치 패널을 사용할 수 있다.

[0019] 메모리(140)는, 컴퓨팅 장치(110)의 동작을 관리하기 위한 운영 시스템(142)을 포함할 수 있다. 한 실시 형태에서, 운영 시스템(142)은, 시스템 하드웨어(120)에 인터페이스를 제공하는 하드웨어 인터페이스 모듈(154)을 포함한다. 또한, 운영 시스템(140)은, 컴퓨팅 장치(110)의 동작에 사용된 파일을 관리하는 파일 시스템(150), 및 컴퓨팅 장치(110)에서 실행되는 프로세스를 관리하는 프로세스 제어 서브 시스템(152)을 포함할 수 있다.

[0020] 운영 시스템(142)은, 원격 소스로부터 데이터 패킷 및/또는 데이터 스트림을 송수신하기 위해 시스템 하드웨어(120)와 연계하여 동작할 수 있는 하나 이상의 통신 인터페이스(146)를 포함(또는 관리)할 수 있다. 운영 시스템(142)은, 상기 운영 시스템(142)과, 메모리(130) 내에 상주하는 하나 이상의 애플리케이션 모듈 사이에 인터페이스를 제공하는 시스템 호출 인터페이스 모듈(144)을 더 포함할 수 있다. 운영 시스템(142)은, UNIX 운영 시스템 또는 임의의 이들의 유도체(예를 들어, 리눅스, 안드로이드 등)로서, 또는 윈도우® 브랜드 운영 시스템, 또는 다른 운영 시스템으로서 구체화될 수 있다.

[0021] 전자 장치(110)는 신뢰 실행 엔진(170)을 포함할 수 있다. 일부 실시 형태에서, 신뢰 실행 엔진(170)은 전자 장치(110)의 마더 보드 위에 위치한 독립적인 집적 회로로서 구현될 수 있으며, 다른 실시 형태에서는, 신뢰 실행 엔진(170)은 동일한 SOC 다이 위의 전용 프로세서 블록으로서 구현될 수 있으며, 다른 실시 형태에서, 신뢰 실행 엔진은 HW 강제 메커니즘을 사용하여 상기 프로세서(들)의 나머지 부분으로부터 분리되는 프로세서(들)(122)의 부분 위에 구현될 수 있다.

[0022] 도 1에 도시된 실시 형태에서, 신뢰 실행 엔진(170)은 프로세서(172), 메모리 모듈(174), 하나 이상의 인증 모듈(들)(176), 및 I/O 모듈(178), 근거리 통신(NFC) 모듈, WYSIWYS(what you see is what you sign) 모듈(182), 강화된 개인 식별(EPID) 모듈(184) 및 하나 이상의 애플리케이션 프록시(186)를 포함한다. 일부 실시 형태에서, 메모리 모듈(174)은 영구 플래시 메모리 모듈을 포함할 수 있고, 다양한 기능 모듈은 영구 플래시 메모리 모듈 내에 인코딩된 로직 명령어, 예를 들면 펌웨어 또는 소프트웨어로서 구현될 수 있다. I/O 모듈(178)은 직렬 I/O 모듈 또는 병렬 I/O 모듈을 포함할 수 있다. 신뢰 실행 엔진(170)은 메인 프로세서(들)(122) 및 운영 시스템(142)으로부터 분리되기 때문에, 신뢰 실행 엔진(170)은 보안이 될 수 있다, 즉, 일반적으로 호스트 프로세서(122)로부터의 SW 공격을 마운트하는 해커에게 접근 불가능하게 될 수 있다.

[0023] 일부 실시 형태에서, 신뢰 실행 엔진은, 처리 태스크의 일부가 다른 전자 장치의 원격 프로세서에 오프로드되도록 확장성 보안 실행 절차가 구현될 수 있는 호스트 전자 장치 내의 신뢰 실행 복합체를 정의할 수 있다. 원격 프로세서에의 프로세싱의 오프로딩은, 바신뢰 실행 복합체에서 실행되는 소프트웨어의 스누핑 또는 멀웨어의 능력을 억제하여, 입력, 출력, 또는 동작으로부터의 처리 결과를 조작하거나 판독하게 한다.

[0024] 도 2는 확장성 보안 실행 절차가 구현될 수 있는 네트워크 환경의 하이-레벨의 개략도이다. 도 2를 참조하면, 전자 장치(110) 및 원격 장치(112)는 네트워크(240)를 통해 하나 이상의 원격 서버(230)에 결합될 수 있다. 전자 장치(110)는 적절한 근거리 통신 링크를 통해 원격 장치(112)와 무선 통신이 가능하도록 근거리 통신(NFC) 인터페이스를 포함할 수 있다. 일부 실시 형태에서는, 상기 전자 장치 (110)를 참조하여 설명한 바와 같이, 전자 장치(110) 및 원격 장치(112)의 각각은, 모바일 전화, 태블릿, PDA 또는 다른 모바일 컴퓨팅 장치로서 구체화될 수 있다. 네트워크(240)는, 예를 들어, 인터넷 등의 공중 통신망으로서, 또는 사설 통신 네트워크, 또는 이들의 조합으로서 구체화될 수 있다.

[0025] 원격 서버(들)(230)는 컴퓨터 시스템으로서 구현될 수 있다. 일부 실시 형태에서, 서버(들)(230)는 전자 상거래 서버로서 구현될 수 있으며, 공급업자에 의해 또는 보안 플랫폼을 동작하는 제3자에 의해 관리될 수 있다. 다른 원격 서버(들)(230)는 공급업자에 의해 또는 제3자 지불 시스템, 예를 들면, 거래 청산 서비스 또는 신용

카드 서비스에 의해 운영될 수 있다.

[0026] 도 3은 일부 실시 형태에 따른 확장성 보안 실행을 구현하는 시스템의 보다 상세한 개략도이다. 도 3을 참조하면, 전자 장치(110)는 네트워크(340)를 통해 거래 시스템(350)에 결합될 수 있다. 또한, 전자 장치(110)는 거래 시스템(350)으로부터 분리되거나 이와 통합될 수 있는 검증 시스템(360)에 결합될 수 있다. 마찬가지로, 일부 실시 형태에서는, 원격 장치(112)는 네트워크(340)를 통해 거래 시스템(350) 및 검증 시스템(360)에 결합될 수도 있다.

[0027] 일부 실시 형태에서, 브라우저 또는 다른 애플리케이션(320)은, 전자 장치(110)의 비신뢰 실행 복합체에서 실행될 수 있다. 브라우저(320)는, 전자 장치(110)의 신뢰 실행 복합체에서 실행되는 인증 모듈(176)과 협력하는 인증 플러그인(322)을 포함할 수 있다. 원격 장치(112)는 입/출력 모듈(336), 프로세서(334), 및 메모리(330) 내에 상주하는 인증 모듈(322)을 포함한다.

[0028] 도 2에서 거래 시스템(350)으로서 식별된 거래를 관리하는 원격 엔티티는, 전자 상거래 웹 사이트 등으로서 구체화될 수 있고, 통신 네트워크(340)를 통해 호스트 장치에 결합될 수 있다. 사용 시에, 전자 장치(110)의 소유자 또는 운영자는, 네트워크를 통해 브라우저(320) 또는 다른 애플리케이션 소프트웨어를 사용하여 거래 시스템(350)에 액세스할 수 있어, 시스템(350)에서 전자 상거래를 개시할 수 있다.

[0029] 인증 모듈(176)은, 단독으로 또는 인증 플러그인(322), 입/출력 모듈(178) 및 보안 스프라이트 생성기(179), 및 원격 장치(112) 위의 프로세서(334) 및 인증 모듈(332)과 조합하여, 프로세서(172)에 의해 구현된 처리 태스크의 일부가 원격 장치(112)의 원격 프로세서(334)에 오프로드되는 확장성 보안 실행 동작을 구현할 수 있다.

[0030] 확장성 보안 실행을 구현하는 시스템의 다양한 구조를 설명하면, 시스템의 동작 양태는 도 4를 참조하여 설명한다. 일부 실시 형태에서, 도 4의 흐름도에 도시된 동작은, 신뢰 실행 엔진(170)의 프로세서(172)에 의해, 단독으로 또는 전자 장치의 비신뢰 실행 복합체에서 실행되는 프로세서(122) 및 원격 장치(112)의 프로세서(334)와 조합하여 구현될 수 있다.

[0031] 도 4를 참조하면, 일부 실시 형태에서, 도 4에 도시된 동작, 동작(405 및 410))에서, 보안 페어링은, 보안 제어기로서 지칭되기도 하는 신뢰 실행 엔진과, 원격 프로세서, 예를 들면 원격 장치(112)의 프로세서(334) 사이에 확립된다. 일부 실시 형태에서, 상기 페어링은, 사용자가 등록 시퀀스를 개시함으로써, 예를 들면 전자 장치(110)의 원격 장치(112)를 태핑(tapping)하거나, 그렇지 않으면 등록 프로세스를 론칭(launching)함으로써 개시될 수 있다. 등록 요청에 응답하여, 신뢰 실행 엔진(170)의 프로세서(172)는 인증 모듈(176)을 론칭하고, 원격 장치(112)의 프로세서(334)는 인증 모듈(332)을 론칭한다. 각각의 인증 모듈(322, 332)은, 적절한 암호 알고리즘, 예를 들면 디피-헬만 키 교환 프로토콜(Diffie-Hellman key exchange protocol) 등을 이용하여 공유 비밀을 개발할 수 있다.

[0032] 동작(415 및 420)에서, 신뢰 실행 엔진(170) 및 원격 프로세서(334)는, 각각의 입/출력 모듈(178, 336)에 의해 보안 통신 연결을 확립한다. 통신 연결은, 무선 연결 또는 임의의 다른 적절한 통신 매체, 예를 들면 적외선 연결 또는 유선 네트워크 연결을 통해 구현될 수 있다.

[0033] 동작(425)에서, 브라우저(320) 또는 다른 적절한 애플리케이션은 전자 장치(110)의 로컬 프로세서(122)에서 론칭된다. 동작(430 및 435)에서, 탐색 프로세스는, 전자 장치(110)와 원격 장치(112) 사이에서 구현된다. 예로서, 일부 실시 형태에서는, 장치(110, 112)는, 블루투스 또는 다른 무선 네트워크 기능을 포함할 수 있으며, 무선 네트워크를 통해 서로를 발견할 수 있다.

[0034] 동작(440)에서, 브라우저에서의 애플리케이션은 원격 서버에 연결된다. 예로서, 도 3에 도시된 실시 형태에서, 브라우저는 전자 상거래 웹 사이트 등일 수 있는 거래 시스템(350)에 연결하는 데 사용될 수 있다. 일부 실시 형태에서, 전자 장치(110)는 원격 서버로부터 로그인 요청을 수신하고, 비신뢰 실행 복합체에서 실행되는 인증 플러그인(322)에 응답하여 신뢰 실행 복합체 내의 인증 모듈(176)을 호출한다.

[0035] 일부 실시 형태에서, 신뢰 실행 복합체는, 로그인 화면에 대한 비트 맵 이미지를 생성할 수 있고, 이를 전자 장치의 디스플레이(138)에 제시할 수 있다. 예로서, 일부 실시 형태에서, WYSIWYS 모듈(182)은 전자 장치의 디스플레이 상에 보안 창을 열고, 창의 대화 상자(380)에 인가 요청을 제시한다. 전자 장치(110)의 사용자는, 로그인 요청을 인가하는 입력을 보안 창에 입력함으로써 인가 요청에 응답한다. WYSIWYS 모듈(182)은 입력과 연관되는 핀을 생성할 수 있다.

[0036] 그러나, 일부 실시 형태에서, 신뢰 실행 복합체는 비트 맵을 생성하는 프로세스를 원격 장치(112)의 프로세서

(334)에 오프로드한다. 이러한 실시 형태에서, 프로세서(172)에서 실행되는 인증 모듈(176)은 확인 코드를 생성하고, 확인 코드 및 확인 페이지를 원격 장치(112)의 프로세서(334)에 전달한다.

[0037] 동작(450)에서, 원격 장치(112)의 프로세서(334)는 확인 코드를 수신하고, 동작(455)에서, 프로세서(334)는 비트 맵을 구성하고, 공유 비밀을 사용하여 비트 맵을 암호화한다. 또한, 원격 장치(112)의 프로세서(334)는 사용자 명과 패스워드 조합 등의 사용자 입력 요소들에 대한 좌표들을 생성한다.

[0038] 비트 맵은 전자 장치(110)에 다시 전달된다. 일부 실시 형태에서, 보안 스프라이트 생성기(179)는 디스플레이(138) 상에 비트 맵을 렌더링할 수 있다. 다른 실시 형태에서, 비신뢰 실행 복합체 내의 그래픽 프로세서(들)(124)는 디스플레이(138) 상에 비트 맵을 렌더링할 수 있다. 도 3을 간단히 참조하면, 렌더링된 비트 맵은 디스플레이 상에 대화 상자(380)를 제시한다. 대화 상자(380)는, 사용자 명 용도의 입력 윈도우(382), 패스워드 용도의 입력 윈도우(384), 및 사용자가 대화 상자(380)에 입력을 입력하기 위한 키보드(386) 등의 입력 메카니즘을 포함할 수 있다.

[0039] 사용자는 키보드(386)를 이용하여 각각의 윈도우(382, 384)에서 사용자 명/패스워드 조합을 입력할 수 있다. 동작(475)에서, 입력은 보안 제어기에 수신된다. 일부 실시 형태에서, 신뢰 실행 엔진은, 대화 상자(380)에의 입력이 비신뢰 실행 복합체에 보이지 않도록, 시스템 하드웨어로부터 비트 맵 영역을 차단한다. 이러한 실시 형태에서, 입력은 입/출력 인터페이스(178)에 의해 직접 검출될 수 있다. 다른 실시 형태에서, 입력은, 비신뢰 실행 복합체에서 실행되는 인증 플러그 인(322)에 의해 포착될 수 있는 입력에 의해 검출될 수 있다. 이러한 실시 형태에서, 입력 좌표가 원격 장치(112)의 프로세서(334)에서 생성되었기 때문에, 멀웨어에 의한 스니핑(sniffing)이 억제됨을 유의해야 한다. 따라서, 멀웨어는 입력 좌표 또는 좌표와 연관된 입력에 대한 지식이 부족하다.

[0040] 동작(480)에서, 사용자 입력은 유효성이 검증된다. 예로서, 일부 실시 형태에서, 인증 모듈(176)은, 식별 패킷을 생성하여 래핑하고(wraps), 패킷이 안전하게 NFC 통신 링크를 통해 얻어지고 WYS 핀이 WYSIWYS 모듈(182)을 이용하여 안전하게 얻어졌음을 증명하는 서명을 적용하는 EPID 모듈(184)을 호출한다. 전자 장치(110)는, 사용자 입력을 검증하고 전자 장치(110)에 인가 응답을 반환하는 원격 검증 서버(460)에 래핑된 식별 패킷을 전달한다. 일부 실시 형태에서, 검증 응답이, 신뢰 실행 엔진(170) 내의 I/O 인터페이스(178)를 통해 수신되고, 따라서 전자 장치(110)의 비신뢰 운영 환경에 액세스할 수 없다.

[0041] 동작(485)에서, 인증 모듈(176)은 원격 검증 서버(460)로부터의 응답을 리뷰한다. 만약, 동작(485)에서, 원격 인증 서버(430)로부터의 응답이, 로그인이 인가되지 않은 것을 나타내면, 제어가 동작(490)으로 진행되고 로그인 절차가 종료되며 액세스가 거부된다. 이와 대조적으로, 동작(485)에서, 원격 인증 서버(430)로부터의 응답이, 로그인이 인가된 것을 나타내면, 제어는 동작(495)으로 진행되고, 보안 통신 세션이 전자 장치(110)와 거래 시스템(350) 사이에서 개시될 수 있다.

[0042] 상술한 바와 같이, 일부 실시 형태에서, 전자 장치(110)는 컴퓨터 시스템으로서 구체화될 수 있다. 도 5는 일부 실시 형태에 따른 컴퓨터 시스템(500)의 개략도이다. 컴퓨터 시스템(500)은 컴퓨팅 장치(502) 및 (예를 들어, 컴퓨팅 장치(502)에 전력을 공급하는) 전원 어댑터(504)를 포함한다. 컴퓨팅 장치(502)는 랩톱(또는 노트북) 컴퓨터, 개인 휴대 정보 단말기, 데스크톱 컴퓨팅 장치(예를 들면, 워크 스테이션 또는 데스크탑 컴퓨터), 랙 장착형 컴퓨터 장치 등과 같은 소정의 적절한 컴퓨팅 장치일 수 있다.

[0043] 컴퓨팅 장치(502)의 다양한 구성 요소에는 하나 또는 그 이상의 다음과 같은 소스로부터 (예를 들어, 컴퓨팅 장치의 전력 공급 장치(506)를 통해) 전력이 제공될 수 있다: 하나 이상의 배터리 팩, 교류 전류(AC) 콘센트(예를 들면, 변압기 및/또는 전원 어댑터(504) 등의 어댑터를 통해), 차량용 전원 공급 장치, 비행기 전력 공급 장치 등. 일부 실시 형태에서, 전원 어댑터(504)는 전력 공급원의 출력(예를 들어, 약 110VAC 내지 240VAC의 AC 콘센트 전압)을 약 5VDC 내지 12.6VDC 사이의 범위의 직류(DC) 전압으로 변환할 수 있다. 따라서, 전원 어댑터(504)는 AC/DC 어댑터일 수 있다.

[0044] 컴퓨팅 장치(502)는 하나 이상의 중앙 처리 장치(508)(들)(CPU들)을 포함할 수 있다. 일부 실시 형태에서, CPU(508)는, 캘리포니아주 산타 클라라 소재의 인텔® 주식회사에서 이용할 수 있는 펜티엄® II 프로세서 제품군, 펜티엄® III 프로세서, 펜티엄® IV, 또는 코어2 듀오 프로세서를 포함하는 프로세서의 펜티엄® 제품군 중 하나 이상의 프로세서일 수 있다. 대안적으로, 인텔의 아이테니엄®, XEON 및 셀러론® 프로세서와 같은 다른 CPU가 사용될 수 있다. 또한, 다른 제조업자로부터의 하나 또는 그 이상의 프로세서가 이용될 수 있다. 또한, 프로세서는 단일 또는 다중 코어 설계를 가질 수 있다.

[0045] 칩셋(512)은 CPU(508)에 결합 또는 통합될 수 있다. 칩셋(512)은, 메모리 제어 허브(MCH)(514)를 포함할 수 있다. MCH(514)는 메인 시스템 메모리(518)에 결합되는 메모리 제어기(516)를 포함할 수 있다. 메인 시스템 메모리(518)는 CPU(508), 또는 시스템(500)에 포함된 임의의 다른 장치에 의해 실행되는 명령어의 시퀀스 및 데이터를 저장한다. 일부 실시 형태에서, 메인 시스템 메모리(518)는 랜덤 액세스 메모리(RAM)를 포함하지만; 메인 시스템 메모리(518)는 동적 RAM(DRAM), 동기식 DRAM(SDRAM) 등과 같은 다른 메모리 유형을 사용하여 구현될 수 있다. 추가 장치는 또한 다중 CPU 및/또는 다중 시스템 메모리와 같이, 버스(510)에 결합될 수 있다.

[0046] MCH(514)는 또한 그래픽 가속기(522)에 연결된 그래픽 인터페이스(520)를 포함할 수 있다. 일부 실시 형태에서, 그래픽 인터페이스(520)는 가속 그래픽 포트(AGP)를 통해 그래픽 가속기(522)에 결합된다. 일부 실시 형태에서, (평판 디스플레이와 같은) 디스플레이(540)는, 예를 들어, 비디오 메모리 또는 시스템 메모리 등의 기억 장치에 저장된 이미지의 디지털 표현을, 디스플레이에 의해 해석되고 표시되는 디스플레이 신호로 변환하는 신호 변환기를 통해 그래픽 인터페이스(520)에 결합될 수 있다. 디스플레이 장치에 의해 생성된 디스플레이(540)의 신호는, 디스플레이에 의해 해석되고 이어서 디스플레이에 표시되기 전에 다양한 제어 장치를 통과할 수 있다.

[0047] 허브 인터페이스(524)는 플랫폼 컨트롤 허브(PCH)(526)에 MCH(514)를 결합시킨다. PCH(526)는 컴퓨터 시스템(500)에 결합된 입/출력(I/O) 장치에 인터페이스를 제공한다. PCH(526)는 주변 컴포넌트 상호 접속(PCI) 버스에 결합될 수 있다. 따라서, PCH(526)는 PCI 버스(530)에 인터페이스를 제공하는 PCI 브릿지(528)를 포함한다. PCI 브릿지(528)는 CPU(508)와 주변 장치 간의 데이터 경로를 제공한다. 또한, I/O 상호 접속 토폴로지의 다른 유형은, 미국 캘리포니아주 산타 클라라 소재의 인텔® 주식회사를 통해 이용할 수 있는 PCI 익스프레스 아키텍처와 같이 이용될 수 있다.

[0048] PCI 버스(530)는 오디오 장치(532)와 하나 이상의 디스크 드라이브(들)(534)에 결합될 수 있다. 다른 장치가 PCI 버스(530)에 결합될 수 있다. 또한, CPU(508)와 MCH(514)는 단일 칩을 형성하도록 조합될 수 있다. 또한, 그래픽 가속기(522)는 다른 실시 형태에서 MCH(514) 내에 포함될 수 있다.

[0049] 또한, PCH(526)에 결합된 다른 주변 장치는, 다양한 실시 형태에서, 통합형 드라이브 전자 장치(IDE) 또는 소형 컴퓨터 시스템 인터페이스(SCSI) 하드 드라이브(들), 범용 직렬 버스(USB) 포트(들), 키보드, 마우스, 병렬 포트(들), 직렬 포트(들), 플로피 디스크 드라이브(들), 디지털 출력 지원(예를 들면, 디지털 비디오 인터페이스(DVI)) 등을 포함할 수 있다. 따라서, 컴퓨팅 장치(502)는 휘발성 및/또는 비휘발성 메모리를 포함할 수 있다.

[0050] 따라서, 전자 장치 내에서 확장성 보안 실행을 구현하는 아키텍처 및 관련 방법이 여기에 설명되어 있다. 일부 실시 형태에서, 아키텍처는 별도 장치의 보안 제어기를 위해 계산 비용 처리 작업을 수행하도록 원격 전자 장치 플랫폼에 내장된 하드웨어 기능을 사용한다. 실행 복합체는 전자 장치의 멀웨어에 동작이 접근하지 않도록 신뢰 실행 엔진에서 구현될 수 있다. 일부 실시 형태에서, 신뢰 실행 엔진은 원격 또는 부착 장치, 예를 들면, 동글(dongle)에서 구현될 수 있다.

[0051] 본원에 언급된 바와 같은 용어 "로직 명령어"는 하나 이상의 논리 연산을 수행하기 위한 하나 이상의 머신에 의해 이해될 수 있는 표현에 관한 것이다. 예를 들어, 로직 명령어는 하나 이상의 데이터 객체에 대해 하나 이상의 동작을 실행하기 위한 프로세서 컴파일러에 의해 해석될 수 있는 명령어를 포함할 수 있다. 그러나, 이것은 단지 머신-판독 가능한 명령어의 일례이며, 실시 형태는 이에 국한되지 않는다.

[0052] 본원에 언급된 바와 같은 용어 "컴퓨터 판독 가능 매체"는 하나 이상의 머신에 의해 인지가능한 표현을 유지할 수 있는 매체에 관한 것이다. 예를 들어, 컴퓨터 판독 가능 매체는 컴퓨터 판독 가능 명령어 또는 데이터를 저장하기 위한 하나 이상의 저장 장치를 포함할 수 있다. 이러한 저장 장치는, 예를 들어, 광학, 자기 또는 반도체 저장 매체 등의 저장 매체를 포함할 수 있다. 그러나, 이것은 단지 컴퓨터 판독 가능 매체의 일례이며, 실시 형태는 이에 국한되지 않는다.

[0053] 본 명세서에서 언급되는 용어 "로직"은 하나 이상의 논리 연산을 수행하기 위한 구조에 관한 것이다. 예를 들어, 로직은 하나 이상의 입력 신호에 기초하여 하나 이상의 출력 신호를 제공하는 회로를 포함할 수 있다. 이러한 회로는 디지털 입력을 수신하고 디지털 출력을 제공하는 유한 상태 머신, 또는 하나 이상의 아날로그 입력 신호에 응답하여 하나 이상의 아날로그 출력 신호를 제공하는 회로를 포함할 수 있다. 이러한 회로는 주문형 집적 회로(ASIC) 또는 필드 프로그래머블 게이트 어레이(FPGA)에 제공될 수 있다. 또한, 로직은 이러한 머신 판독 가능한 명령어를 실행하는 처리 회로와 조합하여 메모리에 저장된 머신 판독 가능 명령어를 포함할 수 있다. 그러나, 이들은 단지 로직을 제공할 수 있는 구조의 일례이며, 실시 형태는 이에 국한되지 않는다.

[0054] 여기에 설명된 방법 중 일부는, 컴퓨터 판독 가능 매체 상의 로직 명령어로서 구체화될 수 있다. 프로세서 상에서 실행될 때, 논리 명령어는 프로세서가 상기 설명한 방법을 구현하는 특수 목적 머신로서 프로그램되게 한다. 여기에 설명된 방법을 실행하는 논리 명령어에 의해 구성될 때, 프로세서는, 상기 방법을 수행하기 위한 구조를 구성한다. 대안적으로, 여기에 설명된 방법은, 예를 들어, 필드 프로그래머블 게이트 어레이(FPGA), 주문형 집적 회로(ASIC) 등에서의 논리로 축소될 수 있다.

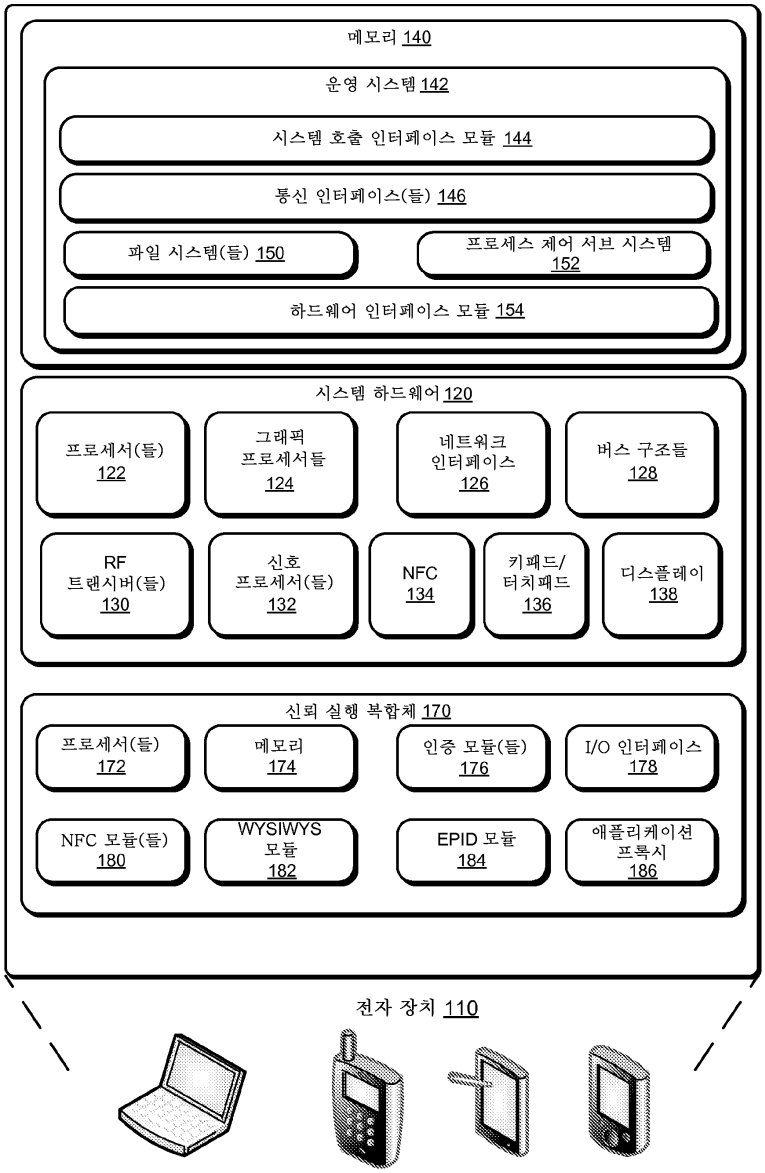
[0055] 설명 및 특허 청구 범위에서, 용어 "결합 및 연결"이, 그들 파생어와 함께, 사용될 수 있다. 특정 실시 형태에서, 연결은 2개 이상의 요소가 서로 직접 물리적으로 또는 전기적으로 접촉되는 것을 나타내기 위해 사용될 수 있다. 결합은 2개 이상의 요소들이 직접 물리적으로 또는 전기적으로 접촉하고 있음을 의미할 수 있다. 그러나, 결합은 또한 2개 이상의 소자가 서로 직접 접촉하고 있지는 않지만, 여전히 서로 협력하거나 상호 작용할 수 있음을 의미할 수 있다.

[0056] "한 실시 형태" 또는 "일부 실시 형태"에 대한 명세서에서의 참조는, 실시 형태와 관련하여 설명된 특별한 특징, 구조, 또는 특성이, 적어도 구현에 있어서 포함된다는 것을 의미한다. 명세서의 여러 곳에서 "한 실시 형태에서"라는 문구의 출연은 모두 동일한 실시 형태를 지칭할 수도 있거나 그렇지 않을 수도 있다.

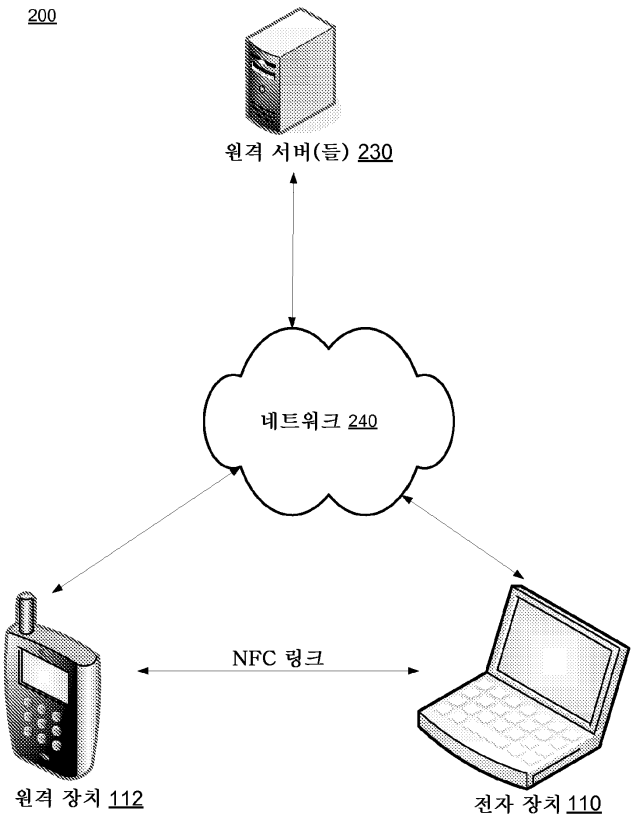
[0057] 실시 형태는 구조적 특징 및/또는 방법론적 작용에 특정한 언어로 설명되었지만, 그 청구된 주제가, 설명된 특정한 특징 또는 동작에 한정되지 않을 수 있다는 것이 이해되어야 한다. 오히려, 특정한 특징 및 작용은 청구된 주제를 구현하는 샘플 형태로서 개시된다.

도면

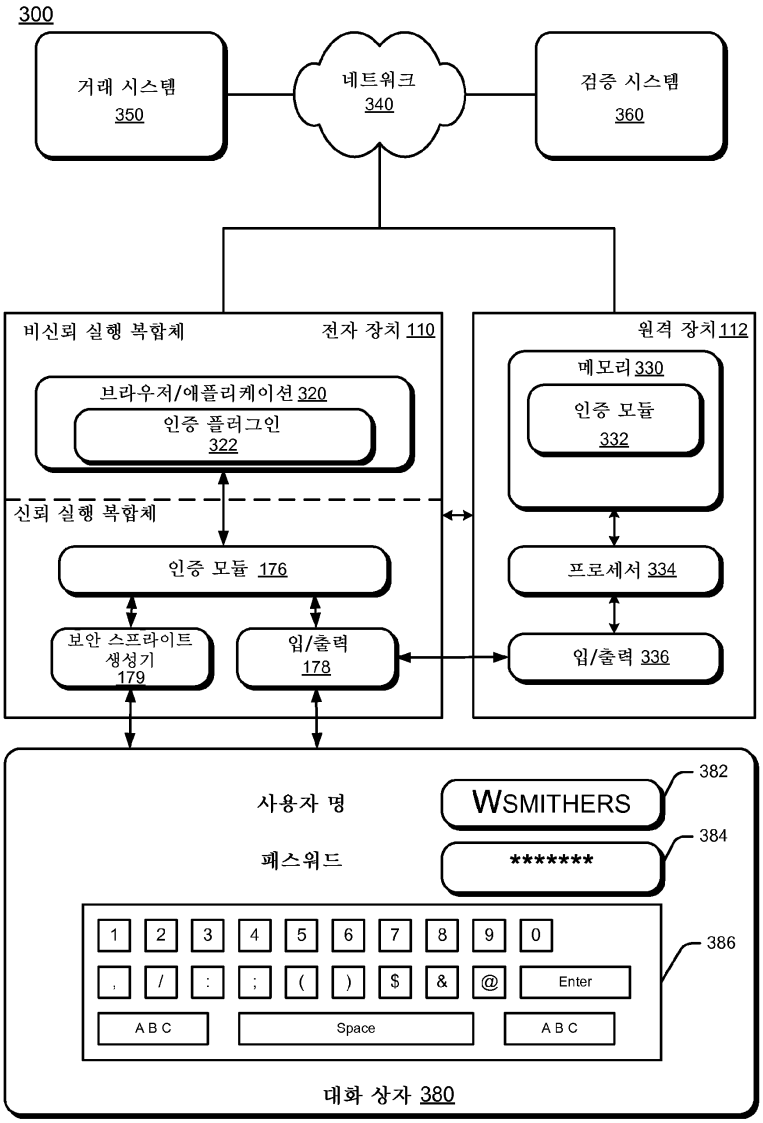
도면1


메모리 140
운영 시스템 142
시스템 호출 인터페이스 모듈 144
통신 인터페이스(들) 146
파일 시스템(들) 150
프로세스 제어 서브 시스템 152
하드웨어 인터페이스 모듈 154
시스템 하드웨어 120
프로세서(들) 122
그래픽 프로세서들 124
네트워크 인터페이스 126
버스 구조들 128
RF 트랜시버(들) 130
신호 프로세서(들) 132
NFC 134
키패드/터치패드 136
디스플레이 138
신뢰 실행 복합체 170
프로세서(들) 172
메모리 174
인증 모듈(들) 176
I/O 인터페이스 178
NFC 모듈(들) 180
WYSIWYS 모듈 182
EPID 모듈 184
애플리케이션 프록시 186
전자 장치 110

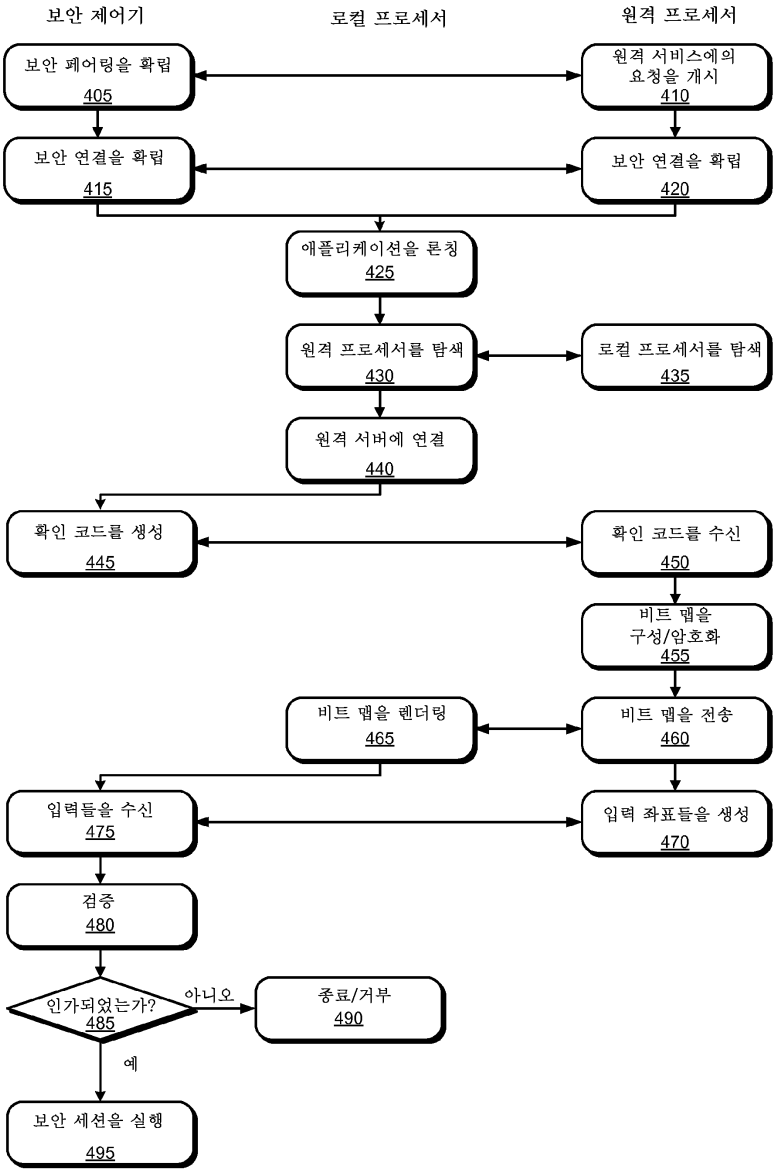
도면2



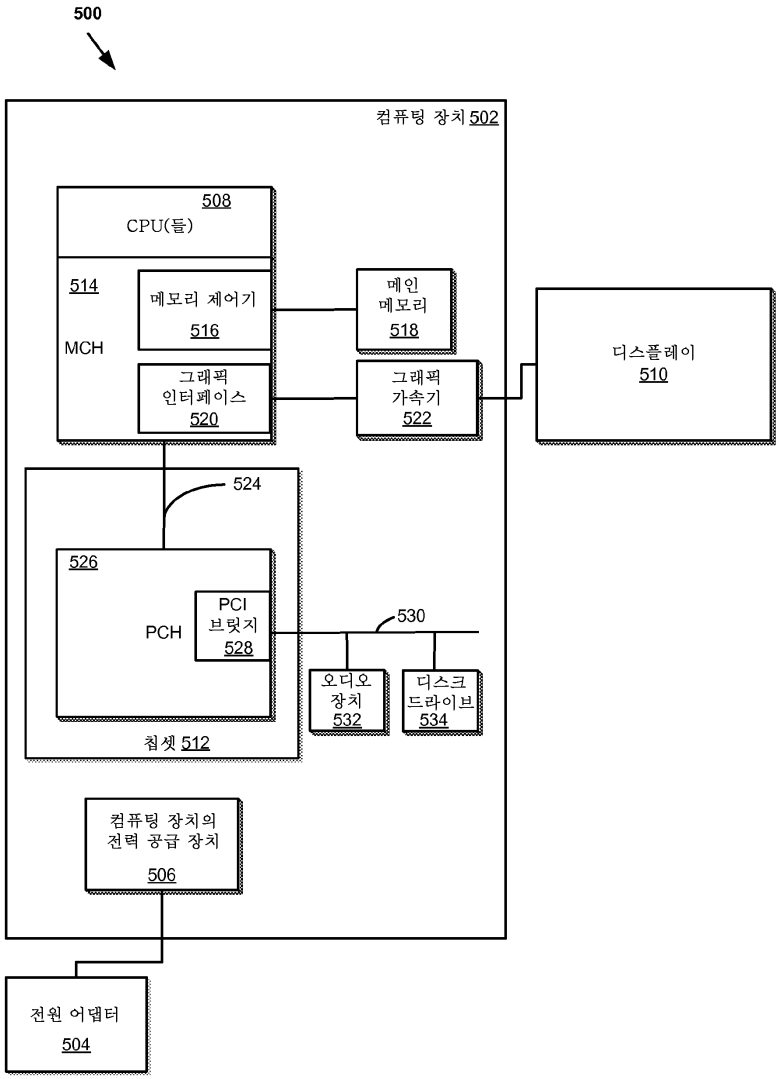
도면3


300
거래 시스템
350
네트워크
340
검증 시스템
360
비신뢰 실행 복합체
전자 장치 110
브라우저/애플리케이션 320
인증 플러그인
322
신뢰 실행 복합체
인증 모듈 176
보안 스프라이트
생성기
179
입/출력
178
원격 장치 112
메모리 330
인증 모듈
332
프로세서 334
입/출력 336
사용자 명
WSMITHERS
382
패스워드
****
384
1 2 3 4 5 6 7 8 9 0
, / : ; ( ) $ & @ Enter
A B C
Space
A B C
386
대화 상자 380

도면4


보안 제어기
로컬 프로세서
원격 프로세서
보안 페어링을 확립
405
원격 서비스에의 요청을 개시
410
보안 연결을 확립
415
보안 연결을 확립
420
애플리케이션을 론칭
425
원격 프로세서를 탐색
430
로컬 프로세서를 탐색
435
원격 서버에 연결
440
확인 코드를 생성
445
확인 코드를 수신
450
비트 맵을 구성/암호화
455
비트 맵을 렌더링
465
비트 맵을 전송
460
입력들을 수신
475
입력 좌표들을 생성
470
검증
480
인가되었는가?
485
아니오
종료/거부
490
예
보안 세션을 실행
495

도면5


500
컴퓨팅 장치 502
508
CPU(들)
514
MCH
메모리 제어기
516
그래픽
인터페이스
520
메인
메모리
518
그래픽
가속기
522
디스플레이
510
524
526
PCH
PCI
브릿지
528
530
오디오
장치
532
디스크
드라이브
534
칩셋 512
컴퓨팅 장치의
전력 공급 장치
506
전원 어댑터
504