(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년11월01일
(11) 등록번호 10-1671351
(24) 등록일자 2016년10월26일

(51) 국제특허분류(Int. Cl.)
G06F 21/45 (2013.01) *G06F 21/31* (2013.01)
G06F 21/33 (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06F 21/45 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2015-7013180
(22) 출원일자(국제) 2013년12월03일
심사청구일자 2015년05월19일
(85) 번역문제출일자 2015년05월19일
(65) 공개번호 10-2015-0070388
(43) 공개일자 2015년06월24일
(86) 국제출원번호 PCT/US2013/072911
(87) 국제공개번호 WO 2014/099355
국제공개일자 2014년06월26일
(30) 우선권주장
13/721,760 2012년12월20일 미국(US)
(56) 선행기술조사문헌
US20080123862 A1*
WO2012087844 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인텔 코포레이션
미합중국 캘리포니아 95054 산타클라라 미션 칼리지 블러바드 2200
(72) 발명자
스미스 네드 엠
미국 오레곤주 97124 힐스보로 엠에스: 에이치에프3-27 노스이스트 엘람 영 파크웨이 5200
카힐 코노어 피
미국 버지니아주 20197 워터포드 데이몬트 레인 38580
(뒷면에 계속)
(74) 대리인
제일특허법인

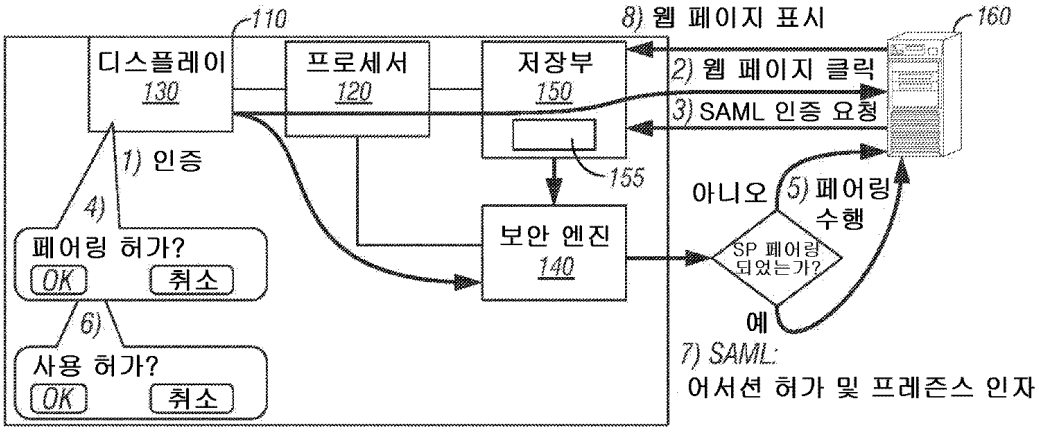
전체 청구항 수 : 총 20 항 심사관 : 문남두

(54) 발명의 명칭 **통합 보안 엔진을 사용하는 웹 서비스 제공자를 위한 프라이버시 강화 키 관리**

(57) 요 약

실시예에서, 프로세서의 보안 엔진은 웹 서비스를 제공하고 네트워크를 통해 시스템에 연결된 제 2 시스템을 가진 서비스 제공자와 시스템의 사용자를 연관시키는 키 페어링의 제 1 키 페어를 생성하고, 제 2 시스템이 식별자 제공자 로직부가 신뢰 실행 환경에서 실행중임을 검증할 수 있게 하도록 제 2 시스템과 보안 통신을 수행하며, 검증에 응답하여, 제 2 시스템으로 제 1 키 페어의 제 1 키를 전달하는 식별자 제공자 로직부를 포함한다. 이 키는 제 2 시스템이 사용자가 멀티-인자 인증에 따라 시스템에 인증되었다는 식별자 제공자 로직부에 의해 전달된 어서션을 검증할 수 있게 할 수 있다. 다른 실시예가 설명되고 청구된다.

대 표 도



(52) CPC특허분류
G06F 21/33 (2013.01)
H04L 63/0815 (2013.01)
H04L 2463/082 (2013.01)
(72) 발명자
무어 빅토리아 씨
미국 애리조나주 85044 피닉스 사우스 콜라 캐년 드라이브 14244
마틴 제이슨
미국 오레곤주 97007 비버톤 사우스웨스트 153번 애비뉴 6248
쉘러 마이카 제이
미국 오레곤주 97124 힐스보로 노스이스트 하이드 스트리트 2447

명 세 서

청구범위

청구항 1

시스템(a system)으로서,

식별자 제공자 로직부(an identity provider logic)를 포함한 보안 엔진(a security engine)과,

상기 보안 엔진에 상기 시스템의 사용자에 관하여 센싱된 정보를 제공하는 적어도 하나의 센서-상기 보안 엔진은 상기 센싱된 정보를 사용하여 상기 사용자를 인증(authenticate)하는 것임-를 포함하되,

상기 식별자 제공자 로직부는,

상기 시스템의 사용자와 서비스 제공자(a service provider)를 연관(associating)시키는 키 페어링(a key pairing)의 제 1 키 페어(a first key pair)를 생성 - 상기 서비스 제공자는 웹 서비스(a web service)를 제공하고, 네트워크를 통해 상기 시스템에 연결된 제 2 시스템(a second system)을 포함함 - 하고,

상기 제 2 시스템과의 보안 통신(a secure communication)을 수행하여, 상기 식별자 제공자 로직부가 상기 시스템의 신뢰 실행 환경(trusted execution environment) 내에서 실행중임을 상기 제 2 시스템이 검증(verify)할 수 있게 하도록 하고,

상기 검증(verification)에 응답하여, 상기 제 1 키 페어의 제 1 키(a first key)를 상기 제 2 시스템으로 전달 - 상기 제 1 키 페어의 제 1 키는, 상기 사용자가 멀티-인자 인증(a multi-factor authentication)에 따라 상기 시스템에 인증되었다고 상기 식별자 제공자 로직부가 전달한 어서션(assertion)을 상기 제 2 시스템이 검증(verify)할 수 있도록 하기 위한 것이고, 상기 키 페어링은 상기 서비스 제공자에 의해 생성되는 제 2 키 페어(a second key pair)를 더 포함함 - 하는

시스템.

청구항 2

제 1 항에 있어서,

상기 식별자 제공자 로직부는 상기 어서션을 생성하고 상기 제 1 키 페어의 제 2 키로 상기 어서션에 서명하며,

상기 서비스 제공자는, 상기 서명된 어서션의 검증에 응답하여, 상기 제 2 시스템을 통해 상기 웹 서비스에 대한 액세스를 가능하게 하는

시스템.

청구항 3

제 2 항에 있어서,

상기 보안 엔진은 상기 사용자가 상기 사용자와 상기 서비스 제공자를 연관시키는 상기 키 페어링을 생성하도록 시도하고 있음을 확인하는 요청을 생성하되, 상기 요청은 상기 시스템의 신뢰 경로를 따라 전달되는 것인

시스템.

청구항 4

제 2 항에 있어서,

상기 보안 엔진은 상기 사용자가 상기 웹 서비스에 액세스하도록 시도하기 전에 상기 멀티-인자 인증에 따라 상

기 사용자를 인증하는

시스템.

청구항 5

제 1 항에 있어서,

상기 식별자 제공자 로직부는 상기 제 2 시스템으로부터 인증 요청을 수신하고 상기 인증 요청에 응답하여 상기 어서션을 생성하는

시스템.

청구항 6

제 1 항에 있어서,

상기 보안 엔진은 프레즌스 검출 센서 또는 사용자 인증 센서에 대응하는 상기 적어도 하나의 센서로부터 상기 센싱된 정보를 수신하는

시스템.

청구항 7

클라이언트 시스템의 보안 엔진의 식별자 제공자 로직부에서 인증 요청을 수신하는 단계 -상기 인증 요청은 서비스 제공자로부터 수신되며, 상기 서비스 제공자는 상기 클라이언트 시스템의 사용자가 액세스하도록 시도하는 웹 서비스를 가짐- 와,

상기 사용자가 멀티-인자 인증을 통해 상기 클라이언트 시스템에 인증되었다는 어서션을 생성하고, 상기 사용자와 상기 서비스 제공자를 연관시키는 키 페어링의 제 1 키로 상기 어서션에 서명하는 단계 -상기 키 페어링은 상기 보안 엔진에 의해 생성되는 제 1 키 페어 및 상기 서비스 제공자에 의해 생성되는 제 2 키 페어를 포함함- 와,

상기 서비스 제공자에게 상기 서명된 어서션을 전달하는 단계 -상기 서비스 제공자는, 상기 서명된 어서션의 검증에 응답하여 상기 사용자와의 시도-응답 상호작용 없이 상기 사용자가 상기 웹 서비스에 대한 액세스를 가능하게 함- 를 포함하는

방법.

청구항 8

제 7 항에 있어서,

상기 사용자가 상기 웹 서비스에 액세스하도록 시도하기 전에 상기 멀티-인자 인증에 따라 상기 사용자를 인증하는 단계를 더 포함하는

방법.

청구항 9

제 7 항에 있어서,

상기 클라이언트 시스템의 브라우저 애플리케이션에서 상기 인증 요청을 수신하고 상기 인증 요청을 상기 보안 엔진으로 재지정하는 단계를 더 포함하는

방법.

청구항 10

제 7 항에 있어서,

상기 클라이언트 시스템의 신뢰 경로를 통해 전달되는 요청에 응답하여, 상기 사용자가 사용자 입력을 통해 상기 웹 서비스에 액세스하도록 시도한다는 것을 확인하는 단계를 더 포함하되,

상기 신뢰 경로는 상기 클라이언트 시스템 상에서 실행되는 멀웨어에게는 액세스불가능한 것인

방법.

청구항 11

제 10 항에 있어서,

상기 키 페어링을 생성하기 위한 사용자 승인에 응답하여 상기 보안 엔진 내에 상기 제 1 키 페어를 생성하는 단계를 더 포함하는

방법.

청구항 12

제 11 항에 있어서,

상기 클라이언트 시스템의 신뢰 실행 환경을 검증하고 상기 제 1 키 페어의 공개 키를 제공하며 상기 서비스 제공자에 의해 생성된 상기 제 2 키 페어의 공개 키를 수신하기 위해, 상기 클라이언트 시스템과 상기 서비스 제공자 사이에서 시그마 세션을 통해 통신하는 단계를 더 포함하는

방법.

청구항 13

제 12 항에 있어서,

상기 클라이언트 시스템 내에 데이터 구조를 저장하는 단계를 더 포함하되,

상기 데이터 구조는 상기 제 1 키 페어의 개인 키 및 공개 키와, 상기 제 2 키 페어의 공개 키를 포함하는

방법.

청구항 14

제 13 항에 있어서,

상기 어서션에 서명하도록 상기 데이터 구조에 액세스하는 단계를 더 포함하는

방법.

청구항 15

제 7 항에 있어서,

상기 사용자로부터 사용자 이름 또는 암호를 수신하지 않고도 상기 웹 서비스로의 사용자 액세스를 가능하게 하

는 단계를 더 포함하는

방법.

청구항 16

제 7 항에 있어서,

상기 웹 서비스를 위한 사용자 계정을 사용자 이름 및 암호 메커니즘을 통해 연관(association)하는 것으로부터 상기 키 페어링을 통해 연관하는 것으로 바꾸는 단계를 더 포함하는

방법.

청구항 17

명령어를 포함하는 컴퓨터 판독가능 기록 매체로서,

상기 명령어는 실행되는 경우 서비스 제공자의 시스템으로 하여금

서비스 제공자의 시스템에서, 사용자 이름 또는 암호 없이 상기 서비스 제공자의 웹사이트를 통해 계정에 액세스하기 위한 사용자 요청을 수신하는 것과,

상기 시스템에서 사용자의 클라이언트 시스템으로 승인 요청을 전달하여, 상기 사용자가 멀티-인자 인증을 통해 상기 클라이언트 시스템에 인증되었다는 어서션을 획득하도록 하는 것 －상기 어서션은 상기 사용자와 상기 서비스 제공자를 연관시키는 키 페어링의 제 1 키로 서명되고, 상기 키 페어링은 제 1 키 페어 및 제 2 키 페어를 포함하며, 상기 제 1 키 페어는 상기 제 1 키를 포함하고 상기 클라이언트 시스템에서 생성되고, 상기 제 2 키 페어는 상기 서비스 제공자의 시스템에서 생성됨－ 과,

상기 클라이언트 시스템으로부터 상기 어서션을 수신하는 것과,

상기 어서션을 검증하고, 상기 검증에 응답하여 상기 웹사이트를 통해 상기 계정에 대한 액세스를 허가하게 하는 것을 가능하게 하는

컴퓨터 판독가능 기록 매체.

청구항 18

제 17 항에 있어서,

상기 서비스 제공자의 시스템이, 상기 클라이언트 시스템의 신뢰 실행 환경을 검증하고 상기 키 페어링의 제 1 키 페어의 제 2 키를 수신하기 위해, 시그마 세션을 통해 상기 클라이언트 시스템과의 통신을 수행할 수 있도록 하는 명령어를 더 포함하는

컴퓨터 판독가능 기록 매체.

청구항 19

제 17 항에 있어서,

상기 서비스 제공자의 시스템이, 상기 클라이언트 시스템에 제공할 인증서 정보를 획득하기 위해, 상기 서비스 제공자의 시스템과 원격 온라인 인증서 상태 제공자 간의 통신을 수행할 수 있도록 하는 명령어를 더 포함하는

컴퓨터 판독가능 기록 매체.

청구항 20

제 17 항에 있어서,

상기 서비스 제공자의 시스템이 사용자 이름 및 암호 메커니즘을 통한 계정의 연관을 상기 키 페어링을 통한 연관으로 바꿀 수 있도록 하는 명령어를 더 포함하는

컴퓨터 판독가능 기록 매체.

발명의 설명

배 경 기 술

[0001] 컴퓨터 사용자는 인터넷 및 웹 기반 상호작용의 급증 때문에 루틴 기반으로 10 명 심지어 100 명의 인터넷 기반 웹 서비스 제공자와 상호작용한다. 각각의 서비스 제공자는 자신의 고객에 대한 근접 액세스를 유지하도록 가입자 베이스를 유지하기를 원한다. 그 결과, 사용자는 10 개 및 심지어 100 개의 계정 및 대응하는 사용자 이름과 암호를 관리할 것으로 예상된다. 사용자는 흔히 웹 기반 서비스에 쉽게 액세스하도록 암호 크리덴셜을 오용한다(예컨대, 취약한 암호를 사용하고, 암호와 사용자 이름을 재사용한다). 크로스 사이트 계정 해킹, 서비스 제공자 공모 및 사용자 트랜잭션의 추적을 포함하는 몇몇 문제가 발생할 수 있다. 이들 공격은 정보, 실제 자산의 사용자 손실 제어, 명예 훼손 및 심지어 실직을 초래한다.

[0002] 사용자 연구는 암호 관리가 주요 유용성 시도이고 웹 계정 관리 부실에 대한 기여 인자임을 나타낸다. 현재 해결책은 사용자가 암호를 생성하고 일련의 암호 리셋 시도 질의(예컨대, 좋아하는 애완동물)를 제공하는 것을 수반하는 사용자 계정 생성 프로토콜에 의존한다. 여러 번 시도 정보가 공개되고/되거나 쉽게 추측될 수 있으므로 이들 메커니즘은 취약하다. 다른 방안은 공개 키 기반구조(public key infrastructure:PKI)를 웹사이트 및 클라이언트로 통합한다. 그러나, 사용자 클라이언트는 각각의 서비스 제공자와 함께 사용할 클라이언트 X.509 인증서를 구입해야 하는데, 이 인증서의 가격은 대부분의 사용자에게 엄청나게 비싸다. 이와 유사하게, 특정 서비스 제공자에게 사용자를 인증하는 OTP(one-time-password) 디바이스의 사용은 별도의 OTP 디바이스로 인해 비싼 가격이다. 비용을 줄이는 데 소프트웨어 OTP 디바이스가 사용될 수 있지만, 각각의 서비스 제공자는 특정 OTP 구현을 지원해야 하며, 어떤 경우에 OTP 디바이스는 인증에만 사용될 수 있고 데이터를 암호화하거나 서명하는 데에는 사용될 수 없다.

도면의 간단한 설명

[0003] 도 1은 본 발명의 실시예에 따라 다양한 구성요소 사이의 통신을 도시하는 시스템의 블록도이다.

도 2는 본 발명의 실시예에 따라 시그마 세션에서 발생하는 통신의 하이레벨 뷰이다.

도 3은 본 발명의 실시예에 따라 웹 서비스 제공자와 보안 방법으로 통신하는 방법의 흐름도이다.

도 4는 본 발명의 실시예에 따른 시스템 배치의 블록도이다.

도 5는 실시예가 사용될 수 있는 예시적인 시스템의 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0004] 다양한 실시예에서, 프로세서, 칩셋 등과 같은 반도체 디바이스 내에 신뢰 실행 환경(trusted execution environment:TEE)을 제공하는 보안 엔진에 식별자 제공자(identity provider:IdP) 로직부가 내장될 수 있다. 이 보안 엔진은 본 명세서에서 통합 보안 엔진(converged security engine:CSE)으로 지칭된다. IdP는 실시예에서 표준 SAML(security assertion markup language) 메시지를 사용하여 사용자의 인증 상태를 보고한다. CSE는 민감한 사용자 인증 데이터 및 사용자-서비스 제공자 페어링 키를 보호하는 데 사용된다. 사용자가 서비스 제공자 웹 페이지를 브라우징할 때, 서비스 제공자(SP)는 SAML 재지정 메커니즘을 사용하여 사용자를 인증하도록 시도한다. 이 시도는 사용자가 SP와의 시도-응답 상호작용을 직접 수행할 필요 없이, 시스템에서 자동으로 처리된다. IP를 호스팅하는 CSE는 SAML 시도를 수락한다. 이 방안은, 시도가 재지정될 수 있는 IdP를 사용자가 항상 가질 것이므로, SP로 하여금 SAML을 채용하게 한다. TEE에서 실행하는 CSE도 (이 태스크를 수행할 것을 SP에게 요구하기보다) 사용자를 직접 인증한다. 국부적인 인증 시도 처리는 상당량의 멀티-인자 인증의 복잡도가 SP에게 비밀이 되어, 암호 대안의 채용에 대한 장벽을 낮춘다.

[0005] 보다 구체적으로, 실시예는 사용자를 SP와 연관시키는 사용자-SP 키 페어링의 동적 생성을 지시하고 조정하는 데 SAML 메시지 교환을 사용할 수 있으며, 각각의 SP에는 SP 웹사이트에 대한 사용자의(클라이언트의) 후속 액

세스를 인증하는 상이한 비대칭 또는 대칭 키가 제공된다. 암호를 관리하는 데 사용된 방안과 유사하지만, 이 페어링은 암호를 강한 암호화 크리덴셜로 대체한다. 본 명세서에 설명된 실시예는 사용자 계정, 웹사이트 콘텐츠 등에 대한 인터넷 네트워크 액세스에 관한 것이지만, 인증 프로세스가 SP에 의해 제공된 임의의 웹 서비스에 대한 액세스에 보다 일반적으로 적용가능함을 알아야 한다.

[0006] 사용자는 페어링 관계를 수립하는 데 옵트인(opt-in) 승인을 포함하는 프라이버시 제어를 사용하여 그리고 또한 페어링 키를 사용하는 데(예컨대, SP 인증 시도에 응답하는 데) 옵트인 승인을 사용함으로써 사용자와 SP 사이의 관계의 제어를 유지한다. 프라이버시는 페어링시에 익명의 보안 채널을 수립하도록 제조시에 클라이언트 플랫폼에 내장되는 EPID(enhanced privacy identifier) 키를 사용함으로써 더 강화된다. 익명 식별자는 클라이언트 TEE가 인증됨을 알리지만 어떤 특정 플랫폼이 페어링을 수립하고 있는지는 알리지 않는다. 이 때문에, 프로토콜은 SP가 페어링과 연관되는 이전에 생성된 계정을 사용자가 사용하는 것을 가능하게 한다. 실시예는 또한 페어링 키를 사용자의 계정 정보에 연관시키는 데 OTP 또는 대역 외 메커니즘의 사용을 지원할 수 있다(예컨대, SP는 페어링 키를 사용하여 리턴되는 PIN(personal identification number)과 함께 사용자에게 텍스트 또는 폰 메시지를 전달한다).

[0007] 이제 도 1을 참조하면, 시스템의 다양한 구성요소들 사이의 통신을 나타내는 시스템(100)의 블록도가 도시된다. 보다 구체적으로, 시스템(100)은 클라이언트 시스템(110)이 웹 페이지 서버 또는 서비스 제공자의 다른 시스템을 통해 웹 기반 정보를 제공하는 웹 서비스 제공자와 같은 서비스 제공자(160)의 정보에 액세스하려고 하는 네트워크 환경이다. 다른 구현에서, 클라이언트 시스템(110)은 임의의 유형의 컴퓨팅 디바이스, 예컨대, 데스크톱 컴퓨터, 랩톱 컴퓨터, 울트라북™, 태블릿 컴퓨터, 전자 판독기, 스마트폰 또는 다른 디바이스일 수 있다. 일반적으로, 클라이언트 시스템(110)은 하나 이상의 프로세서 코어 및 다른 엔진을 포함하는 중앙 처리 유닛(CPU)과 같은 프로세서(120), 디스플레이(130), CSE(140), 및 사용자가 인터넷을 통해 웹 페이지에 액세스할 수 있게 하는 브라우저(155)를 포함하며 다양한 애플리케이션을 저장하도록 구성된 저장부(150)를 포함하는 다양한 구성요소를 포함한다. 물론, 쉬운 설명을 위해 이 제한된 개수의 구성요소가 도시되지만, 클라이언트 시스템은 다수의 다른 구성요소를 포함할 수 있다.

[0008] 또한 도 1에 클라이언트 시스템(110) 내의 구성요소들 사이뿐만 아니라 클라이언트 시스템(110)과 서비스 제공자(160) 사이에서 발생하는 다수의 통신이 도시된다. 실시예의 하이레벨 특징부를 설명하기 위해 특정 순서로 도시되었지만, 이들 통신의 전부가 필요한 것은 아님을 알아야 하며 상이한 순서 및 상이한 통신이 발생할 수 있음도 알아야 한다. 초기 동작으로서, 사용자는 시스템 초기화 시에 시스템에 인증하도록 요청될 수 있다. 다수의 상이한 유형의 인증 메커니즘이 제공될 수 있음에 유의해야 하며 몇몇 실시예는 멀티-인자 인증 프로세스가 발생함을 지시하는 것임을 알아야 한다. 본 발명의 범위는 이것으로 제한되지 않지만, 그러한 멀티-인자 인증은 키보드, 터치패드, 터치 스크린 등을 통한 사용자 입력, 근거리 무선 통신, 무선 통신 및/또는 사용자가 시스템의 위치 내에 존재하며 인증된 사용자임을 나타내는 프레즌스 인증을 포함하는 복수의 상이한 인증 메커니즘을 포함할 수 있다. 또 다른 인증 메커니즘은 예컨대, 망막 스캔, 지문 또는 다른 생체인증 기반 식별 메커니즘에 의한 다른 생체인증 특징부를 포함할 수 있다. 그 중에서도 디바이스에 대한 사용자의 운반 또는 액세스, 키 입력 힘 및/또는 속도의 생체인증 감지에 기초한 가속도계 기반 인증을 포함하는 인증에 시스템의 다양한 센서가 사용될 수 있음에 유의한다. 일반적으로, 복수의 생체인증, 근접 및 종래의 (예컨대, 암호) 센서를 포함하는 인증에 사용된 센서는 복수의 상이한 인증 및 프레즌스 모니터링 메커니즘을 포함할 수 있다.

[0009] 이 사용자 인증은 클라이언트 시스템을 사용하는 프로세스에서 초기에 발생할 수 있고, 서비스 제공자에 대한 임의의 액세스와 무관할 수 있다. 이들 인증 절차는 본 명세서에 설명된 바와 같이 IdP 로직부를 포함하는 CSE(140)를 사용하여 적어도 일부분 수행될 수 있다. 본 발명의 범위는 이것으로 제한되지 않지만, CSE(140)는 TEE 내에서 실행될 수 있고, 예컨대, 가상화 기술에 의해 신뢰 실행 환경이 생성되고 실행되게 하는 칩셋의 ME(manageability engine)의 펌웨어와 같은 칩셋 구성요소의 펌웨어로서 구현될 수 있다. 그러므로 이 펌웨어는 ME와 같은 칩셋의 엔진 및/또는 클라이언트 시스템의 범용 코어와 같은 엔진을 포함하는 시스템의 하나 이상의 처리 엔진 상에서 실행할 수 있다.

[0010] 도 1은 웹사이트에 대한 액세스를 위해 사용자를 인증할 때 수행되는 동작의 하이레벨 뷰를 더 도시한다. 보이는 바와 같이, 이 프로세스는 사용자가 브라우저(155)를 통해 액세스하려고 할 때 시작한다. 이 액세스 요청에 응답하여, 서비스 제공자(160)는 실시예에서 SAML 요청일 수 있는 인증 요청을 통신한다. 이 인증 프로세스를 수행하기 전에, 사용자는 클라이언트 시스템과 서비스 제공자 사이에서 암호화 키를 통한 페어링이 허가되는지 여부를 나타내도록 프롬프트될 수 있다. 실시예에서, 이 허가 요청은 프로세서(120)와 디스플레이(130) 사이의 신뢰 경로를 통하여 수행되며, 이에 따라 이 경로는 클라이언트 시스템(110) 상에서 실행하는 멀웨어 엔티티에

도 숨겨지게 된다. 그러므로 다양한 실시예에서, 사용자 승인을 요구하는 이 디스플레이 프레임 이미지는 플랫폼의 사용자에게는 보일 수 있지만, 플랫폼 상에서 실행하는 (잠재적으로 멀웨어 애플리케이션을 포함하는) 애플리케이션 및 운영 시스템(OS)을 포함하는 비신뢰 소프트웨어에 의해서는 액세스될 수 없다. 일 실시예에서, 디스플레이 프레임 이미지는 신뢰 디스플레이 기술을 사용하여 생성될 수 있다. 이 방법에서, 호스트 소프트웨어 및 OS는 그 프레임의 콘텐츠를 복호화할 수 없고, 대신에 그 프레임은 신뢰 엔진으로부터 (예컨대, 집적된) 그래픽 디스플레이 프로세서로 신뢰 출력 경로를 통해 제공된다.

[0011] 사용자 승인이 제공되면, 그 다음에 사용자와 서비스 제공자 사이에 암호화 키의 페어링이 이미 존재하는지 여부가 판정된다. 만일 아니라면, 이 페어링은 예컨대, 시그마(Sigma:Sign-and-mac) 프로토콜을 사용하여 생성될 수 있으며, 그 세부사항은 후술될 것이다. 그 다음에, 개인 페어링 키 정보의 사용이 허용되어야 하는지 여부를 판정하도록 사용자로부터 다른 승인이 요구될 수 있다. 허용된다고 가정하면, 통신은 사용자를 인증할 때 사용된 인증 인자를 기술하는 어서션(assertion)을 제공하기 위해 예컨대, SAML 메커니즘을 통해 CSE(140)로부터 서비스 제공자(160)로 전달된다. 서비스 제공자(160)에 의한 이 응답의 검증에 응답하여, 요청된 웹 페이지에 대한 액세스가 제공될 수 있다. 이에 따라, 브라우저(155)는 디스플레이(130)를 통해 사용자에게 웹 페이지 및/또는 요청된 데이터의 디스플레이를 가능하게 하도록 동작할 수 있다. 도 1의 실시예에서 이 하이레벨로 도시되지만, 본 발명의 범위가 이것으로 제한되지 않음을 알아야 한다.

[0012] 다음으로 도 2를 참조하면, 본 발명의 실시예에 따라 시그마 세션에서 발생하는 통신의 하이레벨 뷰가 도시된다. 보이는 바와 같이, 시그마 세션(200)은 실시예에서 클라이언트 시스템일 수 있는 증명기(prover)(210)와 실시예에서 주어진 인증 기관일 수 있는 온라인 인증서 상태 프로토콜(OCSP) 응답기(230)에 대한 프록시로서 동작하는 서비스 제공자일 수 있는 검증기(220) 사이에서 발생할 수 있다. 보이는 바와 같이, 시그마 세션의 생성을 요구하도록 제 1 메시지가 증명기(210)로부터 검증기(220)로 제공될 수 있다. 이 요청은 차례로 검증기(220)로부터 응답기(230)로의 OCSP 요청 및 결과 응답을 발생시키고 차례로 이 응답에 관한 특정 정보를 제공하는 검증기(220)로부터 증명기(210)로의 메시지로 이어진다. 그 다음에, 증명기(210)는 실시예에서 검증기(220)가 증명기(210)의 진위를 검증하게 하는 EPID 서명과 함께 증명기에 대한 EPID 인증서일 수 있는 인증서 정보를 통신할 수 있다. 따라서, 후속 메시지는 양 방향으로 통신되어 사용자-서비스 제공자 키 페어링이 생성될 수 있다. 이 키 페어링은 각각의 공개 및 개인 키 페어를 포함할 수 있으며, 클라이언트 및 서비스 제공자의 각각이 키 페어를 생성하고 생성된 공개 키를 다른 것에 제공한다. 페어링은 예컨대, 시그마 핸드쉐이크 또는 전송 계층 보안(TLS) 핸드쉐이크의 결과로서 대칭 키도 포함할 수 있다. 페어링 관계가 무-사용자 이름/암호 인증을 레버리지하지 않는 레거시 SPs를 나타내는 데 사용될 수 있는 암호와 같은 덜 강한 다른 속성을 가질 수 있음에 유의한다.

[0013] 이제 도 3을 참조하면, 브라우저 세션의 콘텍스트에서 사용자-서비스 제공자 키 페어링의 생성을 가능하게 하도록 웹 서비스 제공자와 보안 방식으로 통신하는 방법의 흐름도가 도시된다. 도 3에서 보이는 바와 같이, 방법(300)은 서비스 제공자 시스템의 구성요소뿐만 아니라 클라이언트 시스템 내의 다양한 구성요소 양자 모두를 사용하여 수행될 수 있다. 또한 방법(300)에서 상이한 흐름이 존재하며, 주어진 인증 프로세스에서 모든 동작이 수행될 수 있는 것은 아님을 알아야 한다. 보이는 바와 같이, 방법(300)은 블록(310)에서 하나 이상의 인자를 사용하여 클라이언트 시스템에서 CSE에 대해 사용자를 인증함으로써 시작한다. 전술한 바와 같이, 이 인증은 사전 부팅 환경과 같은 클라이언트 시스템과의 세션에서 초기에 발생할 수 있고, 임의의 미래의 웹 브라우징 활동과 무관하게 수행될 수 있다. 또한 전술한 바와 같이, 멀티-인자 인증 프로세스의 다양한 인자가 수행될 수 있다.

[0014] 다음 제어는 사용자가 주어진 서비스 제공자 사이트로 내비게이팅하고 데이터에 액세스하려고 할 수 있는 블록(315)으로 넘어간다. 이 액세스는 클라이언트 시스템 상에서 실행하는 브라우저를 통해서일 수 있다. 검색 엔진, 정보 사이트 등과 같은 다수의 웹사이트에 대해 어떠한 추가 인증도 필요하지 않으며 대신에 웹 페이지의 직접 내비게이팅이 발생할 수 있음에 유의한다. 오히려 본 명세서에 설명된 실시예는 사용자가 예컨대, 구매, 금융 거래 등을 포함하는 인터넷을 통한 임의의 유형의 상업 활동을 의미하도록 본 명세서에서 광범위하게 사용되는 e-커머스를 위해 웹사이트와 보안 방식으로 통신하려고 하는 경우에 사용될 수 있다. 그러한 e-커머스는 사용자가 본 명세서에 설명된 사용자-SP 페어링 키를 사용하지 않고, 종래의 사용자 이름과 암호 없이 사용자의 계정에 로그인하는 것을 가능하게 하는 것도 포함할 수 있다.

[0015] 그러므로 도 3을 더 참조하면, 제어는 그 다음으로 서비스 제공자로부터 인증 요청 메시지가 수신되는 블록(320)으로 넘어간다. 실시예에서 이 메시지는 사용자가 인증의 증거를 제공하도록 요구하는 SAML 인증 요청 메시지이다. 브라우저 내에서 이 메시지의 수신에 응답하여, 브라우저는 SAML 인증 요청을 시스템 CSE 내에서 실

행하는 IdP 로직부로 재지정할 수 있다. 블록(330)에서 이 IdP 로직부는 SAML 요청을 내부 포맷 메시지로 변환할 수 있다. 본 발명의 범위는 실시예에서 이것으로 제한되지 않지만, 이 내부 메시지 포맷은 자바, C++, 자바스크립트 또는 다른 컴퓨터 프로그래밍 언어 데이터 구조 표현을 포함할 수 있다. 제어는 그 다음으로 이 특정 서비스 제공자 내에 페어링이 존재하는지 여부를 판정할 수 있는 다이아몬드(335)로 넘어간다. 만일 예라면, 제어는 블록(375)으로 넘어가며 이하에서 더 논의된다.

[0016] 이와 달리, 페어링이 존재하지 않으면, 제어는 사용자가 예컨대, 신뢰 채널을 통해 페어링 키의 생성을 승인하거나 거절하도록 프롬프트될 수 있는 블록(340)으로 넘어간다. 실시예에서, 이 신뢰 경로는 사용자가 요청 메시지를 수신하게 하지만 (멀웨어를 포함하는) 플랫폼 상에서 실행하는 임의의 다른 엔티티가 이 메시지에 액세스하지 못하게 하는, CSE와 디스플레이 사이의 스푸핑 불가(non-spoofable) 보안 채널일 수 있다. 제어는 그 다음으로 사용자가 이 페어링의 생성을 승인하였는지 여부를 판정하는 다이아몬드(350)로 넘어간다. 실시예에서, 이 승인은 마우스 클릭, 키보드 승인과 같은 사용자 입력 메커니즘을 통해 또는 제스처 입력 디바이스에 의해 수신된 사용자 제스처를 통해서와 같은 다른 방법으로 수신될 수 있다.

[0017] 사용자가 생성을 승인한다고 가정하면, 제어는 페어링 키가 생성될 수 있는 블록(355)으로 넘어간다. 실시예에서, 비대칭 또는 대칭 키 생성 프로세스가 수행되어 이 키를 생성할 수 있다. 그 다음으로 제어는 시그마 세션이 생성될 수 있는 블록(360)으로 넘어간다. 실시예에서 이 시그마 세션은 도 2에 관하여 전술한 바와 같이 수행될 수 있다. 이 세션 동안에, 시그마 메시지는 서비스 제공자가 클라이언트 시스템이 인증된 신뢰 실행 환경 내에 있는지 검증하는 것을 가능하게 하도록 서비스 제공자와 교환될 수 있다. 그 다음에 이 시그마 세션 동안에 페어링 공개 키는 서비스 제공자로 전달될 수 있다(블록 365). 공개 키를 전달하는 대신에, 대칭 키의 사본이 전달될 수 있다. 본 명세서에 설명된 실시예를 사용하여, 사용자가 보안 정보에 액세스하려고 하고/하거나 계정을 가진 각각의 서비스 제공자마다 개별 개인 키 및 공개 키가 생성될 수 있음에 유의한다. 또한 도시되지는 않았지만 쉬운 설명을 위해 이 시그마 세션 동안에 클라이언트 시스템이 서비스 제공자로부터 서비스 제공자의 공개 키 및/또는 서비스 제공자의 인증에 관한 인증서를 포함하는 인증 정보를 수신함을 알아야 한다.

[0018] 이 정보를 사용하여, 데이터 구조가 생성될 수 있다(블록 370). 예컨대, 실시예에서, 서비스 제공자로부터 수신된 공개 키뿐만 아니라 클라이언트에 의해 생성된 공개 키 및 개인 키도 포함하는 페어링 관계, 서비스 제공자 인증서 및 웹사이트 활동 동안에 시그마 세션을 유지/복원하는 데 사용될 수 있는 시그마 세션 키와 같은 추가 정보를 기술하는 기록물(a record)이 암호화된 방식으로 생성 및 저장될 수 있다. 즉, 실시예는, 사용자가 인증된 채로 클라이언트 시스템의 위치에 있음을 보장하도록 몇몇 사전결정된 간격에 따라 웹사이트가 활성을 유지하는 동안 발생하는 시그마 세션을 제공할 수 있다.

[0019] 도 3에 도시되지 않았지만, 사용자 기록물을 생성 및/또는 업데이트하는 유사한 동작이 서비스 제공자 측에서 발생할 수 있다. 특히 사용자가 종래의 사용자 이름과 암호를 사용하여 액세스되는 서비스 제공자와의 계정을 이미 가지고 있는 경우에, 이 사용자 기록물은 본 명세서에 설명된 바와 같이 생성된 키 페어에 따라 발생하는 인증을 제공하는 대신에 기록물을 수정하도록 업데이트될 수 있다. 이와 같이, 실시예는 종래의 사용자 이름과 암호를 사용하여 액세스되는 레거시 웹사이트 계정이 키 페어 메커니즘을 사용하여 액세스되는 웹사이트 계정으로 이동하게 한다. 이를 위해, 서비스 제공자는 레거시 사용자 이름과 암호를 제거하고 웹 서비스와 상호작용할 목적의 키 페어 기반 인증으로 이동하도록, 서비스 제공자 측에서 사용자의 기록물을 업데이트하기 위해 사용자로부터 인증을 더 요구할 수 있다.

[0020] 도 3을 더 참조하면, 이 시점에 사용자와 서비스 제공자 사이에 적합한 키 페어링 구성이 수립될 수 있다. 따라서, 제어가 다이아몬드(335)로 다시 넘어갈 때, 결정은 긍정적이며 이에 따라 동작은 블록(375)으로 넘어간다. 다음 동작은 웹 브라우징 세션이 발생하는 것을 가능하게 하도록 인증된 사용자를 검증하는 것에 관한 것이다. 특히 블록(375)에서 사용자는 브라우징 세션을 가능하게 하기 위해 페어링 키의 사용을 승인하도록 신뢰 채널을 통해 다시 프롬프트될 수 있다. (다이아몬드 378에서) 이 사용자 승인이 수신된다고 가정하면, 제어는 CSE에 사용자를 인증하는 데 사용된 인증 인자를 기술하는 어서션이 생성될 수 있는 블록(380)으로 넘어간다. 실시예에서, 이 어서션은 블록(310)에서 수행된 사용자 멀티-인자 사용자 인증을 기술하는 서명된 SAML 어서션일 수 있다. 이 세션에서는 어떠한 사용자 식별자도 존재하지 않으며, 사용자의 생체인증 또는 다른 정보도 개시되지 않음에 유의한다. 그 대신에, 기술되는 모든 것은 이 인증과 연관된 임의의 특정 사용자 정보라기보다는, 사용자가 사실상 인증되었다는 것과, 이 인증을 수행할 때 사용된 인자라는 것이다. 제어는 그 다음으로 SAML 응답이 서비스 제공자로 전달될 수 있는 블록(385)으로 넘어간다. 그 다음에 블록(390)에서 서비스 제공자는 SAML 응답을 검증할 수 있고 그 후에 검증 하의 데이터 및/또는 웹 페이지에 대한 액세스를 허가할 수 있으며(블록 392), 양자 모두 클라이언트 시스템에 의해 수신되어 브라우저가 웹 페이지 및/또는 데이터를 수신

할 수 있게 한다(블록 395). 도 3의 실시예에서 이 하이레벨로 도시되지만, 본 발명의 범위는 이것으로 제한되지 않음을 알아야 한다.

[0021] 이제 도 4를 참조하면, 개시 실행 프로세스를 도시하는 본 발명의 실시예에 따라 시스템 배치의 블록도가 도시된다. 도 4에서 보이는 바와 같이, 시스템(400)은 CPU(410)를 포함할 수 있다. 다양한 실시예에서, 이 CPU는 SoC(system on a chip) 또는 다른 멀티코어 프로세서일 수 있고, 보안 실행 기술, 예컨대, 인텔® TXT™ 기술, 인텔® ME 또는 신뢰 실행 환경을 가능하게 하는 ARM TrustZone을 포함할 수 있다. 이 환경은 부트 및 개시 환경에서 플랫폼 구성요소(예컨대, 기본 입출력 시스템(BIOS), OS 로더, 가상 머신 관리자 및 다른 구성요소)를 측정하는 것을 포함하는 컴퓨팅 플랫폼을 평가하는 신뢰 루트를 수립한다. 이 루트는 또한 임의의 다른 구성요소의 무결성을 평가하도록 신뢰 위치를 제공한다. 기본 신뢰 루트와, 측정 및 평가를 위한 보안 기반이 수립되면, 메모리 내에 비밀을 밀봉하고 보호하며 시스템 구성의 로컬 또는 원격 인증을 제공하는 데 다른 메커니즘이 사용될 수 있다.

[0022] 도 4의 실시예에서 보이는 바와 같이, CPU(410)는 칩셋(420)에 연결될 수 있다. 도 4의 실시예에서 개별 구성요소로서 도시되지만, 몇몇 구현에서 칩셋(420)은 CPU(410)로서, 특히 CPU가 SoC로서 구현될 때, 동일한 패키지 내에 구현될 수 있음을 알아야 한다. 보이는 바와 같이, 칩셋(420)은 본 명세서에 설명된 바와 같이, 서비스 제공자와 사용자 및 키 기반 인증의 멀티-인자 인증을 수행하도록 IdP 로직부를 포함할 수 있는 CSE(428)를 포함하는 관리 엔진(425)을 포함할 수 있다. 실시예에서, 클라이언트 시스템이 서비스 제공자에게 아직도 익명인 채로 인증될 수 있도록 EPID를 사용하여 시그마 세션이 수행될 수 있다.

[0023] CSE(428)는 ME 내에 있는 것으로 도시되지만, 본 발명의 범위는 이것으로 제한되지 않으며 본 명세서에 설명된 인증 및 키 페어링 활동이 신뢰 실행 환경으로서 또한 적합한 다른 위치에서 수행될 수 있음에 유의한다. 실시예에서, CSE(428)는 ME의 펌웨어 내의 자바 가상 머신(JVM) 상에서 구동하는 자바™ 애플릿과 같은 애플릿에 의해 구현될 수 있다. 그러나, 본 명세서에 설명된 인증용으로 사용된 보안 엔진이 시스템의 다른 실행 엔진 상에서 구동하는 가상 머신 또는 다른 가상화 환경의 내부에서 구동하는 일반 엔진일 수 있음에 유의한다.

[0024] 도 4의 실시예에서, 칩셋(420) 내에 구성되거나 독립 허브일 수 있는 센서/통신 허브(430)를 포함하는 추가 구성요소가 존재할 수 있다. 보이는 바와 같이, 하나 이상의 센서(440)는 허브(430)와 통신할 수 있다. 설명을 위한 예로써, 센서는 GPS 모듈 또는 다른 전용 위치 센서를 포함할 수 있다. 관성 및 환경 센서와 같은 다른 센서가 존재할 수 있다. 몇몇 예로써, 가속도계 및 힘 검출기가 제공될 수 있고 이들 센서로부터 획득된 정보가 생체인증에 사용될 수 있다. 또한, 다양한 실시예에서 3G 또는 4G/LTE 통신 프로토콜에 따라 주어진 셀룰러 시스템과 같은 로컬 또는 광역 무선 네트워크와의 통신을 가능하게 하도록 하나 이상의 무선 통신 모듈(445)도 존재할 수 있다.

[0025] 도 4에서 더 볼 수 있듯이, 플랫폼(400)은 본 명세서에 설명된 바와 같이 (키 페어링 및 인증 동작을 승인하도록 사용자로의 요청을 포함하는) 디스플레이 프레임 이미지의 스누핑을 방지하도록 보안 채널(455)을 통해 ME(425)에 연결될 수 있는 디스플레이 프로세서(450)를 더 포함할 수 있다. 보이는 바와 같이, 디스플레이 프로세서(450)는 그러한 요청에 대한 응답과 같은 사용자 입력을 수신하도록 터치 스크린 디스플레이일 수 있는 디스플레이(470)에 연결될 수 있다. 그러므로 이 예에서, 디스플레이 내에 구성된 것은 터치 스크린(475) 및 터치 스크린 제어기(480)(물론 디스플레이 자체 뒤에 숨겨져 있음)일 수 있다. 이들 구성요소로부터 ME(425)로의 입력 채널이 비신뢰 채널일 수 있음에 유의한다. 유사하게, 다른 사용자 인터페이스, 즉, 예로서 키보드 및 마우스일 수 있는 사용자 인터페이스(495_1 및 495_2)는 내장형 제어기(490)를 통해 센서/통신 허브(430)에 연결될 수 있다. 다시 한번 이들 사용자 인터페이스로부터의 이 입력 경로는 비신뢰 채널을 경유할 수 있다.

[0026] 실시예는 다수의 상이한 환경에서 사용될 수 있다. 이제 도 5를 참조하면, 실시예가 사용될 수 있는 예시적인 시스템(500)의 블록도가 도시된다. 보이는 바와 같이, 시스템(500)은 스마트폰 또는 다른 무선 통신기일 수 있다. 도 5의 블록도에 도시된 바와 같이, 시스템(500)은 예컨대, 시스템의 부트업시에 하나 이상의 사용자 인증을 수행하고, 본 명세서에 설명된 바와 같이 원격 서비스 제공자와 키 페어링 동작 및 신뢰 어서션을 더 수행하도록 관리 엔진 및 다른 신뢰 하드웨어 지원과 같은 보안 엔진을 포함할 수 있는 베이스밴드 프로세서(510)를 포함할 수 있다. 일반적으로, 베이스밴드 프로세서(510)는 디바이스에 대한 컴퓨팅 동작뿐만 아니라 통신에 관하여 다양한 신호 처리를 수행할 수 있다. 그 다음에, 베이스밴드 프로세서(510)는 몇몇 실시예에서 서비스 채널을 통해 키 페어링 동작의 사용자 승인을 위한 요청을 제공할 수 있는 터치 스크린 디스플레이에 의해 구현될 수 있는 사용자 인터페이스/디스플레이(520)에 연결될 수 있다. 또한, 베이스밴드 프로세서(510)는 도 5의 실시예에서 비휘발성 메모리, 즉, 플래시 메모리(530) 및 시스템 메모리, 즉, 동적 랜덤 액세스 메모리

(DRAM)(535)를 포함하는 메모리 시스템에 연결될 수 있다. 더 볼 수 있듯이, 베이스밴드 프로세서(510)는 비디오 및/또는 스틸 이미지를 기록할 수 있는 이미지 캡처 디바이스와 같은 캡처 디바이스(540)에 연결될 수 있다.

[0027] 통신이 송신되고 수신되는 것을 가능하게 하기 위해, 베이스밴드 프로세서(510)와 안테나(590) 사이에 다양한 보안 회로가 연결될 수 있다. 특히, 무선 주파수(RF) 송수신기(570) 및 WLAN 송수신기(575)가 존재할 수 있다. 일반적으로, RF 송수신기(570)는 예컨대, CDMA(code division multiple access), GSM(global system for mobile communication), LTE(long term evolution) 또는 다른 프로토콜에 따라서 3G 또는 4G 무선 통신 프로토콜과 같은 주어진 무선 통신 프로토콜에 따라 무선 데이터 및 호출을 수신하고 송신하는 데 사용될 수 있다. 또한 GPS 센서(580)가 존재할 수 있다. 무선 신호, 예컨대, AM/FM 및 다른 신호의 수신 또는 송신과 같은 다른 무선 통신이 또한 제공될 수 있다. 또한, WLAN 송수신기(575)를 통해, 예컨대, 블루투스™ 표준 또는 IEEE 802.11a/b/g/n과 같은 IEEE 802.11 표준에 따라 로컬 무선 신호가 또한 구현될 수 있다. 도 5의 실시예에서 이 하이레벨로 도시되지만, 본 발명의 범위는 이것으로 제한되지 않음을 이해해야 한다.

[0028] 그러므로 실시예는 SP 또는 2차 Idp로의 Idp TEE 구동 및 IdP 작업부하를 구동하는 TEE를 인증하는 데 키 암호화를 사용할 수 있다. 이들 인증 어서션은 다수의 인증 인자의 표현을 포함하며, 실제 인증은 서비스 제공자 또는 제 3 자 인증 권한에 의해서가 아니라, 클라이언트 TEE에 의해 수행된다.

[0029] 그러므로 다양한 실시예에서, 웹서비스에 대한 사용자 인증은 멀티-인자 인증의 복잡성을 숨기는 TEE를 사용하여 클라이언트에서 수행될 수 있다. 실시예에서, 암호화 키(대칭 또는 비대칭)는 SP에 사용자를 인증하는 데 사용될 수 있다. 특히, MITM(man-in-the-middle) 공격자가 트랜잭션을 상관시킬 수 없음을 보장하도록 (예컨대, 페어링 관계로서 수립된) 각각의 SP마다 상이한 키가 사용될 수 있다. 또한, 초기 셋업 동안에 EPID 키의 사용은 트랜잭션 세부사항을 공유하도록 다수의 SP 간의 충돌을 방지한다. 그리고 멀티-인자 인증으로 사용자 인증을 수행하는 데 TEE를 사용함으로써, 인증의 복잡성은 SP에게 비밀이 되어, SP 백엔드가 강한 인증을 위한 광범위한 지원을 제공하기가 쉬워진다. 실시예는 페어링 키 생성 및 페어링 키 사용을 위해 사용자로부터 옵트인 승신을 수신하는 데 신뢰 입출력 메커니즘을 더 사용할 수 있다.

[0030] 실시예는 다수의 상이한 유형의 시스템에서 사용될 수 있다. 예컨대, 일 실시예에서 통신 디바이스는 본 명세서에 설명된 다양한 방법 및 기술을 수행하도록 구성될 수 있다. 물론, 본 발명의 범위는 통신 디바이스로 제한되지 않으며, 그 대신에 다른 실시예는 명령어를 처리하는 다른 유형의 장치, 또는 컴퓨팅 디바이스 상에서 실행되는 것에 응답하여 디바이스가 본 명세서에 설명된 하나 이상의 방법 및 기술을 수행하게 하는 명령어를 포함하는 하나 이상의 머신 판독가능 매체에 관한 것일 수 있다.

[0031] 후속하는 예는 다른 실시예에 관한 것이다. 실시예에서, 시스템은 웹 서비스를 제공하고 네트워크를 통해 시스템에 연결된 제 2 시스템을 가진 서비스 제공자와 시스템의 사용자를 연관시키는 키 페어링의 제 1 키 페어를 생성하고, 제 2 시스템이 식별자 제공자 로직부가 신뢰 실행 환경에서 실행중임을 검증할 수 있게 하도록 제 2 시스템과 보안 통신을 수행하며, 검증에 응답하여, 제 2 시스템으로 제 1 키 페어의 제 1 키를 전달 -제 1 키는 제 2 시스템이 사용자가 멀티-인자 인증에 따라 시스템에 인증되었다는 식별자 제공자 로직부에 의해 전달된 어서션을 검증할 수 있게 함- 하는 식별자 제공자 로직부를 포함하는 보안 엔진을 구비한다. 시스템은 사용자에 관하여 센싱된 정보를 보안 엔진에 제공하는 적어도 하나의 센서 수단을 더 구비하며, 보안 엔진은 센싱된 정보를 사용하여 사용자를 인증한다.

[0032] 일 실시예에서, 식별자 제공자 로직부는 어서션을 생성하고 키 페어링의 제 2 키로 어서션에 서명하며, 서비스 제공자는 서명된 어서션의 검증에 응답하여 제 2 시스템을 통해 웹 서비스에 액세스할 수 있게 한다. 또한, 보안 엔진은 사용자가 사용자와 서비스 제공자를 연관시키는 키 페어링을 생성하려고 한다는 것을 확인하도록 시스템의 신뢰 경로를 따라 전달되는 요청을 생성한다. 실시예에서, 보안 엔진은 사용자가 웹 서비스에 액세스하려고 하기 전에 멀티-인자 인증에 따라 사용자를 인증한다.

[0033] 실시예에서, 식별자 제공자 로직부는 제 2 시스템으로부터 인증 요청을 수신하고 인증 요청에 응답하여 어서션을 생성한다. 그리고, 보안 엔진은 프레즌스 검출 센서 또는 사용자 인증 센서에 대응하는 적어도 하나의 센서로부터 센싱된 정보를 수신한다.

[0034] 다른 실시예에서, 방법은 클라이언트 시스템의 보안 엔진의 식별자 제공자 로직부에서 인증 요청을 수신하는 단계 -인증 요청은 클라이언트 시스템의 사용자가 액세스하려고 하는 웹 서비스를 가진 서비스 제공자로부터 수신됨- 와, 사용자가 멀티-인자 인증을 통해 클라이언트 시스템에 인증되었다는 어서션을 생성하고, 사용자와 서비스 제공자를 연관시키는 키 페어링의 제 1 키로 어서션에 서명하는 단계와, 서비스 제공자에게 서명된 어서션을

전달하는 단계 -서비스 제공자는 서명된 어서션의 검증에 응답하여 사용자와의 시도-응답 상호작용 없이 사용자가 웹 서비스에 액세스할 수 있게 함- 를 포함한다.

[0035] 실시예에서, 방법은 사용자가 웹 서비스에 액세스하려고 하기 전에 멀티-인자 인증에 따라 사용자를 인증하는 단계를 더 포함한다. 인증 요청은 인증 요청을 보안 엔진으로 재지정하는 클라이언트 시스템의 브라우저 애플리케이션에서 수신될 수 있다.

[0036] 방법은 클라이언트 시스템의 신뢰 경로를 통해 전달되는 요청에 응답하여, 사용자가 사용자 입력을 통해 웹 서비스에 액세스하려고 한다는 것을 확인하는 단계를 더 포함할 수 있고, 신뢰 경로는 클라이언트 시스템 상에서 실행하는 멀웨어에 액세스할 수 없다.

[0037] 방법은 키 페어링을 생성하기 위한 사용자 승인에 응답하여 보안 엔진에서 제 1 키 페어를 생성하는 단계를 더 포함할 수 있다. 이는 클라이언트 시스템과 서비스 제공자 사이의 시그마 세션을 통해, 클라이언트 시스템의 신뢰 실행 환경을 검증하고 제 1 키 페어의 공개 키를 제공하며 서비스 제공자에 의해 생성된 제 2 키 페어의 공개 키를 수신하도록 통신하는 단계를 포함할 수 있다.

[0038] 실시예에서, 데이터 구조는 클라이언트 시스템에 저장될 수 있고, 데이터 구조는 제 1 키 페어의 개인 키와 공개 키 및 제 2 키 페어의 공개 키를 포함한다. 이 데이터 구조는 어서션에 서명하도록 액세스될 수 있다.

[0039] 설명된 바와 같이 방법을 사용하면, 사용자는 사용자로부터 사용자 이름 또는 암호를 수신하지 않고도 웹 서비스에 액세스할 수 있게 된다. 또한, 웹 서비스를 위한 사용자 계정은 사용자 이름 및 암호 메커니즘으로부터 키 페어링을 통한 연관으로 바뀔 수 있다.

[0040] 또 다른 실시예는 명령어를 포함하는 적어도 하나의 컴퓨터 판독가능 매체를 포함하고, 명령어는 실행될 때 시스템이 서비스 제공자의 시스템에서, 사용자 이름 또는 암호 없이 서비스 제공자의 웹사이트를 통해 계정에 액세스하라는 사용자 요청을 수신하고, 사용자가 멀티-인자 인증을 통해 클라이언트 시스템에 인증되었다는 어서션을 획득하도록 인증 요청을 시스템으로부터 사용자의 클라이언트 시스템으로 전달 -어서션은 사용자와 서비스 제공자를 연관시키는 키 페어링의 제 1 키로 서명됨- 하며, 클라이언트 시스템으로부터 어서션을 수신하고, 어서션을 검증하고 검증에 응답하여 웹사이트를 통해 계정에 대한 액세스를 허가할 수 있게 한다.

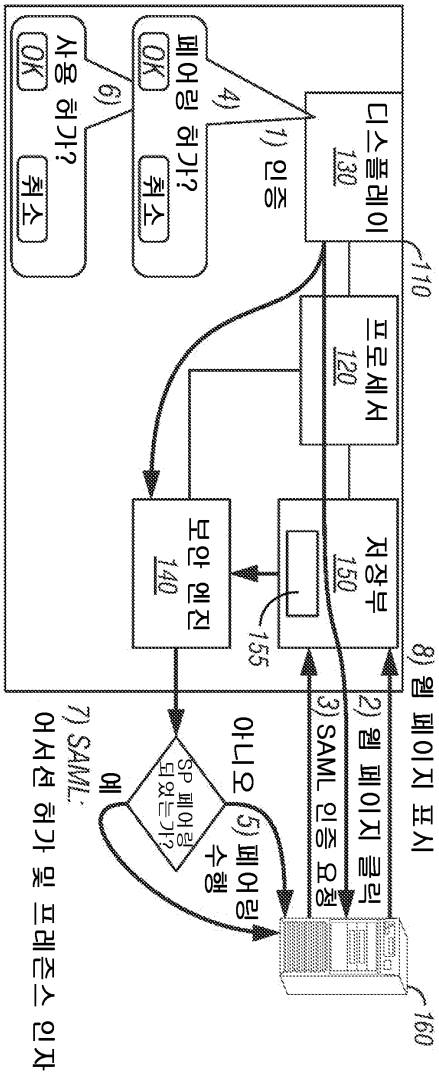
[0041] 실시예에서, 다른 명령어는 시스템이 클라이언트 시스템의 신뢰 실행 환경을 검증하고 키 페어링의 제 2 키를 수신하도록 시그마 세션을 통해 클라이언트 시스템과 통신할 수 있게 한다. 추가 명령어는 시스템이 클라이언트 시스템에 제공할 인증서 정보를 획득하도록 시스템과 원격 온라인 인증서 상태 제공자 간에 통신을 수행할 수 있게 한다. 또 다른 명령어는 시스템이 사용자 이름 및 암호 메커니즘을 통한 계정의 연관을 상기 키 페어링을 통한 연관으로 바꿀 수 있게 한다.

[0042] 실시예는 코드로 구현될 수 있고 명령을 수행하도록 시스템을 프로그래밍하는 데 사용될 수 있는 명령어를 저장한 비일시적 저장 매체 상에 저장될 수 있다. 저장 매체는 플로피 디스크, 광디스크, 고체 상태 드라이브(SSD), 콤팩트 디스크 판독전용 메모리(CD-ROM), 콤팩트 디스크 리라이터블(CD-RW) 및 광자기 디스크를 포함하는 임의의 유형의 디스크, 판독 전용 메모리(ROM), 랜덤 액세스 메모리(RAM), 예컨대, 동적 랜덤 액세스 메모리(DRAM), 정적 랜덤 액세스 메모리(SRAM), 소거가능한 프로그램가능 판독 전용 메모리(EPROM), 플래시 메모리, 전기적으로 소거가능한 프로그램가능 판독전용 메모리(EEPROM)와 같은 반도체 디바이스, 자기 또는 광 카드, 또는 전자 명령어를 저장하기에 적합한 임의의 유형의 매체를 포함할 수 있지만, 이들로 제한되지 않는다.

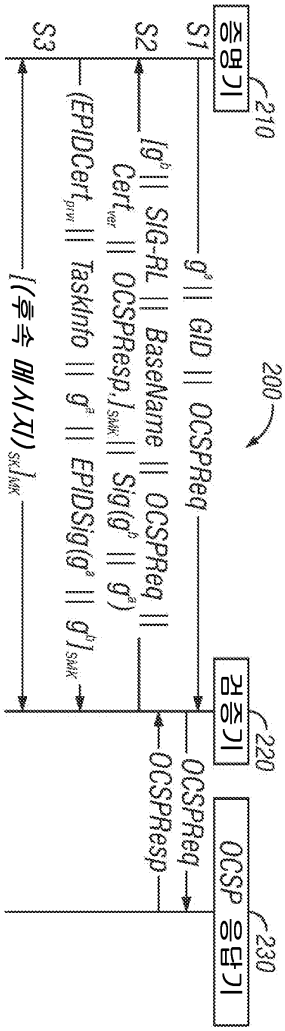
[0043] 본 발명은 한정된 수의 실시예에 관하여 설명되었지만, 당업자는 그러한 실시예로부터의 다수의 변경 및 수정을 알 것이다. 첨부된 특허청구범위는 그러한 모든 변경 및 수정을 본 발명의 진정한 사상 및 범주 내에 있는 것으로 커버하도록 의도된다.

도면

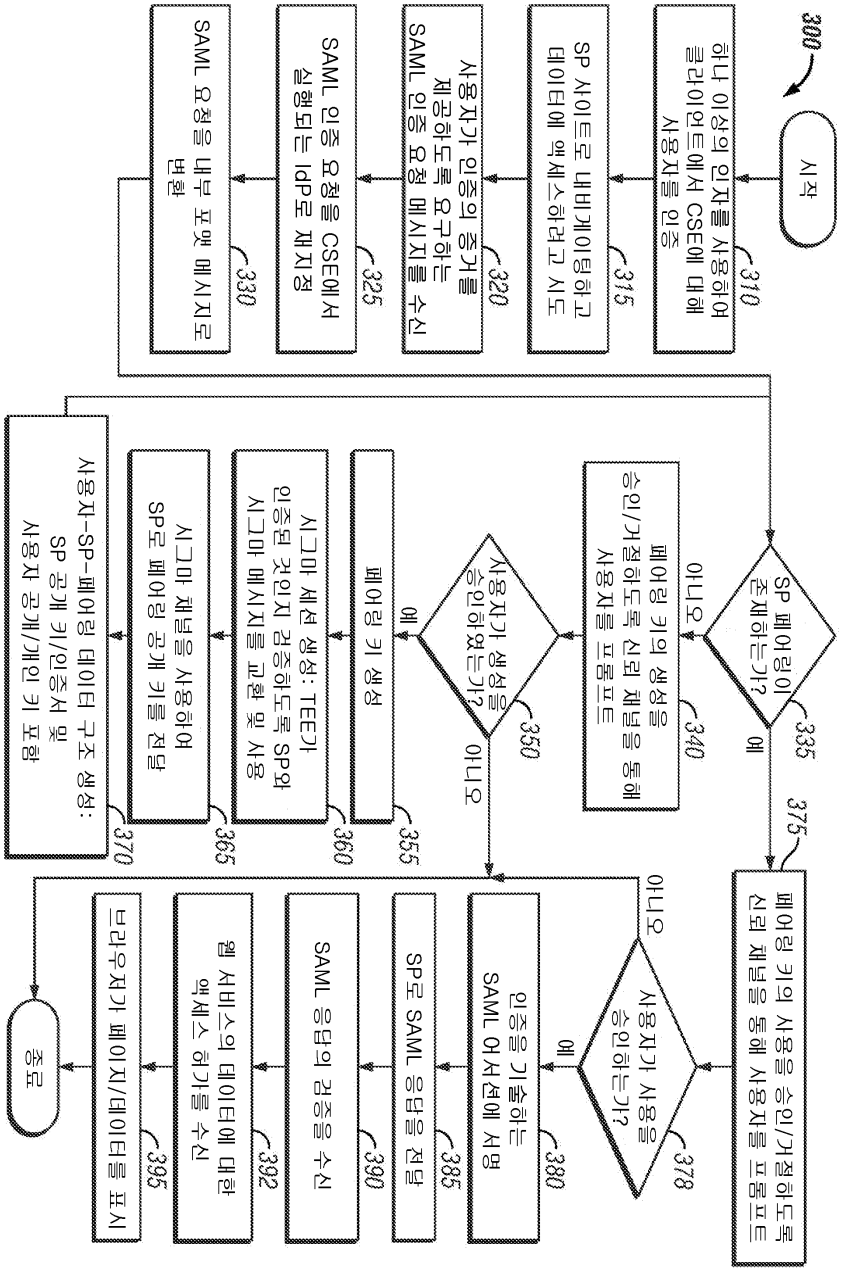
도면1


디스플레이
130
110
프로세서
120
보안 엔진
140
저장부
150
155
160
1) 인증
4)
페어링 허가?
OK
취소
6)
사용 허가?
OK
취소
2) 웹 페이지 클릭
3) SAML 인증 요청
8) 웹 페이지 표시
SP 페어링 됐는가?
아니오
5) 페어링 수행
예
7) SAML: 어서션 허가 및 프레즌스 인자

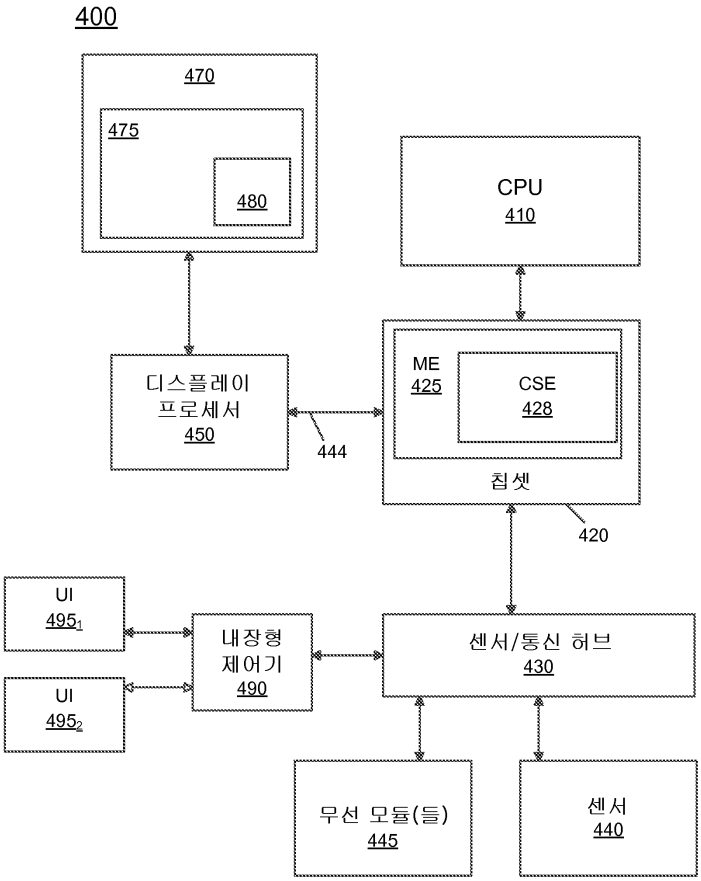
도면2


증명기
210
검증기
220
OCSP 응답기
230
200
S1
S2
S3
g^a || GID || OCSPReq
Ig^b || SIG-RL || BaseName || OCSPReq || $Cert_{ver}$ || OCSPResp, J_{SMK} || $Sig(g^b$ || $g^a)$
$(EPIDCert_{priv}$ || TaskInfo || g^a || $EPIDSig(g^a$ || $g^b)]_{SMK}$
[(응용 메시지)$_{SK}$]$_{MK}$
OCSPReq
OCSPResp

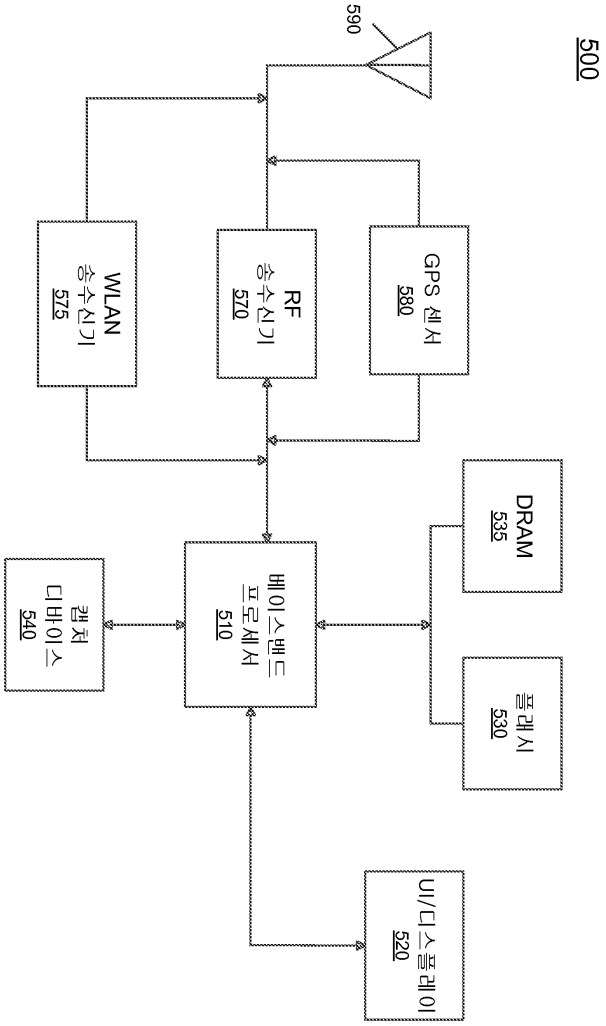
도면3


300
시작
하나 이상의 인자를 사용하여 클라이언트에서 CSE에 대해 사용자를 인증
310
SP 사이트로 내비게이팅하고 데이터에 액세스하려고 시도
315
사용자가 인증의 증거를 제공하도록 요구하는 SAML 인증 요청 메시지를 수신
320
SAML 인증 요청을 CSE에서 실행되는 IdP로 재지정
325
SAML 요청을 내부 포맷 메시지로 변환
330
SP 페어링이 존재하는가?
335
예
아니오
375
페어링 키의 사용을 승인/거절하도록 신뢰 채널을 통해 사용자를 프롬프트
사용자가 사용을 승인하는가?
378
예
아니오
인증을 기술하는 SAML 어서션에 서명
380
SP로 SAML 응답을 전달
385
SAML 응답의 검증을 수신
390
웹 서비스의 데이터에 대한 액세스 허가를 수신
392
브라우저가 페이지/데이터를 표시
395
종료
페어링 키의 생성을 승인/거절하도록 신뢰 채널을 통해 사용자를 프롬프트
340
사용자가 생성을 승인하였는가?
350
예
아니오
페어링 키 생성
355
시그마 세션 생성: TEE가 인증된 것인지 검증하도록 SP와 시그마 메시지를 교환 및 사용
360
시그마 채널을 사용하여 SP로 페어링 공개 키를 전달
365
사용자-SP-페어링 데이터 구조 생성: SP 공개 키/인증서 및 사용자 공개/개인 키 포함
370

도면4


400
470
475
480
CPU
410
ME
425
CSE
428
칩셋
420
디스플레이
프로세서
450
444
UI
495₁
UI
495₂
내장형
제어기
490
센서/통신 허브
430
무선 모듈(들)
445
센서
440

도면5


500
590
WLAN
송수신기
575
RF
송수신기
570
GPS 센서
580
DRAM
535
베이스밴드
프로세서
510
캘처
디바이스
540
플래시
530
UI/디스플레이
520