(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년05월28일
(11) 등록번호 10-2257943
(24) 등록일자 2021년05월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/31 (2013.01) *G06F 21/40* (2013.01)
G06F 21/44 (2013.01) *H04L 29/06* (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
G06F 21/31 (2013.01)
G06F 21/40 (2013.01)
(21) 출원번호 10-2015-7029514
(22) 출원일자(국제) 2014년03월07일
심사청구일자 2019년03월06일
(85) 번역문제출일자 2015년10월14일
(65) 공개번호 10-2015-0132467
(43) 공개일자 2015년11월25일
(86) 국제출원번호 PCT/US2014/022075
(87) 국제공개번호 WO 2014/150064
국제공개일자 2014년09월25일
(30) 우선권주장
13/844,619 2013년03월15일 미국(US)
(56) 선행기술조사문헌
US20060037073 A1*
US20130046993 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
구글 엘엘씨
미국 캘리포니아 마운틴 뷰 엠피시어터 파크웨이 1600 (우:94043)
(72) 발명자
버크만, 오메르
이스라엘 69400 텔 아비브 케히랏 베네지아 스트리트 2
영, 마르셀 엠.엠.
미국 94043 캘리포니아 마운틴 뷰 앰피시어터 파크웨이 1600
(74) 대리인
특허법인 남앤남

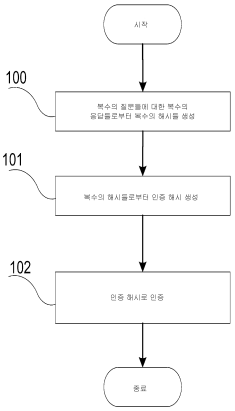
전체 청구항 수 : 총 18 항 심사관 : 문남두

(54) 발명의 명칭 **영구 인증을 위한 프라이버시 보호 지식/팩터 보유 테스트들**

(57) 요 약

본원에 설명된 예시적 구현들은 서버(또는 서버 정보를 가진 누군가)가 사적 대답들을 추론하게 하는 서버측 정보를 드러내지 않으면서, 사용자의 사적 팩터들에 기초한 인증에 관련된다. 예시적 구현들에서, 사용자는 인증 팩터들을 가진 질문지에 대답하고, 대답들은 일방향 방식으로 변환되고 변환된 대답들은 서버측에 제공된다. 예시적 구현들은, 사용자가 질문들 모두를 올바르게 대답하지 못하더라도, 사용자가 인증하게 하는 다항식 보간 또는 다른 방법들에 기초하여 인증을 가능하게 한다.

대 표 도 - 도1a



(52) CPC특허분류
G06F 21/44 (2013.01)
H04L 63/0407 (2013.01)
H04L 63/08 (2013.01)
H04L 9/3218 (2013.01)
G06F 2221/2103 (2013.01)

명 세 서

청구범위

청구항 1

디바이스로서,

프로세서를 포함하고, 상기 프로세서는,

복수의 질문들에 대한 복수의 응답들로부터 복수의 해시(hash)들을 생성하고;

상기 복수의 해시들의 다항식 보간 또는 상기 복수의 질문들 중 선택된 그룹에 기초하여 선택된 상기 복수의 해시들 중 하나 이상의 해시들의 다항식 보간; 및

상기 복수의 해시들에 걸친 대수 연산(algebric operation)들 또는 상기 복수의 해시들 중 상기 하나 이상의 해시들에 걸친 대수 연산들

로부터 노이지 보간 알고리즘(noisy interpolation algorithm)을 사용함으로써 인증 해시를 생성하고; 그리고

상기 인증 해시를 이용하여 인증하도록 구성되는,

디바이스.

청구항 2

제1항에 있어서,

상기 프로세서는, 상기 복수의 해시들 중 하나를 상기 인증 해시로서 선택하는 것에 기초하여, 상기 선택으로부터 상기 인증 해시를 생성하도록 구성되고,

상기 프로세서는 상기 복수의 응답들 중 적어도 두 개로부터 상기 복수의 해시들의 각각을 생성하도록 구성되는,

디바이스.

청구항 3

제1항에 있어서,

비밀 인증 해시를 저장하도록 구성된 메모리를 더 포함하고,

상기 프로세서는 상기 인증 해시와 상기 비밀 인증 해시의 비교를 통해 상기 인증 해시를 이용하여 인증하도록 구성되고, 상기 인증 해시가 상기 비밀 인증 해시에 매칭하면 인증을 위하여 상기 비밀 인증 해시를 사용하고, 그리고 상기 인증 해시가 상기 비밀 인증 해시에 매칭하지 않으면 인증을 거부하도록 추가로 구성되는,

디바이스.

청구항 4

삭제

청구항 5

제1항에 있어서,

상기 프로세서는, 상기 다항식 보간을 위한 하나 이상의 에러 포인트들 및 상기 다항식 보간을 위한 하나 이상의 올바른 포인트들 중 하나의 도입을 통해 상기 노이지 보간 알고리즘의 임계치를 조절하도록 추가로 구성되는,

디바이스.

청구항 6

제1항에 있어서,

상기 프로세서는, 상기 인증 해시를 형성하기 위하여 상기 복수의 질문들 중 선택된 그룹과 연관된 상기 복수의 응답들에 대응하는 복수의 해시들의 사용에 기초하여 상기 선택으로부터 상기 인증 해시를 생성하도록 구성되는,

디바이스.

청구항 7

프로세스를 실행하기 위한 명령들을 저장하는 컴퓨터 판독가능 저장 매체로서,

상기 명령들은,

복수의 질문들에 대한 복수의 응답들로부터 복수의 해시들을 생성하는 것;

상기 복수의 해시들의 다항식 보간 또는 상기 복수의 질문들 중 선택된 그룹에 기초하여 선택된 상기 복수의 해시들 중 하나 이상의 해시들의 다항식 보간; 및

상기 복수의 해시들에 걸친 대수 연산들 또는 상기 복수의 해시들 중 상기 하나 이상의 해시들에 걸친 대수 연산들

로부터 노이지 보간 알고리즘을 사용함으로써 인증 해시를 생성하는 것; 및

상기 인증 해시를 이용하여 인증하는 것

을 포함하는,

컴퓨터 판독가능 저장 매체.

청구항 8

삭제

청구항 9

제7항에 있어서,

상기 인증 해시를 이용하여 인증하는 것은,

비밀 인증 해시를 상기 인증 해시와 비교하는 것;

상기 인증 해시가 상기 비밀 인증 해시에 매칭하면 인증을 위해 상기 비밀 인증 해시를 사용하는 것, 및

상기 인증 해시가 상기 비밀 인증 해시에 매칭하지 않으면 인증을 거부하는 것

을 포함하는,

컴퓨터 판독가능 저장 매체.

청구항 10

삭제

청구항 11

제7항에 있어서,

상기 명령들은 상기 다항식 보간에 대한 하나 이상의 에러 포인트들, 및 상기 다항식 보간에 대한 하나 이상의 올바른 포인트들 중 하나의 도입을 통해 상기 노이지 보간 알고리즘의 임계치를 조절하는 것을 더 포함하는,

컴퓨터 판독가능 저장 매체.

청구항 12

제7항에 있어서,

상기 복수의 해시들 각각은 복수의 응답들 중 적어도 두 개로부터 생성되고; 그리고 상기 복수의 해시들로부터 상기 인증 해시를 생성하는 것은 상기 복수의 질문들 중 선택된 그룹에 기초하여 상기 인증 해시로서 상기 복수의 해시들 중 하나를 선택하는 것을 포함하는,

컴퓨터 판독가능 저장 매체.

청구항 13

서버로서,

프로세서를 포함하고, 상기 프로세서는,

복수의 질문들을 전송하고; 그리고

상기 전송된 복수의 질문들에 응답하는 인증 해시가 비밀 인증 해시에 매칭하면 액세스를 승인하고; 그리고

상기 인증 해시가 상기 비밀 인증 해시에 매칭하지 않으면 액세스를 거부하도록 구성되고,

상기 인증 해시는,

상기 복수의 해시들의 다항식 보간 또는 상기 복수의 질문들 중 선택된 그룹에 기초하여 선택된 상기 복수의 해시들 중 하나 이상의 해시들의 다항식 보간; 및

상기 복수의 해시들에 걸친 대수 연산들 또는 상기 복수의 해시들 중 상기 하나 이상의 해시들에 걸친 대수 연산들

로부터 노이지 보간 알고리즘을 사용함으로써 생성되는,

서버.

청구항 14

제13항에 있어서,

상기 프로세서는 상기 비밀 인증 해시 및 임계치에 기초하여, 노이지 보간 알고리즘에 사용하기 위한 하나 이상의 에러 포인트들, 및 하나 이상의 올바른 포인트들 중 적어도 하나를 생성 및 전송하도록 구성되는,

서버.

청구항 15

제13항에 있어서,

상기 프로세서는 상기 전송된 질문들 중 선택된 그룹에 기초하여 복수의 비밀 인증 해시들로부터 상기 비밀 인증 해시를 선택하도록 구성되고, 상기 복수의 비밀 인증 해시들 각각은 상기 복수의 질문들 중 적어도 두 개와 연관되는,

서버.

청구항 16

제13항에 있어서,

상기 프로세서는,

상기 복수의 질문들에 대한 응답을 수신하고 – 상기 응답은 상기 복수의 질문들 중 하나 또는 서브세트에 대한 응답 해시 및 대답을 포함함 –; 및

상기 응답 해시 및 대답으로부터 상기 인증 해시를 구성하도록

추가로 구성되는,

서버.

청구항 17

제16항에 있어서,

상기 프로세서는 상기 응답 해시 및 상기 대답으로부터 네스팅된(nest) 해시를 구성함으로써 상기 인증 해시를 구성하도록 구성되는,

서버.

청구항 18

제16항에 있어서,

상기 프로세서는 상기 응답 해시를 상기 대답의 해시와 곱셈함으로써 상기 인증 해시를 구성하도록 구성되는,

서버.

청구항 19

제13항에 있어서,

상기 프로세서는 상기 비밀 인증 해시를 수신하고 그리고 사용자와 연관된 디바이스 및 상기 사용자와 연관된 계정으로부터 확인을 수신한 후 상기 비밀 인증 해시를 메모리에 저장하도록 추가로 구성되는,

서버.

청구항 20

제13항에 있어서,

상기 복수의 질문들은 생체 측정 정보에 대한 요청을 포함하는,

서버.

청구항 21

사용자 디바이스가 서버에 인증을 위하여 등록하고 서버에서 추가로 인증하기 위한 방법으로서,

복수의 질문들에 대한 복수의 대답들을 수신하는 단계 – 상기 질문들은 사용자의 하나 이상의 팩터(factor)들과 연관됨 –,

상기 복수의 대답들로부터 인증 비밀 해시를 생성하는 단계,

인증 세션에 기초하여 상기 사용자 디바이스를 상기 서버에 인증하는 단계, 및

상기 인증 세션의 성공적 결과에 기초하여 상기 서버에 액세스를 허용하거나 거부하는 단계 – 상기 성공적 결과는 상기 사용자 디바이스가 상기 인증 비밀 해시를 보유하는지에 기초함 –

를 포함하고,

상기 인증 세션에 기초하여 상기 사용자 디바이스를 상기 서버에 인증하는 단계에서,

복수의 질문들에 대한 복수의 응답들로부터 생성된 복수의 해시들의 다항식 보간 또는 상기 복수의 질문들 중 선택된 그룹에 기초하여 선택된 상기 복수의 해시들 중 하나 이상의 해시들의 다항식 보간; 및

상기 복수의 해시들에 걸친 대수 연산들 또는 상기 복수의 해시들 중 상기 하나 이상의 해시들에 걸친 대수 연산들

로부터 노이지 보간 알고리즘을 사용함으로써 상기 인증 비밀 해시가 상기 사용자 디바이스에 의해 재생성되는,

방법.

발명의 설명

기 술 분 야

[0001] [1] 1. 기술 분야

[0002] [2] 예시적인 실시예들의 양상들은 영구 인증을 위한 프라이버시 보호 테스트들에 관한 것이고, 보다 구체적으로 사적 질문들에 대한 대답들이 서버 측에서 드러나지 않도록, 인증 해시 또는 그 밖의 역변환이 어려운 일방향 함수를 생성하고, 생성된 인증 해시에 기초하여 인증하기 위한 디바이스들, 방법, 및 시스템에 관한 것이다.

배 경 기 술

[0003] [3] 2. 관련 기술

[0004] [4] 사용자는 계정들의 액세스 및 복구를 위하여 사용자들의 인증 프로세스 동안 다양한 상황들에서 사용자의 아이덴티티를 증명할 필요가 있을 수 있다. 인증을 용이하게 하거나 또는 인증을 위한 대안적인 방법들(예를 들어, 결함 허용오차/복구)을 용이하게 하기 위하여, 사용자들은 액세스를 보유하는 서버(예를 들어, 계정 제공자)에 팩터(factor)들(예를 들어, 사용자의 생활 및 취미에 특정한 질문들에 대한 대답)을 등록한다. 대답들을 포함하여 사용자에 의한 등록은 사적 사용자 정보를 서버에 드러낼 수 있다. 악의적인 파티에 의한 서버에 대한 인증되지 않은 액세스는 사적 사용자 정보를 그 악의적인 파티에 드러내 보일 수 있다. 예를 들어, 그 파티(예를 들어, 서버 조직 내부자 또는 외부자 또는 피싱 공격자(phishing attacker)는 유사한 대답들을 요구하는 다른 또는 동일한 계정 제공자들에 등록된 대답을 이용하여 사용자를 가장(impersonate)할 수 있다.

[0005] [5] 프라이버시 이유들 때문에, 서버가 사적 정보를 보유하여 사용자로부터의 정보를 검증하도록 하지 않으면서, 인증을 위해 사용자가 질문들에 대답하게 (또는 생체 측정 정보, 시스템 외측에 저장된 소유된 정보 등과 같은 그 밖의 사적 팩터들을 제공하게) 할 필요가 있다.

발명의 내용

[0006] [6] 본 출원의 양상들은 복수의 질문들에 대한 복수의 응답들로부터 복수의 해시들을 생성하고; 복수의 해시들의 다항식 보간 중 적어도 하나로부터 인증 해시를 생성하고, 그리고 복수의 질문들 중 선택된 그룹에 기초하여 인증 해시를 형성하기 위하여 복수의 해시들 중 하나 이상의 선택을 생성하고; 그리고 인증 해시로 인증하도록 구성된 프로세서를 포함하는 디바이스를 포함할 수 있다.

[0007] [7] 본 출원의 양상들은 프로세스를 실행하기 위한 명령들을 저장하는 컴퓨터 판독가능 저장 매체를 더 포함한다. 명령들은 복수의 질문들에 대한 복수의 응답들로부터 복수의 해시들을 생성하는 것; 복수의 해시들의 다항식 보간, 및 복수의 질문들 중 선택된 그룹에 기초하여 인증 해시를 형성하기 위하여 복수의 해시들 중 하나 이상의 선택 중 적어도 하나로부터 인증 해시를 생성하는 것; 및 인증 해시로 인증하는 것을 포함할 수 있다.

[0008] [8] 본 출원의 양상들은 복수의 질문들을 전송하도록 구성된 프로세서; 및 전송된 복수의 질문들에 응답하는 인증 해시가 비밀 인증 해시에 매칭할 때 승인 액세스; 및 인증 해시가 비밀 인증 해시에 매칭하지 않을 때 거부 액세스를 포함할 수 있는 서버를 더 포함하고; 상기 인증 해시는 복수의 해시들의 다항식 보간, 및 복수의 질문들 중 선택된 그룹에 기초하여 인증 해시를 형성하기 위하여 복수의 해시들 중 하나 이상의 선택 중 적어도 하나로부터 생성된다.

도면의 간단한 설명

[0009] [9] 도 1a 및 도 1b는 예시적 구현에 따른 장치에 대한 흐름도를 도시한다.

[10] 도 2a 및 도 2b는 예시적 구현에 따른 서버에 대한 흐름도를 도시한다.

[11] 도 3은 몇몇 예시적 구현들에 사용하기에 적당한 예시적 컴퓨팅 디바이스를 갖는 예시적 컴퓨팅 환경을 예시한다.

[12] 도 4는 예시적 구현에 따른 예시적 프로세싱 환경을 예시한다.

발명을 실시하기 위한 구체적인 내용

[0010] [13] 본원에 설명된 청구 대상은 예시적 구현들에 의해 가르침을 받는다. 다양한 상세들은 명확성을 위해

그리고 청구 대상을 모호하게 함을 회피하기 위하여 생략되었다. 하기 도시된 예들은 프라이버시 보호를 갖는 캠페인 성능의 측정을 구현하기 위한 구조들 및 기능들에 관련된다. 예시적 구현들의 양상들은 예를 들어, 전자상거래, 정보 공유, 프라이버시 보호 방법들, 인크립션 및 암호 방법론들, 트랜잭션 시스템들, 사적 정보 공유, 및 보안 컴퓨팅에 관한 것일 수 있다. 그러나, 예시적 구현들은 거기에 제한되지 않고, 본 발명의 개념의 범위에서 벗어남이 없이 다른 분야들에 적용될 수 있다.

[0011] [14] 본원에 설명된 예시적 구현들은 서버(또는 서버의 정보를 가진 누군가)가 사적 대답들을 추론할 수 있게 하는 정보를 서버측에 드러내지 않으면서, 사용자의 사적 팩터들에 기초한 인증에 관련된다. 예시적 구현들에서, 사용자는 인증 팩터들을 가진 질문지에 대답하고, 대답들은 일방향 방식으로 변환되고 변환된 대답들은 서버측에 제공된다. 이것은 서버에 정보를 등록한 원래 사용자를 서버가 인증할 수 있게 하면서 사용자의 프라이버시를 보호한다.

[0012] [15] 예시적 구현들은 충분한 엔트로피(예를 들어, 문자열들)를 가진 복수의 팩터들이 일방향(예를 들어, 암호 해시) 함수 하에서 사용자 디바이스 상에서 함께 변환되도록 하고, 그리고 변환된 값들을 등록시 서버에 전송하는 것에 관련된다. 인증 세션에서, 사용자는 다시 대답들을 요청받고, 이 대답들은 디바이스에 의해 상기 설명된 바와 유사한 방식으로 변환되고, 그리고 서버에 전송된다. 그 다음 서버는 일방향 변환된 대답들을 등록된 정보와 비교한다. 다음 설명은 예시적인 구현들에 사용된 메커니즘들을 개요하는 보다 상세한 프로그램들/프로토콜에 관련된다.

[0013] [16] 예를 들어 프로토콜 엔티티들 구현들은 사용자, 사용자 디바이스, 및 서버를 포함할 수 있다. 명확성의 목적들을 위해, 프로토콜 파라미터들은 하기 설명되는 n, t, r 및 m으로서 표현된다.

[0014] [17] 예시적인 프로토콜 환경에서, 하기 설명된 바와 같이 몇몇 양상들이 고려된다.

[0015] [18] 사적 등록 정보: 사용자는 사적 정보의 n개의 라벨링된 문자열들을 가진다. 이것은 사용자가 알고 기억할 것 같은 무언가, 또는 사용자가 소유하거나 그렇지 않으면 보유한 팩터들일 수 있다. 예시적 구현들에서, 예를 들어, 사용자가 사용자와 연관된 디바이스(예를 들어, 사용자의 전화 및 사용자와 연관된 계정, 예컨대 대안적인 이메일 또는 친구의 계정)에 전송된 확인응답을 수신하고 이에 응답한 후에 초기 등록이 유효화될 수 있다.

[0016] [19] 비사적 라벨링: 라벨들, 포맷, 아마도 힌트들, 및 문자열들의 순서는 사적이지 않다.

[0017] [20] 영구성: 언제라도, 사용자는 적어도 n-t개의 문자열들을 안다. 즉, 사용자는 n개의 문자열들을 등록할 수 있고, 이들 전부를 항상 기억하고 있지는 않다고 가정될 수 있고 이들 중 t개를 잊어버릴 수 있다. 따라서, 사용자는 문자열들 중 n-t개의 일부 임계치를 알도록 요구받는다. 인증 세션들마다 요구되는 레벨은 서버에 의해 조절될 수 있다는 것이 주의된다.

[0018] [21] 사용자 디바이스: 사용자는 데이터를 보안적으로 입력하고, 계산하고, 데이터를 소거하고, 데이터를 저장하고, 데이터를 출력할 수 있는 디바이스에 액세스를 가진다. 디바이스는 사용자의 제어하에 있다(예를 들어, 피싱 가능하지 않다). 이것은 웹에 연결되지 않은 스마트폰 또는 소프트웨어 엘리먼트일 수 있다.

[0019] [22] 디바이스 부분적 무결성(partial integrity): 디바이스는 올바르게 동작하지만(특히, 데이터는 요청될 때 영구적으로 소거됨), 잃어버리거나 훔쳐질 수 있다.

[0020] [23] 서버 무결성: 서버는 올바르게 동작하고 서버가 사용자를 인증하는데 관심이 있을 때 결코 어떠한 데이터도 손실하지 않는다. 게다가, 서버에 장기간 동안 저장되는 데이터는 공격자들이 사용자를 가장(impersonate)할 수 있게 하는 데이터를 포함하지 않는다.

[0021] [24] 셋업: 셋업 동안, 디바이스 및 서버는 정보를 보안적으로 교환할 수 있다.

[0022] [25] 예시적 프로토콜 환경은 또한 하기와 같은 몇몇 요건들을 포함할 수 있다:

[0023] [26] 프라이버시: 사적 문자열들 중 r개가 알려지더라도, 서버 상의 정보, 디바이스 상의 정보, 또는 서버와 디바이스 사이에서 교환되는 정보는, 나머지 n-r개의 문자열들 중 임의의 문자열을 드러내기에, 또는 나머지 n-r개의 문자열들 중 임의의 문자열을 처음보다 잘 추측하기에 실질적으로 불충분해야 한다.

[0024] [27] 진정성(Authenticity): 언제라도, 사용자는 사용자가 적어도 n-t개의 입력 문자열들(n-t는 r보다 훨씬 큼)을 안다는 것을 서버에게 (디바이스를 사용하여) 증명할 수 있다. 이런 진정성 동작은 동작의 성공적인 결과를 결정하고 서버는 요구되는 임계치 n-t를 다양한 인증 세션들에서 가능하게는 동적으로 변경할 수 있다.

[0025] [28] 보안성(Security): 서버 상의 정보, 사용자에 의해 사용되지 않는 디바이스 상의 정보, 또는 서버와 디바이스 사이에서 교환되는 정보는, 처음에 등록된 본래의 사용자가 아닐 수 있는 사용자를 인증하는데 사용하기에 실질적으로 불충분하여야 한다.

[0026] [29] 예시적 프로토콜 환경은 다양한 프로토콜들을 이용할 수 있다. 예를 들어, 팩터 등록은 다양한 팩터들을 셋업하기 위하여 수행될 수 있다. 팩터 등록은 랜덤화, 태뷸레이션(tabulation), 대답 및 생성을 포함할 수 있다.

[0027] [30] 팩터 등록의 랜덤화 양상에서, 디바이스 및 서버는 난수 생성기 또는 다른 방법들을 사용하여 임의성을 함께 생성할 수 있다. 예시적 구현에서, 서버는 긴 랜덤(비밀이 아님) 솔트(salt) Rs를 디바이스에 제공한다. 사용자는 긴 랜덤(비밀이 아님) 솔트 Ru를 생성하고, Rs 및 Ru를 디바이스에 입력할 수 있다. 디바이스는 긴 랜덤(비밀이 아님) 솔트 Rd를 생성하고 3개의 랜덤 솔트들을 모두 하나의 랜덤 솔트 R(솔트 R은 추가 상호작용들시 서버에 의해 이용될 팩터일 수 있음)로 연결시킨다.

[0028] [31] 팩터 등록의 태뷸레이션 양상에서, 라벨 제공이 수행될 수 있다. 서버는 문자열 라벨들 및 각 문자열의 개별 가능한 포맷들의 세트 및 사용자에 의해 이용될 표준 "힌트"들의 세트를 사용자에게 제공한다. 라벨은 값이 주어진 포맷의 문자열로 사용자가 값을 제공하는 변수이다. 사용자는 질문지를 정의하기 위하여 제공된 순서화된 라벨들의 세트 중에서 n개의 라벨들을 선택할 수 있다. 예시적인 구현들에서, 질문지 내의 몇몇 엘리먼트들은 반드시 "당신이 알고 있는 것" 타입일 필요가 없고, 다른 타입들의 정보(예를 들어, 생체 측정치, 맞춤화된 질문들 등)가 사용될 수도 있다.

[0029] [32] 팩터 등록의 대답 양상에서, 사용자는 질문지 대답들을 n개의 문자열들로서 제공한다. 사용자는 시스템에 의해 프로세스의 일부로서 대답들을 반복하도록 훈련될 수 있다(예를 들어, 사용자에게 두 번 질문을 하고, 시스템은 대답들의 사용자의 기억을 증가시키기 위한 기술들을 이용하는 등). 대답들은 디바이스로 이동될 수 있다.

[0030] [33] 질문지는 원해진 구현에 따라, 비밀로 유지될 수 있거나 공개된(예를 들어, 서버가 직접 대답들을 앎) 다른 방법들과 혼합될 수 있다. 예를 들어, 질문지는 다른 인증 방법들(예를 들어, 유일한 방법이기보다 오히려 아이덴티티를 위한 주장을 강화하는 것과 같이)과 결합하여 사용될 수 있다. 예를 들어, 결합은, 다른 방법들의 실패시, 다른 방법들을 사용한 몇몇 초기 성공 후, 다른 방법들이 사용되기 전, 사용자가 이미 인증되었지만 추가의 민감한 액세스/동작을 요청할 때에만 사용될 수 있다.

[0031] [34] 팩터 등록의 팩터 생성 양상에서, 시스템은 대답들에 기초하여, 그리고 알고리즘을 활용함으로써 기억할 팩터들을 생성한다. 알고리즘을 초기화하기 위하여, 디바이스에는 n개의 사용자 비밀들(u_1, ...,u_n)이 주어지고, 여기에서, u_i=질문(q_i)과 대답(a_i)이다. 디바이스는 n개의 비밀들(s_1, ..., s_n)을 생성하고, 이는 q_i들의 해싱 또는 일방향 함수이다(s_i=HASH(a_i, R)). 포인트들(q_i, s_i)(for i=1,n)로부터 디바이스는 유한체(finite field)에 걸친 보간에 의해, 평면의 모든 포인트들을 통해 통과하는 n-1차의 다항식(P)을 생성할 수 있다. q_i 및 s_i의 각각은 유한체 내에 있는 것으로 해석되고, 예를 들어 해시는 소수(prime)에 의해 정의되는 유한체 내의 원소로서 256 비트 크기의 소수로 모듈로(modulo) 해석된 256 비트의 문자열일 수 있고, q_1 및 해싱을 통해 생성된 s_i는 유한체 내에 X 및 Y 좌표들을 갖는 데카르트 평면에 놓이는 포인트로서 보여질 수 있는 랜덤하게 보이는 포인트에 맵핑될 것이다. 유한체들, 소수들, 및 다항식 보간들은 당업자에게 기본적 관념이다. 비밀(s)은 0에서의 다항식의 값(즉, P(0)=s)이고, 일련 번호와 함께 서버에 등록될 수 있다. 게다가, 포인트들(1, P(1)), (2, P(2)),… (k, P(k)) 같은, 다항식 상의 부가적인 k=2t개의 포인트들이, 이들이 보간에 본래 사용된 포인트들에 있지 않다는 것을 가정하여 서버에 전송되고 등록된다. 이는 추후 인증시 사용자가 n개의 문자열들 중 가능하게는 t개를 틀리거나 빠뜨리는 것을 허용하기 위한 것이다. 다항식(P)은 n-1 차수(이는 n개의 포인트들에 의해 생성되었기 때문에) 및 포인트(o, P(0))인 비밀 및 부가된 k개의 포인트들의 등록을 가지며, k+1은 n보다 작아야 하고, 이런 k+1개의 포인트들의 지식은 다항식 특성들을 서버에게 제공하지 않는다. 예를 들어, 추후에 단지 15개의 대답들을 요구하는 임계치를 가지면서 사용자가 대답으로 20개의 팩터들에 대해 질문받는 경우, 비밀에 부가되어 10개의 포인트들이 서버에 전송된다. 사용자가 추후에 인증할 때(예시적 구현으로서 후술됨), 사용자는 다시 팩터들을 전송하고 부가된 10개의 포인트들은 다항식의 표현에 부가되고, 이들 포인트들을 포함하여 노이지(noisy) 보간이 사용자에 의해 시도될 수 있다. 공격자가 가장하도록 시도하는 경우, 팩터들이 사용자 지식 및 팩터들의 보유를 나타내도록 주의 깊게 선택되었기 때문에, 공격자는 항상 10개의 포인트들보다 적게 알 것이다. 따라서, 서버에 의해 전송된 포인트들 및 가장을 시도하는 사람의 지식은 다항식(P)을 복구하기 위하여 이용 가능한 포인트들을 보간하는 것을 실패할 것이다.

[0032] [35] 다른 예시적 구현에서, s 자체보다 오히려 HASH(s)가 로컬로 유지된다. 다른 정보는 디바이스에 의해 유지되거나 삭제될 수 있고, 또는 k개의 포인트들이 원해진 구현에 따라 서버에 유지될 수 있다. 예를 들어, 다른 정보를 소거하는 것은 사용자가 인증시 다시 정보를 입력하게 강제하는 한편, 정보를 유지하는 것은 디바이스의 소유를 증명하는데에 사용할 수 있다. HASH는 임의의 일방향 함수, 암호 해시 알고리즘, 또는 암호 문헌에서 모듈식 거듭제곱에 대해 알려진 바와 같은 몇몇 유한체 또는 다른 대수 구조에 걸쳐 생성기를 사용한 거듭제곱일 수 있다. 서버에 s보다 오히려 HASH(s)를 유지하는 것은 서버를 침투한 공격자들이 s 자체를 학습하는 것을 방지한다.

[0033] [36] 예시적 구현에서, 인증 세션은 하기 설명된 바와 같이 이용될 수 있다. 인증 세션은 팩터들의 다양한 사용 모드들을 포함할 수 있다. 제1 모드에서, 디바이스가 이용 가능하고, 사용자는 디바이스에 액세스하고 비밀(s)은 삭제되지 않았다. 제1 모드에서, 그 다음 디바이스는 해시의 일련 번호를 서버에게 알리고 보안 프로토콜을 사용함으로써 비밀의 지식을 증명한다.

[0034] [37] 제2 사용 모드에서, 서버, 사용자 및 디바이스(또는 다른 디바이스)는 해시들 중 하나를 협력적으로 생성한다. 서버는 n개의 라벨들(질문들) 및 이들의 포맷을 사용자에게 전송한다. 그 다음, 서버는 n개의 라벨들 및 솔트 R를 디바이스에게 전송한다. 사용자는 대답들(a_i)을 디바이스에 입력한다. 서버는 또한 k개의 부가된 포인트들((1,P(1)),...(k,P(k)))을 전송한다. 노이즈 보간 알고리즘(예를 들어, Berlekamp Welch, Guruswami-Sudan, 등)을 사용하여, 디바이스는 다항식을 계산하고 대답들의 임계치가 올바르면(예를 들어, 상기의 20개 중 15개의 예에서처럼 2/3, 또는 1/2 등), 노이즈 보간 알고리즘은 s를 생성한다. 만약 디바이스가 HASH(s)를 가지면, 생성된 s는 올바름에 대해 체크될 수 있고, 사용자에게 새로운 대답들을 요구할 수 있다(예를 들어, 올바르지 않은 경우, 초기화의 경우 등). 결과 s는 서버에 전송되고, 서버는 사용자를 인증하거나, 대안적으로, 사용자의 디바이스는 서버에 전송된 HASH(s)에 기초하여 s의 소유를 증명하고, 이런 목적을 위하여 제로-지식 프로토콜들 또는 기술 분야에서 알려진 도전-응답(challenge-response) 프로토콜들이 활용될 수 있다.

[0035] [38] 노이지 보간 알고리즘에 대한 포인트들 중 하나가 랜덤화기이면(예를 들어, 서버 또는 로컬 소프트웨어에 의해 제공됨), 결과적 팩터는 랜덤화된다(즉, 사용자의 대답들과 무관함). 예를 들어, 서버가 몇몇 포인트들을 제공하게 함으로써 Berlekamp Welch 노이지 보간 알고리즘으로부터 한정된 2/3가 튜닝될 수 있다는 것을 처음에 가정하자. 보다 높은 임계치가 원해지면, 서버는 (다항식 상에 있지 않은) 에러 포인트들을 제공할 수 있다. 그러므로, 원해진 임계치가 예를 들어 18개 중 16개(16/18)의 포인트들이고 Berlekamp Welch 노이지 보간 알고리즘이 이용되면, 16/24의 포인트들이 올바르도록 6개의 에러들이 서버 또는 디바이스에 의해 도입될 수 있고, 이에 의해 Berlekamp Welch 임계치를 충족한다. 다른 예에서, 구현된 임계치가 대답들 중 절반만이 올바를 것을 요구하면, "우수한 다항식 포인트들"이 서버 또는 디바이스에 의해 도입될 수 있다. 예를 들어, 10/18(대답들 중 절반 초과가 올바름)이 충분한 것으로 고려되면, 결과가 16/24이 되도록 6개의 우수한 포인트들이 도입될 수 있고, 이는 2/3 Berlekamp Welch 임계치를 충족한다. 요구된 임계치의 튜닝은 하나의 인증 세션으로부터 다른 인증 세션으로 가변할 수 있다.

[0036] [39] 선택된 정보가 매우 사적이기 때문에, 사용자는 정보의 거의 모두를 기억해 낼 수 있어야 한다. 복잡성은 유한체 내 다항식의 평가의 복잡성이다.

[0037] [40] 문자열들은 매우 사적일 수 있고, 요구받을 때 사용자가 문자열들 대부분을 기억해 낼 수 있는 것을 보장하는 비밀 정보를 포함할 수 있다. 예들은 원해진 구현에 따라, 형제, 자녀, 배우자, 부모들, 조부모들, 친구들의 이름들, 자신 및 친척의 주소들, 계정 이름들 및/또는 번호들, 고용주들의 이름 및 다른 것들을 포함한다. 문자열들에 대한 선택 기준들은, 사용자가 필요한 경우 대답들을 재-생성할 수 있도록 하는 것이어야 한다. 데이터의 양 및 변동성은, 서버로부터의 추가 포인트들을 이용하더라도 공격자가 우수한 보간 포인트들을 생성할 수 없고 다항식이 공격자에게 비밀로 유지되기에 충분한 문자열들이 결코 공격자에게 알려지 않도록 해야 한다.

[0038] [41] 예시적 구현들에서, 몇몇 보안 레벨들이 또한 도입될 수 있다. 예를 들어, 문자열들의 라벨들, 포맷팅 및 순서 그 자체는, 몇몇의 기본적이고 기억하기 쉬운 문자열들(예를 들어, 사용자의 패스워드)에 의해 보호될 수 있다.

[0039] [42] 계정 복구 및 강탈자들에 의해 취득된 계정들을 해제(releasing)하기 위해, 복구 프로세스를 위해 사용되고 다음 특성들을 가지는 인증 팩터가 이용되어야 한다.

[0040] [43] 영구성: 사용자에게 항상 이용 가능함; 사용자는, 팩터를 포함하는 물리적 객체를 분실하거나 자신의 계정을 분실하더라도(예를 들어, 강탈에 의해) 인증 팩터를 손실할 수 없다(또는 재-생성할 수 있다).

[0041] [44] 위조 불가능: 계정 또는 개인 사용자 정보에 액세스가 주어지더라도 추측하는 것은 사실상 불가능하다. 랜덤한 공격자들 및 사용자와 연관된 자들 모두에게 위조 불가능해야 한다.

[0042] [45] 사적: 계정 제공자 또는 공격자에게 개인 데이터를 드러내지 않는다; 그리고

[0043] [46] 이용 가능: 특수 목적 디바이스들 없이도 일반적 소프트웨어 시스템들로 구현 가능하다.

[0044] [47] 팩터들을 선택하기 위한 몇몇 고려사항들이 있다. 예를 들어, 영구적 팩터가 "사용자가 가진 무언가"이면, 사용자는 팩터를 분실할 수 있거나 팩터는 공격자의 수중에 들어갈 수 있다. 영구적 팩터가 "사용자가 아는 무언가"이면, 팩터는 시스템이 체크하기에 사적이지 않을 수 있고, 사용자가 팩터를 잊어버릴 수 있다. 영구적 팩터가 "사용자가 가지고 있는 무언가"이면, 팩터는 몇몇 인간 특징 인식(생체 측정 디바이스들 등)을 요구하고 쉽게 이용 가능하지 않을 수 있고, 또한 제공자에게 개인 정보를 드러낼 수 있다.

[0045] [48] 예시적 구현들에서, 영구적 팩터들은 사용자 지식("당신이 알고 있는 무언가")에 기초하여 활용될 수 있고 또한 사용자가 소유한 무언가에 기초할 수 있다. 그런 요건들은 기존 상황들 중 많은 상황들을 충족시키기에 어려울 수 있다. 그러므로, 예시적 구현들은 사용자 지식에 기초한 솔루션을 포함할 수 있어서, 사용자가 많은 기본적 질문들을 신뢰성 있게 기억할 수 있다는 것을 가정하고, 대답들은 암호화 동작들과 얽힌다.

[0046] [49] 자신 및 다른 사람의 지식: 예시적 구현들이 "사용자 지식"에 기초하여 제시되었지만, 지식은 수탁자(trustee)들 및 다른 소스들로부터 실시간으로 획득될 수 있고, 지식의 누적은 사용자 개인 지식 및 수탁자들에 대한 사용자 액세스를 나타낼 수 있다. 수탁자들은 사용자에 관한 지식의 일부를 나타낼 수 있고 필요한 팩터들을 생성하도록 사용자를 도울 수 있다.

[0047] [50] 예시적 구현들은 계정에 대한 액세스의 긴급 복구에 대한 기본적 프로세스를 포함할 수 있지만, 또한 프라이버시 및 진정성을 밸런싱하고 계정에 대한 이용 가능성을 취하는 일반 인증 방법으로서 구현될 수 있다(예를 들어, 팩터가 필요할 때 사용자 훈련 및 사용자를 훈련하기 위한 인터페이스들).

[0048] [51] 사용자들이 인터넷 계정 제공자로부터 가진 계정들은 사용자들이 그 계정에 그들의 이메일, 전자-지불들, 개인 콘텐츠 등을 유지하기 때문에 중요성을 얻고 있다. 이들 계정들은 주요 개인 리소스들이고 공격자들에게 영향을 받기 쉽다. 예시적인 구현들은, 사용자에게 항상 이용 가능하고 공격자에게는 결코 이용 가능하지 않은 영구적 인증 팩터를 사용자가 가지는 경우, 강탈범이 할 수 없는 방식으로 사용자가 계정을 유지하고 재주장할 수 있도록 하는 시스템들 및 방법들에 관련된다. 그런 팩터를 근사화하는 것은 복구 프로세스를 용이하게 할 수 있다.

[0049] [52] 관련 기술에서 이메일 계정 같은 계정이 강탈당하면 공격자가 계정의 상태를 가지며, 사용자인 비-악의적인 계정 홀더에 의한 복구가 더 어려워질 수 있도록 계정을 조작하는 경우가 있다. 공격자는 또한 계정에 저장된 데이터 모두로부터 학습할 수 있다. 그러므로 예시적 구현들은 계정에 대한 액세스로부터 추론될 수 없는 메커니즘을 활용한다. 유사하게, 메커니즘은 계정이 이용 가능하지 않은 경우(예를 들어, 강탈당함) 소실되지 않는 것이어야 한다. 복구는 이후 영구적 팩터들의 홀더에 의해 좌우된다.

[0050] [53] 예시적 구현들은 사용자 지식, 또는 필요할 때 사용자가 재-생성할 수 있는 지식의 높은-엔트로피 소스를 이용한다. 이런 목적을 위하여, 많은 양의 매우 사적인 사용자 정보가 이용된다 - 형제, 자녀, 배우자, 부모들, 조부모들, 친구들의 이름들, 자신 및 친척의 주소들, 계정 이름들 및/또는 번호들, 고용주들의 이름 및 그 이상. 정보는 필요한 경우 사용자가 대답들을 재-생성할 수 있도록 하는 것이어야 하고, 데이터의 양 및 변동성은 충분한 비트들이 공격자에게 결코 알려지지 않도록 하는 것이어야 한다. 유사하게, 생체 측정 판독 또는 은행 서버들 같은 수탁자들에 대한 액세스 같은 다른 팩터들이 또한 결합하여, 공격자에게 알려지지 않은 것으로 가정된다.

[0051] [54] 다른 예시적 구현에서, 팩터는 팩터를 생성 및 체킹하기 위한 입력, 프로세싱 및 출력을 가진 프로세스에 의해 생성될 수 있다. 프로세스는 각각 역할을 가진 사용자 입력, 시스템 입력 및 암호 계산을 포함할 수 있다.

[0052] [55] 입력은 사용자에게 문의되는 질문들(Q1, Q2, Q3 등) 및 대답들(A1, A2, A3)의 세트 등과 같은 지식의 높은-엔트로피 소스를 포함할 수 있다. 대답들(Ai)은 사용자가 기억할 수 있는 것이어야 한다(질문들은 다수회 요청될 수 있고 이에 의해 사용자는 이들에 대답하도록 훈련받을 수 있음). 그런 질문들의 선택은 생활

질문들, 취미 질문들(다양한 영역들에서), 개인 이력 질문들 등을 포함할 수 있다. 게다가, 질문들의 횟수는 원해진 엔트로피를 생성하기 위하여 충분히 커야 한다. 원해진 구현에 따라, 사용자가 핸드 헬드 디바이스 또는 종이 조각에 유지할 수 있거나 또는 사용자에게 메일링되어 인터넷 계정들에 유지되는 랜덤 값들(R1, R2 등) 및/또는 사용자 로컬 시스템이 유지하는 부가적인 랜덤 값들, 및 비밀(S)이 또한 사용될 수 있다.

[0053] [56] 프로세싱은 팩터 생성을 포함할 수 있다. 질문들에 대한 입력들(A1, A2,....An)이 주어지면, 대답들은 그룹들로 조직된다(반복들을 가짐. 예를 들어, G1=A1,A3,A5, G2=A1,A3,A6,A7). 그룹은 사용자가 전부 대답할 것으로 예상되는 연결된 대답들의 세트를 나타낸다. m개의 그룹들이 각각 충분히 높은 엔트로피를 가진다고 가정한다. 원해진 구현에 따라, 랜덤 값들(R1,...Rm) 및 비밀(S)이 또한 부가(연결)될 수 있고, 예를 들어 S는 각각의 그룹에 그리고 Ri는 Gi에 부가되어, G1=S,R1,A1,A3,A5일 수 있다.

[0054] [57] 각각의 Gi는 암호화 해시 함수(예를 들어, Sha1 등)(H)로 해싱된다. 예를 들어, H1= H(H(H(H(H(R), S1) A1)A3)A5)이다. 계산을 느리게 하기 위한 부가적인 해싱은 또한 발생할 수 있다. H_i들은 표시자들로 불린다.

[0055] [58] 각각의 그룹은 그 자신의 표시자(Hi: H1, H2,....Hm)를 가진다. 랜덤화기(randomizer)들이라 불리는 랜덤 값들(Ri)은 사용자 시스템에 유지되고(예를 들어, 서버에 의해 액세스 가능하지 않거나, S 하에서 암호화되어 서버로 전송됨), S는 시스템 외부(예를 들어, 종이에 또는 복구를 위해 유지된 다른 디바이스에, 또는 수탁자들에, 그리고 다른 장소에는 없음)에 유지된 사용자의 비밀이다. E_S(Ri)=Xi라고 하고, Xi는 Hi에서 사용된 Ri의 인크립션이고 S는 시드(seed)라 불린다. Hi,Xi i=1,..,m은 서버에 전송된다. 표시자들 Hi들은 이후 클라이언트 측 및 그의 디바이스에서 소거된다.

[0056] [59] 시드(S)는 계정 저장부 외부의 사용자의 메모리(예를 들어, 디바이스상 또는 종이)에 유지된다. Hi들은 복구 유효화를 위해 유지되도록 서버에 전송되고 로컬 카피는 소거된다. 서버는 침투 공격자들이 표시자들을 학습하는 것을 방지하기 위하여, 표시자들을 일방향 함수들로 추가로 해싱할 수 있다.

[0057] [60] 상기 예시적 구현으로부터, 그러므로 서버는 대답들에 대한 어떠한 정보도 수신하지 못하고, 단지 충분한 엔트로피를 가진 해싱된 값만을 수신한다. 사용자는 하나의 그룹에 매칭하기에 충분한 질문들에 대답할 수 있어야 한다. 공격자는 하나의 그룹조차 커버하기 위한 대답들을 추측할 수 없어야 하고, S에 대한 액세스를 갖지 못한다.

[0058] [61] 팩터들은 이후 인증을 위해 사용될 수 있다. 인증 프로세스 또는 계정 복구 프로세스에서, 영구적 팩터를 사용하기 위한 시도가 발생한다. 서버는 그룹 중 하나의 질문들을 제시하고, 여기서 사용자는 그룹을 선택하고, 질문들에 대답하고, 그의 S 및 그의 디바이스를 입력하고, 차례로 그의 비밀(S)을 사용하여 Xi로부터 Ri를 복구한다. 대답 그룹 Gi-현재(Gi에 대한 후보)를 생성하는 사용자 현재 대답들에 기초하여 Hi가 스크래치(scratch)로부터 계산되고 생성된 Hi는 서버에 전송된다. 사용자는 대답들로부터 전체 표시자를 계산할 수 있다; 대안으로 표시자들의 대답들 중 몇몇(예에서 A5 같은)은 예에서 명확하고 부분적으로 평가된 표시자(H(H(H(H(R), S1) A1)A3)) 상에 전송될 수 있고, 전송될 수 있고 사용자는 표시자 계산을 완료할 수 있다(따라서 몇몇 대답들은 숨겨지고 몇몇은 공개된다--단지 복구시).

[0059] [62] 서버는 계산되어 생성되고 이후 해싱되는 Hi를, 해싱되고 저장된 Hi와 비교한다. 만약 매칭이 있다면, 사용자는 인증된다. 그렇지 않으면(예를 들어, 만약 생성된 Hi가 다양한 그룹들에서 실패함) 청구자는 실패되고 본래의 사용자로서 인식되지 못한다. 대안적인 예시적 구현에서, 사용자는 해싱된 버전 HASH(Hi)에 관하여 Hi의 소유를 증명하는 프로토콜에 참여할 수 있다는 것이 주의된다.

[0060] [63] 대답들은 사용자에 관한 개인 정보를 요구할 수 있지만, 정보는 사용자 컴퓨터 또는 사용자 디바이스에 대해 모두 로컬이고, 프라이버시 목적들을 위해 서버에 의해서도 액세스 가능하지 않고 서버인 것으로 가장하는 피싱 파티들에게도 액세스 가능하지 않다. 대답들이 소거되기 때문에, 대답들은 질문 시간에 재구성된다. 또한, 부분 정보가 주어질 수 있다: 부분 네스팅(nest)된 해싱이 계산되고 A5는 명확하게 주어지고, 그리고 서버는 해싱을 완료하는 것과 같음.

[0061] [64] 결합 함수로서 H(R)*H(A1)*H(A3)*H(A5)(즉, 충분히 큰 체(field)에서 개별 값들의 해시들의 곱셈) 같은 구현에 대해, 부분 곱(partial product)이 제공될 수 있고, 여기서 대답들 중 몇몇은 공개될 수 있고 서버는 그 곱(product)을 완료할 수 있다. 위치 고정 테스트(position fixed test)의 경우, 질문지의 위치(j)에서 대답(Ai)이 위치(j)와 연관되도록 H(R)*H(1, A1)*H(2, A3)*H(3, A5)가 제공될 수 있다. 곱(product)은 큰 소수 차수(large prime order)의 체(field) 상에서 수행될 수 있다.

[0062] [65] 정보는 서버의 상태가 주어지면 개별 필드들을 숨기기 위하여 충분한 엔트로피를 가져야 하고, 따라서 공격자가 대답을 형성할 가능성은 실질적으로 작다. 사용자는, 팩터가 올바른 서버에 제공되는 것을 추가로 보장할 필요가 있다. 팩터(오프 라인 공격들) 또는 대답들의 몇몇을 공개한 팩터들(실시간 공격들)을 학습하기 위한 노력은 가능하고 구현시 고려되어야 한다.

[0063] [66] 게다가, 고도로 기억된 대답들의 세트가 사용되어야 하고 사용자 훈련은 적소에서 서버가 이를 도울 값들이 서버에 위임(기록)되기 전에 있어야 한다. 기억하기 쉽지 않은 대답들은, 팩터가 영구적인 것을 보장하기 위하여 적혀질 수 있다. 예시적 구현들은, 일반 소프트웨어 시스템이 특정 디바이스들/판독기들/등 없이 이용될 수 있도록 한다.

[0064] [67] 예시적 구현들은, 대답들이 기억되기 보다 사용자들에 의해 외부 에이전시들로부터 얻어지는 시스템 또는 프로세스를 포함할 수 있다. 이들 에이전시들은 사용자가 대답을 리트리브하게 하는 인증에 의존하고, 따라서 구현은 상기 영구적 팩터를 사용하여 내재적인 "소셜 복구"를 만들 수 있다. 팩터는 먼저 이전 테스트를 통과하고 그 다음 팩터에 임베딩된 지식을 업데이팅함으로써 증가적으로 만들어질 수 있다. 게다가, 영구적 팩터는, 필요할 때 사용되고 다른 팩터들에 의해 지원될 수 있도록 제한될 수 있고, 계정의 복구 또는 계정 프로세스의 재-주장이 하나의 부가적인 결정적 팩터로서 포함될 수 있다. 사용자 및 수탁자들로부터의 대답들이 임의의 입력 방법(타이핑, 음성, 생체 측정 판독, 카메라 등)을 이용하여 얻어질 수 있다는 것이 주의된다.

[0065] [68] 이에 의해 상기 설명된 예시적 구현들은 사용자가 입력하는 지식으로 사용자가 패스워드를 대체하게 한다. 패스워드들과 달리, 사용자는 사용자에 관한 지식 부분(이들의 대부분)들을 알 가능성이 크다. 패스워드 이용은 (사적 키(private key) 같은) 패스워드 암호화 정보의 로컬 암호해제를 위하여 활용될 수 있다. 이런 새로운 생각을 확장하는 것은 그런 목적들을 위해 패스워드 드롭-인(drop-in) 대체를 위하여 사용될 수 있고, "디바이스"가 단지 로컬 계산인 다른 설계 문제이다. "로컬 계산"은 모바일 디바이스상에서 행해질 수 있고 최종 결과는 대답들이 도난당하지 않는 것을 사용자에게 보장하기 위하여 무선, USB 또는 물리적 연결 같은 로컬 통신 방법을 통해 컴퓨터 또는 서버에 전송된다.

[0066] [69] 예시적 구현들은 또한, 식별의 다른 수단이 손실되었더라도, 사용자가 항상 재구성할 수 있는 영구적 팩터를 포함할 수 있다. 이것은 계정 강탈범으로부터 사용자를 구별할 수 있고, 사용자들에 의해 다시 계정들을 주장하기 위하여 사용될 수 있다(예를 들어, 질문지 및 최소 노출에 기초하여 다시 주장하는 방법이 대신된다).

[0067] [70] 도 1a는 예시적 구현에 따른, 디바이스에 대한 흐름도를 예시한다. 100에서, 디바이스는 복수의 질문들에 대한 사용자에 의해 제공된 복수의 응답들로부터 복수의 해시들을 생성한다. 제공된 질문들은 서버, 또는 디바이스로부터 올 수 있고, 상기 설명된 바와 같이 사용자에 관한 개인 정보를 포함하는 질문지를 활용할 수 있다.

[0068] [71] 101에서, 디바이스는 복수의 해시들로부터 인증 해시를 생성할 수 있다. 이것은 인증 해시를 생성하기 위하여 복수의 해시들의 다항식 보간을 수행함으로써, 그리고/또는 복수의 질문들 중 선택된 그룹에 기초하여 인증 해시를 형성하기 위하여 복수의 해시들 중 하나 이상을 선택함으로써 구현될 수 있다. 상기 예시적 구현들에서 설명된 바와 같이, 사용자는 대답에 대한 질문들의 그룹을 선택할 수 있고, 이에 의해 대답들은 인증 해시를 생성하기 위하여 해싱될 수 있거나, 디바이스는 제공된 대답들(예를 들어, 2 이상)의 서브세트를 선택할 수 있고 서브세트에 기초하여 인증 해시를 생성할 수 있다. 상기 예시적 구현들에 설명된 바와 같이, 비밀 인증 해시는 또한 디바이스에 저장될 수 있고 요건들이 충족될 때(예를 들어, 질문들에 대한 올바른 대답들의 임계치를 충족, 질문들의 서브세트를 올바르게 대답, 비밀 인증 해시에 매칭하는 인증 해시 등) 보안 프로토콜에 의해 서버에 포워딩될 수 있다.

[0069] [72] 디바이스는 또한, 상기 설명된 바와 같이, 인증 해시를 보간하기 위하여 다항식 보간의 사용으로부터 복수의 해시들의 다항식 보간으로부터 인증 해시를 생성할 수 있다. 다항식 보간 알고리즘 및 노이지 보간 알고리즘 같은 구현들이 이용될 수 있다. 서버에서 부가된 포인트들 및/또는 다항식 보간을 위한 하나 이상의 올바른 포인트들을 사용하여, 다항식 보간에 대한 하나 이상의 에러 포인트들의 도입을 통해 임계치가 조절될 수 있고 다항식 보간에 적용될 수 있다. 102에서, 디바이스는 이후 생성된 인증 해시를 이용하여 서버에 인증하도록 시도한다.

[0070] [73] 도 1b는 예시적 구현에 따른, 복구 프로세스에 대한 흐름도를 예시한다. 상기 예시적 구현들에서 설명된 바와 같이, 103에서, 디바이스는 복수의 질문들을 수신하고, 사용자는 상기 복수의 질문들 중에서, 계정에

대한 액세스를 복구하기 위해 대답할 질문들의 서브세트를 선택할 수 있다. 104에서, 제공된 대답들은 사용자 디바이스 외부에 있는 비밀 시드로부터 생성된 난수의 사용에 기초하여 인증 해시로 변환된다. 105에서, 인증 해시는 서버로 포워딩된다.

[0071] [74] 도 2a는 예시적 구현에 따른, 서버에 대한 흐름도를 예시한다. 200에서, 서버는 복수의 개인 질문들을 디바이스에 전송할 수 있다. 201에서, 서버는 전송된 복수의 질문들에 응답하는 디바이스로부터 인증 해시를 수신한다. 202에서, 서버는 이후, 전송된 복수의 질문들에 응답하는 인증 해시가 서버에 저장된 비밀 인증 해시에 매칭하는 경우, 액세스를 승인(204)(예)하기로 결정하고; 그리고 인증 해시가 비밀 인증 해시에 매칭하지 않는 경우 액세스(203)를 거부(아니오)하기로 결정할 수 있다. 인증 해시는 복수의 질문들 중 선택된 그룹에 기초하여 인증 해시를 형성하기 위하여, 복수의 해시들 중 하나 이상의 선택 및 복수의 해시들의 다항식 보간으로부터 생성될 수 있다. 구현에 따라, 서버는, 비밀 인증 해시 및 임계치에 기초하여, 하나 이상의 에러 포인트들, 및 노이지 보간 알고리즘에 사용하기 위한 하나 이상의 올바른 포인트들을 전송할 수 있다. 서버는 또한, 해시가 저장된 비밀 해시에 매칭하는지를 결정하기 위하여 수신된 인증 해시의 해싱을 수행할 수 있다.

[0072] [75] 다른 예에서, 서버는 전송된 질문들 중 선택된 그룹에 기초하여 복수의 비밀 인증 해시들로부터 비밀 인증 해시를 선택할 수 있고, 복수의 비밀 인증 해시들 각각은 복수의 질문들 중 적어도 두 개와 연관된다. 전송된 질문들 중 선택된 그룹은 디바이스에서 또는 서버에 의해 선택될 수 있다. 이것은 예를 들어, 상기 설명된 바와 같이 복구 프로세스에서 구현될 수 있다.

[0073] [76] 도 2b는 예시적 구현에 따른 서버로부터의 복구 프로세스를 위한 흐름도를 예시한다. 205에서, 서버는 복수의 개인 질문들을 디바이스에 전송할 수 있다. 206에서, 서버는 전송된 복수의 질문들에 응답하여 디바이스로부터 인증 해시를 수신하고, 여기서 인증 해시는 잠재적으로 상기 예시적 구현들에 설명된 바와 같이 표시자들 중 하나이다. 207에서, 서버는 이후, 인증 해시가 서버에 저장된 표시자들 중 하나에 매칭하면 사용자 계정을 복구하기 위한 프로세스를 시작(209)(예)하기로 결정할 수 있고; 그리고 인증 해시가 저장된 표시자들 중 임의의 표시자에 매칭하지 않으면 액세스를 거부(208)(아니오)하기로 결정할 수 있다.

[0074] [77] 예시적 프로세싱 환경

[0075] [78] 도 3은 몇몇 예시적 구현들에 사용하기에 적당한 예시적 컴퓨팅 디바이스를 가진 예시적 컴퓨팅 환경을 도시한다. 컴퓨팅 환경(300)에서 컴퓨팅 디바이스(305)는 하나 이상의 프로세싱 유닛들, 코어들, 또는 프로세서들(310), 메모리(315)(예를 들어, RAM, ROM, 등), 내부 스토리지(320)(예를 들어, 자기, 광학, 고체 상태 스토리지, 및/또는 유기), 및/또는 I/O 인터페이스(325)를 포함할 수 있고, 이들 중 임의의 것은 정보를 통신하기 위하여 통신 메커니즘 또는 버스(330)에 커플링되거나 컴퓨팅 디바이스(305)에 임베딩될 수 있다.

[0076] [79] 컴퓨팅 디바이스(305)는 입력/사용자 인터페이스(325) 및 출력 디바이스/인터페이스(340)에 통신 가능하게 커플링될 수 있다. 입력/사용자 인터페이스(325) 및 출력 디바이스/인터페이스(340) 중 어느 하나 또는 둘 다는 유선 또는 무선 인터페이스일 수 있고 제거 가능할 수 있다. 입력/사용자 인터페이스(325)는 임의의 디바이스, 컴포넌트, 센서, 또는 입력을 제공하기 위하여 사용될 수 있는 물리 또는 가상의 인터페이스(예를 들어, 버튼들, 터치-스크린 인터페이스, 키보드, 포인팅/커서 제어, 마이크로폰, 카메라, 브라유 점자, 모션 센서, 광학 판독기, 등)를 포함할 수 있다. 출력 디바이스/인터페이스(340)는 디스플레이, 텔레비전, 모니터, 프린터, 스피커, 브라유 점자 등을 포함할 수 있다. 몇몇 예시적 구현들에서, 입력/사용자 인터페이스(325) 및 출력 디바이스/인터페이스(340)는 컴퓨팅 디바이스(305)에 임베딩되거나 상기 컴퓨팅 디바이스(305)에 물리적으로 커플링될 수 있다. 다른 예시적 구현들에서, 다른 컴퓨팅 디바이스들은 컴퓨팅 디바이스(305)에 대한 입력/사용자 인터페이스(325) 및 출력 디바이스/인터페이스(340)로서 기능할 수 있거나 그런 기능들을 제공할 수 있다.

[0077] [80] 컴퓨팅 디바이스(305)의 예들은 고도의 모바일 디바이스들(예를 들어, 스마트폰들, 차량들 및 다른 머신들 내 디바이스들, 인간들 및 동물들에 의해 휴대되는 디바이스들 등), 모바일 디바이스들(예를 들어, 테블릿들, 노트북들, 랩톱들, 개인용 컴퓨터들, 휴대용 텔레비전들, 라디오들 등), 및 이동성을 위하여 설계되지 않은 디바이스들(예를 들어, 데스크톱 컴퓨터들, 다른 컴퓨터들, 정보 키오스크(kiosk)들, 임베딩되고 및/또는 커플링된 하나 이상의 프로세서들을 가진 텔레비전들, 라디오들, 서버들, 등)(이들로 제한되지 않음)을 포함할 수 있다.

[0078] [81] 컴퓨팅 디바이스(305)는 동일하거나 상이한 구성의 하나 이상의 컴퓨팅 디바이스들을 포함하는 임의의 수의 네트워킹된 컴포넌트들, 디바이스들, 및 시스템들과 통신하기 위하여 네트워크(350) 및 외부 스토리지

(345)에 통신 가능하게 커플링(예를 들어, I/O 인터페이스(325)를 통해)될 수 있다. 컴퓨팅 디바이스(305) 또는 임의의 연결된 컴퓨팅 디바이스는 서버, 클라이언트, 소형 서버, 일반 머신, 특수-목적 머신, 또는 다른 라벨로서 기능하거나, 이들의 서비스들을 제공하거나, 이들로 지칭될 수 있다.

[0079] [82] I/O 인터페이스(325)는 컴퓨팅 환경(300)에서 적어도 모든 연결된 컴포넌트들, 디바이스들, 및 네트워크에 및/또는 이들로부터 정보를 통신하기 위하여 임의의 통신 또는 I/O 프로토콜들 또는 표준들(예를 들어, 이더넷, 802.11x, USB(Universal System Bus), WiMax, 모뎀, 셀룰러 네트워크 프로토콜 등)을 사용하는 유선 및/또는 무선 인터페이스(이들로 제한되지 않음)를 포함할 수 있다. 네트워크(350)는 임의의 네트워크 또는 네트워크들의 결합(예를 들어, 인터넷, 로컬 영역 네트워크, 광역 네트워크, 전화 네트워크, 셀룰러 네트워크, 위성 네트워크 등)일 수 있다.

[0080] [83] 컴퓨팅 디바이스(305)는 신호 매체들 및 저장 매체들을 포함하여, 컴퓨터-사용 가능 또는 컴퓨터-판독 가능 매체들을 사용하고 및/또는 이들을 사용하여 통신할 수 있다. 신호 매체들은 전송 매체들(예를 들어, 금속 케이블들, 광섬유들), 신호들, 반송파들 등을 포함한다. 저장 매체들은, 자기 매체들(예를 들어, 디스크들 및 테이프들), 광학 매체들(예를 들어, CD ROM, 디지털 비디오 디스크들, 불루-레이 디스크들), 고체 상태 매체들(예를 들어, RAM, ROM, 플래시 메모리, 고체-상태 스토리지), 및 다른 비휘발성 스토리지 또는 메모리를 포함한다.

[0081] [84] 컴퓨팅 디바이스(305)는 몇몇 예시적 컴퓨팅 환경들에서 기술들, 방법들, 애플리케이션들, 프로세스들, 또는 컴퓨터-실행 가능 명령들을 구현하기 위하여 사용될 수 있다. 컴퓨터-실행 가능 명령들은 일시적 매체들로부터 리트리브될 수 있고 비-일시적 매체들 상에 저장되고 리트리브될 수 있다. 실행 가능 명령들은 임의의 프로그래밍, 스크립팅, 및 기계 어들(예를 들어, C, C++, C#, 비주얼 베이직, 파이선, 펄, 자바스크립트, 및 다른 것들) 중 하나 이상으로부터 발생할 수 있다.

[0082] [85] 프로세서(들)(310)는 본래 또는 가상 환경에서 임의의 오퍼레이팅 시스템(OS)(도시되지 않음) 하에서 실행 가능할 수 있다. 하나 이상의 애플리케이션들은 전개될 수 있고 논리 유닛(360), 애플리케이션 프로그래밍 인터페이스(API) 유닛(365), 입력 유닛(370), 출력 유닛(375), 인증 유닛(380), 복구 유닛(385), 난수 생성기 유닛(390), 및 서로 통신하고, OS를 가지며, 그리고 다른 애플리케이션(도시되지 않음)들을 가진 상이한 유닛들에 대한 유닛간 통신 메커니즘(395)을 포함한다. 예를 들어, 인증 유닛(380), 복구 유닛(385), 및 난수 생성기 유닛(390)은 디바이스로서 구현되는지 또는 서버로서 구현되는지에 따라 도 1a, 도 1b, 도 2a 및 도 2b에 도시된 바와 같이 하나 이상의 프로세스들을 구현할 수 있다. 복구 유닛(385)은 또한 도 1b 및 도 2b의 상기 예시적 구현들에 설명된 바와 같이 복구 프로세스들을 구현할 수 있다. 설명된 유닛들 및 엘리먼트들은 설계, 기능, 구성, 또는 구현이 가변될 수 있고 제공된 설명들로 제한되지 않는다.

[0083] [86] 몇몇 예시적 구현들에서, 정보 또는 실행 명령이 API 유닛(365)에 의해 수신될 때, 하나 이상의 다른 유닛들(예를 들어, 논리 유닛(360), 입력 유닛(370), 출력 유닛(375), 인증 유닛(380), 복구 유닛(385), 및 난수 생성기 유닛(390))에 통신될 수 있다. 예를 들어, 난수 생성기 유닛(390)은 해시들을 생성하거나 제출을 위한 질문들을 선택하기 위해 사용될 수 있고, 상기 예시적인 구현들에 설명된 바와 같이 난수들을 제공하기 위하여 인증 유닛(380) 및 복구 유닛(385)에 통신하도록 API 유닛(365)을 사용할 수 있다. 인증 유닛(380)은, 인증 해시를 저장된 비밀 인증 해시와 비교하기 위하여 API 유닛(365)을 통해 복구 유닛(385)과 상호작용할 수 있다.

[0084] [87] 몇몇 예들에서, 논리 유닛(360)은 상기 설명된 몇몇 예시적인 구현들에서 유닛들 사이의 정보 흐름을 제어하고 API 유닛(365), 입력 유닛(370), 출력 유닛(375), 인증 유닛(380), 복구 유닛(385), 및 난수 생성기 유닛(390)에 의해 제공된 서비스들을 지시하도록 구성된다. 예를 들어, 하나 이상의 프로세스들 또는 구현들의 흐름은 논리 유닛(360) 단독 또는 API 유닛(365)과 결합하여 제어될 수 있다.

[0085] [88] 예시적 프로세싱 환경

[0086] [89] 도 4는 몇몇 예시적 실시예들이 구현될 수 있는 예시적 온라인 환경을 도시한다. 환경(400)은 디바이스들(405-445)을 포함하고, 이들 각각은 예를 들어 네트워크(450)를 통해 적어도 하나의 다른 디바이스에 통신 가능하게 연결된다. 몇몇 디바이스들은 하나 이상의 저장 디바이스들(430 및 445)에 통신 가능하게 연결될 수 있다(예를 들어, 디바이스(425)를 통해).

[0087] [90] 하나 이상의 디바이스들(405-450)의 예는 도 4에 하기 설명된 컴퓨팅 디바이스(405)일 수 있다. 디바이스들(405-450)은 컴퓨터(425)(예를 들어, 개인용 또는 상업용), 차량(420)과 연관된 디바이스, 모바일 디바이스(410)(예를 들어, 스마트폰), 텔레비전(415), 모바일 컴퓨터(405), 서버 컴퓨터(450), 컴퓨팅 디바이스들

(435-440), 저장 디바이스들(430, 445)을 포함(이들로 제한되지 않음)할 수 있다. 디바이스들(405-450) 중 임의의 디바이스는 환경(400)에 도시된 하나 이상의 디바이스들 및/또는 환경(400)에 도시되지 않은 디바이스들로부터 하나 이상의 서비스들을 액세스하고 및/또는 상기 디바이스들에 하나 이상의 서비스들을 제공할 수 있다. 디바이스들 사이에서 액세싱은 유선, 무선일 수 있고, 그리고 사용자 음성, 카메라 사진들, 등 같은 멀티미디어 통신에 의해서 일 수 있다.

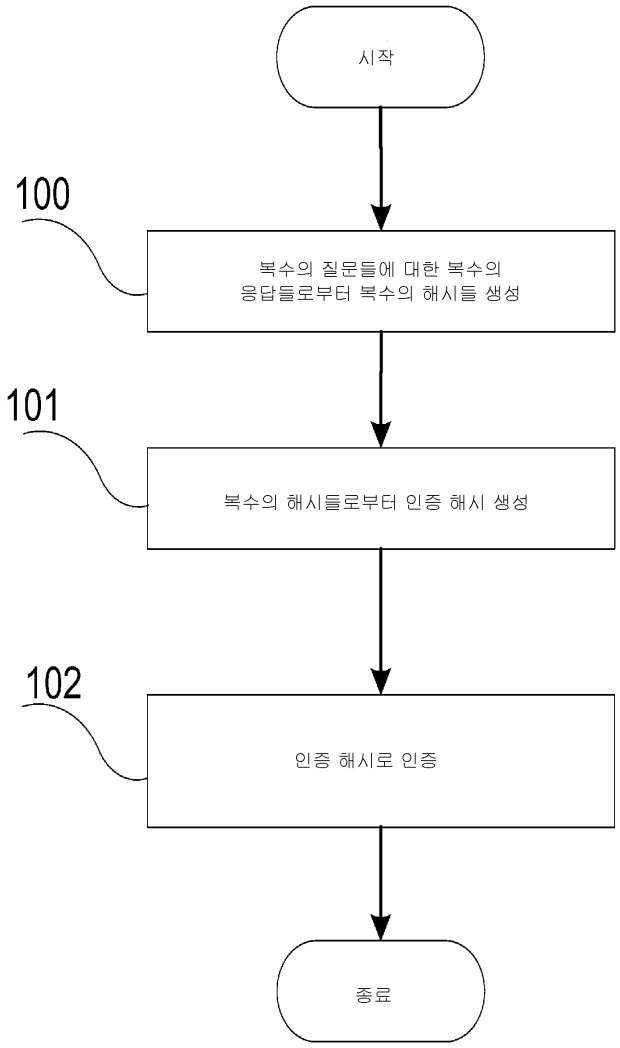
[0088] [91] 사용자는 상기 설명된 바와 같이, 네트워크(450)를 통해 예시적 구현들을 구현하기 위하여 디바이스를 제어할 수 있다. 예시적 구현들과 연관된 정보는 예를 들어, 각각 저장 디바이스(430 또는 445)에 저장될 수 있다.

[0089] [92] 여기서 논의된 시스템들이 사용자들에 관한 개인 정보를 수집하거나, 개인 정보를 이용할 수 있는 상황들에서, 사용자들에게는 프로그램이 사용자 정보(예를 들어, 사용자의 소셜 네트워크에 관한 정보, 소셜 동작들 또는 활동들, 직업, 사용자의 선호도들, 또는 사용자의 현재 위치)를 수집하는지 피처들이 이들을 수집하는지를 제어하거나, 사용자에 보다 관련될 수 있는 콘텐츠 서버로부터 콘텐츠를 수신할지 및/또는 수신하는 방법을 제어할 기회가 제공된다. 게다가, 특정 데이터는 저장되거나 사용되기 전에 하나 이상의 방식들로 처리될 수 있어서, 개인적으로 식별 가능한 정보가 제거된다. 예를 들어, 사용자의 아이덴티티는, 사용자에 대한 개인적으로 식별 가능한 어떠한 정보도 결정될 수 없거나, 위치 정보(도시, ZIP 코드, 또는 상태 레벨 같은)가 얻어지는 경우 사용자의 지리적 위치가 일반화될 수 없도록 처리될 수 있어서, 사용자의 특정 위치가 결정될 수 없다. 따라서, 사용자는 정보가 사용자에 관해 어떻게 수집되는지 및 콘텐츠 서버에 의해 어떻게 사용되는지를 제어할 수 있다.

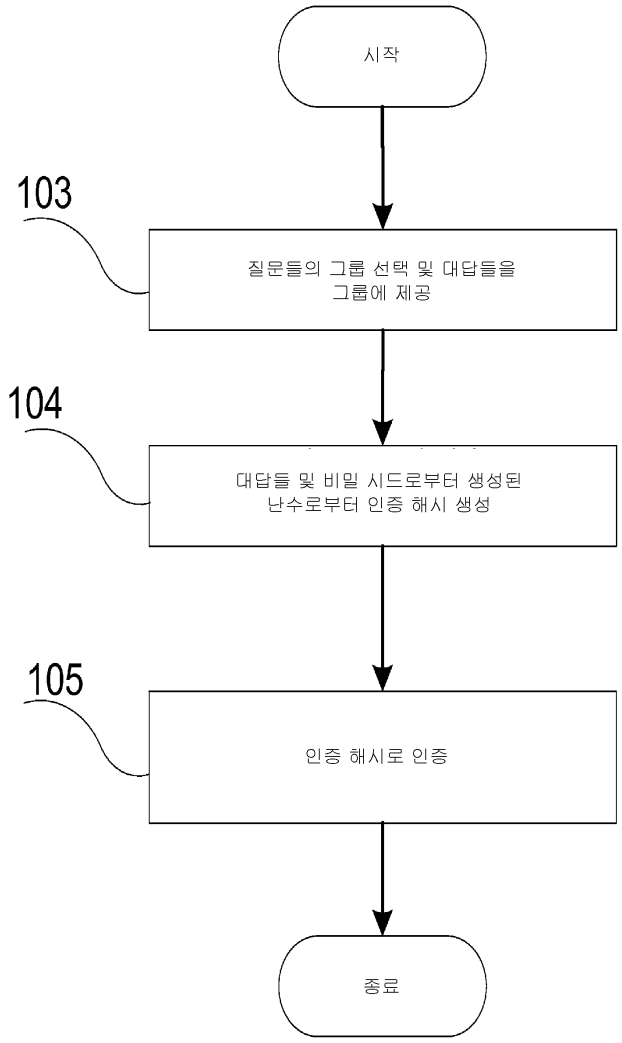
[0090] [93] 비록 몇몇 예시적 구현들이 도시되고 설명되었지만, 이들 예시적 구현들은 이 분야에 친밀한 사람들에게 본원에 설명된 청구 대상을 전달하기 위하여 제공된다. 본원에 설명된 청구 대상이 설명된 예시적 구현들로 제한됨이 없이 다양한 형태들로 구현될 수 있다는 것이 이해되어야 한다. 본원에 설명된 청구 대상은 특정하게 정의되거나 설명된 문제들 없이 또는 설명되지 않은 다른 또는 상이한 엘리먼트들 또는 문제들을 가지고 실시될 수 있다. 변경들이 첨부된 청구항들 및 이들의 등가물들에서 정의된 바와 같이 본원에 설명된 청구 대상으로부터 벗어남이 없이 이들 예시적 구현들에서 이루어질 수 있다는 것이 당업자에 의해 이해될 것이다.

도면

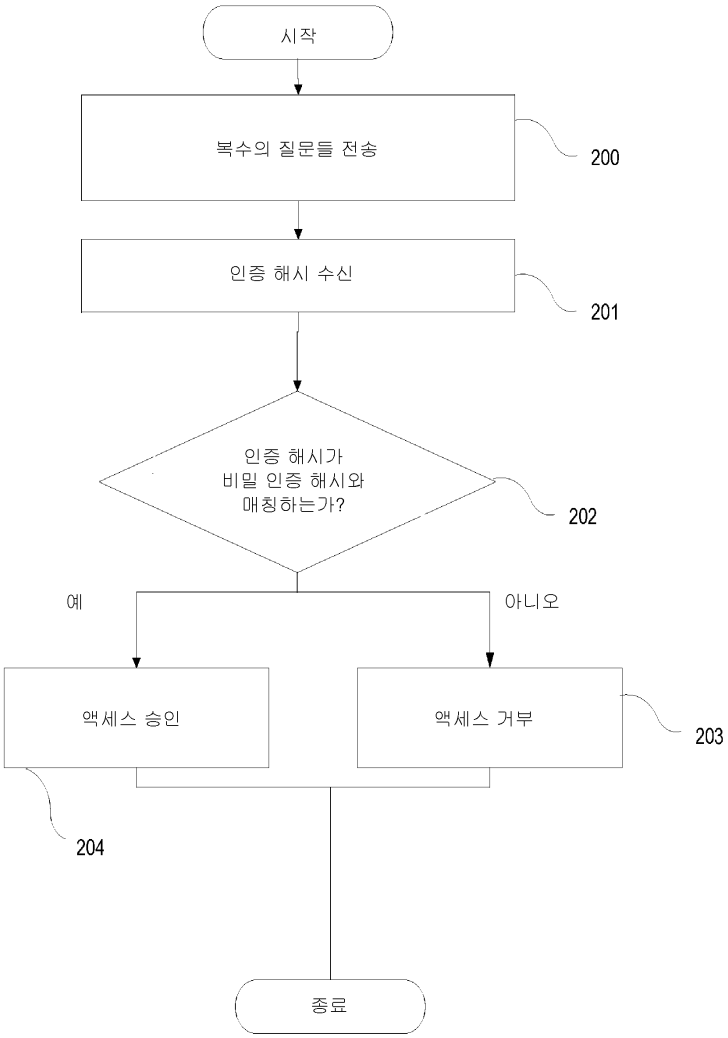
도면1a


시작
100
복수의 질문들에 대한 복수의
응답들로부터 복수의 해시들 생성
101
복수의 해시들로부터 인증 해시 생성
102
인증 해시로 인증
종료

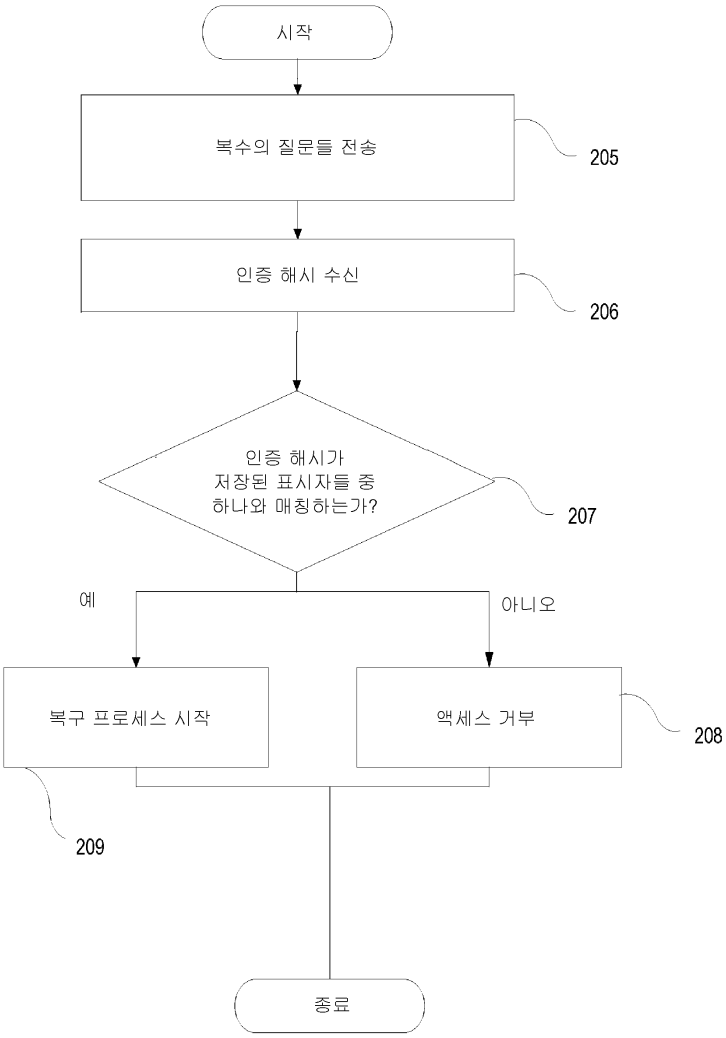
도면1b


시작
103
질문들의 그룹 선택 및 대답들을 그룹에 제공
104
대답들 및 비밀 시드로부터 생성된 난수로부터 인증 해시 생성
105
인증 해시로 인증
종료

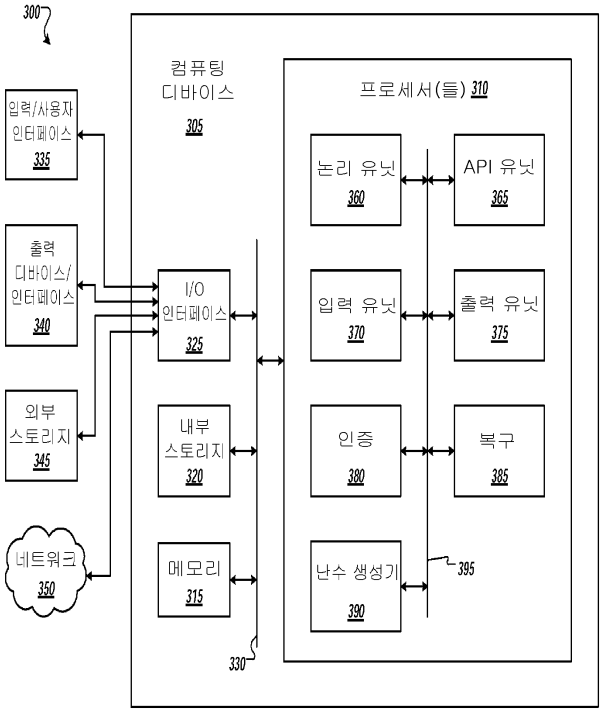
도면2a


시작
복수의 질문들 전송
200
인증 해시 수신
201
인증 해시가
비밀 인증 해시와
매칭하는가?
202
예
아니오
액세스 승인
액세스 거부
203
204
종료

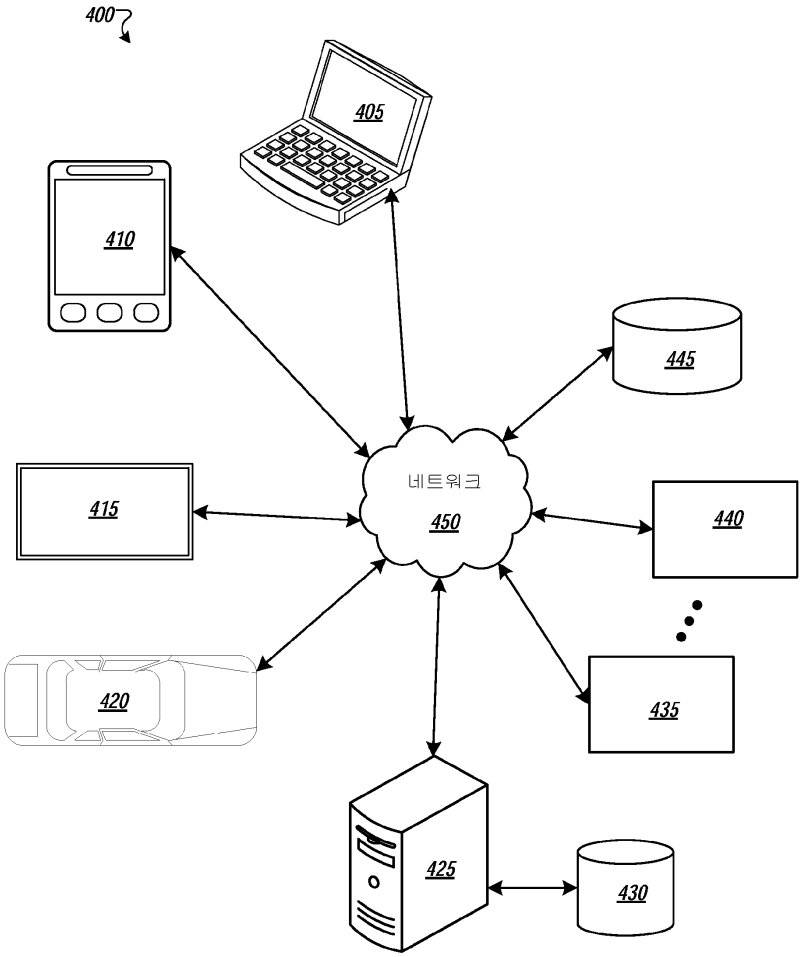
도면2b


시작
복수의 질문들 전송
205
인증 해시 수신
206
인증 해시가
저장된 표시자들 중
하나와 매칭하는가?
207
예
아니오
복구 프로세스 시작
액세스 거부
208
209
종료

도면3


300
컴퓨팅 디바이스
305
프로세서(들) 310
입력/사용자 인터페이스
335
출력 디바이스/ 인터페이스
340
외부 스토리지
345
네트워크
350
I/O 인터페이스
325
내부 스토리지
320
메모리
315
330
논리 유닛
360
API 유닛
365
입력 유닛
370
출력 유닛
375
인증
380
복구
385
난수 생성기
390
395

도면4


400
405
410
445
415
네트워크
450
440
420
435
425
430