(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년09월18일
(11) 등록번호 10-1554442
(24) 등록일자 2015년09월14일

(51) 국제특허분류(Int. Cl.)
G06F 21/30 (2013.01) *G06F 15/16* (2006.01)
(21) 출원번호 10-2014-7002570
(22) 출원일자(국제) 2012년06월29일
심사청구일자 2014년01월28일
(85) 번역문제출일자 2014년01월28일
(65) 공개번호 10-2014-0043137
(43) 공개일자 2014년04월08일
(86) 국제출원번호 PCT/US2012/045057
(87) 국제공개번호 WO 2013/003782
국제공개일자 2013년01월03일
(30) 우선권주장
13/174,558 2011년06월30일 미국(US)
(56) 선행기술조사문헌
US20030131266 A1

(73) 특허권자
퀄컴 인코포레이티드
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
리 칭
미국 92121 캘리포니아주 샌디에고 모어하우스 드라이브 5775
(74) 대리인
특허법인코리아나

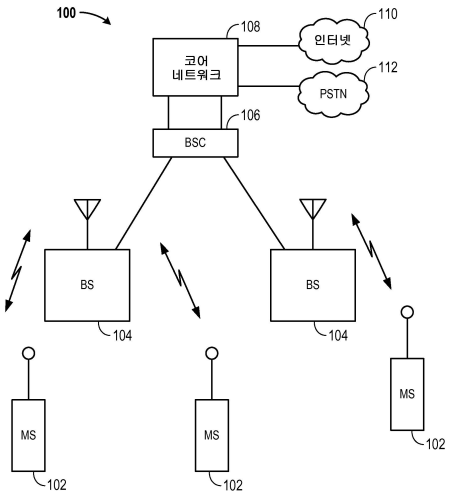
전체 청구항 수 : 총 28 항 심사관 : 문남두

(54) 발명의 명칭 **홈쳐 보기 방지 인증 방법**

(57) 요 약

개시된 것은: 사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 사용자 인터페이스; 난수를 발생시키는 난수 발생기; 및 제 1 패스워드와 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키고, 난수, 사용자이름, 및 연관된 서버 사이트의 저장을 지시하는 프로세서를 포함하는 클라이언트 디바이스이다. 사용자가 그들의 사용자이름 및 제 2 패스워드를 입력함으로써 서버 사이트에 로그온하려고 시도하는 경우, 프로세서는 사용자이름 및 서버 사이트와 연관된 난수를 추출하고, 제 2 패스워드 및 난수에 기초하여 함수를 구현하여 제 1 패스워드를 발생시키며, 제 1 패스워드는 사용자에 의해 입력된 제 2 패스워드를 대체하여 서버 사이트에 제출된다.

대 표 도 - 도1



명 세 서

청구범위

청구항 1

클라이언트 디바이스로서,

저장 디바이스;

사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 사용자 인터페이스;

난수를 발생시키는 난수 발생기; 및

프로세서로서,

상기 제 1 패스워드 및 상기 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키고;

상기 저장 디바이스에 상기 난수, 상기 사용자이름, 및 연관된 상기 서버 사이트의 저장을 지시하는, 상기 프로세서를 포함하고,

상기 제 1 패스워드 및 상기 제 2 패스워드는 상기 클라이언트 디바이스에 저장되지 않으며,

상기 사용자가 그들의 사용자이름 및 상기 제 2 패스워드를 입력함으로써 상기 서버 사이트에 로그인하려고 시도하는 경우, 상기 프로세서는 상기 저장 디바이스로부터 상기 사용자이름 및 상기 서버 사이트와 연관된 상기 난수를 추출하고, 상기 제 2 패스워드 및 상기 난수에 기초하여 상기 함수의 역을 구현하여 상기 사용자에 의해 입력된 상기 제 2 패스워드를 대체하여 상기 서버 사이트에 제출되는 상기 제 1 패스워드를 발생시키도록 더 구성되는, 클라이언트 디바이스.

청구항 2

제 1 항에 있어서,

상기 함수는 일 대 일 맵핑 함수인, 클라이언트 디바이스.

청구항 3

제 1 항에 있어서,

상기 함수는 블록 암호 알고리즘인, 클라이언트 디바이스.

청구항 4

제 3 항에 있어서,

상기 블록 암호 알고리즘은 고급 암호화 표준 (advanced encryption standard; AES) 대칭 키 암호화 동작이고, 상기 제 2 패스워드는 키로서의 상기 난수 및 상기 제 1 패스워드를 이용하여 상기 대칭 키 암호화 동작으로부터 출력되는, 클라이언트 디바이스.

청구항 5

제 4 항에 있어서,

상기 키로서의 상기 난수 및 상기 제 2 패스워드로 대칭 키 복호화 동작을 이용하는 것은 출력으로서 상기 제 1 패스워드를 초래하는, 클라이언트 디바이스.

청구항 6

제 1 항에 있어서,

상기 사용자는 정규 모드 또는 보호 모드 중 하나의 모드를 선택하고, 상기 정규 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 1 패스워드가 상기 사용자에 의해 입력되며, 한편, 상기 보호

모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 2 패스워드가 상기 사용자에 의해 입력되는, 클라이언트 디바이스.

청구항 7

제 1 항에 있어서,

상기 사용자에 의해 방문되는 상기 서버 사이트는 인터넷을 통한 웹 사이트인, 클라이언트 디바이스.

청구항 8

클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법으로서,

사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 단계;

상기 클라이언트 디바이스의 난수 발생기를 이용하여 난수를 발생시키는 단계;

상기 클라이언트 디바이스의 프로세서를 이용하여 상기 제 1 패스워드 및 상기 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키는 단계; 및

상기 난수, 상기 사용자이름, 및 연관된 상기 서버 사이트의 저장을 지시하는 단계로서, 상기 제 1 패스워드 및 상기 제 2 패스워드는 상기 클라이언트 디바이스에 저장되지 않는, 상기 저장을 지시하는 단계를 포함하고,

상기 사용자가 그들의 사용자이름 및 상기 제 2 패스워드를 입력함으로써 상기 서버 사이트에 로그인하려고 시도하는 경우, 상기 사용자이름 및 상기 서버 사이트와 연관된 상기 난수가 저장부로부터 추출되고, 상기 제 2 패스워드 및 상기 난수에 기초하여 상기 함수의 역이 구현되어 상기 사용자에 의해 입력된 상기 제 2 패스워드를 대체하여 상기 서버 사이트에 제출되는 상기 제 1 패스워드를 발생시키는, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 9

제 8 항에 있어서,

상기 함수는 일 대 일 맵핑 함수인, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 10

제 8 항에 있어서,

상기 함수는 블록 암호 알고리즘인, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 11

제 10 항에 있어서,

상기 블록 암호 알고리즘은 고급 암호화 표준 (AES) 대칭 키 암호화 동작이고, 상기 제 2 패스워드는 키로서의 상기 난수 및 상기 제 1 패스워드를 이용하여 상기 대칭 키 암호화 동작으로부터 출력되는, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 12

제 11 항에 있어서,

상기 키로서의 상기 난수 및 상기 제 2 패스워드로 대칭 키 복호화 동작을 이용하는 것은 출력으로서 상기 제 1 패스워드를 초래하는, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 13

제 8 항에 있어서,

상기 사용자는 정규 모드 또는 보호 모드 중 하나의 모드를 선택하고, 상기 정규 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 1 패스워드가 상기 사용자에 의해 입력되며, 한편, 상기 보호 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 2 패스워드가 상기 사용자에 의

해 입력되는, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 14

제 8 항에 있어서,

상기 사용자에 의해 방문되는 상기 서버 사이트는 인터넷을 통한 웹 사이트인, 클라이언트 디바이스에 대한 제 2 패스워드를 생성하는 방법.

청구항 15

클라이언트 디바이스로서,

사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 수단;

난수를 발생시키는 수단;

상기 제 1 패스워드 및 상기 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키는 수단; 및

상기 난수, 상기 사용자이름, 및 연관된 상기 서버 사이트의 저장을 지시하는 수단으로서, 상기 제 1 패스워드 및 상기 제 2 패스워드는 상기 클라이언트 디바이스에 저장되지 않는, 상기 저장을 지시하는 수단을 포함하고,

상기 사용자가 그들의 사용자이름 및 상기 제 2 패스워드를 입력함으로써 상기 서버 사이트에 로그인하려고 시도하는 경우, 상기 사용자이름 및 상기 서버 사이트와 연관된 상기 난수가 저장부로부터 추출되고, 상기 제 2 패스워드 및 상기 난수에 기초하여 상기 함수의 역이 구현되어 상기 사용자에 의해 입력된 상기 제 2 패스워드를 대체하여 상기 서버 사이트에 제출되는 상기 제 1 패스워드를 발생시키는, 클라이언트 디바이스.

청구항 16

제 15 항에 있어서,

상기 함수는 일 대 일 맵핑 함수인, 클라이언트 디바이스.

청구항 17

제 15 항에 있어서,

상기 함수는 블록 암호 알고리즘인, 클라이언트 디바이스.

청구항 18

제 17 항에 있어서,

상기 블록 암호 알고리즘은 고급 암호화 표준 (AES) 대칭 키 암호화 동작이고, 상기 제 2 패스워드는 키로서의 상기 난수 및 상기 제 1 패스워드를 이용하여 상기 대칭 키 암호화 동작으로부터 출력되는, 클라이언트 디바이스.

청구항 19

제 18 항에 있어서,

상기 키로서의 상기 난수 및 상기 제 2 패스워드로 대칭 키 복호화 동작을 이용하는 것은 출력으로서 상기 제 1 패스워드를 초래하는, 클라이언트 디바이스.

청구항 20

제 15 항에 있어서,

상기 사용자는 정규 모드 또는 보호 모드 중 하나의 모드를 선택하고, 상기 정규 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 1 패스워드가 상기 사용자에 의해 입력되며, 한편, 상기 보호 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 2 패스워드가 상기 사용자에 의해 입력되는, 클라이언트 디바이스.

청구항 21

제 15 항에 있어서,

상기 사용자에 의해 방문되는 상기 서버 사이트는 인터넷을 통한 웹 사이트인, 클라이언트 디바이스.

청구항 22

클라이언트 디바이스에 대한 제 2 패스워드를 생성하기 위한 프로그램이 기록된 컴퓨터 판독가능 매체로서,

사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하기 위한 코드;

난수를 발생시키기 위한 코드;

상기 제 1 패스워드 및 상기 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키기 위한 코드; 및

상기 난수, 상기 사용자이름, 및 연관된 상기 서버 사이트의 저장을 지시하기 위한 코드로서, 상기 제 1 패스워드 및 상기 제 2 패스워드는 상기 클라이언트 디바이스에 저장되지 않는, 상기 저장을 지시하기 위한 코드를 포함하고,

상기 사용자가 그들의 사용자이름 및 상기 제 2 패스워드를 입력함으로써 상기 서버 사이트에 로그인하려고 시도하는 경우, 상기 사용자이름 및 상기 서버 사이트와 연관된 상기 난수가 저장부로부터 추출되고, 상기 제 2 패스워드 및 상기 난수에 기초하여 상기 함수의 역이 구현되어 상기 사용자에 의해 입력된 상기 제 2 패스워드를 대체하여 상기 서버 사이트에 제출되는 상기 제 1 패스워드를 발생시키는, 컴퓨터 판독가능 매체.

청구항 23

제 22 항에 있어서,

상기 함수는 일 대 일 맵핑 함수인, 컴퓨터 판독가능 매체.

청구항 24

제 22 항에 있어서,

상기 함수는 블록 암호 알고리즘인, 컴퓨터 판독가능 매체.

청구항 25

제 24 항에 있어서,

상기 블록 암호 알고리즘은 고급 암호화 표준 (AES) 대칭 키 암호화 동작이고, 상기 제 2 패스워드는 키로서의 상기 난수 및 상기 제 1 패스워드를 이용하여 상기 대칭 키 암호화 동작으로부터 출력되는, 컴퓨터 판독가능 매체.

청구항 26

제 25 항에 있어서,

상기 키로서의 상기 난수 및 상기 제 2 패스워드로 대칭 키 복호화 동작을 이용하는 것은 출력으로서 상기 제 1 패스워드를 초래하는, 컴퓨터 판독가능 매체.

청구항 27

제 22 항에 있어서,

상기 사용자는 정규 모드 또는 보호 모드 중 하나의 모드를 선택하고, 상기 정규 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 1 패스워드가 상기 사용자에 의해 입력되며, 한편, 상기 보호 모드에서는, 상기 사용자에 의해 방문되는 상기 서버 사이트와 연관된 상기 제 2 패스워드가 상기 사용자에 의해 입력되는, 컴퓨터 판독가능 매체.

청구항 28

제 22 항에 있어서,

상기 사용자에 의해 방문되는 상기 서버 사이트는 인터넷을 통한 웹 사이트인, 컴퓨터 판독가능 매체.

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 훔쳐 보기 방지 인증 방법에 관한 것이다.

배 경 기 술

[0002] 오늘날, (액세스 단말기들, 원격국들, 컴퓨팅 디바이스들 등이라고도 알려진) 클라이언트 디바이스들의 이용은 널리 퍼져있다. 이러한 클라이언트 디바이스들은 고정식 (예를 들어, 데스크톱 컴퓨터) 또는 이동식 중 어느 일방일 수 있다. 이러한 모바일 디바이스들은 사용자에게 무선 폰 액세스, 인터넷 액세스, 컴퓨터 시스템들 (개인, 기업, 정부 등) 에 대한 액세스를 제공할 수도 있으며, 사용자가 온라인 쇼핑, 온라인 뱅킹과 같은 온라인 트랜잭션들, 뿐만 아니라 특정 위치들에 대한 지도 찾기와 같은 다른 애플리케이션들 등을 수행하는 것을 허용한다. 따라서, 오늘날의 모바일 디바이스들은 무선 통신 뿐만 아니라 비이동식 컴퓨터 시스템 또는 고정식 컴퓨터 시스템과 연관된 거의 모든 통신과 인터넷 피쳐들을 허용한다. 이러한 모바일 디바이스들의 예들은: (노트북이라고도 알려진) 랩탑 컴퓨터들, 스마트 폰들, 셀룰러 폰들, 개인 휴대 정보 단말기 (personal digital assistant; PDA) 들, 디지털 카메라들, 태블릿 컴퓨터들 등을 포함한다.

[0003] 사용자가 서버 사이트에 접속하는 경우 개인 정보 및 자산 정보를 보호하는데 패스워드들이 널리 이용된다. 이러한 보호 방법은 사용자에 의한 패스워드 세트를 이용한 서버 사이트로의 접속 및 개인 정보에 대한 액세스를 허용한다. 불행히도, 패스워드가 노출되는 경우, 공격자들이 패스워드를 획득하여 가능하게는 사용자의 개인 정보 및 자산 정보에 액세스할 수도 있다. 패스워드 보호를 이용하는 이러한 서버 사이트들의 예들은 은행들, 상점들, 직장, 학교, 데이터 센터들 등과 관련된 서버 사이트들을 포함한다.

[0004] 특히, 모바일 디바이스들의 증가로 인해, 종종 모바일 디바이스들은 훔쳐 보기 공격이 발생할 수도 있는 붐비는 위치들에서 개인 트랜잭션들을 수행하는 서버 사이트들에 액세스한다. 훔쳐 보기는, 예를 들어, 누군가의 어깨 너머로 직접적으로 봄으로써 (또는 다른 수단에 의해) 모바일 디바이스에 입력되는 사용자 정보의 직접적인 관찰을 통해 공격자가 민감한 정보를 획득하는 보안 공격이다. 패스워드 기반 인증은 가장 널리 전개된 인증 기법들 중 하나의 기법이다. 훔쳐 보기 공격들은 패스워드 기반 인증에 대해 심각한 위협을 제기한다.

[0005] 이의 예가 사용자가 사용자들의 모바일 디바이스로 공공 위치 (예를 들어, 회의실, 커피 숍, 도서관, 몰 등) 에서 서버 사이트 (예를 들어, 은행, 상점, 직장, 학교, 데이터 센터 등) 에 있는 사용자들의 사적 계정에 로그인

하는 경우이다. 모바일 디바이스의 화면, 키보드, 또는 사용자의 손 움직임들이 완전히 노출되어 공격자에게 보여진다. 공격자의 직접적인 관찰들에 기초하여, 공격자는 관찰된 사용자이름 및 패스워드로 서버 사이트에 있는 동일한 계정에 추후에 성공적으로 로그인할 수 있다. 많은 온라인 애플리케이션들 및 서비스들은 클라이언트-서버 모델에서 패스워드 기반 인증을 사용한다. 사용자는 서버 측에서의 구현에 대해 임의의 제어를 갖지 않는다. 따라서, 공격자에 의한, 사용자이름, 패스워드, 및 사용자들의 클라이언트 디바이스로 사용자에 의해 방문되는 서버 사이트의 잠재적인 직접적인 관찰들에 기초한 훔쳐 보기 공격들을 방지하기 위한 기법들이 요구되고 있다.

발명의 내용

과제의 해결 수단

[0006] 본 발명의 양상들은 제 2 패스워드를 생성하는 클라이언트 디바이스에 대한 장치, 시스템, 및 방법에 관한 것일 수도 있다. 클라이언트 디바이스는: 저장 디바이스; 사용자에 의해 방문되는 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 사용자 인터페이스; 난수를 발생시키는 난수 발생기; 및 제 1 패스워드와 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키고, 저장 디바이스에 난수, 사용자이름, 및 연관된 서버 사이트의 저장을 지시하는 프로세서를 포함할 수도 있다. 사용자가 그들의 사용자이름 및 제 2 패스워드를 입력함으로써 서버 사이트에 로그온하려고 시도하는 경우, 프로세서는 저장 디바이스로부터 사용자이름 및 서버 사이트와 연관된 난수를 추출하고, 제 2 패스워드 및 난수에 기초해 함수를 구현하여 사용자에 의해 입력된 제 2 패스워드를 대체하여 서버 사이트에 제출되는 제 1 패스워드를 발생시킨다.

도면의 간단한 설명

[0007] 도 1 은 무선 통신 시스템의 예의 블록 다이어그램이다.

도 2 는 본 발명의 양상들이 실시될 수도 있는 시스템의 블록 다이어그램이다.

도 3 은 사용자에게 제 2 패스워드를 제공하는 프로세스를 도시하는 플로 다이어그램이다.

도 4 는 클라이언트 디바이스로 제 2 패스워드를 이용하는 예의 블록 다이어그램이다.

도 5 는 제 2 패스워드를 이용하여 서버 사이트에 액세스하는 프로세스를 도시하는 플로 다이어그램이다.

발명을 실시하기 위한 구체적인 내용

[0008] 단어 "예시적인" 은 본원에서 "예, 사례, 또는 실례의 역할을 하는" 것을 의미하기 위해 이용된다. "예시" 또는 "예" 로 본원에서 설명된 임의의 실시예는 반드시 다른 실시예들보다 바람직하거나 유리한 것으로 해석되지는 않는다.

[0009] 도 1 을 참조하면, 무선 이동국 (mobile station; MS) (102) 은 무선 통신 시스템 (100) 의 하나 이상의 기지국 (base station; BS) (104) 과 통신할 수도 있다. 무선 통신 시스템 (100) 은 하나 이상의 기지국 제어기 (base station controller; BSC) 들 (106), 및 코어 네트워크 (108) 를 더 포함할 수도 있다. 코어 네트워크는 적합한 백홀들을 통해 인터넷 (110) 및 공중 교환 전화망 (Public Switched Telephone Network; PSTN) (112) 에 접속될 수도 있다. 통상적인 무선 이동국은 핸드헬드 폰, 또는 랩탑 컴퓨터를 포함할 수도 있다. 무선 통신 시스템 (100) 은 코드 분할 다중 접속 (code division multiple access; CDMA), 시간 분할 다중 접속 (time division multiple access; TDMA), 주파수 분할 다중 접속 (frequency division multiple access; FDMA), 공간 분할 다중 접속 (space division multiple access; SDMA), 편광 분할 다중 접속 (polarization division multiple access; PDMA) 과 같은 다수의 다중 접속 기법들, 또는 공지된 다른 변조 기법들 중 임의의 하나를 사용할 수도 있다.

[0010] 무선 디바이스 (102) 는 임의의 적합한 무선 통신 기술에 기초하거나 그렇지 않으면 그를 지원하는 하나 이상의 무선 통신 링크들을 통해 통신할 수도 있다. 예를 들어, 일부 양상들에서, 무선 디바이스는 네트워크와 연관할 수도 있다. 일부 양상들에서, 네트워크는 인체 영역 네트워크 (body area network) 또는 개인 영역 네트워크 (예를 들어, 울트라 광대역 네트워크) 를 포함할 수도 있다. 일부 양상들에서, 네트워크는 근거리 네트워크 또는 광역 네트워크를 포함할 수도 있다. 무선 디바이스는, 예를 들어, CDMA, TDMA, OFDM, OFDMA, WiMAX, 및 Wi-Fi 와 같은 다양한 무선 통신 기술들, 프로토콜들, 또는 표준들 중 하나 이상을 지원하거나 그렇지 않으면 이용할 수도 있다. 유사하게, 무선 디바이스는 다양한 대응하는 변조 기법 또는 다중화 기법 중

하나 이상을 지원하거나 그렇지 않으면 이용할 수도 있다. 무선 디바이스는 따라서 위의 또는 다른 무선 통신 기술들을 이용하여 하나 이상의 무선 통신 링크들을 통해 확립하고 통신할 적절한 컴포넌트들 (예를 들어, 무선 인터페이스들) 을 포함할 수도 있다. 예를 들어, 디바이스는 무선 매체를 통한 통신을 가능하게 하는 다양한 컴포넌트들 (예를 들어, 신호 발생기들 및 신호 프로세서들) 을 포함할 수도 있는 연관된 송신기 컴포넌트 및 수신기 컴포넌트 (예를 들어, 송신기 및 수신기) 를 갖는 무선 송수신기를 포함할 수도 있다.

[0011] 본 발명의 양상들은 공격자에 의해, 공공 영역에서 서버 사이트에 액세스하기 위해 모바일 클라이언트 디바이스 (102) 를 이용하는 사용자이름, 패스워드, 및 사용자에 의해 방문되는 서버 사이트의 직접적인 관찰들에 기초한, 훔쳐 보기 공격들 또는 다른 유형의 공격들을 방지하는 것과 관련된다. 이후 설명되는 수정예들은 오직 모바일 클라이언트 디바이스 (102) 에서의 수정들에 관한 것이고, 서버 사이트의 수정들은 요구하지 않는다는 것이 유의되어야 한다. 또한, 예들로서, 모바일 클라이언트 디바이스 (102) 는: 랩탑 컴퓨터들, 스마트 폰들, 셀룰러 폰들, 개인 휴대 정보 단말기 (PDA) 들, 디지털 카메라들, 모바일 컴퓨터들 등일 수도 있고, 통상적으로 무선 디바이스라고 지칭될 수도 있다. 그러나, 본 발명의 양상들은 유선 디바이스들과도 관련된다. 이후에, 용어 클라이언트 디바이스 (102) 는 무선 또는 유선 디바이스, 고정식 또는 이동식 중 어느 일방일 수도 있는 것으로 이용될 것이다.

[0012] 특히, 본 발명의 양상들은 사용자에 대한 제 2 패스워드를 생성하는 장치, 방법, 및 시스템과 관련된다. 예를 들어, 클라이언트 디바이스 (102) 는: 저장 디바이스; 사용자에 의해 방문되는 특정 서버 사이트와 연관된 사용자이름 및 제 1 패스워드를 수신하는 사용자 인터페이스; 난수를 발생시키는 난수 발생기; 및 프로세서를 포함할 수도 있다. 프로세서는: 제 1 패스워드 및 난수에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시키고; 저장 디바이스에 난수, 사용자이름, 및 연관된 서버 사이트의 저장을 지시하는데 이용될 수도 있다. 제 2 패스워드를 발생시킨 후에, 사용자가 그들의 사용자이름 및 제 2 패스워드를 입력함으로써 특정 서버 사이트에 로그온하려고 시도하는 경우, 프로세서는 저장 디바이스로부터 사용자이름 및 서버 사이트와 연관된 난수를 추출할 수도 있다. 프로세서는 그 다음에 제 2 패스워드 및 난수에 기초하여 함수를 구현해 제 1 패스워드를 발생시킬 수도 있으며, 제 1 패스워드는 사용자에 의해 입력된 제 2 패스워드를 대체하여 특정 서버 사이트에 제출되어 사용자가 서버 사이트에 액세스할 수 있다. 따라서, 클라이언트 디바이스 (102) 는 훔쳐 보기 방지 인증 매커니즘으로서의 역할을 한다.

[0013] 도 2 를 참조하면, 도 2 는 본 발명의 양상들이 실시될 수도 있는 시스템 (101) 의 블록 다이어그램이다. 특히, 시스템 (101) 은 사용자에 대한 제 2 패스워드를 생성할 수 있는 클라이언트 디바이스 (102) 를 포함한다. 클라이언트 디바이스 (102) 는 디스플레이 디바이스 (142), 사용자 인터페이스 (140), 난수 발생기 (132), 및 프로세서 (130) 를 포함할 수도 있다. 디스플레이 디바이스 (142) 는 모바일 디바이스, 셀폰, 개인 휴대 정보 단말기, 랩탑 컴퓨터 등과 같은 클라이언트 디바이스 (102) 상의 통상적인 디스플레이 디바이스일 수도 있다. 사용자 인터페이스 (140) 는 통상적으로 클라이언트 디바이스 (102) 와 이용되는 키패드, 키보드, 또는 다른 유형의 사용자 입력 디바이스일 수도 있다.

[0014] 일 양상에서, 클라이언트 디바이스 (102) 는, 이후에서 논의될 것으로, 제 2 패스워드를 생성하여 이용하는 명령들을 실행하도록 구성된 프로세서 (130) 및 메모리 (131) 를 포함할 수도 있다. 메모리 (131) 는 프로세서 (130) 에 의한 구현을 위한 명령들을 저장하기 위해 프로세서 (130) 에 커플링될 수도 있다. 따라서, 클라이언트 디바이스 (102) 는 제 2 패스워드의 생성 및 제 2 패스워드의 이용을 구현하는 명령들을 실행하도록 구성된다.

[0015] 사용자 인터페이스 (140) 는 사용자에 의해 액세스될 특정 서버 사이트 (103) (예를 들어, 웹사이트) 와 연관된 사용자 이름 (150), 서버 사이트 식별자 (152), 및 제 1 패스워드 (153) 를 수신할 수도 있다. 난수 발생기 (132) 는 사용자이름 (150) 및 서버 사이트 지정자 (152) 와 연관될 난수 (160) 를 발생시킬 수도 있다.

[0016] 프로세서 (130) 는 제 1 패스워드 (153) 및 난수 (160) 에 기초하여 함수를 구현함으로써 제 2 패스워드를 발생시킬 수도 있다. 프로세서 (130) 는 테이블 (162) 의 일부로서 저장 디바이스 (134) 에 사용자이름 (150), 난수 (160), 및 연관된 지정 서버 사이트 (152) 의 저장을 지시할 수도 있다. 도 2 에 도시된 바와 같이, 테이블 (162) 은 다른 정보와 함께 복수의 사용자이름들 (150), 서버 사이트들 (152), 및 연관된 난수들 (160) 을 포함할 수도 있다.

[0017] 발생된 제 2 패스워드 (154) 는 디스플레이 디바이스 (142) 로 사용자에게 디스플레이될 수도 있어 사용자가 제 2 패스워드를 갖는다. 그러면, 공격자가 방문된 서버 사이트 (103) 및 사용자에 의해 입력된 패스워드를 관찰하려고 할 수도 있는 영역에서 사용자가 그들의 클라이언트 디바이스 (102) 를 이용하는 경우 제 2 패스워드

(154) 가 이용될 수 있다.

[0018] 일 양상에서, 제 1 패스워드 (153) 는 사용자의 정규 패스워드로 지칭될 수도 있고, 제 2 패스워드 (154) 는 사용자의 보호 패스워드로 지칭될 수도 있다. 또한, 난수 (160) 는 보안 난수일 수도 있다.

[0019] 이후 설명될 것으로, 사용자가 그들의 사용자이름 (150) 및 제 2 패스워드 (154) 를 입력함으로써 특정 서버 사이트 (103) 에 로그온하려고 시도하는 경우, 프로세서 (130) 는 저장 디바이스로부터 사용자이름 (150) 및 서버 사이트 (152) 와 연관된 난수 (160) 를 추출한다. 프로세서는 제 2 패스워드 (154) 및 난수 (160) 에 기초해 함수를 구현하여 제 1 패스워드 (153) 를 발생시키며, 제 1 패스워드는 사용자에 의해 입력된 제 2 패스워드를 대체하여 액세스를 위해 특정 서버 사이트 (103) 에 제출된다.

[0020] 제 1 패스워드 (153) 및 제 2 패스워드 (154) 중 어느 것도 모바일 클라이언트 디바이스 (102) 에 저장되지 않는다는 것이 유의되어야 한다. 또한, 사용자는 그들의 이용을 위한 제 2 패스워드 (154) 를 생성하기 위해 비밀유지를 위한 사적 환경에서 클라이언트 디바이스 (102) 를 가질 수도 있다는 것이 유의되어야 한다. 이러한 방식으로, 오직 사용자만이 제 1 패스워드 (153) 및 제 2 패스워드 (154) 를 알고 있으며, 제 1 패스워드 및 제 2 패스워드 중 어느 것도 클라이언트 디바이스 (102) 에 의해 저장되지 않고, 따라서 공격자에 의한 액세스가 불가능하다.

[0021] 일 양상에서, 사용자가 그들의 제 2 패스워드 (154) 를 생성하는 경우, 사용자는 서버 사이트 (103) 에 실제로 로그온할 필요가 없다. 이러한 구현에서, 사용자는 그들의 사용자이름 (150), 서버 사이트 지정자 (152), 및 제 1 패스워드 (153) 를 국부적으로 입력하고, 프로그램 (예를 들어, 소프트웨어, 펌웨어, 또는 미들웨어) 를 구현하는 프로세서가 앞서 설명된 바와 같이 디스플레이 디바이스 (142) 상에 사용자에게 디스플레이를 위해 제 2 패스워드 (154) 를 발생시킨다. 이러한 프로세스에서, 난수 (160), 서버 사이트 (152), 및 사용자이름 (150) 은 저장 디바이스 (134) 상에 저장된다. 따라서, 이러한 프로세스는 오프라인으로 수행될 수 있다.
그러나, 클라이언트 디바이스 (102) 가 서버 사이트 (103) 와 통신 상태에 있도록 링크 (170) 를 통해 유선 또는 무선으로 인터페이스 (136) 를 통해 온라인으로 또한 구현될 수도 있다. 인터페이스 (136) 는 무선 링크 (예를 들어, 도 1), 및/또는 서버 (103) 와 통신하도록 유선 링크 (예를 들어, 케이블 시스템, PSTN, 다른 링크들, 및 이들의 조합) 를 통한 통신을 위한 유선 인터페이스를 통해 서버 (103) 와 통신할 수도 있는 송신기 및 수신기를 포함하는 무선 인터페이스일 수도 있다.

[0022] 도 3 을 간단히 참조하면, 사용자에게 제 2 패스워드를 제공하는 프로세스 (300) 를 예시하는 플로 다이어그램이 도시된다. 블록 (302) 에서, 사용자가 제 2 패스워드 함수의 생성을 선택한다. 사용자는 그 다음에 사용자 인터페이스 (140) 를 통해 그들의 사용자이름 (150), 특정 서버 사이트 (152), 및 그들의 제 1 패스워드 (153) 를 입력한다 (블록 (304)). 난수 (160) 가 그 다음에 발생된다 (예를 들어, 보안 난수) (블록 (306)). 프로세서 (130) 는 제 1 패스워드 (153) 및 난수 (160) 에 기초하여 함수를 구현함으로써 제 2 패스워드 (154) 를 발생시킨다 (블록 (308)).

[0023] 예를 들어, 제 2 패스워드 (154) 는 제 1 패스워드 (153) 및 난수 (160) 의 함수일 수도 있다. 제 2 패스워드는 식: 제 2 패스워드 = f(제 1 패스워드, 난수) 에 의해 결정될 수도 있다. 다음으로, 프로세스 (300) 는 저장 디바이스 (134) 에 사용자이름 (150), 서버 사이트 (152), 및 난수 (160) 를 저장한다 (블록 (310)).
제 2 패스워드 (154) 는 그 다음에 디스플레이 디바이스 (142) 로 사용자에게 디스플레이된다 (블록 (312)).

[0024] 일 양상에서, 함수 (f) 는 블록 암호 알고리즘과 같은 일 대 일 맵핑 함수일 수도 있다. 일 특정 양상에서, 블록 암호 알고리즘은 고급 암호화 표준 (advance encryption standard; AES) 대칭 키 암호화 동작일 수도 있으며, 제 2 패스워드 (154) 는 키로서 난수 (160) 및 평문으로서 제 1 패스워드 (153) 를 이용하여 대칭 키 암호화 동작으로부터 출력된다. 또한, 추후 보다 상세히 설명될 것으로, 제 1 패스워드 (153) 를 결정하기 위해, 키로서 난수 (160) 및 제 2 패스워드 (154) 를 이용하는 대칭 키 복호화 동작 (f^{-1}) 이 출력으로서 제 1 패스워드를 초래한다.

[0025] 도 4 를 또한 참조하면, 클라이언트 디바이스 (102) 로 제 2 패스워드 (154) 를 이용하는 예가 도시된다. 도 4 에 도시된 바와 같이, 사용자는 클라이언트 디바이스 (102) 의 사용자 인터페이스 (140) 를 통해 그들의 사용자이름 (150), 서버 사이트 지정자 (152), 및 제 2 패스워드 (154) 를 입력함으로써 특정 서버 사이트 (103) 에 로그온하려고 시도할 수도 있다. 프로세서 (130) 는 저장 디바이스 (134) 로부터 사용자이름 (150) 및 서버 사이트 (152) 와 연관된 난수 (160) 를 추출하고, 제 2 패스워드 (154) 및 난수 (160) 에 기초해 함수를 구현하여 제 1 패스워드 (153) 를 발생시키며, 제 1 패스워드는 사용자에 의해 입력된 제 2 패스워드

를 대체하여 특정 서버 사이트 (103) 에 제출된다. 특히, 사용자이름 (150) 및 제 1 패스워드 (153) 를 이용하여 인터페이스 (136) 및 링크 (170) 를 통해 서버 사이트 (103) 로의 액세스가 발생한다. 사용자이름 (150) 및 제 1 패스워드 (153) 는 숨겨지거나 암호화된 포맷일 수도 있다. 또한, 앞서 설명된 바와 같이, 링크 (170) 는 무선 링크나 유선 링크, 또는 이들의 조합들일 수도 있다.

[0026] 동작에서, 사용자는 정규 모드 또는 보호 모드 중 하나의 모드를 선택할 수도 있다. 정규 모드에서, 사용자에 의해 방문될 특정 서버 사이트 (103) 에 대한 제 1 패스워드 (153) 및 서버 사이트 지정자 (152) 가 사용자 인터페이스 (140) 를 통해 사용자에 의해 입력되고 정규 동작이 발생한다. 반면, 보호 모드에서는, 사용자에 의해 방문될 특정 서버 사이트 (103) 와 연관된 서버 사이트 지정자 (152) 및 제 2 패스워드 (154) 가 클라이언트 디바이스 (102) 에 사용자 인터페이스 (140) 를 통해 사용자에 의해 입력된다. 다양한 양상들에서, 프로세서 (130) 는 미들웨어, 소프트웨어, 펌웨어, 또는 이들의 조합들과 연계하여 동작할 수도 있다. 또한, 예들로서, 사용자에 의해 방문되는 서버 사이트들 (103) 은 은행들, 상점들, 기업, 학교, 데이터 센터들 등과 같이 인터넷을 통한, 또는 인증을 위해 패스워드를 필요로 하는 임의의 유형의 네트워크를 통한 (예를 들어, 공공 네트워크, 사설 네트워크, 기업 네트워크, 정부 네트워크 등을 통한) 서버 사이트들 또는 웹사이트들일 수도 있다. 또한, 이러한 서버 사이트들로의 액세스는 무선 링크 및/또는 유선 링, 그리고 이들의 조합들로 발생할 수도 있다.

[0027] 도 5 를 간략히 참조하면, 제 2 패스워드 (154) 를 이용하여 서버 사이트 (103) 에 액세스하는 프로세스 (500) 를 예시하는 플로 다이어그램이 도시된다. 결정 블록 (502) 에서, 사용자는 정규 모드 또는 보호 모드를 선택한다. 정규 모드가 선택되는 경우, 클라이언트 디바이스 (102) 는 정규 프로세싱을 진행한다 (블록 (504)). 그러나, 보호 모드가 사용자에 의해 선택되는 경우, 사용자는 그들의 사용자이름 (150), 서버 사이트 지정자 (152), 및 제 2 패스워드 (154) 를 입력함으로써 서버 사이트 (103) 에 로그온한다 (블록 (506)). 사용자이름 (150) 및 서버 사이트 지정자 (152) 와 연관된 난수 (160) (예를 들어, 보안 난수) 가 추출된다 (블록 (508)).

[0028] 다음으로, 제 2 패스워드에 기초하여 함수를 구현함으로서 제 1 패스워드 (153) 가 발생된다 (블록 (510)). 예를 들어, 제 1 패스워드는 식: 제 1 페스워드 = f^{-1}(제 2 패스워드, 난수) 에 의해 얻게될 수도 있다. 제 1 패스워드 (153) 는 제 2 패스워드 (154) 를 대체하여, 서버 사이트 (103) 에 링크 (170) 를 거쳐 인터페이스 (136) 를 통해 서버 사이트 (103) 에 제출된다 (블록 (512)). 예를 들어, 서버 사이트 (103) 로의 액세스가 암호화되고 숨겨진 형태인 제 1 패스워드를 이용해 발생할 수도 있다. 사용자가 그러면 서버 사이트 (103) 에 액세스할 수도 있다 (블록 (514)).

[0029] 함수: (f) 는 일 대 일 맵핑 함수일 수도 있다. 일 양상에서, 함수는 블록 암호 알고리즘일 수도 있다. 일 특정 양상에서, 블록 암호 알고리즘은 고급 암호화 표준 (AES) 대칭 키 암호화 동작이다. 상술된 바와 같이, 제 2 패스워드는 키로서 난수 및 평문으로서 제 1 패스워드를 이용하여 대칭 키 암호화 동작으로부터 출력될 수도 있다. 제 1 패스워드에 있어서, 키로서의 난수 및 제 2 패스워드로 대칭 키 복호화 동작 (f^{-1}) 을 이용하는 것은 출력으로서 제 1 패스워드를 초래한다. 매우 다양한 상이한 유형의 알고리즘들이 이용될 수도 있다는 것이 이해되어야 한다.

[0030] 일 특정 양상에서, 미들웨어 모듈이 클라이언트 디바이스 (102) 에 의해 이용될 수도 있으며, 여기서, 미들웨어 모듈의 기능은 사용자이름 필드 및 패스워드 필드를 포함하는 서버/웹 서식들을 검사하고 프로세싱하는 것이다. 미들웨어는 특정 서버 사이트들에 대한 보호된 액세스를 지원하도록 구성될 수도 있다. 미들웨어는 2 개의 모드들: 정규 모드 및 보호 모드로 동작할 수도 있다. 미들웨어는 제 2 패스워드 (154) 를 발생시키도록 보호 모드에 의한 이용을 위한 서버 사이트 지정자 (152) 에 의해 지정된 특정 서버 사이트 (103) 에 대해 사용자에 의해 입력된 제 1 패스워드 (153) 를 설정하기 위한 사용자 화면을 제공할 수도 있다. 중간 층은 먼저 난수 (160) 를 발생시키고, 그 다음에 사용자에 의해 입력된 제 1 패스워드 (153) 를 요청할 수도 있다. 대안으로, 클라이언트 디바이스 (102) 는 다른 유형의 하드웨어, 펌웨어, 또는 소프트웨어를 포함하여 난수 발생기 (132) 를 구현할 수도 있다. 미들웨어는 제 1 패스워드 (153) 및 난수 (160) 의 함수로 제 2 패스워드 (154) 를 산출할 수도 있다. 미들웨어는 그 다음에 저장 디바이스 (134) 에 난수 (160), 사용자이름 (150), 및 서버 사이트 지정자 (152) 의 저장을 지시할 수도 있다.

[0031] 다른 예로서, 동작에서, 보호 모드에서는, 사용자가 웹 서식에 제 2 패스워드 (154) 를 입력하고, 미들웨어가 웹 서식으로부터 제 2 패스워드를 추출하고, 저장된 난수 (160) 를 검색하여, 제 1 패스워드 (153) 를 산출한다. 미들웨어는 제 2 패스워드 (154) 를 제 1 패스워드 (153) 로 대체하여, 요청을 서버 사이트

(103) 에 제출한다. 반면 정규 모드에서는, 임의의 수정 없이 웹 서식이 서버로 송신된다. 미들웨어, 펌웨어, 소프트웨어, 또는 하드웨어의 임의의 조합이 본 발명의 양상들을 구현하는데 이용될 수도 있다는 것이 이해되어야 한다.

[0032] 본 발명의 양상들은 서버 사이트 (103) 에서의 임의의 수정을 요구하지 않는다. 또한, 제 1 패스워드 (153) 또는 제 2 패스워드 (154) 중 어느 것도 클라이언트 디바이스 (102) 에 저장되지 않는다. 이에 따라, 공격자가 사용자에 의해 입력되는 제 2 패스워드 (154) 및 사용자이름 (150) 을 관찰할지라도, 사용자는 동일한 난수 (160) 없이는 서버 사이트 (103) 에 여전히 로그온할 수 없다. 따라서, 모두 동시에, 동일한 난수를 획득하기 위해 클라이언트 디바이스 (102) 를 노출시키고, 제 2 패스워드를 획득하고, 동일한 프로그램일 설치함으로써, 공격자가 인증 프로세스를 우회하는 위험이 상대적으로 낮다. 또한, 유출이 발생했을 수도 있다고 사용자가 믿는 경우 사용자는 언제든지 새로운 난수 (160) 로 새로운 제 2 패스워드 (154) 를 재발생시킬 수 있다. 따라서, 본 발명의 양상들은: 1) 제 2 (예를 들어, 보호) 패스워드; 및 2) 난수를 갖는 디바이스에 기초하여 2 팩터 인증을 제공한다. 당업자들에게 알려진 바와 같이, 2 팩터 인증은 1 팩터 인증과는 대조적으로 인증의 2 개의 레벨들 또는 2 개의 인스턴스들을 요구하고, 따라서 2 팩터 인증은 제 2 보안 층을 추가한다.

[0033] 본원의 사상들은 다양한 장치들 (예를 들어, 디바이스들) 에 포함될 (예를 들어, 그 내에 구현되거나 그에 의해 수행될) 수도 있다. 예를 들어, 본원에 교시된 하나 이상의 양상들은 폰 (예를 들어, 셀룰러 폰), 퍼스널 데이터 어시스턴트 ("PDA"), 엔터테인먼트 디바이스 (예를 들어, 음악 디바이스 또는 비디오 디바이스), 헤드셋 (예를 들어, 헤드폰들, 이어폰 등), 마이크로폰, 의료 디바이스 (예를 들어, 생체인식 센서, 심장 박동 모니터, 만보기, EKG 디바이스 등), 사용자 I/O 디바이스 (예를 들어, 시계, 리모콘, 전등 스위치, 키보드, 마우스 등), 타이어 압력 모니터, 컴퓨터, POS (point-of-sale) 디바이스, 엔터테인먼트 디바이스, 보청기, 셋톱 박스, 또는 임의의 다른 적합한 디바이스에 포함될 수도 있다.

[0034] 이러한 디바이스들은 상이한 전력 및 데이터 요구들을 가질 수도 있다. 일부 양상들에서, 본원의 교시들은 (예를 들어, 임펄스 기반 시그널링 기법 및 저 듀티 사이클 모드들의 이용을 통해) 저 전력 애플리케이션들에서의 이용을 위해 적응될 수도 있고, (예를 들어, 고 대역폭 펄스들의 이용을 통해) 상대적으로 높은 데이터 레이트들을 포함하여 다양한 데이터 레이트들을 지원할 수도 있다.

[0035] 일부 양상들에서, 무선 디바이스는 통신 시스템에 대한 액세스 디바이스 (예를 들어, Wi-Fi 액세스 포인트) 를 포함할 수도 있다. 이러한 액세스 디바이스는, 예를 들어, 유선 또는 무선 통신 링크를 통한 다른 네트워크 (예를 들어, 인터넷 또는 셀룰러 네트워크와 같은 광역 네트워크) 와의 접속성을 제공할 수도 있다. 이에 따라, 액세스 디바이스는 다른 디바이스 (예를 들어, Wi-Fi 스테이션) 가 다른 네트워크 또는 일부 다른 기능성에 액세스하는 것을 가능하게 할 수도 있다. 또한, 디바이스들 중 하나 또는 양자 모두가 휴대가능할 수도 있거나, 일부 경우들에서는, 비교적 휴대불가능할 수도 있다는 것이 이해되어야 한다.

[0036] 정보 및 신호들이 임의의 다양한 상이한 기술들 및 기법들을 이용하여 표현될 수도 있다는 것을 당업자들은 이해할 것이다. 예를 들어, 위의 설명 전반에서 참조될 수도 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들, 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 혹은 자기 입자들, 광학 필드들 혹은 광학 입자들, 또는 이들의 임의의 조합에 의해 표현될 수도 있다.

[0037] 본원에서 개시된 실시예들과 연계하여 설명된 다양한 예증적인 논리 블록들, 모듈들, 회로들, 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어, 또는 양자 모두의 조합들로서 구현될 수도 있다는 것을 당업자들은 또한 알 수 있을 것이다. 하드웨어 및 소프트웨어의 이러한 상호교환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들, 및 단계들은 그들의 기능성의 관점에서 일반적으로 상술되었다. 이러한 기능성이 하드웨어 또는 소프트웨어로 구현되는지 여부는 특정 애플리케이션 및 전체 시스템에 부과되는 설계 제약들에 따라 달라진다. 당업자들은 각각의 특정 애플리케이션을 위해 다양한 방식들로 설명된 기능성을 구현할 수도 있으나, 이러한 구현 결정들이 본 발명의 범위로부터 벗어나게 하는 것으로 해석되어서는 안된다.

[0038] 본원에서 개시된 실시예들과 연계하여 설명된 다양한 예증적인 논리 블록들, 모듈들, 및 회로들은 범용 프로세서, 디지털 신호 프로세서 (digital signal processor; DSP), 주문형 반도체 (application specific integrated circuit; ASIC), 필드 프로그래머블 게이트 어레이 (field programmable gate array; FPGA) 혹은 다른 프로그래머블 로직 디바이스, 이산 게이트 혹은 트랜지스터 로직, 이산 하드웨어 컴포넌트들, 또는 본원에서 설명된 기능들을 수행하도록 디자인된 것들의 임의의 조합에 의해 구현되거나 수행될 수도 있다. 범용 프로세서는 마이크로프로세서일 수도 있지만, 대안으로, 프로세서는 임의의 종래의 프로세서, 컨트롤러, 마이크

로컨트롤러, 또는 상태 머신일 수도 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP 와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 연계한 하나 이상의 마이크로프로세서들, 또는 임의의 다른 이러한 구성으로 구현될 수도 있다.

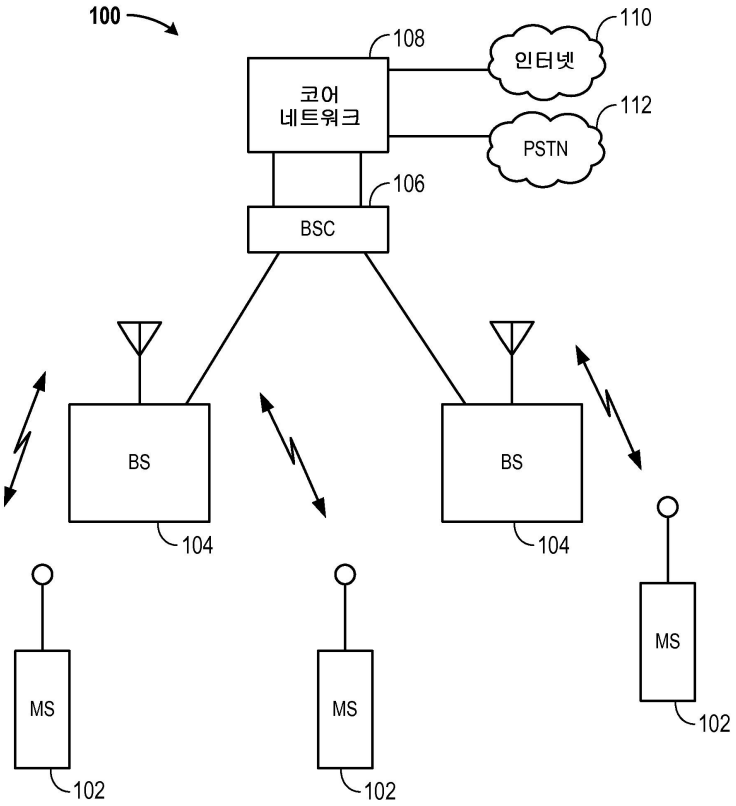
[0039] 본원에서 개시된 실시예들과 연계하여 설명된 방법 또는 알고리즘의 단계들은 하드웨어에서, 프로세서에 의해 실행되는 소프트웨어 모듈에서, 또는 이들 둘의 조합에서 직접적으로 구현될 수도 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 착탈식 디스크, CD-ROM, 또는 공지된 임의의 다른 형태의 저장 매체 내에 상주할 수도 있다. 예시적인 저장 매체는 프로세서가 저장 매체로부터 정보를 판독하고, 저장 매체에 정보를 기록할 수 있도록 프로세서에 커플링된다. 대안에서, 저장 매체는 프로세서에 통합될 수도 있다. 프로세서 및 저장 매체는 ASIC 내에 상주할 수도 있다. ASIC 는 사용자 단말기 내에 상주할 수도 있다. 대안에서, 프로세서 및 저장 매체는 사용자 단말기 내에 개별 컴포넌트들로 상주할 수도 있다.

[0040] 하나 이상의 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 미들웨어, 펌웨어 또는 이들의 임의의 조합으로 구현될 수도 있다. 컴퓨터 프로그램 제품으로서 소프트웨어로 구현되는 경우, 기능들은 하나 이상의 명령들 또는 코드로서 컴퓨터 판독 가능한 매체 상에 저장되거나 또는 그를 통해 송신될 수도 있다. 컴퓨터 판독가능 매체들은 한 장소에서 다른 장소로 컴퓨터 프로그램의 전송을 가능하게 하는 임의의 매체를 포함하여 컴퓨터 저장 매체들 및 통신 매체들 양자를 포함한다. 저장 매체들은 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체들일 수도 있다. 비제한적인 예로서, 이러한 컴퓨터 판독 가능 매체들은 RAM, ROM, EEPROM, CD-ROM 혹은 다른 광학 디스크 스토리지, 자기 디스크 스토리지 혹은 다른 자기 스토리지 디바이스들, 또는 요구되는 프로그램 코드를 명령들 또는 데이터 구조들의 형태로 이송 또는 저장하기 위해 이용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 접속체는 컴퓨터 판독가능 매체라고 적절히 칭해진다. 예를 들어, 소프트웨어가 동축 케이블, 광섬유 케이블, 연선, 디지털 가입자 회선 (digital subscriber line; DSL), 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들을 이용하여 웹 사이트, 서버, 또는 다른 원격 소스로부터 송신되는 경우, 동축 케이블, 광섬유 케이블, 연선, DSL, 또는 적외선, 무선, 및 마이크로파와 같은 무선 기술들은 매체의 정의 내에 포함된다. 본원에서 사용된 디스크 (disk) 와 디스크 (disc) 는, 컴팩트 디스크 (CD), 레이저 디스크, 광학 디스크, 디지털 다기능 디스크 (DVD), 플로피 디스크, 및 블루레이 디스크를 포함하며, 여기서 디스크 (disk) 들은 통상 자기적으로 데이터를 재생하는 반면, 디스크 (disc) 들은 레이저들을 이용하여 광학적으로 데이터를 재생한다. 위의 조합들도 컴퓨터 판독가능 매체들의 범위 내에 포함되어야 한다.

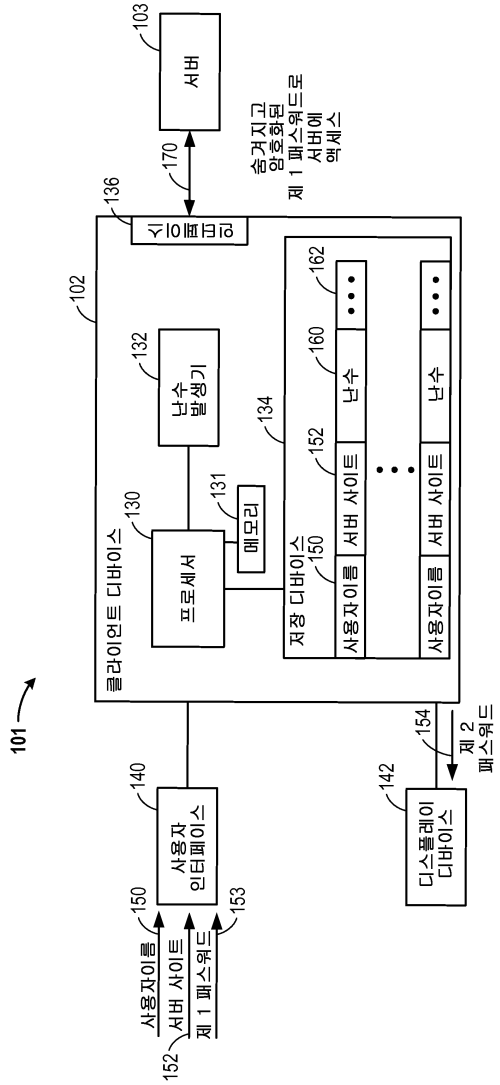
[0041] 개시된 실시예들의 앞서의 설명들은 임의의 당업자가 본 발명을 실시하거나 이용하는 것을 가능하게 하도록 하기 위해 제공된다. 이러한 실시예들에 대한 다양한 수정예들이 당업자들에게는 자명할 것이고, 본원에서 정의된 일반적인 원칙들은 본 발명의 취지와 범위를 벗어나지 않으면서 다른 실시예들에 적용될 수도 있다. 따라서, 본 발명은 본원에서 보여진 예시적인 실시예들로 제한되도록 의도된 것은 아니며 본원에 개시된 원칙들과 신규의 특징들과 일치하는 가장 넓은 범위에 따르고자 한다.

도면

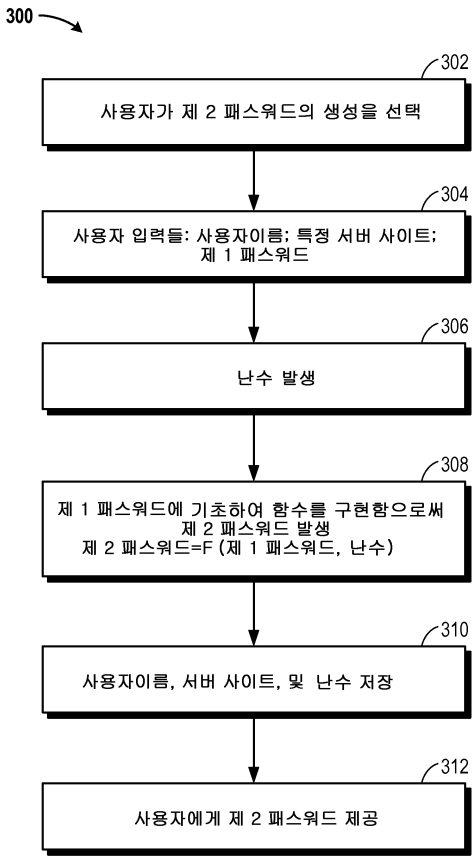
도면1


100
108
110
인터넷
코어
네트워크
112
PSTN
106
BSC
BS
104
BS
104
MS
102
MS
102
MS
102

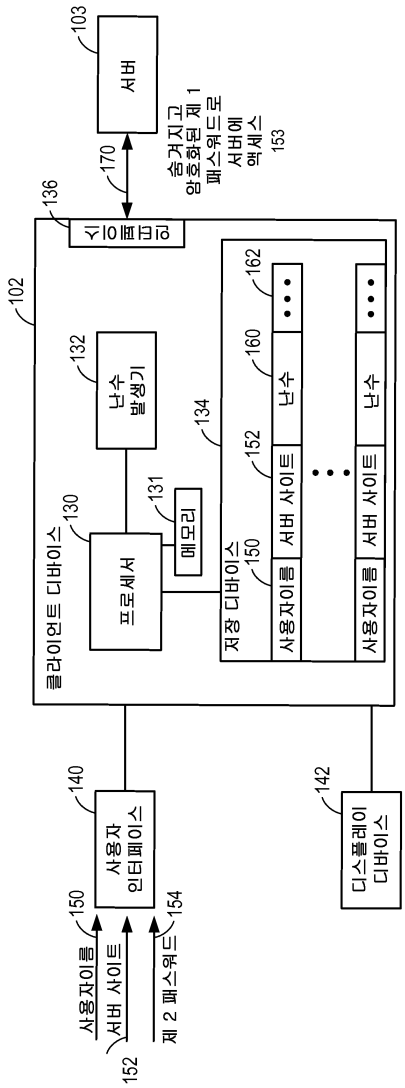
도면2


101
클라이언트 디바이스
102
서버
103
170
136
인터페이스
숨겨지고
암호화된
제 1 패스워드로
서버에
액세스
난수
발생기
132
134
프로세서
130
메모리
131
저장 디바이스
150
사용자이름
서버 사이트
152
162
160
난수
154
제 2
패스워드
142
디스플레이
디바이스
140
사용자
인터페이스
150
153
사용자이름
서버 사이트
152
제 1 패스워드

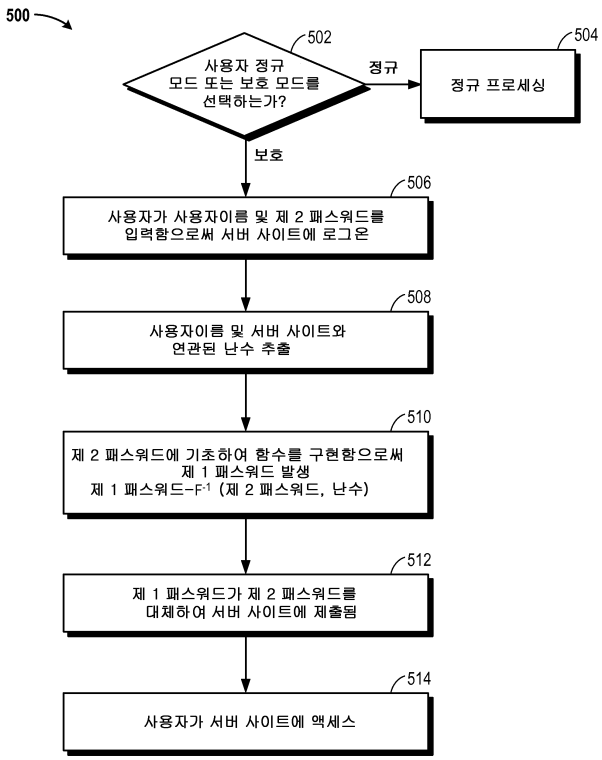
도면3


300
302
사용자가 제 2 패스워드의 생성을 선택
304
사용자 입력들: 사용자이름; 특정 서버 사이트;
제 1 패스워드
306
난수 발생
308
제 1 패스워드에 기초하여 함수를 구현함으로써
제 2 패스워드 발생
제 2 패스워드=F (제 1 패스워드, 난수)
310
사용자이름, 서버 사이트, 및 난수 저장
312
사용자에게 제 2 패스워드 제공

도면4


103
서버
170
숨겨지고 암호화된 제 1 패스워드로 서버에 액세스
153
136
인터페이스
102
클라이언트 디바이스
132
난수 발생기
134
131
메모리
130
프로세서
저장 디바이스
150
152
160
162
사용자이름
서버 사이트
난수
140
사용자 인터페이스
142
디스플레이 디바이스
150
사용자이름
152
서버 사이트
154
제 2 패스워드

도면5


500
502
사용자 정규 모드 또는 보호 모드를 선택하는가?
정규
504
정규 프로세싱
보호
506
사용자가 사용자이름 및 제 2 패스워드를 입력함으로써 서버 사이트에 로그온
508
사용자이름 및 서버 사이트와 연관된 난수 추출
510
제 2 패스워드에 기초하여 함수를 구현함으로써 제 1 패스워드 발생
제 1 패스워드=F-1 (제 2 패스워드, 난수)
512
제 1 패스워드가 제 2 패스워드를 대체하여 서버 사이트에 제출됨
514
사용자가 서버 사이트에 액세스