(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.
G06F 15/00 (2006.01)

(11) 공개번호 10-2007-0055794
(43) 공개일자 2007년05월31일

(21) 출원번호 10-2005-0114217
(22) 출원일자 2005년11월28일
심사청구일자 2005년11월28일

(71) 출원인 고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내

(72) 발명자 이동훈
경기 고양시 일산구 일산3동 후곡마을 동신아파트 808동 804호
구재형
서울 강남구 삼성동 진흥아파트 1동 904호

(74) 대리인 현종철

전체 청구항 수 : 총 22 항

(54) 패스워드 변환 인증을 수행하는 프로그램이 기록된 기록매체, 이를 이용한 패스워드 변환 인증 방법 및 그 시스템

(57) 요약

본 발명은 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 매체 및 이를 이용한 패스워드 인증 방법에 관한 것으로, 본 발명의 패스워드 변환 인증 방법은, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계, 비밀 난수 값(r)이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계, 및 서로 다른 웹 서버의 주소 정보를 갖는 동일한 패스워드가 입력되면 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 새로운 패스워드를 변환 생성하는 단계, 및 변환 생성된 새로운 패스워드를 인증 대상 웹서버에 등록하는 단계를 포함한다. 이에 따라, 서로 다른 주소를 갖는 웹 서버에 대해 동일한 패스워드가 설정된 경우 웹 서버의 주소에 따라 서로 다른 패스워드를 변환 생성하기 때문에 패스워드의 유출에 따라 발생할 수 있는 문제점을 해결 할 수 있다.

대표도

도 1

특허청구의 범위

청구항 1.

분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서,

소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계;

상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계; 및

어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드를 변환 생성하는 단계; 및

상기 변환 생성된 새로운 패스워드를 인증 대상 웹서버에 등록하는 단계를 포함하는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 2.

제 1항에 있어서,

상기 비밀 난수 값은 128비트로 암호화되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 3.

제 1항 또는 제 2항에 있어서,

상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는,

상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 4.

제 3항에 있어서,

상기 인자들에 의해 실행되는 상기 일대일 일방향 매핑 함수 값은, h(ID||PW||r||Svr_addr)로 표현되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 5.

제 4항에 있어서,

상기 생성 변환 단계에서는,

상기 일대일 일방향 매핑 함수의 실행 결과 값이 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보에 따라 서로 다른 패스워드로 변환 생성되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 6.

분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서,

소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계;

상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계;

동일한 패스워드를 갖는 서로 다른 인증 대상 웹 서버에 대한 정보가 입력되면, 상기 일대일 일방향 매핑 함수를 실행시켜 상기 인증 대상 웹 서버마다 서로 다른 패스워드를 변환 생성하는 단계; 및

상기 변환 생성된 새로운 패스워드를 상기 인증 대상 웹 서버에 등록하는 단계를 포함하는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 7.

제 6항에 있어서,

상기 비밀 난수 값은 128비트로 암호화되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 8.

제 6항에 있어서,

상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는,

상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성되는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 9.

분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서,

소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계;

상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계;

임의의 인증 대상 웹 서버에 등록하기 위한, 아이디(ID) 및 둘 이상의 상기 인증 대상 웹 서버에 동일하게 등록된 패스워드(PW), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보의 입력 여부를 판별하는 단계;

상기 정보가 입력되면, 상기 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보를 기초로, 상기 일대일 일방향 매핑 함수를 실행시켜 상기 인증 대상 웹 서버마다 서로 다른 패스워드를 변환 생성하는 단계; 및

상기 변환 생성된 새로운 패스워드를 상기 인증 대상 웹 서버에 등록하는 단계를 포함하는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 10.

제 9항에 있어서,

상기 변환 생성 단계 후, 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하는 단계를 더 포함하는 것을 특징으로 하는 패스워드 변환 인증 방법.

청구항 11.

분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 매체에 있어서,

소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하기 위한 제1영역; 및

상기 비밀 난수 값을 포함하는 소정 값이 입력되면 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정되는 제2영역을 포함하여 구성되며,

이에 의해, 상기 제2영역에서는, 어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드가 변환 생성되는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 12.

제 11항에 있어서,

상기 비밀 난수 값은 128비트로 암호화되는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 13.

제 11항 또는 제 12항에 있어서,

상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는,

상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성되는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 14.

제 13항에 있어서,

상기 인자들에 의해 실행되는 상기 일대일 일방향 매핑 함수 값은, h(ID||PW||r||Svr_addr)로 표현되는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 15.

제 14항에 있어서,

상기 제2영역에서는,

상기 일대일 일방향 매핑 함수의 실행 결과 값이 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보에 따라 서로 다른 패스워드로 변환 생성되는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 16.

제 15항에 있어서,

상기 제2영역에서 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라, 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하기 위한 제3영역을 더 포함하는 것을 특징으로 하는 패스워드 변환 인증 매체.

청구항 17.

분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 시스템에 있어서,

통신을 통해 접속 가능한 웹 주소를 가지며, 설정된 아이디 및 상기 아이디에 대하여 동일하게 설정된 패스워드의 등록을 통해 사용자의 인증 과정을 수행하는 서로 다른 둘 이상의 인증 대상 웹 서버;

상기 인증 대상 웹 서버에 인증을 위한 상기 인증 대상 웹 서버의 서로 다른 주소 정보를 포함하는 인증 정보에 대하여, 일대일 일방향 매핑 함수(h())를 실행하여 서로 다른 난수화된 패스워드를 변환 생성하는 패스워드 변환 인증 매체; 및

상기 패스워드 변환 인증 매체가 소정 인터페이스를 통해 접속되고 상기 인증 대상 웹 서버에 상기 통신을 통해 접근 가능하며, 사용자로부터 상기 인증 정보가 입력되면 상기 인증 정보를 상기 패스워드 변환 인증 매체에 제공하고, 상기 패스워드 변환 인증 매체에서 변환 생성된 상기 난수화된 패스워드를 상기 인증 대상 웹 서버에 등록하는 통신 기기를 포함하는 것을 특징으로 하는 패스워드 변환 인증 시스템.

청구항 18.

제 17항에 있어서,

상기 패스워드 변환 인증 매체는,

소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하기 위한 제1영역; 및

상기 비밀 난수 값을 포함하는 소정 값이 입력되면 상기 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정되는 제2영역을 포함하여 구성되며,

이에 의해, 상기 제2영역에서는, 어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드가 변환 생성되는 것을 특징으로 하는 패스워드 변환 인증 시스템.

청구항 19.

제 18항에 있어서,

상기 비밀 난수 값은 128비트로 암호화되는 것을 특징으로 하는 패스워드 변환 인증 시스템.

청구항 20.

제 19항에 있어서,

상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는,

상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성되는 것을 특징으로 하는 패스워드 변환 인증 시스템.

청구항 21.

제 19항에 있어서,

상기 인자들에 의해 실행되는 상기 일대일 일방향 매핑 함수 값은, h(ID||PW||r||Svr_addr)로 표현되는 것을 특징으로 하는 패스워드 변환 인증 시스템.

청구항 22.

제 21항에 있어서,

상기 패스워드 변환 인증 매체는,

상기 제2영역세서 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라, 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하기 위한 제3영역을 더 포함하는 것을 특징으로 하는 패스워드 변환 인증 시스템.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 웹 서비스를 위한 패스워드 관리 및 인증 방법에 관한 것으로서, 보다 상세하게는, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 매체 및 이를 이용한 인증 방법에 관한 것이다.

컴퓨터 및 네트워크 환경에서 사용자에 대한 인증 시스템으로는 스마트 카드나 ID(IDentifier, 이하 ID라고 약함)카드와 같이 사용자가 갖고 있는 것을 이용하는 것과, 홍체나 지문과 같이 사용자 그 자체를 인식하는 것, 및 패스워드나 개인 ID(일명 PID(Personal ID))와 같이 사용자가 알고 있는 정보를 이용하는 것으로 분류할 수 있다.

그러나, 스마트 카드를 이용한 인증 시스템은 스마트 카드 자체의 보안 및 가격적인 문제 때문에 쉽게 사용되지 않고 있으며, 홍체 인식이나 지문 인식 등을 이용한 인증 시스템 역시 일부에서 사용되고 있긴 하나 가격이 비싸기 때문에 널리 사용되는데 어려움이 있는 반면에, 패스워드 인증 시스템은 다른 인증 시스템에 비해 가격이 저렴하다는 이점으로 널리 사용되고 있다.

그러나, 패스워드는 사용자의 기억력을 기반으로 하고 있어 기억이 용이한 짧은 정보를 선택하는 경향이 있다. 이로 인하여 패스워드 인증 시스템은 다른 인증 시스템에 비해 해커(hacker)와 같은 공격자로부터 쉽게 공격당하는 단점이 있다. 따라서 패스워드 인증 시스템을 보다 안전하게 이용할 수 있는 방법들이 제안되고 있다.

그 중에 하나가 대한민국 특허 공개번호 2001-0027902(2001년 4월 6일)의 '사용자가 기억할 수 있는 패스워드를 이용한 안전한 사용자인증과 키 일치 방법'을 예로 들 수 있다.

상기 문헌에 따르면, 사용자가 외우기 쉬운 패스워드만을 사용하여, 사용자 인증과 암호키 일치에 대한 기법을 제공하고 있다. 이는 패스워드 자체가 안전하게 관리되어야 한다는 가정이 있어야 하는 단점이 있다. 즉, 상기 문헌은 안전하게 공유된 패스워드를 전제로, 인증 및 키 공유가 가능하다는 것을 개시하고 있다.

또 다른 예로, 대한민국 특허 공개번호 2001-0090167(2001년 10월 18일)의 '패스워드를 기반으로 한 상호 인증 및 키 교환 방법과 그 장치'가 있다. 여기서도 상기 대한민국 특허 공개번호 2001-0027902와 마찬가지로 안전하게 공유된 패스워드를 사용하여 인증 및 키 교환하는 방법만을 제시하고 있다.

또 다른 예로는, OTP (One Time Password) 토큰방식을 들 수 있다. 이는 사용자와 서버가 비밀 값과 카운터 값을 공유한 후, 사용자가 로그인 할 때마다 카운트 값을 증가시키는 것을 통해, 사용자가 로그인 할 때마다 서로 다른 패스워드를 사용할 수 있도록 하는 방식이다. 그러나 사용자 입장에서는 각 서버들마다 비밀 값을 공유해야 하며, 서버 자체에도 비밀 값과 카운터 값을 처리하는 모듈이 별도로 필요하기 때문에, 기존 시스템들을 그대로 사용할 수 없는 단점이 있다.

아래에는 패스워드 관리 및 인증과 관련하여 제안된 논문들을 나열한 것이다.

1. S.Bellovin 과 M.Merrit, "Encrypted key exchange : password based protocols secure against dictionary attacks", Symposium on Security and Privacy, pp.72-84, IEEE, 1992.

2. D.Jablon, "Strong password only authenticated key exchange", ACM Computer communication Review, Vol.26, No.5, 1996

3. T.wu, "Secure remote password protocol", Internet Society Symp. on Network and Distributed Sys. Security, 1998.

4. M.Bellare, D.Pointcheval 및 P.Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attack", LNCS Vol.1807, pp.139-155, 2000

위 기술된 논문들은 모두 패스워드를 기반으로 하여, 외부 공격에 대해 안전한 사용자와 서버 간의 인증 및 키 공유 기법을 제시한 것이다.

그런데, 종래에 제안된 패스워드 관리 및 인증 방법에서는, 사용자가 복수의 서버에 동일한 패스워드를 입력함으로서 발생할 수 있는 문제에 대해서는 전혀 고려하고 있지 않은 문제점이 있다. 즉, 복수의 서버에 동일한 패스워드를 설정함에 따라, 설정한 패스워드의 유출에 따른 해결 방안에 대해서 전혀 제시하고 있는 않고 있다.

이 경우, 일반적으로 복수의 서버들에 동일한 패스워드를 사용하고 있기 때문에, 어느 하나의 서버에 저장된 패스워드가 외부로 노출되는 경우, 사용자가 동일한 패스워드로 가입한 다른 서버들 또한 영향을 받게 되는 문제점이 있다.

예를 들어, 사용자 A가 인터넷 뱅킹 서버와 일반 컨텐츠 서버에 같은 아이디와 패스워드를 등록했을 경우, 상대적으로 보안 기능이 약한 컨텐츠 서버에 대한 해킹 등에 의해 노출된 패스워드로 인해 사용자 A는 인터넷 뱅킹 서버를 통한 치명적인 금융적인 피해를 입을 수 있는 가능성이 있다.

이러한 단점을 극복하기 위해 각 웹 서버 마다 서로 다른 패스워드를 설정하여 이용하는 경우, 사용자는 사용하는 모든 패스워드를 관리해야하는 번거로움이 따르게 된다.

발명이 이루고자 하는 기술적 과제

상기와 같은 문제점을 해결하기 위한 본 발명의 제1 목적은, 웹 서버에 접속하기 위한 패스워드를 보다 간편하게 관리할 수 있는 매체 및 이를 이용한 접속 인증 방법과 이것이 적용된 시스템을 제공하는 데 있다.

본 발명의 제2 목적은, 복수의 웹 서버에 접속하기 위한 패스워드를 보다 간편하고 안전하게 관리할 수 있는 매체 및 이를 이용한 접속 인증 방법을 제공하는 데 있다.

본 발명의 제 3목적은, 복수의 웹 서버에 접속하기 위한 패스워드가 동일한 경우 각 웹 서버마다 서로 다른 인증 패스워드가 생성되도록 설정할 수 있는 매체 및 이를 이용한 접속 인증 방법을 제공하는 데 있다.

본 발명의 제 4목적은, 해당 웹 서버에 설정한 패스워드가 유출된 경우 유출된 패스워드를 이용한 외부로부터의 웹 서버 인증을 차단할 수 있는 매체 및 이를 이용한 접속 인증 방법을 제공하는 데 있다.

발명의 구성

상기와 같은 목적은 본 발명의 실시예에 따라, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계; 상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계; 및 어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드를 변환 생성하는 단계; 및 상기 변환 생성된 새로운 패스워드를 인증 대상 웹서버에 등록하는 단계를 포함하는 패스워드 변환 인증 방법에 의해 달성된다.

바람직하게는, 상기 비밀 난수 값은 128비트로 암호화된다.

또한 상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는, 상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성된다.

상기 인자들에 의해 실행되는 상기 일대일 일방향 매핑 함수 값은, h(ID||PW||r||Svr_addr)로 표현될 수 있다.

상기 생성 변환 단계에서는, 상기 일대일 일방향 매핑 함수의 실행 결과 값이 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보에 따라 서로 다른 패스워드로 변환 생성된다.

한편, 상기와 같은 목적은 본 발명의 실시예에 따라, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계; 상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계; 동일한 패스워드를 갖는 서로 다른 인증 대상 웹 서버에 대한 정보가 입력되면, 상기 일대일 일방향 매핑 함수를 실행시켜 상기 인증 대상 웹 서버마다 서로 다른 패스워드를 변환 생성하는 단계; 및 상기 변환 생성된 새로운 패스워드를 상기 인증 대상 웹 서버에 등록하는 단계를 포함하는 패스워드 변환 인증 방법에 의해 달성된다.

또한 상기와 같은 목적은 본 발명의 실시예에 따라, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 방법에 있어서, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하는 단계; 상기 비밀 난수 값이 포함된 입력되는 소정 값에 대하여 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정하는 단계; 임의의 인증 대상 웹 서버에 등록하기 위한, 아이디(ID) 및 둘 이상의 상기 인증 대상 웹 서버에 동일하게 등록된 패스워드(PW), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보의 입력 여부를 판별하는 단계; 상기 정보가 입력되면, 상기 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보를 기초로, 상기 일대일 일방향 매핑 함수를 실행시켜 상기 인증 대상 웹 서버마다 서로 다른 패스워드를 변환 생성하는 단계; 및 상기 변환 생성된 새로운 패스워드를 상기 인증 대상 웹 서버에 등록하는 단계를 포함하는 패스워드 변환 인증 방법에 의해 달성된다.

바람직하게는, 본 실시예의 패스워드 변환 인증 방법은, 상기 변환 생성 단계 후, 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하는 단계를 더 포함할 수 있다.

한편, 상기와 같은 목적은 본 발명의 실시예에 따라, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 매체에 있어서, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하기 위한 제1영역; 및 상기 비밀 난수 값을 포함하는 소정 값이 입력되면 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정되는 제2영역을 포함하여 구성된다. 이에 의해, 상기 제2영역에서는, 어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드가 변환 생성된다.

상기 일대일 일방향 매핑 함수(h())의 실행을 위한 인자는, 상기 인증 대상 웹 서버에 등록된 아이디(ID) 및 패스워드(PW), 상기 비밀 난수 값(r), 및 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보로 구성된다. 상기 인자들에 의해 실행되는 상기 일대일 일방향 매핑 함수 값은, h(ID||PW||r||Svr_addr)로 표현된다.

상기 제2영역에서는, 상기 일대일 일방향 매핑 함수의 실행 결과 값이 상기 인증 대상 웹 서버의 주소(Svr_addr) 정보에 따라 서로 다른 패스워드로 변환 생성된다.

바람직하게는, 본 실시예의 패스워드 변환 인증 매체는, 상기 제2영역세서 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라, 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하기 위한 제3영역을 더 포함한다.

한편, 상기와 같은 목적은, 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 시스템에 있어서, 통신을 통해 접속 가능한 웹 주소를 가지며, 설정된 아이디 및 상기 아이디에 대하여 동일하게 설정된 패스워드의 등록을 통해 사용자의 인증 과정을 수행하는 서로 다른 둘 이상의 인증 대상 웹 서버; 상기 인증 대상 웹 서버에 인증을 위한 상기 인증 대상 웹 서버의 서로 다른 주소 정보를 포함하는 인증 정보에 대하여, 일대일 일방향 매핑 함수(h())를 실행하여 서로 다른 난수화된 패스워드를 변환 생성하는 패스워드 변환 인증 매체; 및 상기 패스워드 변환 인증 매체가 소정 인터페이스를 통해 접속되고 상기 인증 대상 웹 서버에 상기 통신을 통해 접근 가능하며, 사용자로부터 상기 인증 정보가 입력되면 상기 인증 정보를 상기 패스워드 변환 인증 매체에 제공하고, 상기 패스워드 변환 인증 매체에서 변환 생성된 상기 난수화된 패스워드를 상기 인증 대상 웹 서버에 등록하는 통신 기기를 포함하는 패스워드 변환 인증 시스템에 의해 달성된다.

상기 패스워드 변환 인증 매체는, 소정 방식에 따라 암호화되는 임의의 비밀 난수 값(r)을 설정하기 위한 제1영역; 및 상기 비밀 난수 값을 포함하는 소정 값이 입력되면 상기 일대일 일방향 매핑 함수(h())가 실행 가능하도록 설정되는 제2영역; 및 상기 제2영역세서 동일한 패스워드에 대하여 서로 다른 상기 인증 대상 웹 서버 주소 정보가 입력됨에 따라, 상기 일대일 일방향 매핑 함수에 의해 변환 생성된 서로 다른 패스워드를 임시 저장하기 위한 제3영역을 포함하는 패스워드 변환 인증 매체에 의해 달성된다.

이에 의해, 상기 제2영역에서는, 어느 하나의 동일한 패스워드가 입력되면, 상기 동일한 패스워드가 입력될 때마다 상기 일대일 일방향 매핑 함수의 실행을 통해 난수화된 서로 다른 패스워드가 변환 생성된다.

본 발명에 따르면, 128비트로 암호화되는 임의의 비밀 난수 값(r) 및 입력되는 값이 대하여 일대일 일방향 매칭 함수(h())를 수행하도록 설정된 패스워드 변환 인증 매체를 구성하여 입력되는 인증 대상 웹 서버의 주소값에 따라 서로 다른 새로운 패스워드를 변환 생성함으로써, 서로 다른 주소를 갖는 웹 서버에 대해 동일한 패스워드가 설정된 경우 웹 서버의 주소에 따라 서로 다른 패스워드를 변환 생성하기 때문에 패스워드의 유출에 따라 발생할 수 있는 문제점을 해결 할 수 있다. 또한, 동일한 패스워드라 하더라도 입력되는 웹 서버의 주소 정보가 다른 경우 입력되는 패스워드를 서로 다른 새로운 패스워드로 변환 생성하여 웹 서버에 등록함으로써, 패스워드 보안을 위해 패스워드를 웹 서버마다 다르게 설정할 필요가 없으며 웹상에서 패스워드 인증기법의 안전성을 높일 수 있다.

이하, 본 발명의 바람직한 실시예들을 첨부한 도면을 참조하여 상세히 설명한다. 도면들 중 동일한 구성요소들은 가능한 한 어느 곳에서든지 동일한 부호들로 나타내고 있음에 유의해야 한다. 또한 본 발명의 요지를 불필요하게 흐릴 수 있는 공지 기능 및 구성에 대한 상세한 설명은 생략한다.

도 1은 본 발명의 바람직한 실시예에 따른 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 매체를 도시한 도면이다.

본 발명의 실시예에 따른 패스워드 변환 인증 매체(100)는 일대일 일방향 매핑 함수를 통해 입력한 패스워드가 난수화된 서로 다른 패스워드들을 각각의 서로 다른 서버에 등록하여 사용하는 것을 기본 원리로 한다.

도시된 바와 같이, 패스워드 변환 인증 매체(100)는, 암호적으로 안전한 메모리 영역(120), 읽기 전용 영역(140), 및 범용 메모리 영역(160)으로 구분된다.

암호적으로 안전한 메모리 영역(120)은 사용자의 128비트 비밀 값 (r)을 저장하기 위한 공간이다. 이러한 암호적으로 안전한 메모리 영역(120)은 가격이 상대적으로 비싸지만, 요구 공간이 128비트(16바이트)이다.

읽기 전용 영역(140)은 일대일 일방향 매핑 함수(h())를 처리하기 위한 공간이다. 이러한 읽기 전용 영역(140)은 함수실행 코드에 대응하는 공간, 즉 16[Kbit] 내지 32[Kbit] 정도의 공간만을 요구한다.

범용 메모리 영역(160)은 함수 처리 및 임시 데이터 저장을 위한 공간이다. 이러한 범용 메모리 영역(160)은 16[Kbit] 내지 32[Kbit] 정도의 일반적으로 사용되는 저렴한 메모리 공간만을 요구한다.

본 발명의 실시예에 따른 일대일 일방향 매핑 함수(h())의 특성은 입력 값의 한 비트의 차이만 발생해도, 출력 값은 전혀 다른 값이 생성된다. 즉 h(11)과 h(10)은 완전히 다른 값을 출력한다. 이러한 성질을 이용하여, 본 발명의 실시예에서는 사용자의 아이디(ID)와 패스워드(PW), 암호화 비밀 값(r), 및 서버의 주소(Svr_addr)를 일대일 일방향 매핑 함수(h())에 입력하여 각 서버마다 서로 다른 형태의 패스워드를 생성하고 이를 등록할 수 있도록 한다. 본 실시예에 따라 변환 생성되는 패스워드는 상기의 함수 인자값이 입력된 h(ID||pw||r||Svr_Addr)로 나타낼 수 있다.

여기서 아이디(ID)와 패스워드(PW), 및 암호화 비밀 값(r)은 고정된 값이지만, 서버의 주소(Svr_addr)들은 서버마다 모두 다르기 때문에 결과적으로 서버의 주소에 따라 서로 다른 패스워드들을 생성하여 해당 서버에 로그인할 수 있다.

따라서, 본 발명의 패스워드 변환 인증 매체(100)에 따르면, 사용자들이 동일한 패스워드를 복수의 서로 다른 서버들에 설정하여 사용할 때 패스워드의 유출에 따라 발생할 수 있게 하는 문제점을 해결한다. 즉, 본 발명의 패스워드 변환 인증 매체(100)에 따르면, 사용자는 하나의 패스워드만 암기하고 다니면서도 복수의 서버에 서로 다른 패스워드를 생성하고 등록하여 사용할 수 있다. 특히, 본 발명의 패스워드 변환 인증 매체(100)는 기존에 사용되는 어떠한 패스워드 기반 인증 및 키 교환 기법에서도 적용되어 사용될 수 있기 때문에, 실용성면에서도 우수한 장점이 있다.

본 발명의 패스워드 변환 인증 매체(100)는 기본적으로 휴대용 범용 직렬 버스(portable Universal Serial Bus: USB) 장치를 사용할 수 있다. 그러나, 본 발명의 패스워드 변환 인증 매체(100)는 오직 작은 크기의 메모리 공간만을 요구하기 때문에, 사용자들이 비싼 USB를 살 필요 없이, 가격이 저렴한 USB 장치를 통해 사용할 수 있다. 또는, 본 발명의 패스워드 변환 인증 매체(100)용 소형 USB 장치를 마치 열쇄 고리와 같은 형태로 만들어서, 불편함 없이 지니고 다닐 수 있도록 할 수도 있다.

도 2는 본 발명의 패스워드 변환 인증 매체를 이용한 웹 서버 접속을 위한 시스템 구조를 간략하게 도시한 도면이다.

도시된 바와 같이, 본 발명이 적용되는 시스템은, 웹 서버(400), 패스워드 변환 인증 매체(100), 및 컴퓨터와 같은 통신 기기(300)로 구성된다.

웹 서버(400)는 통신을 통해 접속 가능한 웹 주소를 가지며, 설정된 아이디(ID) 및 설정된 아이디에 대하여 동일하게 설정된 패스워드의 등록을 통해 사용자의 인증 과정을 수행한다. 본 실시예에서 웹 서버(400)는 동일한 패스워드를 갖는 서로 다른 둘 이상의 인증 대상 웹 서버인 것을 예로 한다.

패스워드 변환 인증 매체(100)는 도 1에 도시한 본 발명의 실시예와 같이, 인증을 위한 웹 서버(400)의 서로 다른 주소 정보를 포함하는 인증 정보에 대하여, 일대일 일방향 매핑 함수(h())를 실행하여 서로 다른 난수화된 패스워드를 변환 생성한다. 패스워드 변환 인증 매체(100)의 구성 및 각 구성 요소들의 특성 및 기능에 대해서는 도 1을 설명하면서 언급하였기에, 여기서는 생략한다.

통신 기기(300)는 패스워드 변환 인증 매체(100)가 소정 인터페이스(예를 들어, 범용 직렬 버스: USB)를 통해 접속되고, 인증의 대상이 되는 웹 서버(400)에 유무선 인터넷과 같은 소정 통신 방식을 통해 접속되어 있다. 사용자(200)로부터 인증 정보가 입력되면, 통신 기기(300)는 입력된 인증 정보를 패스워드 변환 인증 매체(100)에 제공한다.

패스워드 변환 인증 매체(100)는 입력되는 인증 정보를 도 1에서와 같이 일대일 일방향 매핑 함수(h())를 통해 난수화된 패스워드로 변환 생성하여 통신 기기(300)로 출력한다. 통신 기기(300)는 패스워드 변환 인증 매체(100)에서 변환 생성된 난수화된 패스워드를 웹 서버(400)에 등록한다.

여기서 인증 정보는, 도 1에 나타낸 보와 같이, 웹 서버(400)에 등록된 사용자의 아이디(ID) 및 패스워드(PW), 패스워드 변환 인증 매체(100)에 설정된 비밀 난수 값(r), 및 웹 서버(400)의 주소(Svr_addr) 정보가 포함된다. 따라서 패스워드 변환 인증 매체(100)는 이러한 정보들을 일대일 일방향 매핑 함수(h())에 대입하여 함수를 실행함으로써, 난수화된 패스워드를 변환 생성한다. 여기서 아이디(ID), 패스워드(PW), 및 비밀 난수 값(r)이 동일하더라도, 웹 서버(400)의 주소(Svr_addr) 정보가 웹 서버 마다 다르기 때문에, 결과적으로 패스워드 변환 인증 매체(100)에서 일대일 일방향 매핑 함수(h())에 의해 변환 생성되는 패스워드는 서로 다른 정보를 갖게 된다.

도 3은 본 발명의 바람직한 실시예에 따른 패스워드 변환 인증 매체를 이용한 웹 서버의 인증 방법을 도시한 흐름도이다.

본 실시예는 패스워드 변환 인증 매체(100)가 소정 인터페이스(USB)를 통해 통신 기기(300)에 접속된 상태를 예를 기초로 설명한다. 먼저, 비밀 난수 값(r)이 통신 기기(300)로부터 입력되면(S110), 패스워드 변환 인증 매체(100)는 입력된 비밀 난수 값(r)을 암호적으로 안전한 메모리 영역(120)에 설정 및 저장한다(S120).

이후 통신 기기(300)로부터 아이디(ID)가 입력되고(S130) 패스워드(PW)가 입력되며(S140) 웹 서버(400)의 주소(Svr_addr)가 입력되면(S140), 패스워드 변환 인증 매체(100)는 읽기 전용 영역(140)에 설정된 일대일 일방향 매핑 함수(h())를 통한 새로운 패스워드 'h(ID||pw||r||Svr_Addr)'를 변환 생성한다(S160). 여기서 패스워드 변환 인증 매체(100)는 일대일 일방향 매핑 함수(h())를 통해 변환 생성된 패스워드를 범용 메모리 영역(160)에 임시 저장할 수 있다.

이에 따라, 통신 기기(300)는 입력되는 등록 명령에 따라, S160 단계에서 변환 생성된 패스워드를 웹 서버(400)에 등록한다(S170).

본 실시예에 따라 새로 생성한 패스워드를 웹 서버(400)에 안전하게 등록하는 방법은 기존에 공지되어 있는 어떠한 방법을 사용해도 무방하다. 따라서, 본 실시예에서는 이에 대한 구체적 패스워드 등록 방법에 대해서는 설명을 생략한다. 또한, 사용자가 패스워드를 사용하여 키 교환을 하는 경우에도 본 실시예와 같은 방법이 적용된다.

이하, 패스워드 변환 인증 매체(100)에 저장되는 비밀 난수 값(r)의 갱신 및 복구 예에 대해 설명한다.

사용자가 패스워드 변환 인증 매체(100)를 소지하고 다니다가 패스워드 변환 인증 매체(100)가 망가지거나 분실되는 경우가 발생할 수 있다.

첫째, 패스워드 변환 인증 매체(100)가 망가지는 경우, 기존에 사용되는 키 위탁 방식을 사용하여 비밀 난수 값(r)을 위탁한 뒤 복구하는 방법을 사용할 수 있다. 즉, 사용자는 비밀 난수 값(r)을 자신의 통신 기기(300) 내에 보관하거나, CD나 기타 다른 안전한 저장 매체에 저장할 수 있으며, 필요에 따라 전문 위탁기관 서버에 등록하여 보관할 수도 있다. 따라서, 패스워드 변환 인증 매체(100)가 망가졌을 경우, 새로운 패스워드 변환 인증 매체에 위탁해 놓았던 비밀 난수 값(r)을 재설정해서 사용할 수 있다.

둘째, 패스워드 변환 인증 매체(100)를 분실했을 경우, 사용자가 새로운 비밀 난수 값(r)을 설정해서 사용할 수도 있다. 그러나, 이 경우, 각 서버들에 설정되어 기존 패스워드들을 모두 새로운 패스워드들로 바꿔야하기 때문에, 효율성면에서 좋지 않다. 그러나, 패스워드 변환 인증 매체(100) 내에 암호학적으로 안전한 메모리 공간(120) 내에 저장되어 있는 비밀 난수 값(r)을 제 3자가 알아낼 수 있는 확률은 매우 낮기 때문에 기존의 비밀 난수 값(r)을 그냥 사용해도 무방하다. 즉, 128비트의 비밀 난수 값(r)을 알아낼 확률은 $1/2^{128}$이기 때문에, 계산적으로 알아내기 매우 어렵다.

이하, 실험에 따른 본 발명의 패스워드 변환 인증 매체(100)에 대한 안전성 결과에 대해 설명한다.

도 4는 본 발명에 따른 패스워드 변환 인증 매체(100)에 대한 안전성 실험 평가 결과를 나타낸 도면이다.

패스워드 변환 인증 매체(100)의 안전성은 사용되는 일대일 일방향 매핑함수(h())의 안전성을 기초로 한다. 즉, 하나의 패스워드가 유출된다 하더라도, 함수의 일방향 성질에 의해 해당 패스워드를 생성하는 데 필요한 함수 입력 값인 패스워드(PW)나 비밀 난수 값(r)을 알아내기가 어렵다. 또한, 생성되는 패스워드들은 서로 연관성이 없이 완전히 난수화(randomized) 되어 생성되기 때문에, 하나의 유출된 패스워드를 통해 다른 패스워드들을 유추하는 것도 불가능하다.

도 4에 도시된 바와 같이, 실험 값을 통해 패스워드 변환 인증 매체(100)의 안전성, 즉, 패스워드들이 난수화되어 서로 다른 정보로 생성되는 것을 알 수 있다.

이상에서는 본 발명에서 특정의 바람직한 실시예에 대하여 도시하고 또한 설명하였다. 그러나, 본 발명은 상술한 실시예에 한정되지 아니하며, 특허 청구의 범위에서 첨부하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 및 균등한 타 실시가 가능할 것이다. 따라서 본 발명의 진정한 기술적 보호범위는 첨부한 특허 청구범위에 의해서만 정해져야 할 것이다.

발명의 효과

본 발명에 따르면, 128비트로 암호화되는 임의의 비밀 난수 값(r) 및 입력되는 값이 대하여 일대일 일방향 매칭 함수(h())를 수행하도록 설정된 패스워드 변환 인증 매체를 구성하여 입력되는 인증 대상 웹 서버의 주소값에 따라 서로 다른 새로운 패스워드를 변환 생성함으로써, 서로 다른 주소를 갖는 웹 서버에 대해 동일한 패스워드가 설정된 경우 웹 서버의 주소에 따라 서로 다른 패스워드를 변환 생성하기 때문에 패스워드의 유출에 따라 발생할 수 있는 문제점을 해결 할 수 있다.

또한, 동일한 패스워드라 하더라도 입력되는 웹 서버의 주소 정보가 다른 경우 입력되는 패스워드를 서로 다른 새로운 패스워드로 변환 생성하여 웹 서버에 등록함으로써, 패스워드 보안을 위해 패스워드를 웹 서버마다 다르게 설정할 필요가 없으며 웹상에서 패스워드 인증기법의 안전성을 높일 수 있다.

도면의 간단한 설명

도 1은 본 발명의 바람직한 실시예에 따른 분산된 웹 서비스에 대한 안전한 패스워드 관리를 위한 패스워드 변환 인증 매체를 도시한 도면,

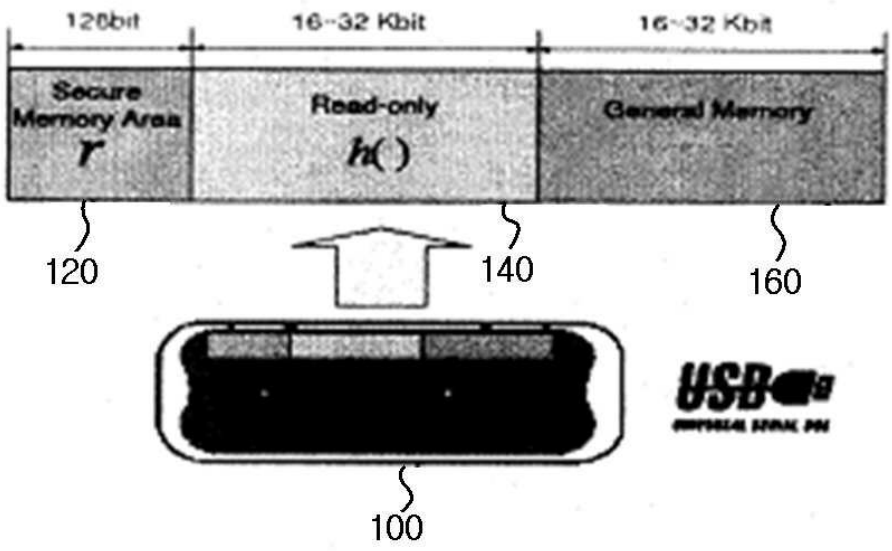
도 2는 본 발명의 패스워드 변환 인증 매체를 이용한 웹 서버 접속을 위한 시스템 구조를 간략하게 도시한 도면,

도 3은 본 발명의 바람직한 실시예에 따른 패스워드 변환 인증 매체를 이용한 웹 서버의 인증 방법을 도시한 흐름도, 그리고

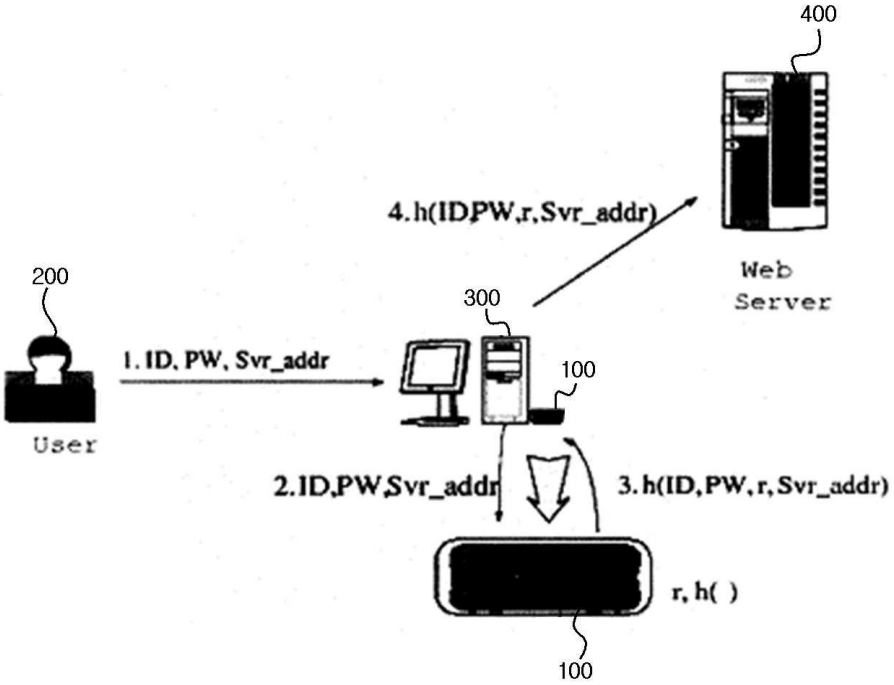
도 4는 본 발명에 따른 패스워드 변환 인증 매체에 대한 안전성 실험 평가 결과를 나타낸 도면이다.

도면

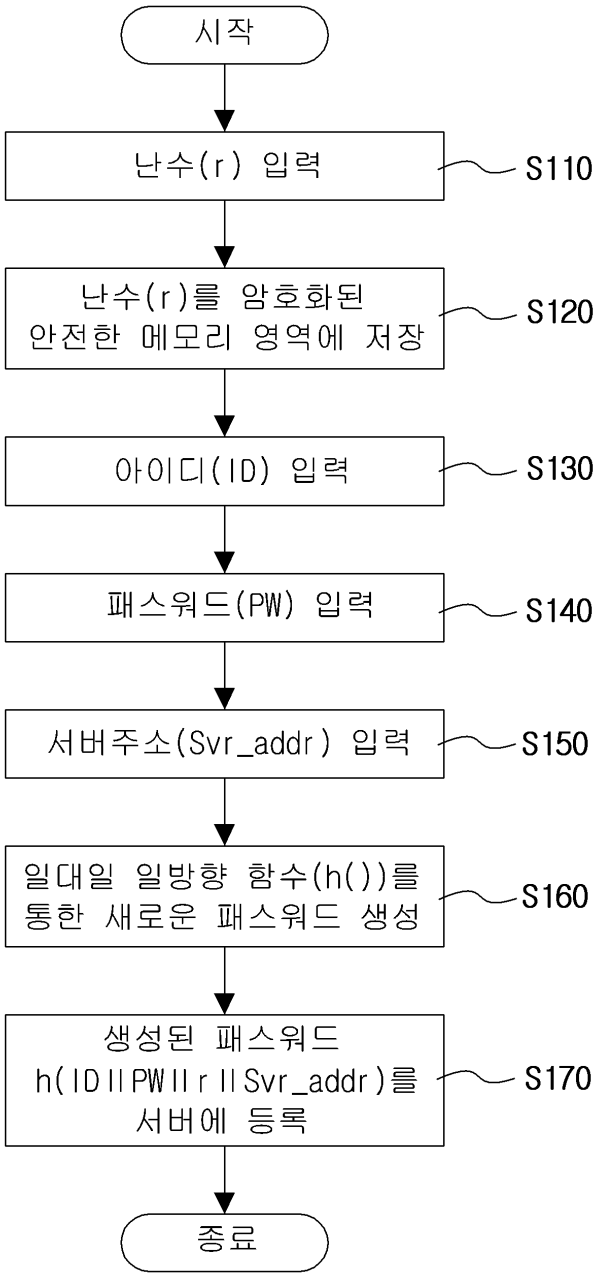
도면1



도면2


400
4. h(ID,PW,r,Svr_addr)
Web
Server
200
300
1. ID, PW, Svr_addr
100
User
2. ID,PW,Svr_addr
3. h(ID,PW,r,Svr_addr)
r, h( )
100

도면3



도면4

ID	*Password*	*Random number (128 bit)*	*Server's Address*	*P_Password*
Robert	Password	0x00112233445566778899aabbccddeeff	*www.security.com*	0xf001e795ac95f23a
Robert	Password	0x00112233445566778899aabbccddeeff	*www.pocket77.com*	0xd0e4bc28106e1c81
Robert	Password	0x00112233445566778899aabbccddeeff	*www.npc05.org*	0x073e160a41738cd2
bobert	Password	0x00112233445566778899aabbccddeeff	www.security.com	0x9ba86eb376b36756
Robert	*Passpord*	0x00112233445566778899aabbccddeeff	www.security.com	0x128d6116fb2faa8e
Robert	Password	0xff112233445566778899aabbccddeeff	www.security.com	0x1080904b14a42155
Robert	*Bassword*	0xff112233445566778899aabbccddeeff	www.security.com	0x0ece1d0612ca374f
Robert	*Pastword*	0xff112233445566778899aabbccddeeff	www.security.com	0xa341bc688d68ab92
Robert	Password	0xff112233445566778899aabbccddeeff	*www.security.org*	0xe1606cf9938c31e9
Robert	Password	0xff112233445566778899aabbccddeeff	*www.security.net*	0xd9c685511c2aceeb