(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06F 15/00 (2006.01)

(45) 공고일자 2006년11월10일
(11) 등록번호 10-0641717
(24) 등록일자 2006년10월26일

(21) 출원번호 10-2005-0049261
(22) 출원일자 2005년06월09일

(65) 공개번호
(43) 공개일자

(73) 특허권자 고려대학교 산학협력단

(72) 발명자 이희조
박범수
오재욱
홍성진

(74) 대리인 유미특허법인

심사관 : 여원현

(54) 안전 인증 방법 및 안전 인증을 수행하는 프로그램이기록된 기록매체

요약

안전 인증을 수행하는 프로그램은 브라우저 기능 확장 모듈(윈도우즈 운영체제에서 BHO로 동작), 마스터 인증 유지 모듈(윈도우즈 운영체제에서 시스템 트레이로 동작), 인증 정보 저장 모듈을 포함하는 구조를 가진다.

안전 인증을 수행하는 프로그램은 설치 및 실행된 후 인증폼을 모니터링하다가 인증폼을 감지하면 마스터 인증을 수행하고, 웹페이지 인증 정보를 얻은 후 의사 인증 정보로 HTTP 요청 메시지를 생성하지만, 서버로 전송하기 전에 이를 가로채 실제 웹페이지 인증 정보로 바꾸어 다시 HTTP 요청을 하는 방법으로 해당 웹페이지에 안전 인증을 수행한다.

안전 인증을 수행하는 프로그램은 악성 프로그램으로부터 웹페이지 인증 정보를 보호하고, 인증 정보의 관리를 용이하게 하며, 인증 절차를 간편하게 한다.

대표도

도 1

색인어

안전 인증, 인증, 로그인, BHO, 트레이, IE

명세서

도면의 간단한 설명

도 1은 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램의 구조를 도시한 개략도이다.

도 2는 본 발명의 실시예에 따른 사용자 인증 정보 저장부의 구조를 도시한 개략도이다.

도 3은 사용자 인증 정보 저장부의 일례를 도시한 도면이다.

도 4는 본 발명에 따른 안전 인증을 수행하는 프로그램을 처음 사용하는 방법을 도시한 흐름도이다.

도 5는 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램이 이미 설치된 환경에서 안전 인증을 하기 위한 방법을 도시한 흐름도이다.

도 6은 본 발명의 실시예에 따른 안전 인증 방법을 도시한 도면이다.

도 7은 본 발명의 실시예에 따른 HTML 형태의 가장 일반적인 인증폼을 나타낸 도면이다.

도 8은 본 발명의 실시예에 따른 HTML 형태의 가장 일반적인 인증폼을 검색하기 위한 방법을 도시한 흐름도이다.

도 9는 윈도우즈 API 함수인 HttpSendRequest 함수의 함수 원형(Prototype)을 나타내는 도면이다.

도 10은 윈도우즈 IE에서 마스터 인증 정보 입력을 위한 대화 상자가 생성된 상태를 나타내는 도면이다.

도 11은 웹페이지 인증 정보를 입력 받기 위한 가상 키보드가 생성된 상태를 나타내는 도면이다.

도 12는 의사 웹페이지 인증 정보로 웹페이지에 대한 인증이 수행되는 상태를 나타내는 도면이다.

도 13은 웹페이지에 대한 인증 절차가 완료된 상태를 나타내는 도면이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 안전 인증 방법 및 안전 인증을 수행하는 프로그램이 기록된 기록매체에 관한 것이다.

더욱 상세하게 본 발명은 인증 정보의 누설을 막으면서 인터넷 웹페이지에 인증할 수 있는 방법 및 그 방법을 위한 프로그램이 기록된 기록매체에 관한 것이다.

마이크로소프트 인터넷 익스플로러(IE)는 2004년 5월 OneStat.com의 조사에 의하면 웹브라우저 분야에서 전 세계의 93.9%를 점유하고 있는 것으로 나타났다.

IE는 브라우저 지원 객체(BHO, Browser Helper Object)라는 확장 프레임워크를 지원하면서 브라우저의 기능을 확대하고 있는데, 즉 이는 IE가 실행될 때마다 자동적으로 수행되는 작은 프로그램을 의미한다. 이러한 BHO는 웹상의 여러 가지

이벤트 동작들을 효율적으로 제어하는 것을 돕기 위해 고안되고 현재 편리하고 사용되고 있지만 반면, 이러한 특성을 이용하여 악성 BHO는 유해 웹페이지로의 강제 이동, 즐겨찾기에 원치 않는 바로가기 정보 추가, 인증 정보(아이디, 패스워드) 등의 개인 정보 취득 등에 악용되고 있다.

악성 BHO는 다양한 방식으로 공격을 주도하고 있는데 크게 3가지로 구분지어 정리할 수 있다.

그 첫째는 브라우저 이벤트를 조정하여 원하는 기능으로 바꾸는 것이다. 예를 들어, 시작 페이지를 특정 페이지로 변경한다거나 팝업 페이지를 띄우는 등을 들 수 있다.

둘째는 웹페이지들이 보여주고 있는 내용에 접근하는 것이다. 따라서 악성 BHO는 웹페이지가 보여주고 있는 개인 정보(아이디, 패스워드 등) 등을 탈취하여 파일로 저장하여 원하는 곳으로 전송할 수 있다.

셋째는 입력된 키와 이벤트들을 제어하고 기록하는 것이다. 즉, 악성 BHO는 사용자가 입력하는 키들을 저장하여 개인 정보를 취득할 수도 있다.

인터넷의 발달로 전자 상거래, 인터넷 뱅킹이 활성화되고 있어 이러한 악성 프로그램에 의한 개인 정보 취득은 날로 문제가 되고 있다. 또한 근래 많은 사람들이 이용하고 있는 온라인 게임에서 현금화할 수 있는 아이템을 악성 BHO를 이용하여 아이디와 패스워드를 몰래 얻어내 아이템을 탈취하는 것도 가능하게 된다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 악성 프로그램으로부터 인증 정보를 보호하면서 웹페이지에 안전하게 인증할 수 있는 방법 및 그 방법을 위한 프로그램이 기록된 기록매체를 제공하는 것이다.

발명의 구성 및 작용

본 발명에 따른 안전 인증을 수행하는 프로그램이 기록된 기록매체는, 브라우저에 표시되는 웹페이지에 안전 인증을 수행하는 프로그램이 기록된 기록매체에 있어서, 적어도 하나의 사용자에 관한 적어도 하나의 웹페이지 인증 정보를 저장하는 인증 정보 저장 모듈, 상기 웹페이지 인증 정보에 대한 접근 권한을 부여하는 마스터 인증을 수행하는 마스터 인증 모듈, 상기 웹페이지에 인증폼의 존재를 모니터링 하는 인증폼 감지 모듈, 상기 인증폼을 감지하면 의사 웹페이지 인증 정보로 웹페이지 인증을 수행하는 웹페이지 인증 모듈 및 의사 웹페이지 인증 정보를 포함하는 웹페이지 요청 메시지를 가로채서 실제 웹페이지 인증 정보로 대체하여 정상적인 웹페이지 요청 메시지를 생성하는 함수 후킹 모듈을 포함하는 구조를 가진다.

이때, 상기 인증폼 감지 모듈, 마스터 인증 모듈, 웹페이지 인증 모듈, 함수 후킹 모듈은 브라우저 기능 확장 모듈의 형태로 설치될 수 있다.

또한, 소정의 마스터 인증 해제 조건이 발생하지 않으면 계속 마스터 인증을 유지하는 마스터 인증 유지 모듈을 더 포함하고, 상기 마스터 인증 모듈은 상기 마스터 인증 유지 모듈에 마스터 인증 유지 상태를 조회하고, 상기 마스터 인증 유지 모듈은 상기 마스터 인증 모듈에 마스터 인증 상태 정보를 보고할 수 있다.

본 발명에 따른 안전 인증을 제공하는 방법은, 브라우저에 표시되는 웹페이지에의 안전 인증을 제공하는 방법에 있어서, 사용자를 고유하게 식별하는 마스터 인증 정보를 통해 마스터 인증을 제공하는 단계, 상기 웹페이지의 인증폼에 대한 모니터링을 제공하는 단계, 상기 인증폼이 감지되면 웹페이지에 대응하는 실제 웹페이지 인증 정보에 대한 검색을 제공하는 단계, 의사 웹페이지 인증 정보로 상기 웹페이지에 대한 인증을 제공하는 단계 및 상기 의사 웹페이지 인증 정보로의 인증 시도를 가로채 상기 웹페이지에 대응하는 실제 웹페이지 인증 정보로의 대체를 제공하는 단계를 포함한다.

이때, 상기 실제 웹페이지 인증 정보의 저장을 제공하는 단계를 더 포함하고, 상기 저장을 제공하는 단계는, 마우스의 조작만으로 상기 웹페이지 인증 정보를 입력할 수 있는 가상 키보드를 제공하는 단계, 해당하는 웹페이지의 URL에 대응하여 상기 가상 키보드로 입력된 웹페이지 인증 정보에 대한 저장을 제공하는 단계를 포함할 수 있다.

아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였다. 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

우선, 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램의 구조를 도 1 내지 도 3을 참조하여 설명한다.

먼저, 도 1은 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램의 구조를 도시한 개략도이고, 도 2는 본 발명의 실시예에 따른 사용자 인증 정보 저장부의 구조를 도시한 개략도이다.

본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램의 동작을 위해서는 브라우저(10)와 웹페이지(20)를 필요로 하며, 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램은 브라우저 기능 확장 모듈(100), 인증 정보 저장 모듈(200), 마스터 인증 유지 모듈(300)을 포함한다. 여기서 모듈은 단위 기능을 수행하는 소프트웨어 또는 하드웨어의 단위를 지칭한다.

브라우저(10)는 인터넷상의 웹 정보를 검색하고, 웹페이지(20)를 표시하는 프로그램이다. 대표적으로는 넷스케이프사의 넷스케이프 네비게이터, 마이크로소프트사의 인터넷 익스플로러(IE), 선 마이크로시스템스사의 핫 자바를 들 수 있다. 본 발명에 따른 안전 인증 방법이 수행되기 위해서는, 브라우저(10)가 기능 확장을 위해 별도의 프로그램을 수행할 수 있는 구조를 가져야 한다. 본 발명의 실시예에서는 인터넷 익스플로러를 사용하지만, 기능 확장을 위해 별도의 프로그램을 수행할 수 있는 구조를 가진 브라우저라면 어떠한 브라우저도 가능하다.

인터넷 익스플로러는 실행이 되면 운영체제인 윈도우즈에 등록된 레지스트리를 검색하여 등록된 BHO가 있는 지 확인하고, 등록된 BHO들을 수행시킨다. 다른 악성 BHO와 함께, 본 발명에 따른 BHO 즉, 브라우저 기능 확장 모듈(100) 또한 레지스트리에 등록되어 브라우저(10)의 실행에 따라 실행된다.

웹페이지(20)는 HTML이 표준으로서 사용되나 본 발명에 따른 안전 인증 방법은 반드시 이에 한정되지는 않는다. 다만 본 발명의 실시예에서는 HTML 방식을 따른다.

브라우저 기능 확장 모듈(100)은 인증폼 감지 모듈(110), 마스터 인증 모듈(140), 웹페이지 인증 모듈(120), 함수 후킹 모듈(130)를 포함한다. 브라우저 기능 확장 모듈(100)은 윈도우즈 운영체제의 인터넷 익스플로러를 브라우저(10)로 사용하는 경우 인터넷 익스플로러의 BHO의 형태로 설치된다.

인증폼 감지 모듈(110)는 웹페이지(20)가 인증폼을 포함하고 있는 지를 상시 모니터링(Monitoring)하고 있다가 인증폼이 존재하면 인증폼 감지 정보를 생성한다. 인증폼이란 웹페이지(20)에 포함되어 있는 것으로써 사용자로부터 인증 정보를 입력 받을 수 있는 형태를 의미한다.

마스터 인증 모듈(140)는 인증폼 감지 정보가 생성되면 마스터 인증 유지 모듈(300)에 마스터 인증을 요청한다. 마스터 인증 유지 모듈(300)은 현재 마스터 인증 상태이면 바로 마스터 인증 상태 정보를 마스터 인증 모듈(140)로 전달하지만, 마스터 인증 상태가 아니라면 마스터 인증 수행 후에 마스터 인증 상태 정보를 마스터 인증 모듈(140)에 전달한다.

웹페이지 인증 모듈(120)는 마스터 인증 모듈(140)로부터의 마스터 인증 상태 조회가 끝나면 해당 웹페이지(20)에 대한 인증을 수행한다. 웹페이지 인증 모듈(120)는 인증 정보 저장 모듈(200)에 해당 웹페이지(20)에 대해 인증할 수 있는 상기 마스터 인증을 한 사용자의 웹페이지 인증 정보가 있는 지 검색한다. 웹페이지 인증 정보는 특정 웹페이지(20)에 대한 접근 권한을 얻기 위한 정보로써, 보통 아이디(이하 웹페이지 아이디)와 패스워드(이하 웹페이지 패스워드)를 포함한다.

웹페이지 인증 모듈(120)는 검색 결과 웹페이지 인증 정보가 없으면, 사용자로부터 웹페이지 인증 정보를 입력 받기 위해 키스트로크 없이 웹페이지 인증 정보를 입력하기 위한 가상 키보드를 생성하고, 사용자로부터 웹페이지 인증 정보가 입력되면 인증 정보 저장 모듈(200)에 저장한다.

웹페이지 인증 모듈(120)는 검색 결과 웹페이지 인증 정보가 있거나 가상 키보드로 웹페이지 인증 정보를 입력 받은 후에는, 실제의 웹페이지 인증 정보가 아닌 의사 웹페이지 인증 정보로 HTTP 요청 메시지를 생성하고, 이 메시지로 HTTP 요

청을 수행한다. 여기서 의사 웹페이지 인증 정보라 함은 실제의 웹페이지 인증 정보와는 상관없는 아이디와 패스워드를 의미한다. 예를 들어 아이디는 IDKIN, 패스워드는 PWKIN으로 의사 웹페이지 인증 정보를 정의하면 웹페이지 인증 모듈(120)는 웹페이지(20)에 아이디를 IDKIN으로 하고 패스워드를 PWKIN으로 하여 인증을 시도한다.

악성 BHO가 존재한다면, 이 과정에서 이 악성 BHO는 웹페이지(20)에 표시되는 IDKIN과 PWKIN을 아이디와 패스워드로 인식하여 개인 정보를 습득하게 되므로, 악성 BHO는 실제의 웹페이지 인증 정보를 얻을 수 없다.

웹페이지 인증 모듈(120)가 의사 웹페이지 인증 정보로 인증을 시도하면, 브라우저(10)는 이 의사 웹페이지 인증 정보를 포함하는 HTTP 요청 메시지를 생성하고 서버로 전달하기 위해 윈도우즈 API 함수인 HttpSendRequest라는 함수를 호출하게 된다.

함수 후킹 모듈(130)는 이 HttpSendRequest 함수를 후킹하고, 의사 웹페이지 인증 정보를 실제의 웹페이지 인증 정보로 대체하여 다시 HttpSendRequest 함수를 호출한다. 이로써 실제의 웹페이지 인증 정보로 해당 웹페이지(20)에 대한 인증이 이루어진다. 여기서 함수 후킹(Hooking)이란 함수 호출이 있는 경우 해당 함수를 먼저 가로채서 조작을 가하는 것을 말한다. 보통 API 함수에 대한 후킹이 많이 이루어진다.

마스터 인증 유지 모듈(300)은 마스터 인증 모듈(140)로부터 마스터 인증 요청이 있으면 마스터 인증 정보를 입력하기 위한 대화 상자(Dialog Box)를 열고 사용자로부터 마스터 인증 정보의 입력이 수행되면 마스터 인증을 수행한다. 또한 마스터 인증 유지 모듈(300)은 브라우저(10)의 실행 종료와 상관없이 마스터 인증 상태를 유지한다. 마스터 인증 유지를 해제하는 조건으로는 사용자에 의한 명시적인 요청(로그아웃) 및 일정 시간의 경과 중 적어도 하나를 사용할 수 있으며, 이 일정 시간에 대해서는 설정이 가능하다. 여기서 마스터 인증 정보는 인증 정보 저장 모듈(200)에 저장된 인증 정보에 접근 권한을 부여하는 정보로써 다른 인증 정보와 마찬가지로 아이디(이하 마스터 아이디)와 패스워드(이하 마스터 패스워드)를 포함한다. 웹페이지 인증 정보와 마스터 인증 정보를 통칭하여 인증 정보라고 부르도록 한다.

인증 정보 저장 모듈(200)은 본 발명에 따른 안전 인증을 수행하는 프로그램이 다수의 사용자를 수용할 수 있도록 하는 인증 정보를 저장한다. 인증 정보 저장 모듈(200)은 적어도 하나의 사용자 인증 정보 저장부(210)를 포함한다.

다수의 사용자를 구별할 수 있도록 하는 절차가 마스터 인증이다. 즉 제1 사용자에 대한 마스터 인증이 수행되면, 제1 사용자 인증 정보 저장부(210)에 포함된 웹페이지 인증 정보만이 본 발명에 따른 안전 인증에 유효하게 된다. 사용자 인증 정보 저장부(210)는 암호화되어 인증 정보의 유출로부터 보호된다. 암호화 알고리즘으로 AES(Advanced Encryption Standard)라는 대칭 키 암호 방식이 사용될 수 있고, 또한 대칭 키로써 마스터 패스워드가 사용될 수 있다.

도 2에 도시된 바와 같이 사용자 인증 정보 저장부(210)는 해당 사용자를 위한 다수의 웹페이지 인증 정보(211)를 포함한다. 웹페이지 인증 정보(211)는 URL(Uniform Resource Locator), 웹페이지 아이디 및 웹페이지 패스워드를 포함하며 구분자(본 발명의 실시예에서는 #을 사용)로 각각 구분된다.

도 3은 사용자 인증 정보 저장부의 일례를 도시한 도면이다. 도 3에 도시된 바와 같이 Http://www.kipo.go.kr 웹페이지에 해당하는 웹페이지 아이디는 user1이고, 웹페이지 패스워드는 1234이다.

이하에서는 사용자가 본 발명에 따른 안전 인증을 수행하는 프로그램을 사용하는 방법을 도 4 및 도 5를 참조하여 설명한다.

도 4는 본 발명에 따른 안전 인증을 수행하는 프로그램을 처음 사용하는 방법을 도시한 흐름도이다.

우선 사용자는 본 발명에 따른 안전 인증을 수행하는 프로그램을 설치하고(S11) 실행시킨다(S12). 사용자는 프로그램에 마스터 아이디와 마스터 패스워드를 포함하는 마스터 인증 정보를 등록한다(S13).

사용자는 브라우저(10)를 실행시키고 다양한 웹페이지를 방문한다(S14). 만약 사용자가 인증폼을 가진 웹페이지(20)를 방문할 경우 인증폼 감지 모듈(110)는 인증폼을 감지하고, 마스터 인증 모듈(140)는 사용자에게 마스터 인증 정보 입력을 요구하는 대화 상자를 열게 되는데, 이때 사용자는 안전 인증을 위해서 앞서 등록한 마스터 인증 정보를 입력하게 되고 마스터 인증 모듈(140)는 마스터 인증을 수행하고 유지한다(S15).

그 후, 웹페이지 인증 모듈(120)는 인증 정보 저장 모듈(200)을 검색하게 되는데, 인증 정보 저장 모듈(200)에 사용자가 방문한 웹페이지(20)에 해당하는 웹페이지 인증 정보가 아직 없기 때문에, 웹페이지 인증 모듈(120)는 사용자에게 웹페이

지 인증 정보 입력을 요구한다. 이때, 악성 BHO 등의 악성 프로그램이 키스트로크에 의한 웹페이지 인증 정보를 취득하는 것을 막기 위하여 마우스 클릭으로 웹페이지 인증 정보를 입력할 수 있는 가상 키보드로 사용자에게 웹페이지 인증 정보 입력을 요구할 수 있다. 사용자는 이 가상 키보드로 웹페이지 인증 정보를 입력하게 되며, 이 웹페이지 인증 정보는 암호화되어 인증 정보 저장 모듈(200)에 저장된다(S16).

사용자는 실제의 웹페이지 인증 정보를 입력하였지만 웹페이지 인증 모듈(120)는 의사 인증 정보를 웹페이지(20)에 보내고 브라우저(10)는 이 의사 웹페이지 인증 정보로 HTTP 요청 메시지를 생성하기 위한 API 함수를 호출한다. 그 후, 함수 후킹 모듈(130)는 이 API 함수를 후킹하여 의사 웹페이지 인증 정보를 실제의 웹페이지 인증 정보로 대체하고 다시 HTTP 요청 메시지를 생성하여 웹페이지(20)에 대한 인증을 수행한다(S17).

도 5는 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램이 이미 설치된 환경에서 안전 인증을 하기 위한 방법을 도시한 흐름도이다.

본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램이 이미 설치되고 실행되고 있는 상태에서 사용자는 브라우저(10)를 실행하고 인증폼을 포함하는 특정 웹페이지(20)에 접속한다(S21).

인증폼 감지 모듈(110)는 인증폼을 감지하고, 마스터 인증 모듈(140)는 마스터 인증 상태인지를 확인한다(S22). 마스터 인증 상태가 아니면 사용자는 마스터 인증을 해야 하지만(S23), 이전에 이미 마스터 인증을 하였고 아직 마스터 인증이 해제되지 않은 상태이면(S22) 바로 웹페이지 인증 정보를 위한 단계로 진행한다.

마스터 인증을 한 사용자가 이전에 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램으로 해당 웹페이지(20)에 인증하지 않았으면(S24) 사용자는 가상 키보드로 웹페이지 인증 정보를 입력하여야 하지만(S25), 사용자가 이미 전에 안전 인증이 있었으면(S24) 웹페이지 인증 모듈(120)는 사용자로부터의 웹페이지 인증 정보 요구 없이 바로 해당 웹페이지(20)에 인증을 수행한다(S26). 이후의 인증 단계는 도 4와 같다.

즉, 사용자는 전에 방문한 웹페이지(20)에 대해서는 마스터 인증을 한 상태라면 인증이 필요한 웹페이지(20)에 방문하면 어떠한 액션을 취하지 않고서도 바로 인증이 이루어지는 편리함을 가진다.

이하에서는 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램의 동작을 도 6을 참고하여 설명한다.

도 6은 본 발명의 실시예에 따른 안전 인증 방법을 도시한 도면이다.

우선 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램이 컴퓨터에 설치된다(S110). 본 발명의 실시예에 따른 안전 인증을 수행하는 프로그램은 브라우저 기능 확장 모듈(100), 인증 정보 저장 모듈(200), 마스터 인증 유지 모듈(300)을 포함한다. 브라우저 기능 확장 모듈(100)은 윈도우즈 운영체제에서는 ActiveX 콘트롤의 형태로 설치되고 레지스트리에 등록된다. 인증 정보 저장 모듈(200)은 파일의 형태로 설치되고, 마스터 인증 유지 모듈(300)은 일반적인 윈도우즈 어플리케이션의 형태로 설치된다.

그 후 안전 인증을 위한 마스터 인증 유지 모듈(300)이 실행되고, 브라우저(10)의 실행에 따라 브라우저 기능 확장 모듈(100)이 실행되어 안전 인증을 수행하는 프로그램이 실행된다(S120). 이때 마스터 인증 유지 모듈(300)은 시스템 트레이 상태로 유지될 수도 있다.

그 후, 인증폼 감지 모듈(110)는 사용자가 접근하는 웹페이지(20)를 분석하면서 인증폼의 존재 여부를 모니터링한다(S130).

만약 인증폼이 존재하게 되면, 마스터 인증 모듈(140)는 마스터 인증 유지 모듈(300)에 마스터 인증 상태를 조회하고(S140), 마스터 인증 유지 모듈(300)은 만약 마스터 인증 상태가 아니면 마스터 인증 정보 입력을 위한 대화 상자를 열어 마스터 인증 요청을 하고, 마스터 인증 정보 입력이 있으면 마스터 인증을 수행한다(S150). 그리고 마스터 인증 유지 모듈(300)은 마스터 인증 해제를 위한 사용자의 명시적인 요청(로그아웃)이 있기 전이거나 일정 시간이 경과하기 전이라면 마스터 인증을 계속 유지한다. 이때 본 발명의 실시예에서는 마스터 인증이 인증폼 감지 후에 수행되었으나 인증폼 감지 전에 수행될 수도 있다.

마스터 인증 모듈(140)가 마스터 인증 유지 모듈(300)로부터 마스터 인증 상태 정보를 수신하면 웹페이지 인증 모듈(120)는 인증 정보 저장 모듈(200)에 마스터 인증을 한 사용자의 해당 웹페이지(20)의 인증 정보의 존재 여부를 검색한다(S160). 이과정에서 웹페이지 인증 모듈(120)가 인증 정보 저장부(210)를 마스터 패스워드를 대칭키로 복호하는 과정이 추가될 수도 있다.

만약 마스터 인증을 한 사용자의 해당 웹페이지(20)의 인증 정보가 없으면, 웹페이지 인증 모듈(120)는 가상 키보드를 생성하여 사용자로부터 웹페이지 인증 정보를 입력받고, 입력받은 웹페이지 인증 정보를 마스터 인증을 한 사용자에 해당하는 인증 정보 저장부(210)에 저장한다(S170). 이 과정에서 웹페이지 인증 모듈(120)가 웹페이지 인증 정보를 사용자 인증 정보 저장부에 마스터 패스워드를 대칭키로 암호화하여 저장하는 과정이 추가될 수 있다.

웹페이지 인증 모듈(120)는 사용자로부터 웹페이지 인증 정보를 입력받거나 인증 정보 저장 모듈(200)로부터 웹페이지 인증 정보를 얻은 경우, 의사 웹페이지 인증 정보를 웹페이지(20)에 표시하게 되고, 이때 브라우저(10)는 웹페이지(20)에 표시된 의사 웹페이지 인증 정보를 포함하는 HTTP 요청 메시지를 생성하기 위하여 윈도우즈 API 함수인 HttpSendRequest 함수를 호출한다(S180). 만약 악성 BHO 등의 악성 프로그램이 존재한다면, 이 악성 프로그램은 웹페이지(20)에 표시된 의사 웹페이지 인증 정보만을 획득할 수밖에 없으므로 실제의 웹페이지 인증 정보는 보호될 수 있다.

윈도우즈 API 함수인 HttpSendRequest 함수의 호출이 있게 되면, 함수 후킹 모듈(130)는 이 HttpSendRequest 함수를 후킹한다(S190). 그 후, 함수 후킹 모듈(130)는 HttpSendRequest 함수의 파라미터에서 의사 웹페이지 인증 정보를 검색하여 실제의 웹페이지 인증 정보로 대체하고(S200), HttpSendRequest 함수를 재호출하여(S210) 해당 웹페이지(20)에 대한 안전 인증을 수행하게 된다.

다음에 인증폼 감지 모듈(110)가 인증폼을 감지하는 방법에 대하여 도 7 및 도 8을 참고로 하여 설명한다.

도 7은 본 발명의 실시예에 따른 HTML 형태의 가장 일반적인 인증폼을 나타낸 도면이다.

도 7에 도시된 바와 같이 HTML 형태의 가장 일반적인 인증폼은 FORM 태그로 둘러 쌓여 있고, 아이디를 입력 받기 위한 INPUT 태그, 패스워드를 입력 받기 위한 INPUT 태그, 전송(submit)를 위한 INPUT 태그를 포함한다. 일반적인 인증폼에서는 name 특성(name property)은 특별히 정하여진 값은 없지만, type 특성(type property)은 아이디의 경우 text type을 가지고, 패스워드의 경우 password type을 가진다. 따라서 본 발명의 실시예에 따른 인증폼을 감지하는 방법은 INPUT 태그를 검색하고, 검색된 INPUT 태그의 type 특성(type property)을 분석하는 단계로 수행된다.

도 8은 본 발명의 실시예에 따른 HTML 형태의 가장 일반적인 인증폼을 검색하기 위한 방법을 도시한 흐름도이다.

먼저 웹페이지(W)에서 아이디 입력부의 위치(P_{ID}), 패스워드 입력부의 위치(P_{PW})의 검색을 시작한다(S300).

인증폼을 검색하기 위해서 웹페이지(W)에 포함된 INPUT 태그를 조사하게 되는데(S310), 각 INPUT 태그에 대해서(S320) type 특성을 분석한다(S330). type 특성이 text type이면(S340) 해당 INPUT 태그를 아이디 입력부의 위치(P_{ID})로 두고(S350), type 특성이 password type이면(S360) 해당 INPUT 태그를 패스워드 입력부의 위치(P_{PW})로 설정한다(S370). 패스워드 입력부의 위치(P_{PW})까지 검색이 되면 인증폼 검색은 종료되고 검색 성공 정보(TRUE)를 생성한다(S380).

만약 웹페이지(W)에 인증폼이 없는 경우에는 웹페이지(W)에 포함되어 있는 프레임(FRAME 또는 IFRAME)을 조사하고(S410), 각 프레임에 대해서(S420) 각 프렘임에 해당하는 웹페이지(V)에 인증폼이 있는 지 검색한다(S440). 이때 웹페이지(V)에 인증폼이 있는 지를 검색하기 위해서 컴퓨터 프로그래밍 기술인 재귀 호출(Recursive Call)을 사용한다. 즉 재귀 호출을 사용하기 위해서 S440 단계에서는 웹페이지(V)를 파라미터로 S300 단계를 다시 진행하게 된다.

웹페이지(V)에 인증폼이 있으면 인증폼 검색을 마치고 검색 성공 정보(TRUE)를 생성하지만(S440), 웹페이지(V)에도 인증폼이 없으면 인증폼 검색을 마치고 검색 실패 정보(FALSE)를 생성한다(S480).

다음, 윈도우즈 운영체제 아래에서 본 발명이 실시될 경우 브라우저(10)가 HTTP 요청 메시지를 생성하기 위해 호출하고, 함수 후킹 모듈(130)가 후킹을 하는 함수에 대해 도 9를 참고로 상세히 설명한다.

도 9는 윈도우즈 API 함수인 HttpSendRequest 함수의 함수 원형(Prototype)을 나타내는 도면이다.

웹페이지(20)에 의사 웹페이지 인증 정보가 입력되고 전송(submit)되면 브라우저(10)는 입력된 의사 웹페이지 인증 정보를 lpOptional field에 포함하여 HttpSendRequest 함수를 호출한다.

그리고 함수 후킹 모듈(130)는 호출된 HttpSendRequest 함수를 후킹하고 lpOptional field에 포함되어 있는 의사 웹페이지 인증 정보를 실제의 웹페이지 인증 정보로 대체한다. 아울러 함수 후킹 모듈(130)는 lpOptional field의 정보를 변경함에 따라 lpOptional field의 길이를 나타내는 dwOptionalLength field를 수정하고, lpszHeaders 또한 수정이 필요하다.

아래에서는 윈도우즈 운영체제 하에서 본 발명의 실제 구현예를 도 10 내지 도 13를 참고하여 상세히 설명한다.

도 10은 윈도우즈 IE에서 마스터 인증 정보 입력을 위한 대화 상자가 생성된 상태를 나타내는 도면이다.

도 10에 나타난 바와 같이, 인증폼 감지 모듈(110)는 웹페이지(20)에 인증폼이 있음을 감지하여, 마스터 인증 모듈(140)는 마스터 인증 정보 입력을 위한 대화 상자를 생성한 상태이다.

도 10의 오른쪽 아래 가장 자리에는 마스터 인증 유지 모듈이 윈도우즈 시스템 트레이 상태로 실행되고 있다.

도 11은 웹페이지 인증 정보를 입력 받기 위한 가상 키보드가 생성된 상태를 나타내는 도면이다.

웹페이지 인증 모듈(120)는 도 10에서와 같이 마스터 인증 모듈(140)에 의해 마스터 인증이 완료되면 인증 정보 저장 모듈(200)을 검색하여 해당 웹페이지(20)의 인증 정보를 검색하고, 검색 결과 해당 웹페이지(20)의 인증 정보가 없으면 도 11에서와 같이 가상 키보드를 생성한다.

도 11에 나타난 바와 같이, 웹페이지 인증 정보는 키보드의 누름에 의해 입력되지 않고 마우스의 클릭에 의해 입력되므로, 악성 BHO 등의 악성 프로그램이 키보드의 누름에 따라 발생하는 이벤트를 탈취하여 개인 정보를 취득하는 것을 막을 수 있다.

도 12는 의사 웹페이지 인증 정보로 웹페이지에 대한 인증이 수행되는 상태를 나타내는 도면이다.

도 11에 나타난 바와 같이, 가상 키보드로 실제의 웹페이지 인증 정보가 입력되었지만, 웹페이지 인증 모듈(120)는 실제의 웹페이지 인증 정보 대신에 의사 웹페이지 인증 정보를 웹페이지(20)에 표시하여 인증을 시도한다. 악성 BHO는 인터넷 익스플로러에 표시된 의사 웹페이지 인증 정보만을 취득할 수가 있어, 실제의 웹페이지 인증 정보는 보호된다.

도 13은 웹페이지에 대한 인증 절차가 완료된 상태를 나타내는 도면이다.

의사 웹페이지 인증 정보가 실제의 웹페이지 인증 정보로 대체되어 정상적인 인증이 이루어지는 절차는 앞서 설명한 바와 같다.

이때, 인터넷 익스플로러를 종료하면 해당 웹페이지(20)의 인증 세션은 종료된다. 그 후, 인터넷 익스플로러를 다시 실행하고 같은 웹페이지(20)를 다시 방문하면 마스터 인증 유지 모듈(300)이 실행되고 있으므로 사용자의 어떠한 액션도 없이 해당 웹페이지(20)에 대한 인증이 이루어지고 도 13과 같은 상태로 된다.

이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

발명의 효과

본 발명에 의한 안전 인증 방법 및 안전 인증을 수행하는 프로그램이 기록된 기록매체는 악성 프로그램에게는 의사 인증 정보만을 취득할 수 있도록 하여 웹페이지에 안전하게 인증을 할 수 있는 효과가 있다. 또한 웹페이지 인증 정보를 별도의 저장 공간에 저장함으로써 사용자에게 인증 정보의 관리를 용이하게 하고, 다시 방문하는 웹페이지에 별도의 인증 절차 없

이 인증할 수 있도록 함으로써 간단하게 인증할 수 있는 효과가 있다. 또한 다수의 마스터 인증 정보를 수용하여 하나의 컴퓨터에서 여러 명의 웹페이지 인증 정보가 관리될 수 있도록 함으로써 여러 명이 하나의 컴퓨터를 사용하면서도 각각 안전 인증이 가능하게 하는 효과가 있다.

(57) 청구의 범위

청구항 1.

브라우저에 표시되는 웹페이지에 안전 인증을 수행하는 프로그램이 기록된 기록매체에 있어서,

적어도 하나의 사용자에 관한 적어도 하나의 웹페이지 인증 정보를 저장하는 인증 정보 저장 모듈;

상기 웹페이지 인증 정보에 대한 접근 권한을 부여하는 마스터 인증을 수행하는 마스터 인증 모듈;

상기 웹페이지에 인증폼의 존재를 모니터링 하는 인증폼 감지 모듈;

상기 인증폼을 감지하면 의사 웹페이지 인증 정보로 웹페이지 인증을 수행하는 웹페이지 인증 모듈; 및

의사 웹페이지 인증 정보를 포함하는 웹페이지 요청 메시지를 가로채서 실제 웹페이지 인증 정보로 대체하여 정상적인 웹페이지 요청 메시지를 생성하는 함수 후킹 모듈을 포함하는 구조를 가진 프로그램이 기록된 기록매체.

청구항 2.

제1항에 있어서,

상기 인증폼 감지 모듈, 마스터 인증 모듈, 웹페이지 인증 모듈, 함수 후킹 모듈은 브라우저 기능 확장 모듈의 형태로 설치되는 프로그램이 기록된 기록매체.

청구항 3.

제2항에 있어서,

상기 인증폼 감지 모듈, 마스터 인증 모듈, 웹페이지 인증 모듈, 함수 후킹 모듈은 윈도우즈 운영체제에서 인터넷 익스플로러의 BHO의 형태로 설치되는 프로그램이 기록된 기록매체.

청구항 4.

제1항에 있어서,

소정의 마스터 인증 해제 조건이 발생하지 않으면 계속 마스터 인증을 유지하는 마스터 인증 유지 모듈을 더 포함하고,

상기 마스터 인증 모듈은 상기 마스터 인증 유지 모듈에 마스터 인증 유지 상태를 조회하고,

상기 마스터 인증 유지 모듈은 상기 마스터 인증 모듈에 마스터 인증 상태 정보를 보고하는 프로그램이 기록된 기록매체.

청구항 5.

제4항에 있어서,

상기 마스터 인증 유지 모듈은 마스터 인증 상태가 아니면 마스터 인증 정보를 입력받을 수 있는 대화 상자를 생성하는 프로그램이 기록된 기록매체.

청구항 6.

제5항에 있어서,

상기 인증 정보 저장 모듈은,

상기 마스터 인증 정보 별로 상기 웹페이지 인증 정보가 분류되어 저장되는 프로그램이 기록된 기록매체.

청구항 7.

제6항에 있어서,

상기 인증 정보 저장 모듈은,

상기 마스터 인증 정보를 키로 하여 상기 웹페이지 인증 정보가 암호화되어 저장되는 프로그램이 기록된 기록매체.

청구항 8.

제4항에 있어서,

상기 마스터 인증 유지 모듈은,

운영체제의 어플리케이션 프로그램의의 형태로 설치되는 프로그램이 기록된 기록매체.

청구항 9.

제8항에 있어서,

상기 마스터 인증 유지 모듈은,

실행되면 시스템 트레이(System Tray) 상태로 유지되는 프로그램이 기록된 기록매체.

청구항 10.

제4항에 있어서,

상기 소정의 마스터 인증 해제 조건은,

사용자에 의한 명시적인 요청 및 일정 시간의 경과 중 적어도 하나를 포함하는 프로그램이 기록된 기록매체.

청구항 11.

브라우저에 표시되는 웹페이지에의 안전 인증을 제공하는 방법에 있어서,

사용자를 고유하게 식별하는 마스터 인증 정보를 통해 마스터 인증을 제공하는 단계;

상기 웹페이지의 인증폼에 대한 모니터링을 제공하는 단계;

상기 인증폼이 감지되면 웹페이지에 대응하는 실제 웹페이지 인증 정보에 대한 검색을 제공하는 단계;

의사 웹페이지 인증 정보로 상기 웹페이지에 대한 인증을 제공하는 단계; 및

상기 의사 웹페이지 인증 정보로의 인증 시도를 가로채 상기 웹페이지에 대응하는 실제 웹페이지 인증 정보로의 대체를 제공하는 단계를 포함하는 안전 인증을 제공하는 방법.

청구항 12.

제11항에 있어서,

상기 실제 웹페이지 인증 정보의 저장을 제공하는 단계를 더 포함하고,

상기 저장을 제공하는 단계는,

마우스의 조작만으로 상기 웹페이지 인증 정보를 입력할 수 있는 가상 키보드를 제공하는 단계;

해당하는 웹페이지의 URL에 대응하여 상기 가상 키보드로 입력된 웹페이지 인증 정보에 대한 저장을 제공하는 단계를 포함하는 안전 인증을 제공하는 방법.

청구항 13.

제12항에 있어서,

상기 가상 키보드로 입력된 웹페이지 인증 정보에 대한 저장을 제공하는 단계는,

해당하는 웹페이지의 URL 및 상기 가상 키보드로 입력된 웹페이지 인증 정보를 상기 마스터 인증 정보를 키로 하여 암호화하여 저장하는 수단을 제공하고,

실제 웹페이지 인증 정보에 대한 검색을 제공하는 단계는,

상기 마스터 인증 정보를 키로 복호하여 실제 웹페이지 인증 정보에 대한 검색을 제공하는 안전 인증을 제공하는 방법.

청구항 14.

제11항에 있어서,

의사 웹페이지 인증 정보로 상기 웹페이지에 대한 인증을 제공하는 단계는,

의사 웹페이지 인증 정보를 포함하는 파라미터로 윈도우즈 API 함수인 HttpSendRequest 함수의 호출을 제공하고,

상기 실제 웹페이지 인증 정보로의 대체를 제공하는 단계는,

상기 HttpSendRequest 함수를 후킹하여 상기 파라미터에 포함된 의사 웹페이지 인증 정보를 상기 웹페이지에 대응하는 실제 웹페이지 인증 정보로의 대체를 제공하는 안전 인증을 제공하는 방법.

청구항 15.

제11항에 있어서,

상기 마스터 인증을 제공하는 단계는,

상기 마스터 인증 정보를 입력받기 위한 대화 상자를 제공하는 단계를 포함하는 안전 인증을 제공하는 방법.

청구항 16.

제11항에 있어서,

상기 웹페이지의 인증폼에 대한 모니터링을 제공하는 단계는,

상기 웹페이지에서 INPUT 태그의 추출을 제공하는 단계;

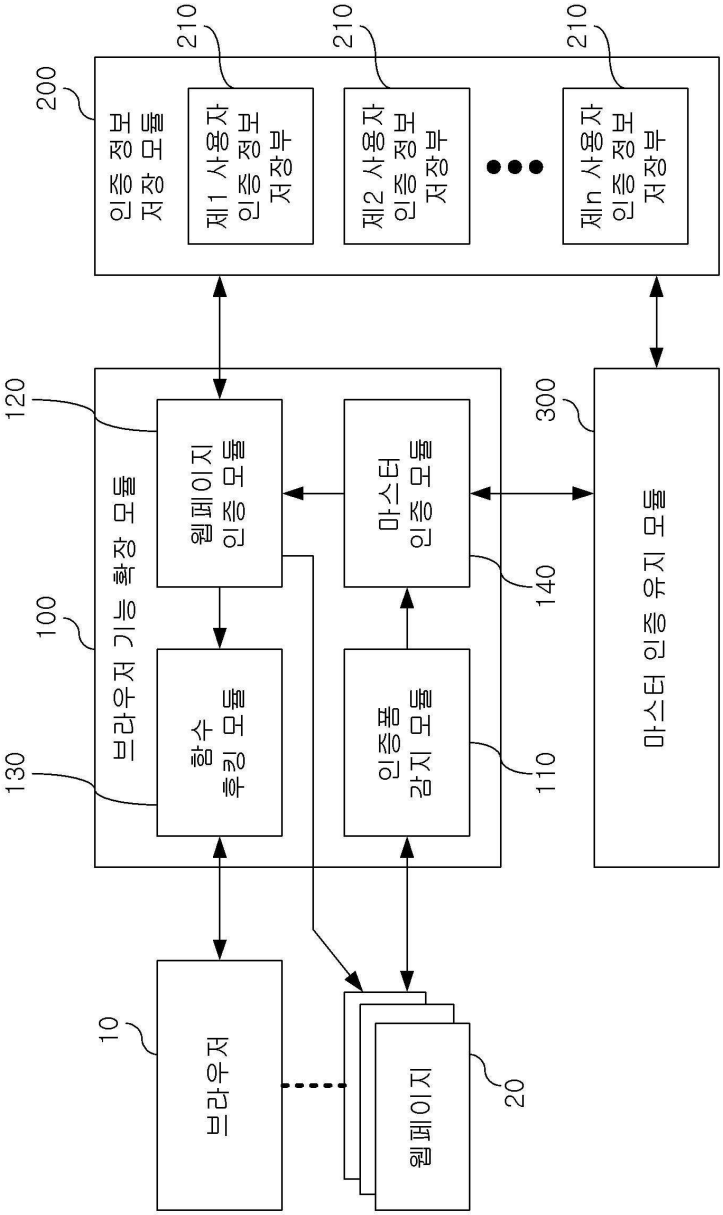
상기 추출된 INPUT 태그의 type 특성이 text인 경우 웹페이지 아이디의 입력부로의 판단을 제공하는 단계;

상기 추출된 INPUT 태그의 type 특성이 password인 경우 웹페이지 패스워드의 입력부로의 판단을 제공하는 단계;

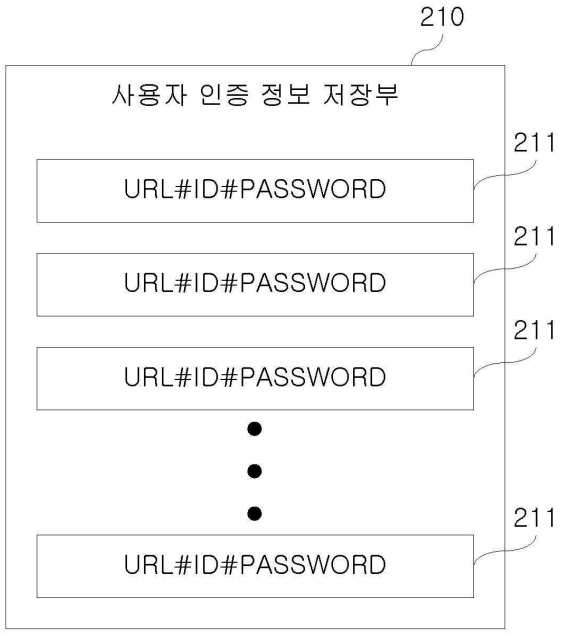
상기 웹페이지에서 상기 웹페이지 아이디의 입력부 또는 웹페이지 패스워드의 입력부를 발견하지 못한 경우 상기 웹페이지에 포함된 프레임에 해당하는 웹페이지에서 다시 인증폼에 대한 모니터링을 제공하는 단계를 포함하는 안전 인증을 제공하는 방법.

도면

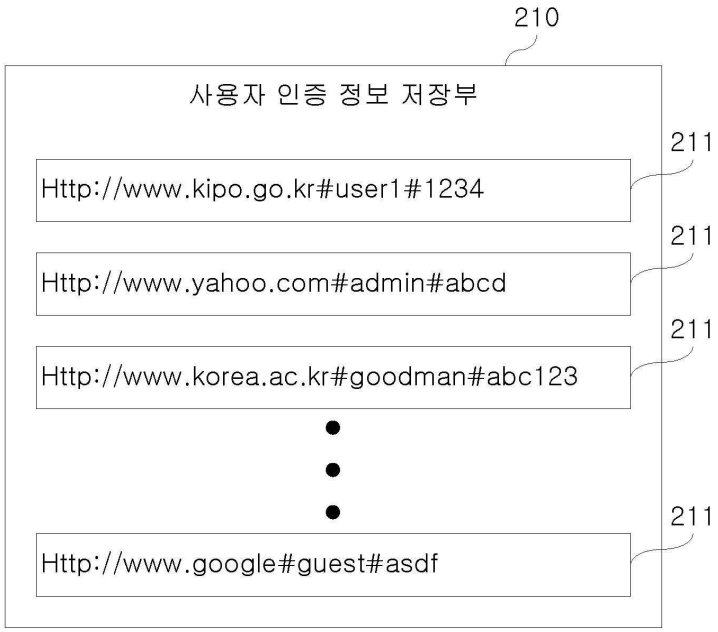
도면1


200
인증 정보
저장 모듈
210
제1 사용자
인증 정보
저장부
210
제2 사용자
인증 정보
저장부
210
제n 사용자
인증 정보
저장부
120
웹페이지
인증 모듈
마스터
인증 모듈
300
마스터 인증 유지 모듈
140
100
브라우저 기능 확장 모듈
130
함수
후킹 모듈
인증품
감지 모듈
110
10
브라우저
20
웹페이지

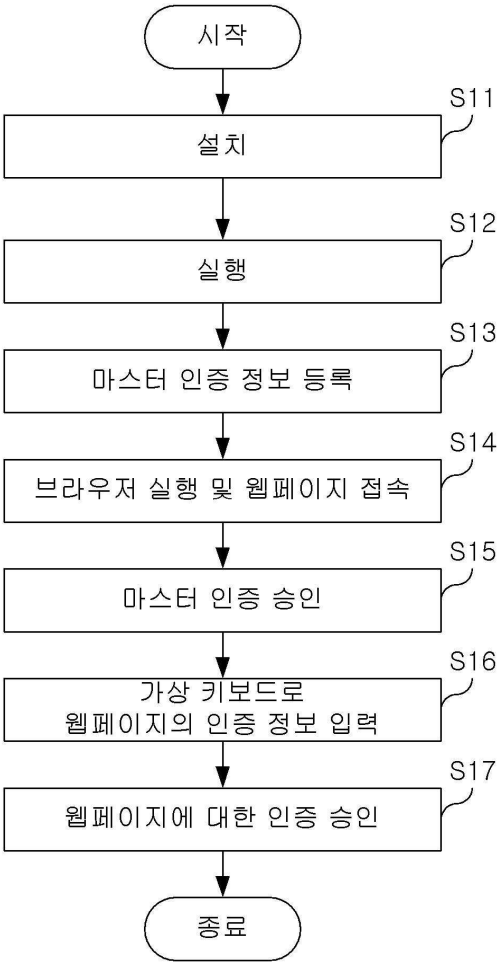
도면2


210
사용자 인증 정보 저장부
211
URL#ID#PASSWORD
211
URL#ID#PASSWORD
211
URL#ID#PASSWORD
211
URL#ID#PASSWORD

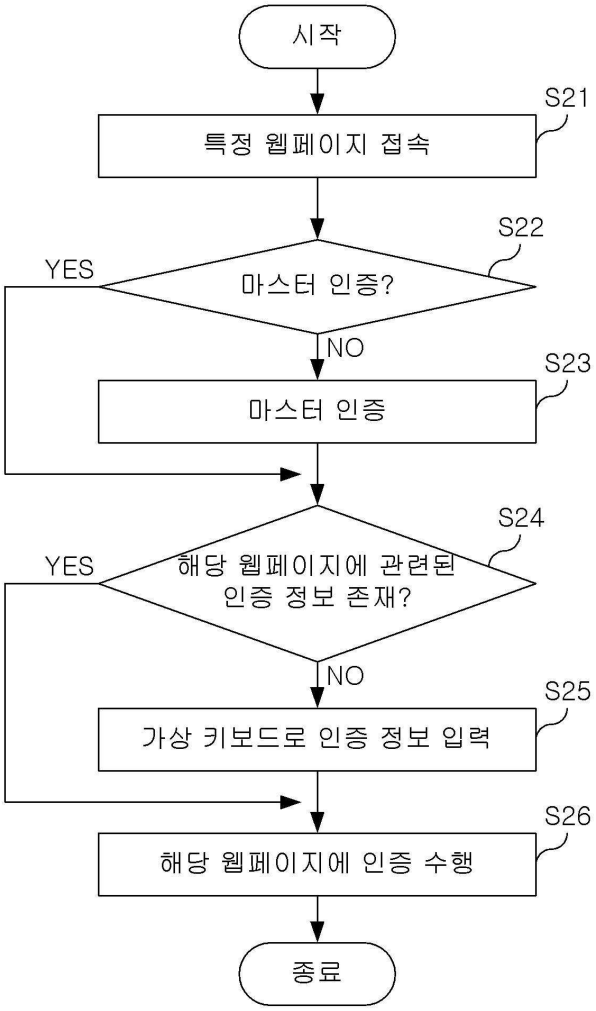
도면3


210
사용자 인증 정보 저장부
211
Http://www.kipo.go.kr#user1#1234
211
Http://www.yahoo.com#admin#abcd
211
Http://www.korea.ac.kr#goodman#abc123
211
Http://www.google#guest#asdf

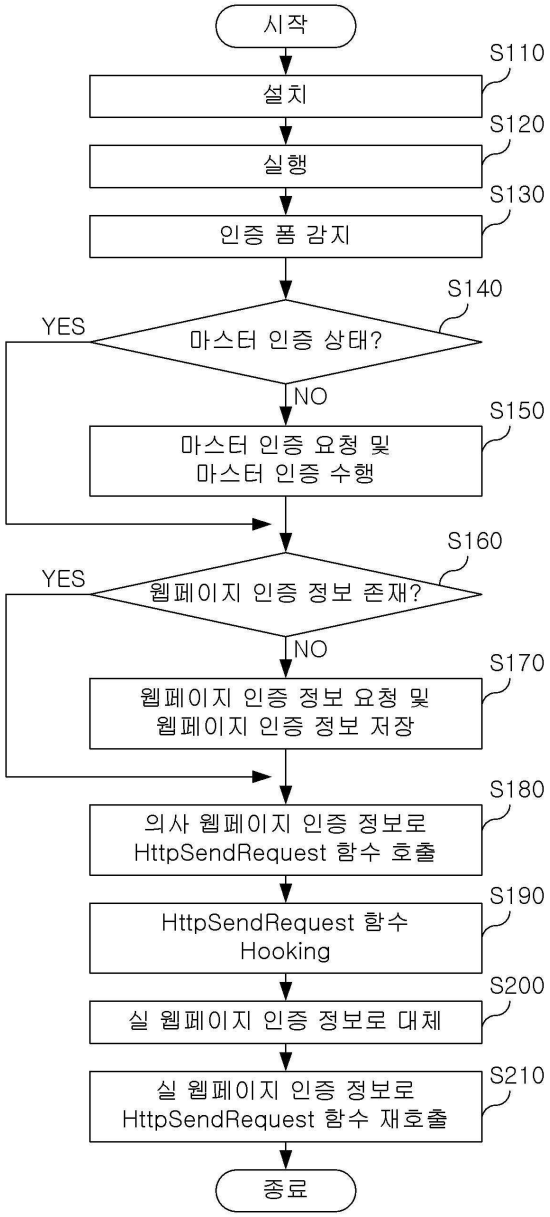
도면4


시작
S11
설치
S12
실행
S13
마스터 인증 정보 등록
S14
브라우저 실행 및 웹페이지 접속
S15
마스터 인증 승인
S16
가상 키보드로
웹페이지의 인증 정보 입력
S17
웹페이지에 대한 인증 승인
종료

도면5


시작
S21
특정 웹페이지 접속
S22
YES
마스터 인증?
NO
S23
마스터 인증
S24
YES
해당 웹페이지에 관련된
인증 정보 존재?
NO
S25
가상 키보드로 인증 정보 입력
S26
해당 웹페이지에 인증 수행
종료

도면6



도면7

```
<FORM>
<INPUT type="text" name="id"> <BR>
<INPUT type="password" name="pw"> <BR>
<INPUT type="submit">
</FORM>
```

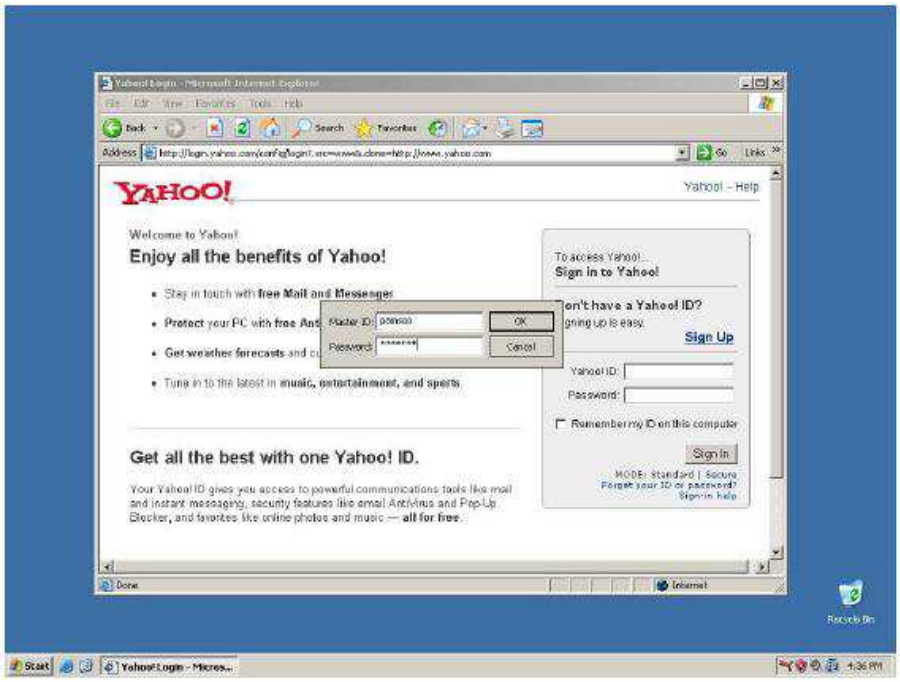
도면8

```
S300: Detect-Sign-in-Form(W,P_ID,P_PW)
S310:     I ← INPUT tags contained in W
S320:     FOR each I_K ∈ I
S330:        T_IK ← the type of I_K
S340:        IF T_IK= "text"
S350:           P_ID ← I_K
S360:        ELSE IF T_IK= "password"
S370:           P_PW ← I_K
S380:           return TRUE
S390:        ENDIF
S400:     ENDFOR
S410:     F ← FRAME and IFRAME tags contained in W
S420:     FOR each F_K ∈ F
S430:        V ← the documemt of F_K
S440:        IF Detect-Sign-in-Form(V,P_ID,P_PW)=TRUE
S450:           return TRUE
S460:        ENDIF
S470:     ENDFOR
S480:     return FALSE
S490: END of Detect-Sign-in-Form
```

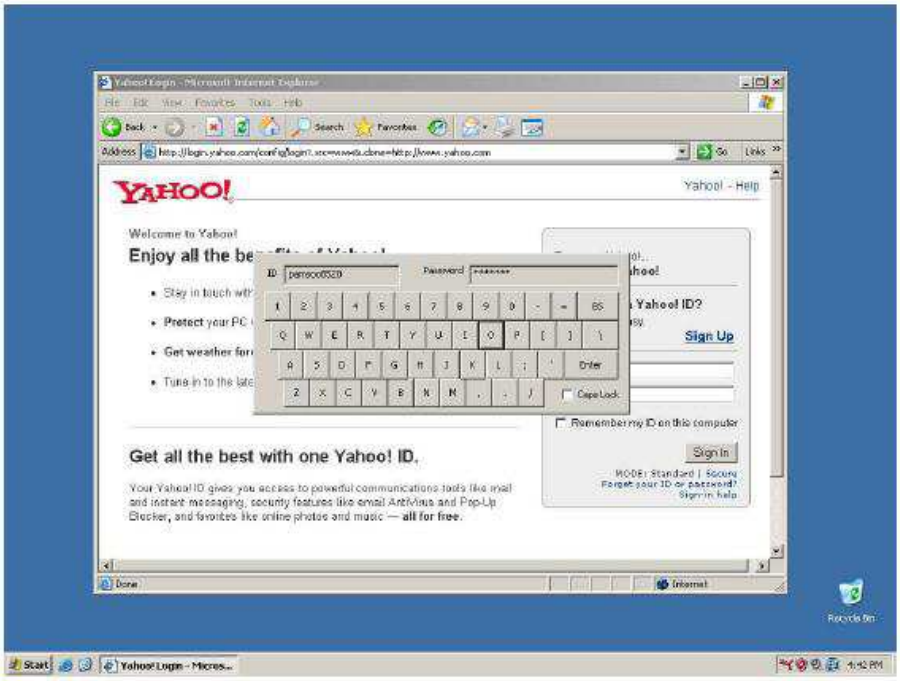
도면9

```
BOOL WINAPI HttpSendRequest(
      HINTERNET hRequest,
      LPCTSTR   lpszHeaders,
      DWORD     dwHeadersLength,
      LPVOID    lpOptional,
      DWORD     dwOptionalLength
);
```

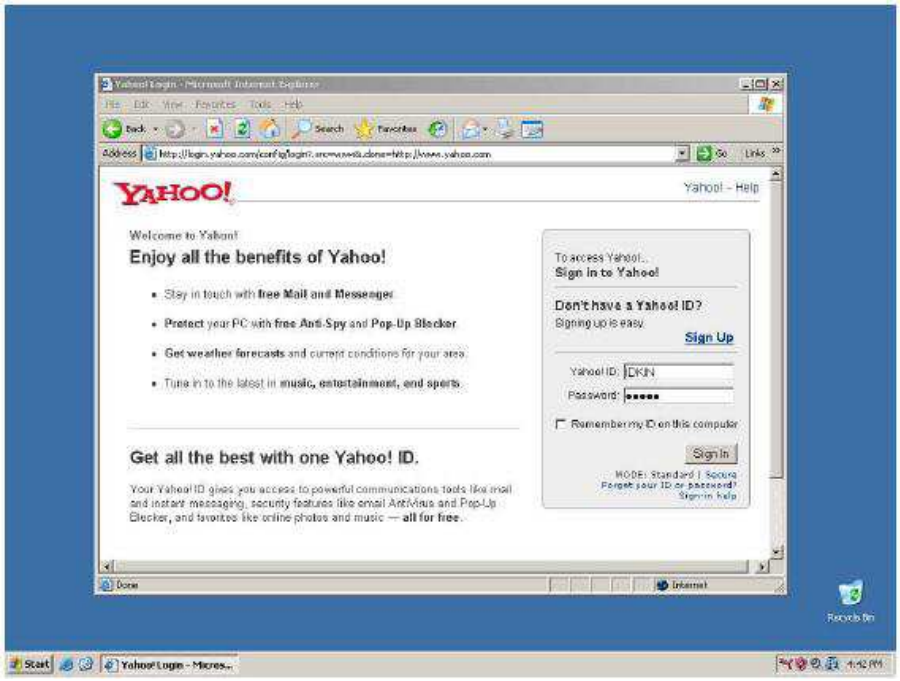
도면10


YAHOO!
Yahoo! - Help
Welcome to Yahoo!
Enjoy all the benefits of Yahoo!
Get all the best with one Yahoo! ID.
Sign Up
Sign In

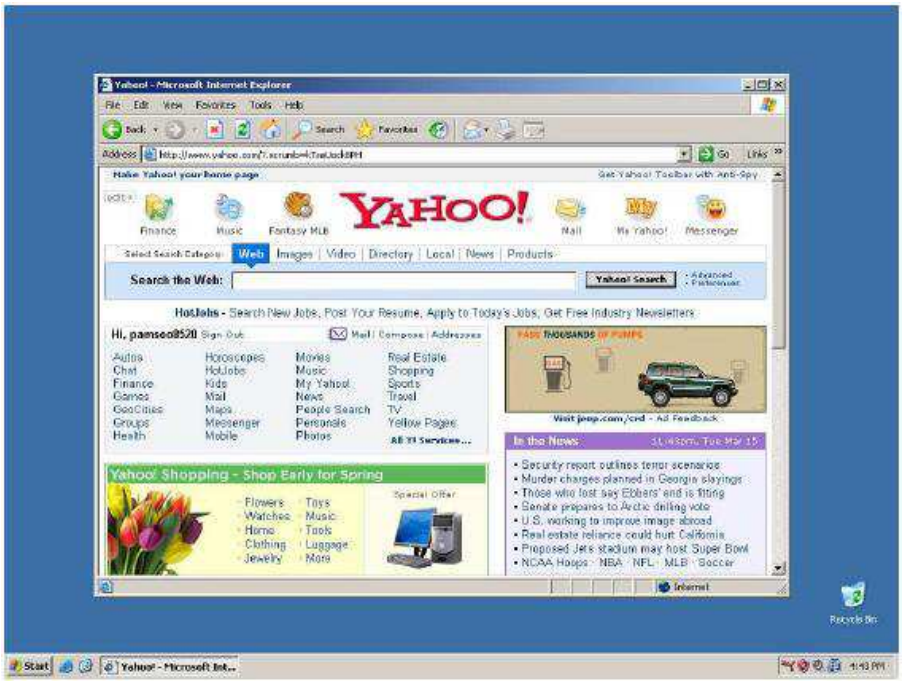
도면11


YAHOO!
Yahoo! - Help
Welcome to Yahoo!
Get all the best with one Yahoo! ID.
Sign Up
Sign In

도면12


YAHOO!
Yahoo! - Help
Welcome to Yahoo!
Enjoy all the benefits of Yahoo!
Stay in touch with free Mail and Messenger
Protect your PC with free Anti-Spy and Pop-Up Blocker
Get weather forecasts and current conditions for your area
Tune in to the latest in music, entertainment, and sports
Get all the best with one Yahoo! ID.
Your Yahoo! ID gives you access to powerful communications tools like mail and instant messaging, security features like email AntiVirus and Pop-Up Blocker, and favorites like online photos and music — all for free.
To access Yahoo!...
Sign in to Yahoo!
Don't have a Yahoo! ID?
Signing up is easy.
Sign Up
Yahoo! ID:
Password:
Remember my ID on this computer
Sign In

도면13


YAHOO!
Search the Web:
Yahoo! Search
Web
Images
Video
Directory
Local
News
Products
Hi, paeseo0520
Yahoo! Shopping - Shop Early for Spring
In the News