(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년05월06일
(11) 등록번호 10-0956452
(24) 등록일자 2010년04월28일

(51) Int. Cl.
G06F 15/00 (2006.01) *G06F 21/00* (2006.01)
(21) 출원번호 10-2008-0069341
(22) 출원일자 2008년07월16일
심사청구일자 2008년07월16일
(65) 공개번호 10-2010-0008729
(43) 공개일자 2010년01월26일
(56) 선행기술조사문헌
US20080046738 A1*
KR1020060022576 A
KR1020070067651 A
KR1020060019926 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초동 삼풍 ATP 3동 405호
김주현
충청북도 청주시 상당구 금천동 94-2번지
(74) 대리인
특허법인태동

전체 청구항 수 : 총 5 항 심사관 : 이종익

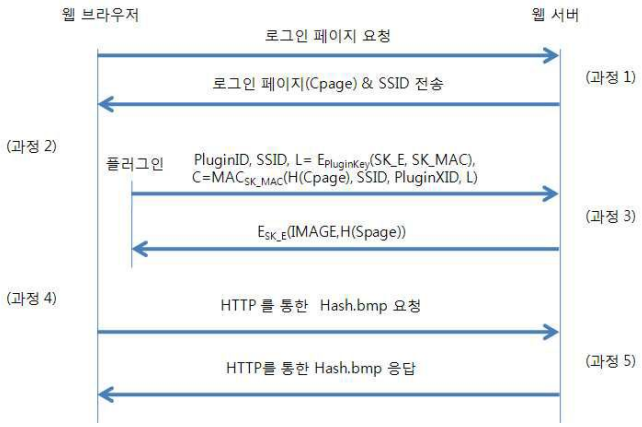
(54) 피싱공격 방지 방법

(57) 요 약

본 발명은 피싱공격 방지 방법에 관한 것으로서, 보다 구체적으로는 (1) 웹 브라우저에서, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시하는 단계; 및 (2) 사용자로 하여금 상기 축소 이미지와 상기 원본 이미지를 비교하도록 함으로써, 현재 웹 페이지가 피싱 사이트인지 여부를 확인하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명에서 제안하고 있는 피싱공격 방지 방법에 따르면, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시한 후, 사용자로 하여금 축소 이미지와 원본 이미지를 비교하는 것에 의해 현재 웹 페이지가 피싱 사이트인지 여부를 직접 확인하도록 함으로써, 자바 스크립트의 기능을 활용한 피싱 사이트를 원천적으로 차단할 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

(1) 웹 브라우저에서, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시하는 단계; 및

(2) 사용자로 하여금 상기 축소 이미지와 상기 원본 이미지를 비교하도록 함으로써, 현재 웹 페이지가 피싱 사이트인지 여부를 확인하는 단계를 포함하되,

상기 단계 (1)은,

a. 상기 웹 브라우저에서, 상기 웹 서버로부터 트레이에 표시할 축소 이미지와 함께 전송받은 웹 페이지에 대한 해시 값(H(Spage))과 자신이 가지고 있는 웹 페이지에 대한 해시 값(H(Cpage))을 비교하는 단계;

b. 상기 웹 브라우저에서, 상기 비교 결과, H(Cpage)와 H(Spage)가 동일하면 상기 웹 서버로부터 전송받은 축소 이미지를 웹 페이지의 트레이에 표시하고, 상기 웹 서버로 원본 이미지를 요청하는 단계; 및

c. 상기 웹 브라우저에서, 상기 웹 서버로부터 전송받은 상기 원본 이미지를 웹 페이지에 표시하는 단계

를 포함하는 것을 특징으로 하는 피싱공격 방지 방법.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 단계 b에서, 웹 페이지 코드 내에 있는 메서드를 통하여 원본 이미지를 요청하는 것을 특징으로 하는 피싱공격 방지 방법.

청구항 4

제1항에 있어서, 상기 단계 a 이전에,

(가) 상기 웹 브라우저에서, 상기 웹 서버로 웹 페이지를 요청하는 단계;

(나) 상기 웹 서버에서, 웹 페이지 및 세션 아이디를 생성하여 상기 웹 브라우저로 전송하고, 생성된 상기 웹 페이지를 해시하며, 생성된 상기 세션 아이디 및 상기 해시 값(H(Space))을 웹 페이지를 요청한 상기 웹 브라우저의 IP(Internet Protocol)와 함께 데이터베이스에 저장하는 단계;

(다) 상기 웹 브라우저에서, 수신한 웹 페이지에 포함된 코드에 의하여 플러그인을 실행시키는 단계;

(라) 상기 웹 브라우저에서, 플러그인이 웹 서버와 공유할 세션 키(SK)를 생성하고 생성된 상기 세션 키를 웹 서버와 공유하는 플러그인 고유키(PluginKey)를 이용하여 암호화한 후, 암호화된 세션 키, 플러그인 고유 아이디(PluginID), 상기 웹 서버로부터 전송받은 세션 아이디를 이용하여 메시지 인증 코드(MAC)를 생성하여, 암호화된 세션 키, 플러그인 고유 아이디(PluginID) 및 세션 아이디와 함께 상기 웹 서버로 전송하는 단계; 및

(마) 상기 웹 서버에서, 전송받은 메시지 인증 코드를 확인하여, 이상이 있으면 상기 플러그인으로 오류를 알리는 이미지를 전송하고, 이상이 없으면 전송받은 암호화된 세션 키를 상기 플러그인에 대한 플러그인 고유키를 이용하여 복호화한 후, 복호화된 세션 키를 이용하여 웹 페이지의 트레이에 표시할 축소 이미지를 데이터베이스에 저장된 상기 웹 페이지에 대한 해시 값(H(Space))과 함께 암호화하여 플러그인으로 전송하는 단계

를 더 포함하는 것을 특징으로 하는 피싱공격 방지 방법.

청구항 5

제4항에 있어서,

상기 단계 (마)에서, 상기 웹 브라우저로 전송한 축소 이미지에 대한 원본 이미지의 이름을 상기 웹 브라우저로 전송한 웹 페이지 및 세션 키를 해시한 값(H(Spage|SK))으로 변경하는 단계를 더 포함하는 것을 특징으로 하는

피싱공격 방지 방법.

청구항 6

제4항에 있어서, 플러그인이 처음 설치되는 경우이면, 상기 단계 (다)와 (라) 사이에,

(바) 상기 웹 브라우저에서, 플러그인이 자신이 사용할 플러그인 고유키(PluginKey)를 생성하고, 생성된 상기 플러그인 고유키를 웹 서버가 플러그인 배포 시에 사용한 공개키를 이용하여 암호화한 후, 이를 웹 서버로 전송하는 단계;

(사) 상기 웹 서버에서, 상기 웹 브라우저로부터 전송받은 암호화된 상기 플러그인 고유키를 개인키를 이용하여 복호화한 후, 플러그인 고유 아이디(PluginID)를 생성하여 상기 웹 브라우저로 전송하는 단계; 및

(아) 상기 웹 서버에서, 플러그인 고유 아이디를 플러그인 고유키와 함께 데이터베이스에 저장하는 단계

를 더 포함하는 것을 특징으로 하는 피싱공격 방지 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 피싱공격 방지 방법에 관한 것으로서, 보다 구체적으로는 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시한 후, 사용자로 하여금 축소 이미지와 원본 이미지를 비교하는 것에 의해 현재 웹 페이지가 피싱 사이트인지 여부를 직접 확인하도록 함으로써, 자바 스크립트의 기능을 활용한 피싱 사이트를 원천적으로 차단할 수 있는 피싱공격 방지 방법에 관한 것이다.

배 경 기 술

[0002] 피싱(phishing)이란, 금융기관 등의 웹사이트나 거기서 보내온 메일로 위장하여 개인의 인증번호나 신용카드번호, 계좌정보 등을 빼내 이를 불법적으로 이용하는 사기 수법을 말한다. 대표적인 피싱 수법으로는, 이메일의 발신자 이름을 금융기관의 창구 주소로 한 메일을 무차별적으로 보내는 것이 있다. 메일 본문에는 개인정보를 입력하도록 촉구하는 안내문과 웹사이트로의 링크가 기재되어 있는데, 링크를 클릭하면 그 금융기관의 정규 웹사이트와 개인정보입력용 팝업 윈도가 표시된다. 메인 윈도우에 표시되는 사이트는 진짜이지만, 팝업 페이지는 가짜이다. 진짜를 보고 안심한 사용자가 팝업에 표시된 입력란에 인증번호나 비밀번호, 신용카드번호 등의 비밀을 입력·송신하면 피싱을 하려는 자에게 정보가 송신된다. URL에 사용되는 특수한 서식을 이용하여, 마치 진짜 도메인에 링크되어 있는 것처럼 보이게 하거나, 팝업 윈도우의 어드레스 바를 비표시로 하는 등 교묘한 수법을 이용하고 있어 피해자가 속출하고 있다.

[0003] 기존의 피싱공격 방지 방법의 경우, 사용자가 스스로 피싱 사이트를 구별하는 방법이 아닌 피싱 사이트 방지 프로그램이 피싱 사이트인지 여부를 판단해주는 방식이었다. 이와 같은 방식에서는, 피싱 사이트가 아님을 알려주는 창을 자바스크립트를 이용하여 위조할 경우, 즉 가짜 창을 만들 경우, 일반인인 사용자가 구별하기가 쉽지 않아 사용자가 피싱공격에 그대로 노출될 수밖에 없다는 문제점이 있다. 실제로, 시중의 피싱 사이트 방지 프로그램의 팝업창을 그대로 복사하여 화면에 출력하는 방식으로 사용자를 속이는 피싱 사이트도 증가하고 있기에, 이에 대한 방지책이 요구된다.

발명의 내용

해결 하고자하는 과제

[0004] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시한 후, 사용자로 하여금 축소 이미지와 원본 이미지를 비교하는 것에 의해 현재 웹 페이지가 피싱 사이트인지 여부를 직접 확인하도록 함으로써, 자바 스크립트의 기능을 활용한 피싱 사이트를 원천적으로 차단할 수 있는 피싱공격 방지 방법을 제공하는 것을 그 목적으로 한다.

과제 해결수단

[0005] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 피싱공격 방지 방법은,

[0006] (1) 웹 브라우저에서, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지를 각각 웹 페이지의 트레이와 웹 페이지에 표시하는 단계; 및

[0007] (2) 사용자로 하여금 상기 축소 이미지와 상기 원본 이미지를 비교하도록 함으로써, 현재 웹 페이지가 피싱 사이트인지 여부를 확인하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

[0008] 바람직하게는, 상기 단계 (1)은,

[0009] a. 상기 웹 브라우저에서, 상기 웹 서버로부터 트레이에 표시할 축소 이미지와 함께 전송받은 웹 페이지에 대한 해시 값(H(Spage))과 자신이 가지고 있는 웹 페이지에 대한 해시 값(H(Cpage))을 비교하는 단계;

[0010] b. 상기 웹 브라우저에서, 상기 비교 결과, H(Cpage)와 H(Spage)가 동일하면 상기 웹 서버로부터 전송받은 축소 이미지를 웹 페이지의 트레이에 표시하고, 상기 웹 서버로 원본 이미지를 요청하는 단계; 및

[0011] c. 상기 웹 브라우저에서, 상기 웹 서버로부터 전송받은 상기 원본 이미지를 웹 페이지에 표시하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

[0012] 더욱 바람직하게는, 상기 단계 b에서, 웹 페이지 코드 내에 있는 메서드를 통하여 원본 이미지를 요청할 수 있다.

[0013] 더욱 바람직하게는, 상기 단계 a 이전에,

[0014] (가) 상기 웹 브라우저에서, 상기 웹 서버로 웹 페이지를 요청하는 단계;

[0015] (나) 상기 웹 서버에서, 웹 페이지 및 세션 아이디를 생성하여 상기 웹 브라우저로 전송하고, 생성된 상기 웹 페이지를 해시하며, 생성된 상기 세션 아이디 및 상기 해시 값(H(Space))을 웹 페이지를 요청한 상기 웹 브라우저의 IP(Internet Protocol)와 함께 데이터베이스에 저장하는 단계;

[0016] (다) 상기 웹 브라우저에서, 수신한 웹 페이지에 포함된 코드에 의하여 플러그인(Plugin)을 실행시키는 단계;

[0017] (라) 상기 웹 브라우저에서, 플러그인이 웹 서버와 공유할 세션 키(SK)를 생성하고 생성된 상기 세션 키를 웹 서버와 공유하는 플러그인 고유키(PluginKey)를 이용하여 암호화한 후, 암호화된 세션 키, 플러그인 고유 아이디(PluginID), 상기 웹 서버로부터 전송받은 세션 아이디를 이용하여 메시지 인증 코드(MAC)를 생성하여, 암호화된 세션 키, 플러그인 고유 아이디(PluginID) 및 세션 아이디와 함께 상기 웹 서버로 전송하는 단계; 및

[0018] (마) 상기 웹 서버에서, 전송받은 메시지 인증 코드를 확인하여, 이상이 있으면 상기 플러그인으로 오류를 알리는 이미지를 전송하고, 이상이 없으면 전송받은 암호화된 세션 키를 상기 플러그인에 대한 플러그인 고유키를 이용하여 복호화한 후, 복호화된 세션 키를 이용하여 웹 페이지의 트레이에 표시할 축소 이미지를 데이터베이스에 저장된 상기 웹 페이지에 대한 해시 값(H(Space))과 함께 암호화하여 플러그인으로 전송하는 단계를 더 포함할 수 있다.

[0019] 더더욱 바람직하게는, 상기 단계 (마)에서, 상기 웹 브라우저로 전송한 축소 이미지에 대한 원본 이미지의 이름을 상기 웹 브라우저로 전송한 웹 페이지 및 세션 키를 해시한 값(H(Spage|SK))으로 변경하는 단계를 더 포함할 수 있다.

[0020] 더더욱 바람직하게는, 플러그인이 처음 설치되는 경우이면, 상기 단계 (다)와 (라) 사이에,

[0021] (바) 상기 웹 브라우저에서, 플러그인이 자신이 사용할 플러그인 고유키(PluginKey)를 생성하고, 생성된 상기 플러그인 고유키를 웹 서버가 플러그인 배포 시에 사용한 공개키를 이용하여 암호화한 후, 이를 웹 서버로 전송하는 단계;

[0022] (사) 상기 웹 서버에서, 상기 웹 브라우저로부터 전송받은 암호화된 상기 플러그인 고유키를 개인키를 이용하여 복호화한 후, 플러그인 고유 아이디(PluginID)를 생성하여 상기 웹 브라우저로 전송하는 단계; 및

[0023] (아) 상기 웹 서버에서, 플러그인 고유 아이디를 플러그인 고유키와 함께 데이터베이스에 저장하는 단계를 더 포함할 수 있다.

효 과

[0024] 본 발명에서 제안하고 있는 피싱공격 방지 방법에 따르면, 웹 서버로부터 전송받은 축소 이미지와 원본 이미지

를 각각 웹 페이지의 트레이와 웹 페이지에 표시한 후, 사용자로 하여금 축소 이미지와 원본 이미지를 비교하는 것에 의해 현재 웹 페이지가 피싱 사이트인지 여부를 직접 확인하도록 함으로써, 자바 스크립트의 기능을 활용한 피싱 사이트를 원천적으로 차단할 수 있다.

발명의 실시를 위한 구체적인 내용

[0025] 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

[0026] 도 1은 본 발명의 일 실시예에 따른 웹 브라우저와 웹 서버 간의 암호화 키 및 이미지 교환 프로토콜을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 피싱공격 방지 방법은, 웹 브라우저와 웹 서버 간의 암호화 키 및 이미지 교환 과정에 의하여 구현된다. 본 발명의 일 실시예에 따른 피싱공격 방지 방법은 다음과 같은 과정들로 구성될 수 있다.

[0027] 과정 1.

[0028] 사용자가 웹 브라우저를 통하여 웹 페이지를 웹 서버에 요청하면, 웹 서버는 도 1의 (과정 1)에서 웹 브라우저에 전송할 웹 페이지 및 세션 아이디를 생성한다. 생성된 웹 페이지를 해시하여 해시 값(H(Spage))을 계산하고, 계산된 해시 값을 세션 아이디 및 웹 페이지를 요청한 웹 브라우저의 IP(Internet Protocol)와 함께 데이터베이스에 저장한다. 이 과정에서, 웹 서버는, 도 1에 도시된 바와 같이, 웹 페이지(Cpage)와 세션 아이디를 웹 브라우저로 전송한다.

[0029] 과정 2.

[0030] 웹 브라우저는 웹 서버로부터 생성된 웹 페이지를 전송받고, 또한 쿠키를 통하여 세션 아이디를 전송받는다. 웹 서버로부터 전송받은 웹 페이지에는 플러그인을 실행시키는 코드가 포함되어 있으며, 그 결과 플러그인을 실행시키게 된다. 도 1의 (과정 2)에서, 플러그인은 웹 서버와 공유할 세션 키(Session Key; SK)를 생성한다. 생성된 세션 키를 웹 서버와 공유하고 있는 플러그인의 고유키를 이용하여 암호화한 후, 플러그인의 고유 아이디, 웹 서버로부터 전송받은 세션 아이디, 및 메시지 인증 코드와 함께 전송한다. 여기서, 메시지 인증 코드(MAC)는, 도 1에 도시된 바와 같이, 암호화된 세션 키, 플러그인의 고유 아이디, 세션 아이디 및 웹 페이지의 해시 값에 기초하여 세션 키(SK)를 이용하여 생성된다.

[0031] 플러그인이 웹 서버와 플러그인의 고유 아이디(PluginID), 및 플러그인의 고유키(PluginKey)를 공유하는 과정을 도 2를 참조하여 설명하기로 한다. 도 2는 본 발명의 일 실시예에 따라서, 플러그인 설치 후 첫 실행 시 수행되는 웹 브라우저와 웹 서버 간의 암호화 키 및 이미지 교환 프로토콜을 나타내는 도면이다.

[0032] 플러그인이 최초로 설치되는 경우에, 도 2의 (과정 1)에서 자신이 사용할 고유키(Pluginkey)를 생성하여 웹 서버에서 플러그인 배포 시에 사용한 공개키를 이용하여 암호화한 후, 이를 웹 서버로 전송한다. 웹 서버는 개인키로 이를 복호화하여, 웹 서버에서 생성한 고유 아이디(PluginID)와 함께 데이터베이스에 저장한 후, 플러그인으로 고유 아이디(PluginID)를 전송한다. 이와 같은 과정을 통하여, 플러그인과 웹 서버는 플러그인 고유키와 플러그인 고유 아이디를 공유할 수 있게 된다.

[0033] 과정 3.

[0034] 웹 서버는 우선 플러그인으로부터 받은 메시지 인증 코드(MAC)를 확인하여, 이상이 있으면 플러그인에 오류를 알리는 이미지를 전송하게 된다. 만약, 메시지 인증 코드(MAC)에 이상이 없다면, 웹 서버는 플러그인으로부터 받은 암호화된 세션 키를 웹 서버에 저장되어 있는 플러그인의 아이디에 지정된 플러그인 고유키(PluginKey)를 이용하여 복원하고, 복원된 세션 키 이용하여 웹 페이지의 트레이(tray)에 표시할 축소 이미지를, 데이터베이스에 저장되어 있는 웹 페이지의 해시 값(H(Spage))과 함께 플러그인으로 전송한다. 추가로, 웹 서버는 플러그인으로 전송한 축소 이미지에 대한 원본 이미지의 이름을 Spage와 세션 키(SK)를 해시한 이름으로 변경한다(Image.bmp -> H(Spage|SK)).

[0035] 과정 4.

[0036] 플러그인은 도 1의 (과정 4)에서, 먼저 웹 서버로부터 받은 내용을 세션 키를 이용하여 복호화한 후, 복호화한 내용 중 H(Spage)를 자신이 가지고 있는 H(Cpage)와 비교한다. 비교 결과, H(Spage)와 H(Cpage)가 동일하면, 웹 서버로부터 올바른 내용을 받은 것이므로 웹 서버로부터 받은 이미지를 웹 페이지의 트레이에 표시하게 된다. 그리고 웹 페이지 코드 내에 있는 메서드를 통하여 원본 이미지(H(Spage|SK).bmp) 파일을 웹 서버에 요청하게 된다. 요청하는 원본 이미지는 웹 페이지에 표시될 그림이며, 앞서 설명한 바와 같이 과정 3에서 웹 서버에서 생성된 바 있다.

[0037] 과정 5.

[0038] 웹 서버는 이미 H(Spage|SK).bmp를 가지고 있으므로 웹 브라우저의 이미지 요청에 응답하게 되고, 이에 따라 웹 브라우저는 정상적인 이미지를 출력하게 된다. 최종적으로, 사용자는 트레이에 표시되는 축소 이미지와 웹 페이지 내에 표시되는 원본 이미지를 비교함으로써, 현재 웹 페이지가 피싱 사이트인지 여부를 직접 판단할 수 있게 된다.

[0039] 도 3은 본 발명의 일 실시예에 따른 예시 화면을 나타내는 도면이다. 도 3의 좌측 웹 페이지는 정상적인 웹 페이지를 나타내며, 우측 웹 페이지는 비정상적인 웹 페이지, 즉 피싱 사이트를 나타낸다. 도 3의 좌측에 도시된 바와 같이, 정상적인 웹 사이트의 경우, 웹 페이지의 트레이에 표시될 축소 이미지와 웹 페이지 내에 표시될 원본 이미지가 동일한 이미지여서 사용자가 손쉽게 정상적인 사이트임을 확인할 수 있다. 이에 비하여, 도 3의 우측에 도시된 바와 같이, 비정상적인 웹 사이트, 즉 피싱 사이트인 경우, 웹 페이지 내에 표시될 원본 이미지 자리에 그림 없음 표시나 경고 이미지가 표시되어 사용자가 손쉽게 피싱 사이트임을 확인할 수 있다.

[0040] 이상 설명한 바와 같이, 본 발명은 피싱 사이트를 이미지 비교를 통하여 사용자가 직접 판단하도록 한 것으로서, 팝업 방식을 이용하는 것이 아닌 트레이의 기능 가운데 풍선 도움말 기능을 이용함으로써 자신의 컴퓨터에 있는 프로그램이 직접 이미지를 보여준다는 신뢰감을 주는 동시에, 웹 서버로부터 온 HTML 코드를 해시 과정을 통하여 비교하는 과정에서 HTML 코드에 대한 신뢰성을 보장하게 된다. 또한, 본 발명은, 플러그인의 Browser Control과 각종 암호화 알고리즘을 이용하여 보안의 신뢰성을 높였다.

[0041] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

도면의 간단한 설명

[0042] 도 1은 본 발명의 일 실시예에 따른 웹 브라우저와 웹 서버 간의 암호화 키 및 이미지 교환 프로토콜을 나타내는 도면.

[0043] 도 2는 본 발명의 일 실시예에 따라서, 플러그인 설치 후 첫 실행 시 수행되는 웹 브라우저와 웹 서버 간의 암호화 키 및 이미지 교환 프로토콜을 나타내는 도면.

[0044] 도 3은 본 발명의 일 실시예에 따른 예시 화면을 나타내는 도면.

[0045] <도면 중 주요 부분에 대한 부호의 설명>

[0046] 플러그인ID: 클라이언트(웹 브라우저)의 플러그인에 주어지는 고유 아이디

[0047] 플러그인Key: 클라이언트(웹 브라우저)의 플러그인에 주어지는 고유키

[0048] SSID: 웹 서버에서 클라이언트(웹 브라우저)에 전달하는 세션 아이디

[0049] SK_E: 웹 서버와 클라이언트(웹 브라우저)에서 공유하는 세션 키

[0050] SK_MAC: 웹 서버와 클라이언트(웹 브라우저)에서 공유하는 MAC을 위한 세션 키

[0051] Cpage: 웹 서버가 클라이언트(웹 브라우저)에게 전송하는 로그인 페이지

[0052] Spage: 웹 서버가 클라이언트(웹 브라우저)에게 전송하기 위해 생성한 페이지

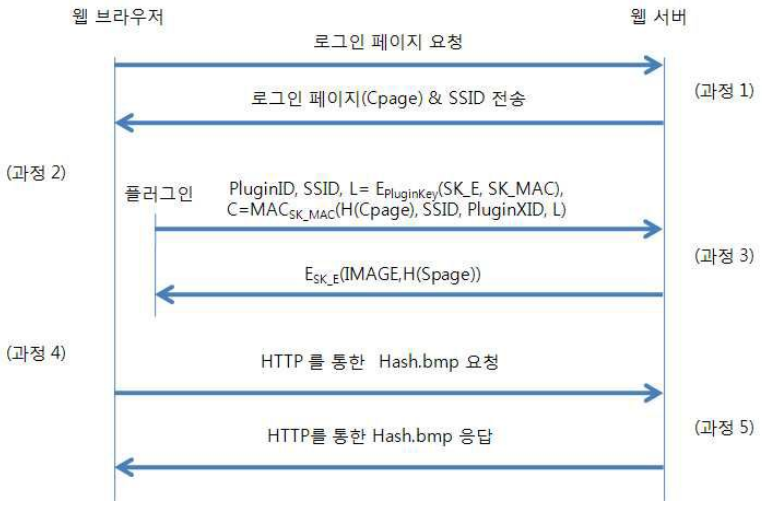
[0053] H( ): 해시 함수

[0054] E_{SK_E}( ): SK_E를 이용한 암호화 함수

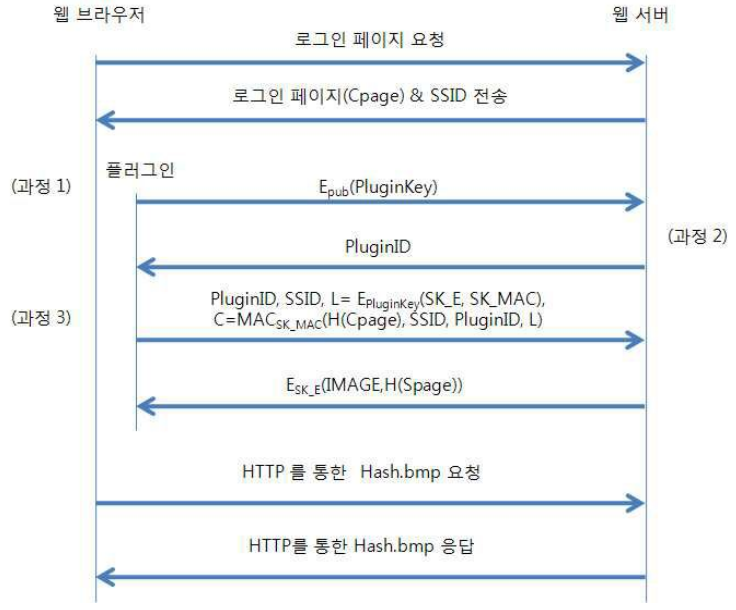
[0055] MAC_{SK_MAC}( ): SK_MAC를 이용한 메시지 인증 코드

도면

도면1



도면2



도면3


이용자 아이디 로그인
아이디
비밀번호
아이디 로그인
주의하세요 !
이용자 아이디는 영문 또는 영문+숫자
6~10자리로 구성되어 있습니다.
바이오 인증 바로가기
세금/공과금 납부 안내
분실신고 안내
계좌관리서비스
조회계좌등록/삭제
출금계좌등록/삭제
자주쓰는입금계좌관리
1일이체한도조회/축소
통지/부가서비스
SMS우리통지서비
E-MAIL우리통지서
포인트조회/사은품
증명서발급서비스
우리은행 -...