(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년12월15일
(11) 등록번호 10-1001765
(24) 등록일자 2010년12월09일

(51) Int. Cl.
G06F 21/20 (2006.01)
(21) 출원번호 10-2008-0120593
(22) 출원일자 2008년12월01일
심사청구일자 2008년12월01일
(65) 공개번호 10-2010-0062144
(43) 공개일자 2010년06월10일
(56) 선행기술조사문헌
KR1020060097583 A
KR100668446 B1
KR1020010097608 A
KR1020000028706 A

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
엔에이치엔비즈니스플랫폼 주식회사
경기 성남시 분당구 서현동 266-1 퍼스트타워 9층
(72) 발명자
조상현
서울특별시 양천구 목6동 목동2단지아파트 219동 1507호
임만기
서울특별시 관악구 신림2동 102-23 301호
(뒷면에 계속)
(74) 대리인
황광연, 강동호, 오정환, 특허법인무한

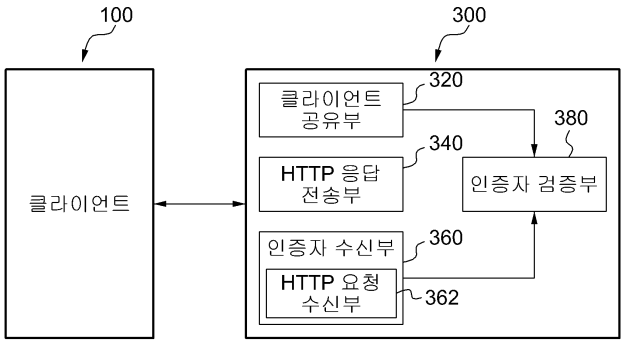
전체 청구항 수 : 총 20 항 심사관 : 신상길

(54) 씨드 공유를 이용한 클라이언트 인증 방법 및 시스템

(57) 요 약

본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 방법은 키(Key) 및 씨드(Seed)를 클라이언트와 공유하는 단계; 상기 클라이언트에 의해 상기 키 및 씨드를 이용하여 생성된 인증자 및 상기 인증자에 대한 카운터를 수신하는 단계; 및 상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하고, 상기 인증자가 사용되지 않은 경우 상기 인증자를 검증하는 단계를 포함한다.

대 표 도 - 도2



(72) 발명자

송민철

서울특별시 중구 신당4동 약수하이츠아파트 108-2005

백종원

경기도 수원시 팔달구 우만동 300 주공 APT 403동 1007호

이성호

경기도 성남시 분당구 야탑동 342-2 르네상스 오피스텔

정영식

경기도 용인시 기흥구 마북동 연원마을현대아파트 104동 1501호

하태기

서울특별시 강남구 청담2동 5-25 청담휴먼스타빌 2701호

양대헌

인천광역시 남구 용현4동 인하대학교 하이테크센터 317호

강전일

충청남도 공주시 옥룡동 284-1

맹영재

서울특별시 광진구 자양1동 226-12호

특허청구의 범위

청구항 1

클라이언트 인증 시스템의 클라이언트 인증 방법에 있어서,

상기 클라이언트 인증 시스템이 클라이언트 공유부, 인증자 수신부 및 인증자 검증부를 포함하여,

상기 클라이언트 인증 방법은,

상기 클라이언트 공유부에서 키(Key) 및 씨드(Seed)를 클라이언트와 공유하는 단계;

상기 인증자 수신부에서 상기 클라이언트에 의해 상기 키 및 씨드를 이용하여 생성된 인증자 및 상기 인증자에 대한 카운터를 수신하는 단계; 및

상기 인증자 검증부에서 상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하고, 상기 인증자가 사용되지 않은 경우 상기 인증자를 검증하는 단계

를 포함하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 2

제 1 항에 있어서,

상기 클라이언트 공유부가 씨드 생성부와 씨드 공유부를 포함하여,

상기 공유하는 단계는,

상기 씨드 생성부에서 상기 키 및 씨드를 생성하는 단계; 및

상기 씨드 공유부에서 상기 생성된 키 및 씨드를 키 동의(Key Agreement) 또는 키 전송(Key Transportation) 방식을 통해 상기 클라이언트와 공유하는 단계

를 포함하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 3

제 1 항에 있어서, 상기 키 및 씨드는

상기 클라이언트와 서버에 각각 따로 저장되며,

상기 클라이언트에는 플러그인(plugin)을 요구하지 않는 웹 브라우저 저장소에 저장되는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 4

제 1 항에 있어서,

상기 클라이언트 인증 시스템이 HTTP 응답 전송부를 더 포함하여,

상기 클라이언트 인증 방법은,

상기 HTTP 응답 전송부에서 상기 클라이언트로 HTTP 응답을 전송하는 단계를 더 포함하며,

상기 HTTP 응답에는 상기 인증자 생성에 관한 클라이언트 사이드 스크립트(Client Side Script)가 포함되어 있는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 5

제 1 항에 있어서,

상기 클라이언트 인증 시스템이 HTTP 요청 수신부를 더 포함하여,

상기 클라이언트 인증 방법은,

상기 HTTP 요청 수신부에서 상기 클라이언트의 HTTP 요청과 함께 상기 인증자 및 카운터를 수신하는 단계

를 더 포함하고,

상기 인증자는 상기 클라이언트에서 HTTP 응답 수신 후 미리 생성되어 상기 카운터와 함께 쿠키에 저장되는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 6

제 1 항에 있어서, 상기 카운터는

상기 인증자가 생성될 때마다 증가하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 7

제 1 항에 있어서, 상기 인증자는

상기 카운터 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 8

제 1 항에 있어서, 상기 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우,

상기 인증자는 상기 적어도 하나의 아이프레임 별로 상기 카운터, 상기 아이프레임의 URL 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 9

제 8 항에 있어서,

상기 인증자 및 카운터는,

URL 주소에 데이터를 포함시켜 전송하는 방식인 GET 형식에 따라 상기 아이프레임의 URL에 포함된 형태로 수신되는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 10

제 1 항에 있어서, 상기 인증자를 검증하는 단계는

상기 수신된 카운터 및 상기 공유된 키 및 씨드를 이용한 해쉬값과 상기 클라이언트로부터 전송된 인증자가 일치하는지 여부를 판단하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 방법.

청구항 11

제 1 항 내지 제 10 항 중 어느 하나의 항에 기재된 방법을 수행하기 위한 프로그램이 기록된 기록매체.

청구항 12

키(Key) 및 씨드(Seed)를 클라이언트와 공유하는 클라이언트 공유부;

상기 클라이언트에 의해 상기 키 및 씨드를 이용하여 생성된 인증자 및 상기 인증자에 대한 카운터를 수신하는 인증자 수신부; 및

상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하고, 상기 인증자가 사용되지 않은 경우 상기 인증자를 검증하는 인증자 검증부를 포함하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 13

제 12 항에 있어서, 상기 클라이언트 공유부는

상기 키 및 씨드를 생성하는 씨드 생성부;

상기 생성된 키 및 씨드를 키 동의(Key Agreement) 또는 키 전송(Key Transportation) 방식을 통해 상기 클라이언트와 공유하는 씨드 공유부; 및

상기 키 및 씨드를 저장하는 저장부를 포함하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스

템.

청구항 14

제 12 항에 있어서,

상기 클라이언트로 HTTP 응답(response)을 전송하는 HTTP 응답 전송부를 더 포함하며,

상기 HTTP 응답에는 상기 인증자 생성에 관한 클라이언트 사이트 스크립트(Client Side Script)가 포함되어 있는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 15

제 12 항에 있어서, 상기 인증자 수신부는

상기 클라이언트의 HTTP 요청(request)과 함께 상기 인증자 및 카운터를 수신하는 HTTP 요청 수신부를 포함하며,

상기 인증자는 상기 클라이언트에서 HTTP 응답 수신 후 미리 생성되어 상기 카운터와 함께 쿠키에 저장되는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 16

제 12 항에 있어서, 상기 카운터는

상기 인증자가 생성될 때마다 증가하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템

청구항 17

제 12 항에 있어서, 상기 인증자는

상기 카운터 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 18

제 12 항에 있어서, 상기 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우,

상기 인증자는 상기 적어도 하나의 아이프레임 별로 상기 카운터, 상기 아이프레임의 URL 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 19

제 18 항에 있어서,

상기 인증자 및 카운터는,

URL 주소에 데이터를 포함시켜 전송하는 방식인 GET 형식에 따라 상기 아이프레임의 URL에 포함된 형태로 수신되는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

청구항 20

제 12 항에 있어서, 상기 인증자 검증부는

상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하는 카운터 확인부;

상기 인증자가 사용되지 않은 경우 상기 수신된 카운터 및 상기 공유된 키 및 씨드를 이용한 해쉬값을 산출하는 해쉬 연산부; 및

상기 산출된 해쉬값과 상기 클라이언트로부터 전송된 인증자가 일치하는지 여부를 판단하는 인증자 판단부를 포함하는 것을 특징으로 하는 씨드 공유를 이용한 클라이언트 인증 시스템.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 클라이언트 인증 방법에 관한 것으로서 보다 상세하게는 씨드 공유를 이용하여 서버에 대한 클라이언트 인증 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 쿠키는 종래의 세션(session) 개념이 없던 서버와 클라이언트 사이의 통신 문제를 해결하기 위하여 웹 페이지에서 클라이언트에 기록하는 데이터로서, 이러한 데이터를 사용하여 사이트의 아이디(ID)와 패스워드(password)를 기억하고 자동으로 입력하도록 설정할 수 있다. 따라서, 웹 브라우저에서 웹 페이지가 바뀌더라도 어떠한 데이터를 그래도 유지하는 방법은 쿠키가 유일한 것으로 알려져 왔다.

[0003] 이와 같은 쿠키의 성질로 인해 일반적으로 클라이언트와 서버 사이에서 쿠키를 이용한 통신이 주로 이루어지며, 이때 HTTP 응답(Response) 및 요청(Request)의 헤더(header)를 통해 이루어진다. 이에 대해 자세히 설명하면, ① 서버가 쿠키 데이터를 생성하고 HTTP 응답 헤더를 통해 클라이언트에 전송하고, ② 클라이언트는 수신된 쿠키를 저장하고 HTTP 요청이 조건(domain, path, expire, secure)을 만족하면 HTTP 요청 헤더에 자동으로 첨부한다.

[0004] 그러나, 이러한 쿠키를 이용한 클라이언트와 서버 사이의 통신에 있어서 기존의 쿠키를 이용한 인증자(authenticator)가 사용자의 세션이 종료할 때까지 동일한 인증자를 받아들이도록 설계되어 있기 때문에, 공격자는 ①, ② 중 하나만 도청해도 쉽게 인증자를 취할 수 있고 인증자를 재전송 공격에 이용할 수 있는 문제점이 있다.

[0005] 또한, HTTP는 이전 정보는 전혀 필요로 하지 않는 비연결유지(stateless) 성질을 가지고 있기 때문에, 아이프레임 또는 탭 브라우징과 같이 세션이 쿠키를 동시 다발적으로 사용하여 인증자가 동일한 경우, HTTP 요청에 의해 마지막으로 전송된 인증자가 제일 먼저 도착하여, 후에 도착한 나머지 인증자는 인증에 성공하지 못하는 경우와 같이 공유된 정보의 비동기화가 발생하는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

[0006] 본 발명은 상술한 문제점을 해결하기 위한 것으로서, 재전송 공격에 대비하여 보안성이 향상된 씨드 공유를 이용한 클라이언트 인증 방법 및 시스템을 제공하는 것을 기술적 과제로 한다.

[0007] 또한, 본 발명은 세션이 쿠키를 동시 다발적으로 사용하여 인증자가 동일함에 따라 발생한 공유된 정보의 비동기화를 해결할 수 있는 씨드 공유를 이용한 클라이언트 인증 방법 및 시스템을 제공하는 것을 다른 기술적 과제로 한다.

과제 해결수단

[0008] 상술한 목적을 달성하기 위한 본 발명의 일 측면에 따른 씨드 공유를 이용한 클라이언트 인증 방법은 키(Key) 및 씨드(Seed)를 클라이언트와 공유하는 단계; 상기 클라이언트에 의해 상기 키 및 씨드를 이용하여 생성된 인증자 및 상기 인증자에 대한 카운터를 수신하는 단계; 및 상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하고, 상기 인증자가 사용되지 않은 경우 상기 인증자를 검증하는 단계를 포함한다.

[0009] 이 때, 상기 공유하는 단계는 상기 키 및 씨드를 생성하는 단계; 및 상기 생성된 키 및 씨드를 키 동의(Key Agreement) 또는 키 전송(Key Transportation) 방식을 통해 상기 클라이언트와 공유하는 단계를 포함하는 것을 특징으로 한다.

[0010] 일 실시예에 있어서, 상기 키 및 씨드는 상기 클라이언트와 서버에 각각 따로 저장되며, 상기 클라이언트에는 플러그인(plugin)을 요구하지 않는 웹 브라우저 저장소에 저장되는 것을 특징으로 한다.

[0011] 이 때, 상기 공유하는 단계 이후에, 상기 클라이언트로 HTTP 응답을 전송하는 단계를 더 포함하며, 상기 HTTP 응답에는 상기 인증자 생성에 관한 클라이언트 사이드 스크립트(Client Side Script)가 포함되어 있는 것을 특

징으로 한다.

[0012] 일 실시예에 있어서, 상기 인증자는 상기 클라이언트에서 HTTP 응답 수신 후 미리 생성되어 상기 카운터와 함께 쿠키에 저장되며, 상기 인증자 및 카운터는 상기 클라이언트의 HTTP 요청과 함께 상기 서버로 전송되는 것을 특징으로 하며, 상기 카운터는 상기 인증자가 생성될 때마다 증가하는 것을 특징으로 한다.

[0013] 다른 실시예에 있어서, 상기 인증자는 상기 카운터 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 한다.

[0014] 상기 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우, 상기 인증자는 상기 적어도 하나의 아이프레임 별로 상기 카운터, 상기 아이프레임의 URL 및 상기 키 및 씨드를 이용한 해쉬값인 것을 특징으로 하며, 이 때, 상기 인증자 및 카운터는 상기 아이프레임의 URL에 GET 형식의 파라미터로 수신하는 것을 특징으로 한다.

[0015] 상기 인증자를 검증하는 단계는 상기 수신된 카운터 및 상기 공유된 키 및 씨드를 이용한 해쉬값과 상기 클라이언트로부터 전송된 인증자가 일치하는지 여부를 판단하는 것을 특징으로 한다.

[0016] 상술한 목적을 달성하기 위한 본 발명의 다른 측면에 따른 씨드 공유를 이용한 클라이언트 인증 시스템은 키(Key) 및 씨드(Seed)를 클라이언트와 공유하는 클라이언트 공유부; 상기 클라이언트에 의해 상기 키 및 씨드를 이용하여 생성된 인증자 및 상기 인증자에 대한 카운터를 수신하는 인증자 수신부; 및 상기 수신된 카운터를 확인하여 상기 인증자의 사용 유무를 확인하고, 상기 인증자가 사용되지 않은 경우 상기 인증자를 검증하는 인증자 검증부를 포함한다.

효 과

[0017] 상술한 바와 같이 본 발명에 따르면, 키 및 씨드 공유를 통한 인증자의 보안성이 강화되었으며, 인증자 생성시마다 새로운 카운터에 의해 인증자가 생성되고, 카운터를 이용해 인증자의 사용 유무 확인이 가능하여 공격자의 재전송 공격을 방어할 수 있는 효과가 있다.

[0018] 또한, 본 발명에 따르면, 웹 페이지가 아이프레임을 포함하는 경우 아이프레임 별로 인증자를 생성하여, 동일한 인증자로 인한 공유된 정보의 비동기화를 방지할 수 있다는 효과가 있다.

발명의 실시를 위한 구체적인 내용

[0019] 이하 첨부된 도면을 참조하여 본 발명의 실시예에 대해 상세히 설명하기로 한다.

[0020] 먼저, 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 시스템을 설명하기에 앞서 본 발명의 이해를 돕기 위해 HTTP(Hyper Text Transfer Protocol) 통신에 대해 도 1을 참조하여 살펴보기로 한다.

[0021] 도 1은 본 발명의 일 실시예에 따른 클라이언트 인증 시스템을 포함하는 서버와 클라이언트 사이에서 HTTP(Hyper Text Transfer Protocol) 통신이 수행되는 예를 보여주는 개략적인 블록도이다. 도시된 바와 같이, 클라이언트(100)와 서버(200) 사이의 화살표 A, B, C, D, E, F는 통신 시퀀스이며, 클라이언트(100)에서 서버(200)로 향하는 화살 A, C 및 E는 클라이언트(100)의 서버에 대한 요구 명령인 HTTP 요청(request)를 나타내고, 서버(200)에서 클라이언트(100)로 향하는 화살표 B, D 및 F는 서버(200)가 클라이언트(100)에 제공하는 HTTP 응답(response)를 나타낸다. 여기서, 본 발명의 일 실 시예에 따른 클라이언트 인증 시스템(300)은 서버(200)에 대한 클라이언트(100) 인증을 위한 시스템으로 이하에서 자세히 살펴보기로 한다.

[0022] 도 2는 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 시스템의 개략적은 블럭도이다. 도 2에 도시된 인증 시스템(300)은 클라이언트 공유부(320), HTTP 응답 전송부(340), 인증자 수신부(360) 및 인증자 검증부(380)를 포함한다.

[0023] 클라이언트 공유부(320)는 사용자 로그인시 키(Key) 및 씨드를 클라이언트와 공유하는 것으로서, 도 3에 도시된 바와 같이, 씨드 생성부(322), 씨드 공유부(324) 및 저장부(326)를 포함한다.

[0024] 씨드 생성부(320)는 클라이언트(100)를 통해 사용자가 서버에 로그인 할 때 키 및 씨드를 생성하고, 씨드 공유부(324)는 생성된 키 및 씨드를 Diffie-Hellman, RSA 등을 이용한 키 동의(Key Agreement) 또는 키 전송(Key Transport) 방식을 통해서 클라이언트와 공유한다. 여기서, 키와 씨드 두 가지를 공유하는 이유는 키 한가지 만으로 클라이언트를 인증 하기에는 랜덤성이 떨어지기 때문이다.

[0025] 저장부(326)는 공유된 키 및 씨드를 저장하며, 예를 들어, 웹 어플리케이션이 제공하는 세션 또는 데이터베이스

가 이에 해당할 수 있다. 또한, 공유된 키 및 씨드는 클라이언트와 서버 각각에 저장될 수 있으며, 클라이언트에서는 플러그인(plugin)을 요구하지 않는 웹 브라우저 저장소에 저장될 수 있다. 이는 웹 브라우저에서는 ActiveX를 이용한 저장소를 사용할 수도 있지만 사용자 접근성에서 부담이 될 수 있으며, 지나친 ActiveX의 사용은 사용자의 부주의를 부추겨 결국 컴퓨터 보안 수준을 낮추는 잠재적인 위험성을 지니기 때문이다. 따라서, 본 발명의 일 실시예에 있어서, 공유된 키 및 씨드는 클라이언트에서 추가적인 플러그인을 요구하지 않고 웹 브라우저의 호환성이 높은 저장소에 저장된다.

[0026] 플러그인을 요구하지 않는 웹 브라우저 저장소의 예가 도 4에 도시되어 있으며, 도시된 바와 같이, globalStorage는 도시된 저장소 중 가장 이상적이지만 FireFox2 이상에서만 사용이 가능하고, oXML은 Internet Exploorer5 이상에서 지원하지만 데이터가 설정된 디렉터리에서만 그 접근이 한정되어 도메인 전역에서 인증자를 생성하기 위한 키 및 씨드 저장소로는 어울리지 않는다. 한편, Local Shared Object는 Flash6 이상에서 제공하는 저장소로 Adobe에 따르면 전 세계 98.8%의 PC에 Flash6 이상의 버전이 설치되어 있고, 도메인 단위로 접근되기 때문에 키 및 씨드를 저장하기 좋은 저장소이다. 또한, window.name은 새 창을 띄우거나 iframe등을 포함하는 부모페이지에서 접근할 때 사용되는 DOM(Document Object Model) 형태의 속성으로, Javascript 1.1 이상을 지원하는 웹 브라우저라면 사용이 가능하기 때문에 호환성이 높지만 도메인 단위 접근을 지원하지 않기 때문에 window.name에 값이 설정된 이후에 이동한 다른 도메인에서 설정된 데이터의 접근이 가능하다.

[0027] 따라서, 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 시스템은 공유된 키 및 씨드를 클라이언트와 서버에서 각각 따로 저장함으로써, 클라이언트 인증에 필요한 중요 정보인 키 및 씨드의 도청을 방지할 수 있다.

[0028] 다시 도 2를 참조하면, HTTP 응답 전송부(340)는 클라이언트(100)로 HTTP 응답(response)을 전송하며, HTTP 응답에는 후술할 인증자 생성에 관한 클라이언트 사이드 스크립트(Client Side Script)가 포함되어 있다. 여기서, 클라이언트 사이드 스크립트란 스크립트가 실행되는 곳이 클라이언트인 스크립트로서, 일 예로 Javascript가 이에 해당할 수 있으며, HTTP 응답 전송부(340)에서는 클라이언트(100)가 인증자를 생성하도록 하는 Javascript를 HTTP 응답에 포함시켜 전송하는 것이다.

[0029] 인증자 수신부(360)는 클라이언트(100)에 의해 키 및 씨드를 이용하여 생성된 인증자 및 인증자에 대한 카운터를 수신하는 것으로서, HTTP 요청 수신부(362)를 포함한다.

[0030] HTTP 요청 수신부(362)는 클라이언트(100)의 HTTP 요청(request)과 함께 인증자 및 카운터를 수신한다. 일 실시예에 있어서, 인증자는 클라이언트(100)에서 HTTP 응답 전송부(340)의 HTTP 응답과 함께 전송된 클라이언트 사이드 스크립트에 의해 미리 생성되어 카운터와 함께 쿠키에 저장된다.

[0031] 다시 말해, HTTP 요청 수신부(362)에서 수신되는 인증자는 클라이언트(100)에서 HTTP 요청 할 때마다 생성되는 것이 아니라, HTTP 응답에 포함된 클라이언트 사이드 스크립트에 의해 인증자를 미리 생성하여 쿠키에 저장해 놓고, 인증자가 서버로 전송될 때 인증자에 대한 카운터도 함께 전달되도록 카운터도 쿠키에 함께 저장하는 것이다. 따라서, 본 발명의 일 실시예에 따른 클라이언트 인증 시스템은 HTTP 요청이 네트워크로 전송되기 전에는 인증자가 노출되지 않아 재전송 공격에 대비할 수 있다.

[0032] 일 실시예에 있어서, 카운터는 인증자가 생성될 때마다 증가하며, 일 예로 인증자가 생성될 때마다 1씩 증가할 수 있다. 카운터는 후술할 인증자 검증부(380)에 의해 인증자 사용 유무를 확인하는 수단이 된다.

[0033] 일 실시예에 있어서, 인증자는 카운터, 키 및 씨드를 이용한 해쉬값일 수 있다. 예를 들어, 클라이언트의 웹 페이지가 아이프레임(iframe)을 포함하지 않는 보통의 페이지인 경우 인증자는 "H(++O|Seed|Key)"와 같이 카운터, 키 및 씨드를 이용한 해쉬값이 될 수 있다. 이 때, 해쉬값으로 생성된 인증자는 쿠키에 저장되며, HTTPP 요청시 인증자가 전송될 때 카운터도 같이 전송되도록 쿠키에 저장될 수 있다.

[0034] 여기서,"O"는 인증자에 대한 카운터를 의미하며, "++O"는 1씩 증가한 카운터 값을 의미한다. 한편, 카운터 값을 인증자 마다 달리하는 이유는 후술할 인증자 검증부(380)에서 카운터를 이용해 인증자에 대한 사용 유무를 확인하고, 인증자를 매번 새로운 해쉬값으로 갱신하여 재전송 공격에 대비하기 위해서이다.

[0035] 다른 실시예에 있어서, 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우, 인증자는 적어도 하나의 아이프레임 별로 카운터, 아이프레임의 URL(Uniform Resource Locator), 키 및 씨드를 이용한 해쉬값일 수 있다.

[0036] 여기서, 아이프레임(iframe)이란 인라인프레임과 같은 의미로 한 사이트 안에 다른 웹 페이지가 표시되는 것을

의미한다. 예를 들어, 하나의 사이트 안에 "다음"과 "네이버" 두 개의 다른 웹 페이지가 표시되는 경우, 웹 페이지가 두 개의 아이프레임을 포함하고 있다고 말할 수 있다.

[0037] 예를 들어, 클라이언트의 웹 페이지가 아이프레임(iframe)을 포함하고 있는 부모 페이지인 경우 인증자는 아이프레임 별로"H(++O|URL|Seed|Key)"와 같이 카운터, 아이프레임의 URL, 키 및 씨드를 이용한 해쉬값이 될 수 있다. 여기서,"O"는 앞에서 살펴본 바와 같이, 인증자에 대한 카운터를 의미하며, "++O"는 1씩 증가한 카운터 값을 의미한다. 따라서, 아이프레임이 3개 있는 경우 아이프레임 별로 각각의 인증자를 생성된 순서대로 U1, U2, U3라고 하고, 인증자 U1의 해쉬값에 이용된 카운터가 "1"이라고 한다면, 인증자 U2 및 U3의 카운터는 1씩 증가한"2" 와 "3"이 될 것이다. 이 때, HTTPP 요청시에는 아이프레임 별로 인증자가 전송되며, 다음 HTTP 응답을 수신한 경우에는 HTTPP 요청시 인증자가 모두 전송되고 난 후 다음에 사용될 인증자를 계산하여 카운터와 함께 쿠키에 저장될 수 있다. 한편, 상술한 바와 같이 인증자가 생성되는 과정은 HTTP 응답에 포함된 클라이언트 사이드 스크립트에 의해 이루어질 수 있다.

[0038] 여기서, 아이프레임 별로 인증자를 생성하는 이유는 클라언트의 웹 페이지가 다수의 아이프레임을 포함하고 있을 경우에 부모페이지의 HTTP 응답을 수신 후 아이프레임에 대한 HTTP 요청들은 동일한 인증자를 가지고 있기 때문에 서버에 처음으로 도착한 HTTP 요청을 제외한 나머지 HTTP 요청은 인증에 실패하는 것을 방지하기 위해서이다.

[0039] 이 때, 인증자 및 카운터는 아이프레임의 URL에 GET 형식의 파라미터로 수신될 수 있다. 여기서, GET 형식이란 클라이언트에서 서버로 데이터를 전송할 때, URL과 함께 전송하는 자료와 변수 이름을 함께 전송하는 것을 의미하며, 클라이언트에서 서버로 데이터를 전송하는 다른 형식으로는 데이터를 HTTP 헤더 안에 포함시키는 POST 형식이 있다.

[0040] 인증자 검증부(380)는 수신된 카운터를 확인하여 인증자의 사용 유무를 확인하고, 인증자가 사용되지 않은 경우 인증자를 검증하는 것으로서, 도 5에 도시된 바와 같이, 카운터 확인부(382), 해쉬 연산부(384) 및 인증자 판단부(386)을 포함한다.

[0041] 카운터 확인부(382)는 클라이언트(100)로부터 수신된 카운터를 확인하여 사용자의 사용 유무를 확인한다. 다시 말해, 카운터 확인부(382)는 인증자 검증에 앞서 클라이언트로부터 수신된 인증자의 카운터를 확인하여, 이전에 검증된 인증자의 카운터와 비교하여 인증자의 사용 유무를 확인하는 것이다.

[0042] 해쉬 연산부(384)는 카운터 확인부(382)의 확인 결과, 인증자가 사용되지 않은 것으로 확인되면, 클라이언트(100)로부터 수신된 카운터 및 공유된 키 및 씨드를 이용한 해쉬값을 산출하며, 인증자 판단부(386)는 해쉬 연산부(384)에 의해 산출된 해쉬값과 클라이언트(100)로부터 전송된 인증자가 일치하는지 여부를 판단한다. 즉, 인증자 검증부(380)는 클라이언트(100)로부터 수신한 인증자와, 클라이언트(100)로부터 수신된 카운터 및 공유된 키 및 씨드를 이용한 해쉬값과 일치하는지 여부를 판단하여, 일치하는 것으로 확인되면 클라이언트에 대한 인증 처리를 하는 것이다. 이 때, 인증자가 상술한 아이프레임 별 인증자인 경우, 해쉬 연산부(384)는 클라이언트로부터 전송된 아이프레임의 URL을 포함시켜 해쉬값을 산출한다.

[0043] 따라서, 본 발명의 일 실싱예에 따른 씨드를 이용한 클라이언트 인증 시스템은 인증에 필요한 중요 정보인 키 및 씨드는 로그인시 공유를 하고, 인증자가 카운터 값이 달라짐에 따라 매번 새로운 값으로 갱신됨에 따라 공격자의 재전송 공격에 대비할 수 있다.

[0044] 이하에서는 도 6을 참조하여 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 방법을 설명하기로 한다.

[0045] 먼저, 서버(200)는 키 및 씨드를 클라이언트와 공유한다(S400). 일 실시예에 있어서, S400은 사용자가 서버에 로그인 할 때 키 및 씨드를 생성하고, 생성된 키 및 씨드를 Diffie-Hellman, RSA 등을 이용한 키 동의(Key Agreement) 또는 키 전송(Key Transport) 방식을 통해서 클라이언트와 공유할 수 있다.

[0046] 이 때, 공유된 키 및 씨드는 클라이언트(100)와 서버(200)에 각각 따로 저정될 수 있으며, 클라이언트(100)에서는 플러그인(plugin)을 요구하지 않는 웹 브라우저 저장소, 서버(200)에서는 웹 어플리케이션이 제공하는 세션 또는 데이터베이스에 저장될 수 있다.

[0047] 다음으로, 클라이언트(100)로 인증자 생성에 관한 클라이언트 사이드 스크립트가 포함된 HTTP 응답을 전송하고(S410), 클라이언트(100)는 인증자 생성에 관한 클라이언트 사이드 스크립트에 의해 웹 브라우저 저장소에 저장된 공유된 키 및 씨드를 이용하여 인증자를 생성하고, 인증자에 대한 카운터와 함께 저장한다(S420). 이 때, 인

증자 및 카운터는 쿠키에 저장될 수 있다.

[0048] 일 실시예에 있어서, 카운터는 인증자가 생성될 때마다 증가하며, 일 예로 인증자가 생성될 때마다 1씩 증가할 수 있다.

[0049] 일 실시예에 있어서, 인증자는 카운터, 키 및 씨드를 이용한 해쉬값일 수 있다. 이 때, 해쉬값으로 생성된 인증자는 쿠키에 저장되며, HTTPP 요청시 인증자가 전송될 때 카운터도 같이 전송되도록 쿠키에 저장될 수 있다. 한편, 카운터 값을 인증자 마다 달리하는 이유는 카운터를 이용해 인증자에 대한 사용 유무를 확인하고, 인증자를 매번 새로운 해쉬값으로 갱신하여 재전송 공격에 대비하기 위해서이다.

[0050] 다른 실시예에 있어서, 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우, 인증자는 적어도 하나의 아이프레임 별로 카운터, 아이프레임의 URL(Uniform Resource Locator), 키 및 씨드를 이용한 해쉬값일 수 있다.

[0051] 여기서, 아이프레임 별로 인증자를 생성하는 이유는 클라언트의 웹 페이지가 다수의 아이프레임을 포함하고 있을 경우에 부모페이지의 HTTP 응답을 수신 후 아이프레임에 대한 HTTP 요청들은 동일한 인증자를 가지고 있기 때문에 서버에 처음으로 도착한 HTTP 요청을 제외한 나머지 HTTP 요청은 인증에 실패하는 것을 방지하기 위해서이다.

[0052] 다음으로, HTTP 요청과 함께 클라이언트(100)에 의해 생성된 인증자 및 카운터를 수신한다(S430). 일 실시예에 있어서, 클라이언트의 웹 페이지가 아이프레임(iframe)을 적어도 하나 포함하는 경우, 인증자 및 카운터는 아이프레임의 URL에 GET 형식의 파라미터로 수신될 수 있다.

[0053] 다음으로, 수신된 카운터를 확인하여 인증자의 사용 유무를 확인하고, 인증자가 사용되지 않은 경우 인증자를 검증한다(S440). 즉, 인증자 검증에 앞서 클라이언트로부터 수신된 인증자의 카운터를 확인하여, 이전에 검증된 인증자의 카운터와 비교하여 인증자의 사용 유무를 확인하는 것이다. 또한, 확인 결과, 인증자가 사용되지 않은 것으로 확인되면, 클라이언트(100)로부터 수신된 카운터 및 공유된 키 및 씨드를 이용한 해쉬값을 산출하며, 산출된 해쉬값과 클라이언트(100)로부터 전송된 인증자가 일치하는지 여부를 판단한다. 즉, 인증자 검증부(380)는 클라이언트(100)로부터 수신한 인증자와, 클라이언트(100)로부터 수신된 카운터 및 공유된 키 및 씨드를 이용한 해쉬값과 일치하는지 여부를 판단하여, 일치하는 것으로 확인되면 클라이언트에 대한 인증 처리를 하는 것이다.

[0054] 한편, 상술한 씨드 공유를 이용한 클라이언트 인증 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터로 판독 가능한 기록 매체에 기록될 수 있다. 이때, 컴퓨터로 판독 가능한 기록매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 한편, 기록매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0055] 컴퓨터로 판독 가능한 기록매체에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-Optical Media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 한편, 이러한 기록매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다.

[0056] 또한, 프로그램 명령에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상술한 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0057] 한편, 본 발명이 속하는 기술분야의 당업자는 본 발명이 그 기술적 사상이나 필수적 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다.

[0058] 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적인 것이 아닌 것으로 이해해야만 한다. 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 등가 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면의 간단한 설명

[0059] 도 1은 본 발명의 일 실시예에 따른 클라이언트 인증 시스템을 포함하는 서버와 클라이언트 사이에서

HTTP(Hyper Text Transfer Protocol) 통신이 수행되는 예를 보여주는 개략적인 블록도이다.

[0060] 도 2는 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 시스템의 개략적은 블럭도이다.

[0061] 도 3은 도 2에 도시된 클라이언트 공유부의 세부 구성을 보여주는 블록도이다.

[0062] 도 4는 플러그인을 요구하지 않는 웹 브라우저 저장소의 예를 보여주는 도면이다.

[0063] 도 5는 도 2에 도시된 인증자 검증부의 세부 구성을 보여주는 블록도이다.

[0064] 도 6은 본 발명의 일 실시예에 따른 씨드 공유를 이용한 클라이언트 인증 방법을 보여주는 플로우차트이다.

[0065] <도면의 주요 부분에 대한 부분의 설명>

[0066] 200 : 서버 300 : 클라이언트 인증 시스템

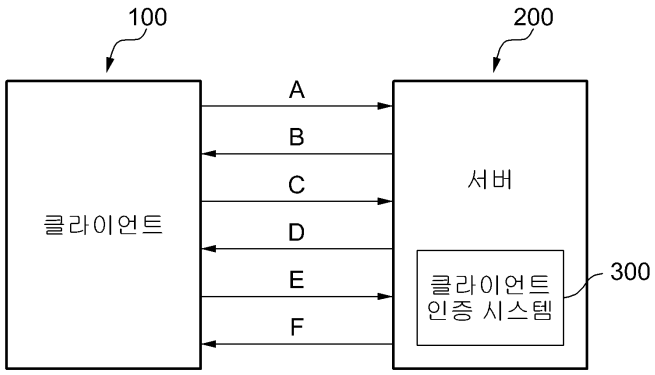
[0067] 320 : 클라이언트 공유부 340 : HTTP 응답 전송부

[0068] 360 : 인증자 수신부 362 : HTTP 요청 수신부

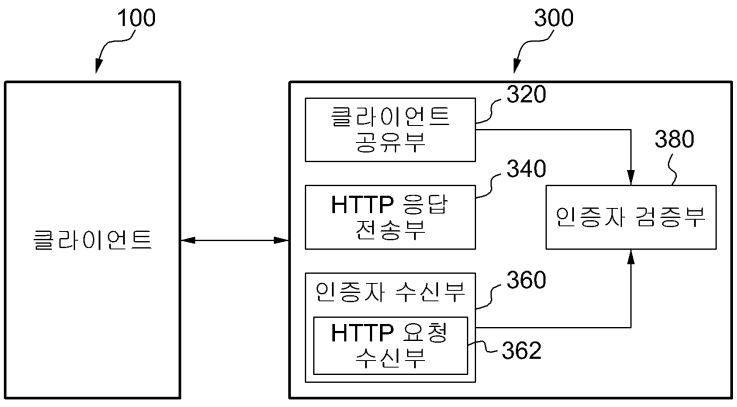
[0069] 380 : 인증자 검증부

도면

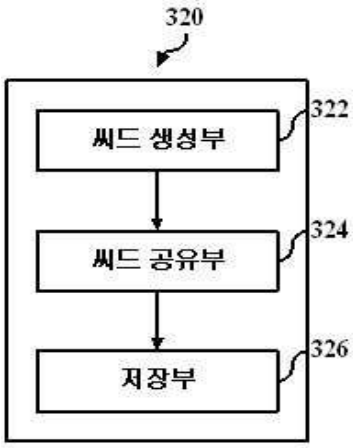
도면1



도면2



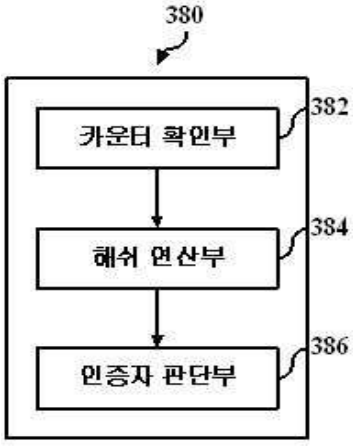
도면3



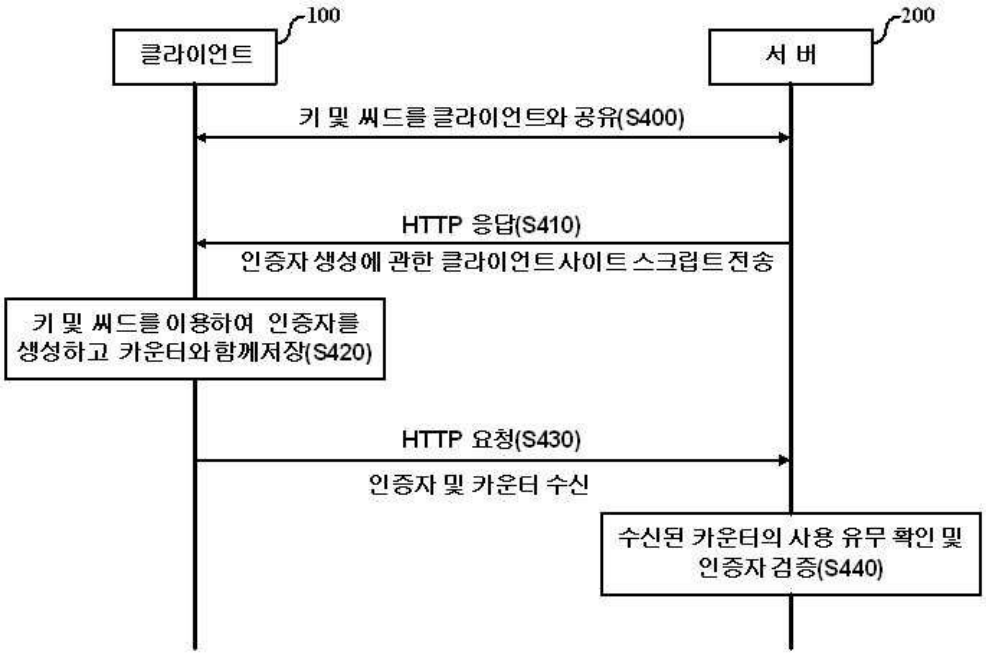
도면4

속성 / 저장소	지원 브라우저 및 버전	도메인 단위 접근	기타
globalStorage	FireFox2 이상	O	
oXML	Internet Explorer5 이상	O	설정 디렉터리에서만 접근가능
window.name	Javascript 1.1 이상을 지원하는 모든 브라우저		크로스 도메인 지원, 큰 용량 (32MB)
Local Shared Object	FLASH PLAYER 6 이상이 설치된 브라우저 (98.8%)	O	설정가능(기본 100KB)

도면5



도면6


100
클라이언트
200
서 버
키 및 씨드를 클라이언트와 공유(S400)
HTTP 응답(S410)
인증자 생성에 관한 클라이언트사이트 스크립트 전송
키 및 씨드를 이용하여 인증자를
생성하고 카운터와 함께저장(S420)
HTTP 요청(S430)
인증자 및 카운터 수신
수신된 카운터의 사용 유무 확인 및
인증자 검증(S440)