(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년12월24일
(11) 등록번호 10-1579801
(24) 등록일자 2015년12월17일

(51) 국제특허분류(Int. Cl.)
*H04L 9/32* (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2014-7012094
(22) 출원일자(국제) 2012년10월04일
심사청구일자 2014년05월02일
(85) 번역문제출일자 2014년05월02일
(65) 공개번호 10-2014-0084126
(43) 공개일자 2014년07월04일
(86) 국제출원번호 PCT/US2012/058789
(87) 국제공개번호 WO 2013/052693
국제공개일자 2013년04월11일
(30) 우선권주장
13/252,931 2011년10월04일 미국(US)
(56) 선행기술조사문헌
US07188181 B1*
US20040111621 A1*
US20070044146 A1*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**퀄컴 인코포레이티드**
미국 92121-1714 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(72) 발명자
**플라나간, 제시카 엠.**
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
**브라운, 크레이그 엠.**
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
**패든, 마이클 더블유.**
미국 92121 캘리포니아주 샌 디에고 모어하우스 드라이브 5775
(74) 대리인
**특허법인 남앤드남**

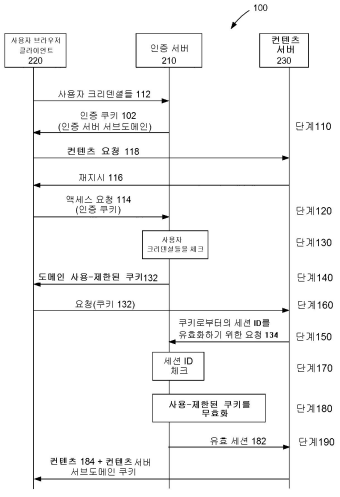
전체 청구항 수 : 총 32 항 심사관 : 장진환

(54) 발명의 명칭 **크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법 및 장치**

## (57) 요 약

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법이 개시된다. 이 방법에서, 인증 서버(210)는 브라우저 클라이언트(220)에 인증 쿠키(102)를 제공한다. 이 쿠키는, 도메인에 대한 인증 크리덴셜을 갖고, 도메인의 인증 서브도메인과 관련된다. 서버(210)는 브라우저 클라이언트(114)로부터 쿠키를 수신한다. 수신된 쿠키에서의 사용자 인증 크리덴셜의 인증시에, 서버(210)는 도메인에 대한 사용-제한된 쿠키(132)를 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답한다. 서버(210)는 브라우저 클라이언트로부터 수신된 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청(134)을 컨텐츠 서버(230)로부터 수신한다. 유효화 시에, 서버(210)는, 컨텐츠 서버가 요청된 컨텐츠(184)를 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지(182)를 컨텐츠 서버(230)에 제공한다.

*대 표 도* - 도1



# 명 세 서

## 청구범위

### 청구항 1

크리덴셜(credential) 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법으로서,

인증 서버에 의해, 사용자 브라우저 클라이언트에 인증 쿠키(authentication cookie)를 제공하는 단계 - 상기 인증 쿠키는, 상기 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 상기 단일 사인-온 도메인의 인증 서브도메인과 관련됨 -;

상기 인증 서버에 의해, 상기 사용자 브라우저 클라이언트로부터의 액세스 요청 내에서 상기 인증 쿠키를 수신하는 단계 - 상기 액세스 요청은 상기 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 상기 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 상기 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(redirection)에 기초함 -;

수신된 인증 쿠키에서의 상기 사용자 인증 크리덴셜의 인증시에, 상기 인증 서버에 의해, 상기 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 상기 사용자 브라우저 클라이언트에 포워딩함으로써 상기 액세스 요청에 응답하는 단계;

상기 인증 서버에 의해, 상기 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 상기 컨텐츠 서버로부터 수신하는 단계 - 상기 컨텐츠 서버는 상기 사용자 브라우저 클라이언트로부터 상기 사용-제한된 쿠키를 수신했음 -;

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 인증 서버에 의해, 상기 컨텐츠 서버가 요청된 컨텐츠를 상기 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 상기 컨텐츠 서버에 제공하는 단계; 및

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 인증 서버에 의해, 상기 사용-제한된 쿠키의 추가적인 이용을 금지하기 위해 상기 사용-제한된 쿠키를 무효화하는 단계를 포함하는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

### 청구항 2

제 1 항에 있어서,

상기 사용-제한된 쿠키는 일회(one-time) 사용 쿠키를 포함하는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

### 청구항 3

삭제

### 청구항 4

제 1 항에 있어서,

상기 사용-제한된 쿠키는 만료 시간을 갖는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

### 청구항 5

제 4 항에 있어서,

상기 만료 시간은 1 분을 포함하는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

**청구항 6**

제 1 항에 있어서,

상기 컨텐츠 서버는 상기 단일 사인-온 도메인의 서브도메인을 포함하는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

**청구항 7**

제 6 항에 있어서,

상기 사용-제한된 쿠키는 오직 상기 컨텐츠 서버의 서브도메인에 대해서만 유효한,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

**청구항 8**

제 1 항에 있어서,

상기 세션 식별자는 일회 세션 키를 포함하는,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

**청구항 9**

인증 서버로서,

사용자 브라우저 클라이언트에 인증 쿠키를 제공하기 위한 수단 - 상기 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 상기 단일 사인-온 도메인의 인증 서브도메인과 관련됨 -;

상기 사용자 브라우저 클라이언트로부터의 액세스 요청 내에서 상기 인증 쿠키를 수신하기 위한 수단 - 상기 액세스 요청은 상기 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 상기 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 상기 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 -;

수신된 인증 쿠키에서의 상기 사용자 인증 크리덴셜의 인증시에, 상기 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 상기 사용자 브라우저 클라이언트에 포워딩함으로써 상기 액세스 요청에 응답하기 위한 수단;

상기 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 상기 컨텐츠 서버로부터 수신하기 위한 수단 - 상기 컨텐츠 서버는 상기 사용자 브라우저 클라이언트로부터 상기 사용-제한된 쿠키를 수신했음 -;

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 컨텐츠 서버가 요청된 컨텐츠를 상기 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 상기 컨텐츠 서버에 제공하기 위한 수단; 및

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 사용-제한된 쿠키의 추가적인 이용을 금지하기 위해 상기 사용-제한된 쿠키를 무효화하기 위한 수단을 포함하는,

인증 서버.

**청구항 10**

제 9 항에 있어서,

상기 사용-제한된 쿠키는 일회 사용 쿠키를 포함하는,

인증 서버.

**청구항 11**

삭제

**청구항 12**

제 9 항에 있어서,

상기 사용-제한된 쿠키는 만료 시간을 갖는,

인증 서버.

**청구항 13**

제 12 항에 있어서,

상기 만료 시간은 1 분을 포함하는,

인증 서버.

**청구항 14**

제 9 항에 있어서,

상기 컨텐츠 서버는 상기 단일 사인-온 도메인의 서브도메인을 포함하는,

인증 서버.

**청구항 15**

제 14 항에 있어서,

상기 사용-제한된 쿠키는 오직 상기 컨텐츠 서버의 서브도메인에 대해서만 유효한,

인증 서버.

**청구항 16**

제 9 항에 있어서,

상기 세션 식별자는 일회 세션 키를 포함하는,

인증 서버.

**청구항 17**

인증 서버로서,

사용자 브라우저 클라이언트에 인증 쿠키를 제공하고 - 상기 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 상기 단일 사인-온 도메인의 인증 서브도메인과 관련됨 -;

상기 사용자 브라우저 클라이언트로부터의 액세스 요청 내에서 상기 인증 쿠키를 수신하고 - 상기 액세스 요청은 상기 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 상기 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 상기 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 -;

수신된 인증 쿠키에서의 상기 사용자 인증 크리덴셜의 인증시에, 상기 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 상기 사용자 브라우저 클라이언트에 포워딩함으로써 상기 액세스 요청에 응답하고;

상기 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 상기 컨텐츠 서버로부터 수신하고 - 상기 컨텐츠 서버는 상기 사용자 브라우저 클라이언트로부터 상기 사용-제한된 쿠키를 수신했음 -;

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 컨텐츠 서버가 요청된 컨텐츠를 상기 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 상기 컨텐츠 서버에 제공하고; 그리고

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 상기 사용-제한된 쿠키의 추가적인 이용을 금지하기 위해 상기 사용-제한된 쿠키를 무효화하도록 구성된 프로세서를 포함하는,

인증 서버.

**청구항 18**

제 17 항에 있어서,

상기 사용-제한된 쿠키는 일회 사용 쿠키를 포함하는,

인증 서버.

**청구항 19**

삭제

**청구항 20**

제 17 항에 있어서,

상기 사용-제한된 쿠키는 만료 시간을 갖는,

인증 서버.

**청구항 21**

제 20 항에 있어서,

상기 만료 시간은 1 분을 포함하는,

인증 서버.

**청구항 22**

제 17 항에 있어서,

상기 컨텐츠 서버는 상기 단일 사인-온 도메인의 서브도메인을 포함하는,

인증 서버.

**청구항 23**

제 22 항에 있어서,

상기 사용-제한된 쿠키는 오직 상기 컨텐츠 서버의 서브도메인에 대해서만 유효한,

인증 서버.

**청구항 24**

제 17 항에 있어서,

상기 세션 식별자는 일회 세션 키를 포함하는,

인증 서버.

**청구항 25**

컴퓨터 판독가능 저장 매체로서,

컴퓨터로 하여금 사용자 브라우저 클라이언트에 인증 쿠키를 제공하게 하기 위한 코드 — 상기 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 상기 단일 사인-온 도메인의 인증 서브도메인과 관련됨 —;

컴퓨터로 하여금 상기 사용자 브라우저 클라이언트로부터의 액세스 요청 내에서 상기 인증 쿠키를 수신하게 하기 위한 코드 — 상기 액세스 요청은 상기 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 상기 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 상기 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 —;

수신된 인증 쿠키에서의 상기 사용자 인증 크리덴셜의 인증시에, 컴퓨터로 하여금 상기 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 상기 사용자 브라우저 클라이언트에 포워딩함으로써 상기 액세스 요청에 응답하게 하기 위한 코드;

컴퓨터로 하여금 상기 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 상기 컨텐츠 서버로부터 수신하게 하기 위한 코드 - 상기 컨텐츠 서버는 상기 사용자 브라우저 클라이언트로부터 상기 사용-제한된 쿠키를 수신했음 -;

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 컴퓨터로 하여금, 상기 컨텐츠 서버가 요청된 컨텐츠를 상기 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 상기 컨텐츠 서버에 제공하게 하기 위한 코드; 및

상기 사용-제한된 쿠키의 상기 세션 식별자의 유효화 시에, 컴퓨터로 하여금 상기 사용-제한된 쿠키의 추가적인 이용을 금지하기 위해 상기 사용-제한된 쿠키를 무효화하게 하기 위한 코드

를 포함하는,

컴퓨터 판독가능 저장 매체.

**청구항 26**

제 25 항에 있어서,

상기 사용-제한된 쿠키는 일회 사용 쿠키를 포함하는,

컴퓨터 판독가능 저장 매체.

**청구항 27**

삭제

**청구항 28**

제 25 항에 있어서,

상기 사용-제한된 쿠키는 만료 시간을 갖는,

컴퓨터 판독가능 저장 매체.

**청구항 29**

제 28 항에 있어서,

상기 만료 시간은 1 분을 포함하는,

컴퓨터 판독가능 저장 매체.

**청구항 30**

제 25 항에 있어서,

상기 컨텐츠 서버는 상기 단일 사인-온 도메인의 서브도메인을 포함하는,

컴퓨터 판독가능 저장 매체.

**청구항 31**

제 30 항에 있어서,

상기 사용-제한된 쿠키는 오직 상기 컨텐츠 서버의 서브도메인에 대해서만 유효한,

컴퓨터 판독가능 저장 매체.

**청구항 32**

제 25 항에 있어서,

상기 세션 식별자는 일회 세션 키를 포함하는,

컴퓨터 판독가능 저장 매체.

**청구항 33**

제 1 항에 있어서,

상기 단일 사인-온 도메인은 도메인 명칭과 관련되고; 그리고

상기 인증 서브도메인은 상기 도메인 명칭을 포함하는 서브도메인 명칭과 관련된,

크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법.

**청구항 34**

제 9 항에 있어서,

상기 단일 사인-온 도메인은 도메인 명칭과 관련되고; 그리고

상기 인증 서브도메인은 상기 도메인 명칭을 포함하는 서브도메인 명칭과 관련된,

인증 서버.

**청구항 35**

제 17 항에 있어서,

상기 단일 사인-온 도메인은 도메인 명칭과 관련되고; 그리고

상기 인증 서브도메인은 상기 도메인 명칭을 포함하는 서브도메인 명칭과 관련된,

인증 서버.

**청구항 36**

제 25 항에 있어서,

상기 단일 사인-온 도메인은 도메인 명칭과 관련되고; 그리고

상기 인증 서브도메인은 상기 도메인 명칭을 포함하는 서브도메인 명칭과 관련된,

컴퓨터 판독가능 저장 매체.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 일반적으로 크리덴셜 유출(credential leakage)로부터 단일 사인-온 도메인(single sign-on domain)을 보호하는 것에 관한 것이다.

### *배 경 기 술*

[0002] 단일 사인-온 기법들은, 인가된 사용자(authorized user)가, 공유 도메인 하에 있는 보호된 서브도메인 웹사이트들 중 하나와의 하나의 사인-온 거래에 기초하여, 보호된 서브도메인 웹사이트들에 액세스하도록 허용한다. 통상적인 단일 사인-온 기법에서, 보호된 서브도메인 웹사이트에 액세스하는 사용자는 인증되어, 사용자의 브라우저에 세션 쿠키를 제공하는 웹사이트에 접속된다. 세션 쿠키는, 사용자가, 서브도메인 웹사이트뿐만 아니라 도메인 하에 있는 모든 웹사이트들에 액세스하도록 허용한다.

[0003] 그러나, 사용자 인증이 보안을 유지하기 위해서는 서브도메인 웹사이트의 모든 각각의 호스트, 및 모든 각각의 호스트 상에서 구동하는 모든 각각의 스크립트가 신뢰되어야만 한다. 보호된 도메인 하에 있는 다른 서브도메인에서 동작하고, 사용자에 의해 방문된 불량 웹사이트(rogue website)가, 사용자의 브라우저로부터 사용자의 세션 쿠키를 수집할 수 있다. 세션 쿠키에서의 유출된 사용자의 크리덴셜은 도메인 하에 있는 서브도메인들의 다른 보호된 내부 웹사이트들에 대한 불법 액세스를 획득하는데 재사용될 수 있다.

[0004] 이에 따라, 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 기법에 대한 필요성이 존재한다.

## 발명의 내용

[0005] 본 발명의 일 양상은 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법에 속할 수 있다. 이 방법에서, 인증 서버는 인증 쿠키를 사용자 브라우저 클라이언트에 제공한다. 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련된다. 인증 서버는 브라우저 클라이언트로부터의 액세스 요청 내에서 인증 쿠키를 수신한다. 액세스 요청은, 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(redirection)에 기초한다. 수신된 인증 쿠키에서의 사용자 인증 크리덴셜의 인증시에, 인증 서버는 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답한다. 인증 서버는 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 컨텐츠 서버로부터 수신한다. 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했다. 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 인증 서버는, 컨텐츠 서버가 요청된 컨텐츠를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 컨텐츠 서버에 제공한다.

[0006] 본 발명의 더욱 세부화된 양상들에서, 사용-제한된 쿠키는 일회(one-time) 사용 쿠키일 수 있다. 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 인증 서버는 사용-제한된 쿠키의 추가적인 사용을 금지하기 위해 사용-제한된 쿠키를 무효화할 수 있다. 사용-제한된 쿠키는 짧은 만료 시간을 가질 수 있다. 짧은 만료 시간은 약 1 분을 포함할 수 있다. 컨텐츠 서버는 단일 사인-온 도메인의 서브도메인을 포함할 수 있다. 사용-제한된 쿠키는 오직 컨텐츠 서버의 서브도메인에 대해서만 유효할 수 있다. 세션 식별자는 일회 세션 키를 포함할 수 있다.

[0007] 본 발명의 다른 양상은, 사용자 브라우저 클라이언트에 인증 쿠키를 제공하기 위한 수단 – 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 –; 브라우저 클라이언트로부터의 액세스 요청 내에서 인증 쿠키를 수신하기 위한 수단 – 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 –; 수신된 인증 쿠키에서의 사용자 인증 크리덴셜의 인증시에, 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하기 위한 수단; 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 컨텐츠 서버로부터 수신하기 위한 수단 – 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 –; 및 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컨텐츠 서버가 요청된 컨텐츠를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 컨텐츠 서버에 제공하기 위한 수단을 포함하는 인증 서버에 속할 수 있다.

[0008] 본 발명의 다른 양상은, 사용자 브라우저 클라이언트에 인증 쿠키를 제공하고 – 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 –; 브라우저 클라이언트로부터의 액세스 요청 내에서 인증 쿠키를 수신하고 – 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 –; 수신된 인증 쿠키에서 사용자 인증 크리덴셜의 인증시에, 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하고; 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 컨텐츠 서버로부터 수신하고 – 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 –; 그리고 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컨텐츠 서버가 요청된 컨텐츠를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 컨텐츠 서버에 제공하도록 구성된 프로세서를 포함하는 인증 서버에 속할 수 있다.

[0009] 본 발명의 다른 양상은, 컴퓨터로 하여금 사용자 브라우저 클라이언트에 인증 쿠키를 제공하게 하기 위한 코드 – 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 –; 컴퓨터로 하여금 브라우저 클라이언트로부터의 액세스 요청 내에서 인증 쿠키를 수신하게 하기 위한 코드 – 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청에 응답하여 단일 사인-온 도메인 내에서의 컨텐츠 서버로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션에 기초함 –; 수신된 인증 쿠키에서 사용자 인증 크리덴셜의 인증시에, 컴퓨터로 하여금 단일 사인-온 도메인에 대한 사용-제한된 쿠키를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하게 하기 위한 코드; 컴퓨터로 하여금 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청을 컨텐츠 서버로부터 수신하게 하기 위한 코드 – 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 –; 및 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컴퓨터로 하여금 컨텐츠 서버가 요청된 컨텐츠를 사용자 브라우저 클라이언

트에 포워딩할 수 있게 하기 위한 유효 세션 메시지를 컨텐츠 서버에 제공하게 하기 위한 코드를 포함하는 컴퓨터-판독가능 매체를 포함하는 컴퓨터 프로그램 물건에 속할 수 있다.

## 도면의 간단한 설명

[0010] 도 1은 본 발명에 따라서 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법의 흐름도이다.

도 2는 인증 서버 및 복수의 컨텐츠 서버들과의 통신들을 가능하게 하는 인터넷에 커플링된 사용자 브라우저 클라이언트를 나타내는 블록도이다.

도 3은 인증 서버를 구현하기 위한 컴퓨터의 일 예시를 나타내는 블록도이다.

도 4는 본 발명에 따라서 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법의 다른 흐름도이다.

## 발명을 실시하기 위한 구체적인 내용

[0011] 단어 "예시적인"은 "예, 예시, 또는 예증으로서 기능하는"을 의미하도록 본원에 이용된다. "예시적인"으로서 본원에 설명된 어떠한 실시예도 반드시 다른 실시예들에 비해 선호되거나 또는 유리한 것으로서 해석되는 것은 아니다.

[0012] 도 1 및 도 2를 참조하면, 본 발명의 일 양상은, 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 방법(100)에 속할 수 있다. 이 방법에서, 인증 서버(210)는 인증 쿠키(102)를 사용자 브라우저 클라이언트(220)에 제공한다(단계 110). 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜(112)을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련된다. 인증 서버는 브라우저 클라이언트로부터의 액세스 요청(114) 내에서 인증 쿠키를 수신한다(단계 120). 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청(118)에 응답하여 단일 사인-온 도메인 내에서의 컨텐츠 서버(230)로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(116)에 기초한다. 수신된 인증 쿠키에서의 사용자 인증 크리덴셜의 인증(단계 130)시에, 인증 서버는 단일 사인-온 도메인에 대한 사용-제한된 쿠키(132)를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답한다(단계 140). 인증 서버는 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청(134)을 컨텐츠 서버로부터 수신한다(단계 150). 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했다(단계 160). 사용-제한된 쿠키의 세션 식별자의 유효화(단계 170)시에, 인증 서버는 컨텐츠 서버가 요청된 컨텐츠(184)를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지(182)를 컨텐츠 서버에 제공한다(단계 190).

[0013] 본 발명의 더욱 세부화된 양상들에서, 사용-제한된 쿠키(132)는 일회 사용 쿠키일 수 있다. 사용-제한된 쿠키의 세션 식별자의 유효화(단계150)시에, 인증 서버는 사용-제한된 쿠키의 추가적인 사용을 금지하기 위해 사용-제한된 쿠키를 무효화할 수 있다(단계 180). 사용-제한된 쿠키는 짧은 만료 시간을 가질 수 있다. 짧은 만료 시간은 약 1 분을 포함할 수 있다. 사용-제한된 쿠키는 특정한 컨텐츠 서버(230)에 특정될 수 있다. 컨텐츠 서버는 단일 사인-온 도메인의 서브도메인을 포함할 수 있다. 사용-제한된 쿠키는 오직 컨텐츠 서버의 서브도메인에 대해서만 유효할 수 있다. 세션 식별자는 일회 세션 키를 포함할 수 있다.

[0014] 도 3을 추가로 참조하면, 인증 서버(210)를 포함하는 스테이션은, 프로세서(320), 메모리(330)(및/또는 디스크 드라이브들), 디스플레이(340), 및 키패드 또는 키보드(350)를 포함하는 컴퓨터(310)일 수 있다. 유사하게, 사용자 클라이언트(220)를 포함하는 다른 스테이션은, 프로세서, 메모리(및/또는 디스크 드라이브들), 디스플레이, 및 키패드 또는 키보드를 포함하는 컴퓨터일 수 있다. 사용자 클라이언트 컴퓨터는 또한 마이크로폰, 스피커(들), 카메라, 웹 브라우저 소프트웨어 등을 포함할 수 있다. 게다가, 스테이션들은 또한 인터넷(240)과 같은 네트워크를 통해서 통신하기 위한, USB, 이더넷 및 유사한 인터페이스들을 포함할 수 있다.

[0015] 도 4를 특히 참조하면, 본 발명은 공유 도메인 명칭을 이용하여 불량(rogue) 서버로의 크리덴셜 유출로부터 단일 사인-온 도메인을 보호하기 위한 다른 방법으로 구현(embody)될 수 있다. 이 방법은, 도메인 레벨(예컨대, domain_name.com) 쿠키를 이용하여 서브도메인 서버들을 인증할 수 있고, 그 이후에 별도의 서브도메인 특정 쿠키들을 생성할 수 있다. 단일 사인-온을 위해, 도메인 내의 서브도메인(예컨대, cs1.domain_name.com)에서의 제 1 컨텐츠 서버(230-1)에 의해 호스팅된 웹사이트로의 액세스를 요청하는(단계 410) 사용자 브라우저 클라이언트(220)는 서브도메인 login.domain_name.com을 이용하는 인증 서버(210)에 리디렉션될 수 있다(단계 414). 인증 서버는 리디렉션 요청을 수신할 수 있고, 그후 그 도메인에 대한 사용자의 크리덴셜들을 입수한다(procure)(단계 418, 422 및 426).

[0016] 이상적으로, 인증 서버는 특정 하위 레벨의 서브도메인들(예컨대, cs1.domain-name.com)에 대한 쿠키들을 생성할 수 있다. 그러나, 일치하지 않는 서브도메인 명칭에 대해서는 쿠키가 설정될 수 없다. 대신에, 인증 서버는 도메인: domain_name.com에 대한 사용-제한된 쿠키(예컨대, 일회 사용 쿠키) 내에 일회 세션 키를 생성할 수 있다. 또한, 인증 서버는 서브도메인: login.domain_name.com에 대한 인증-서버-특정 쿠키를 생성할 수 있고, 그 쿠키들을 브라우저 클라이언트에 제공할 수 있다(단계 430). 사용자의 브라우저 클라이언트가, 액세스하기 원하는 웹사이트에 domain_name.com 쿠키를 먼저 부여하는 경우(단계 434), 웹사이트는 인증 서버와 그 세션을 체크할 수 있다(단계 438 및 442). 인증은 쿠키의 재사용을 방지하기 위해 그 세션을 무효화하고(단계 446), 그후 그 세션이 유효했었음을 웹사이트에 나타낸다(단계 450). 다음으로, 웹사이트는, 자신의 하위 레벨의 서브도메인에 대한 세션 쿠키를 사용자 브라우저 클라이언트에 부여하기에 안전함을 인지한다(단계 454).

[0017] 사용자 브라우저 클라이언트(220)가 제 2 컨텐츠 서버(230-2)에 의해 호스팅된 다른 서브도메인 내의 웹사이트에 대해(against) 인증하기 희망하면(단계 458), 이는 인증 서버(210)로 리디렉션될 수 있다(단계 462). 사용자 브라우저 클라이언트는, 도메인: domain_name.com에 대한 새로운 일회 사용 쿠키를 리턴할 수 있는 인증 서버에 더 일찍 획득된(단계 430) login.domain_name.com 쿠키를 제공할 수 있다(단계들 466 및 470). 제 1 컨텐츠 서버(단계들 434-454)에서와 마찬가지로, 새로운 일회 사용 쿠키는, 인증 서버로의 질의에 의해 사용자 브라우저 클라이언트를 인증하도록 제 2 컨텐츠 서버에 의해 사용될 수 있고 요청된 컨텐츠를 제공한다(단계 474-494). 이제, 사용자 브라우저 클라이언트가 제 2 컨텐츠 서버로부터의 서브도메인 쿠키를 가지는 경우, 세션 동안 그 서브도메인(cs2.domain- name.com) 내에서 재-인증할 필요는 없다.

[0018] domain_name.com 쿠키의 사용-제한된 양상은, 보호된 웹사이트로의 액세스를 획득하기 위해 domain_name.com 쿠키를 다른 웹사이트가 재생하는 것을 방지한다. 무효화된 domain_name.com 쿠키가 재사용되면, 제 2 인증 시도는 실패할 것이며, 그 사용자에게 그들의 크리덴셜들이 프롬프트될 것이다.

[0019] 추가적으로, 무효화된 쿠키를 전송하는 낭비 시간을 방지하기 위해, 짧은 만료 시간들을 갖는 domain_name.com 쿠키들이 생성된다. 본 발명의 방법은 전달되는 메시지들의 수를 증가시키지만, 이는 사용자 대신에 어떠한 추가적인 액션도 요구하지는 않는다.

[0020] 오직 1개보다 많은 접속에 대해 유효한 쿠키들만이 서브도메인 특정 쿠키들이기 때문에, 이러한 쿠키들이 단일 사인-온 도메인 내에서 다른 서브도메인들의 웹사이트들에 전송되지 않으므로 이 방법은 더욱 안전할 수 있다. 따라서, login.domain_name.com 서브도메인에 대한 쿠키가 인증 서버 이외에 어떠한 웹사이트들 또는 서버들에 제공되지 않기 때문에, 예를 들어, 불량 웹사이트로의 크리덴셜 유출이 방지될 수 있다.

[0021] 본 발명의 다른 양상은, 사용자 브라우저 클라이언트(220)에 인증 쿠키(102)를 제공하기 위한 수단(310) — 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜(112)을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 —; 브라우저 클라이언트로부터의 액세스 요청(114) 내에서 인증 쿠키를 수신하기 위한 수단(310) — 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청(118)에 응답하여 단일 사인-온 도메인 내에서 컨텐츠 서버(230)로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(116)에 기초함 —; 수신된 인증 쿠키에서의 사용자 인증 크리덴셜의 인증시에, 단일 사인-온 도메인에 대한 사용-제한된 쿠키(132)를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하기 위한 수단(310); 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청(134)을 컨텐츠 서버로부터 수신하기 위한 수단(310) — 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 —; 및 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컨텐츠 서버가 요청된 컨텐츠(184)를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지(182)를 컨텐츠 서버에 제공하기 위한 수단(310)을 포함하는 인증 서버(210)에 속할 수 있다.

[0022] 본 발명의 다른 양상은: 사용자 브라우저 클라이언트(220)에 인증 쿠키(102)를 제공하고 — 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜(112)을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 —; 브라우저 클라이언트로부터의 액세스 요청(114) 내에서 인증 쿠키를 수신하고 — 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청(118)에 응답하여 단일 사인-온 도메인 내에서 컨텐츠 서버(230)로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(116)에 기초함 —; 수신된 인증 쿠키에서 사용자 인증 크리덴셜의 인증시에, 단일 사인-온 도메인에 대한 사용-제한된 쿠키(132)를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하고; 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청(134)을 컨텐츠 서버로부터 수신하고 — 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 —; 그리고 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컨텐츠 서버가 요청된 컨텐츠(184)를 사

용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지(182)를 컨텐츠 서버에 제공하도록 구성된 프로세서(320)를 포함하는 인증 서버에 속할 수 있다.

[0023] 본 발명의 다른 양상은: 컴퓨터(310)로 하여금 사용자 브라우저 클라이언트에 인증 쿠키(102)를 제공하게 하기 위한 코드 – 인증 쿠키는, 단일 사인-온 도메인에 대한 적어도 하나의 사용자 인증 크리덴셜(112)을 갖고, 단일 사인-온 도메인의 인증 서브도메인과 관련됨 –; 컴퓨터(310)로 하여금 브라우저 클라이언트로부터의 액세스 요청(114) 내에서 인증 쿠키를 수신하게 하기 위한 코드 – 액세스 요청은 사용자 브라우저 클라이언트로부터의 컨텐츠 요청(118)에 응답하여 단일 사인-온 도메인 내에서 컨텐츠 서버(230)로부터 사용자 브라우저 클라이언트에 의해 수신된 리디렉션(116)에 기초함 –; 수신된 인증 쿠키에서 사용자 인증 크리덴셜의 인증시에, 컴퓨터(310)로 하여금 단일 사인-온 도메인에 대한 사용-제한된 쿠키(132)를 사용자 브라우저 클라이언트에 포워딩함으로써 액세스 요청에 응답하게 하기 위한 코드; 컴퓨터(310)로 하여금 사용-제한된 쿠키의 세션 식별자를 유효화하기 위한 요청(134)을 컨텐츠 서버로부터 수신하게 하기 위한 코드 – 컨텐츠 서버는 사용자 브라우저 클라이언트로부터 사용-제한된 쿠키를 수신했음 –; 및 사용-제한된 쿠키의 세션 식별자의 유효화 시에, 컴퓨터(310)로 하여금 컨텐츠 서버가 요청된 컨텐츠(184)를 사용자 브라우저 클라이언트에 포워딩할 수 있게 하기 위한 유효 세션 메시지(182)를 컨텐츠 서버에 제공하게 하기 위한 코드를 포함하는 컴퓨터-판독가능 매체(330)를 포함하는 컴퓨터 프로그램 물건에 속할 수 있다.

[0024] 당업자들은 정보 및 신호들이 다양한 상이한 기술들 및 기법들 중 임의의 것을 이용하여 표현될 수 있다는 것을 이해할 것이다. 예를 들어, 전술한 설명 전반에 걸쳐 참조될 수 있는 데이터, 명령들, 커맨드들, 정보, 신호들, 비트들, 심볼들 및 칩들은 전압들, 전류들, 전자기파들, 자기장들 또는 자기 입자들, 광 필드들 또는 광 입자들, 또는 이들의 임의의 조합에 의해 표현될 수 있다.

[0025] 당업자들은 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 회로들 및 알고리즘 단계들이 전자 하드웨어, 컴퓨터 소프트웨어 또는 이 둘의 조합들로서 구현될 수 있다는 것을 또한 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 교환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 일반적으로 이들의 기능과 관련하여 위에서 설명되었다. 이러한 기능이 하드웨어로서 구현되는지 아니면 소프트웨어로서 구현되는지는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 좌우된다. 당업자들은 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 발명의 범위를 벗어나게 하는 것으로 해석되어서는 안된다.

[0026] 본원에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들 및 회로들은 범용 프로세서, 디지털 신호 프로세서(DSP), 주문형 집적 회로(ASIC), 필드 프로그래머블 게이트 어레이(FPGA) 또는 다른 프로그래머블 로직 디바이스, 이산 게이트 또는 트랜지스터 로직, 이산 하드웨어 컴포넌트들 또는 본원에서 설명된 기능들을 수행하도록 설계된 이들의 임의의 조합을 통해 구현되거나 또는 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안적으로 이 프로세서는 임의의 기존의 프로세서, 컨트롤러, 마이크로컨트롤러 또는 상태 머신일 수 있다. 프로세서는 또한 컴퓨팅 디바이스들의 조합, 예를 들어, DSP와 마이크로프로세서의 조합, 복수의 마이크로프로세서들, DSP 코어와 연결된 하나 또는 그 초과의 마이크로프로세서들 또는 임의의 다른 이러한 구성으로서 구현될 수 있다.

[0027] 본원의 개시된 실시예들과 관련하여 설명된 방법 또는 알고리즘의 단계들은 직접 하드웨어로 구현되거나, 프로세서에 의해 실행되는 소프트웨어 모듈로 구현되거나, 또는 이 둘의 조합으로 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터들, 하드 디스크, 탈착식 디스크, CD-ROM, 또는 당업계에 공지된 임의의 다른 형태의 저장 매체에 상주할 수 있다. 예시적인 저장 매체는, 프로세서가 저장 매체로부터 정보를 판독하고 저장 매체에 정보를 기록할 수 있도록, 프로세서에 커플링된다. 대안적으로, 저장 매체는 프로세서에 통합될 수 있다. 프로세서 및 저장 매체는 ASIC 내에 상주할 수 있다. ASIC는 사용자 단말 내에 상주할 수 있다. 대안적으로, 프로세서 및 저장 매체는 사용자 단말 내에 이산 컴포넌트들로서 상주할 수 있다.

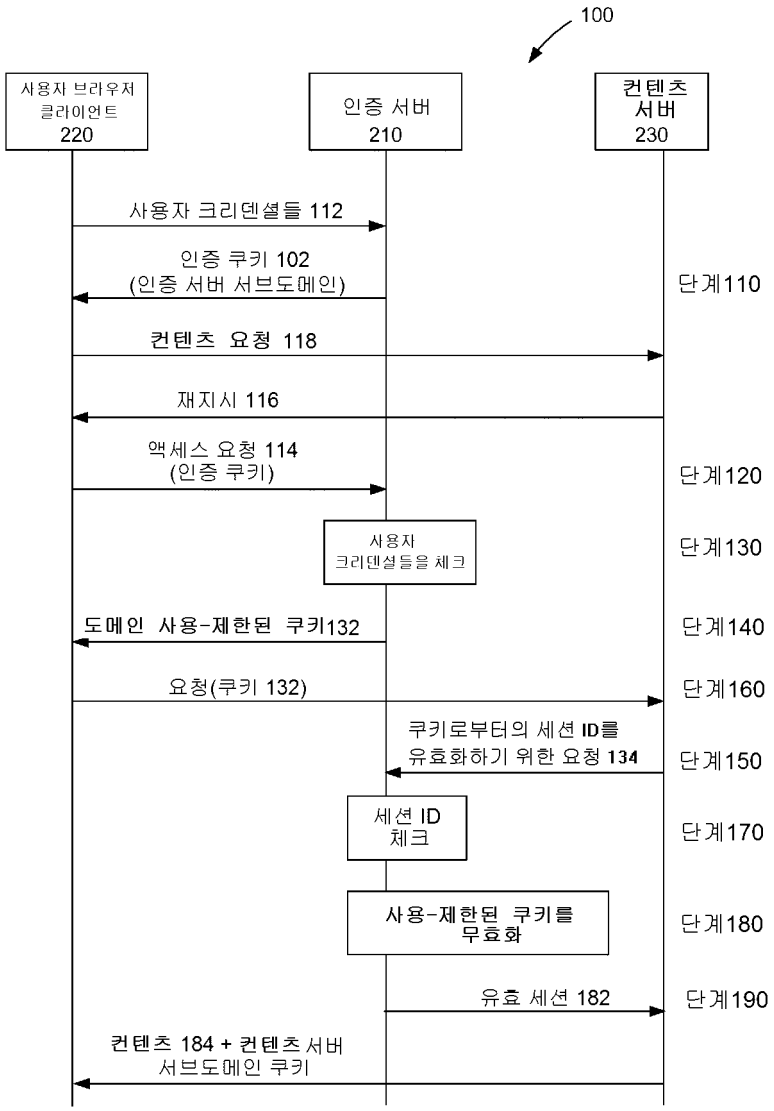
[0028] 하나 또는 그 초과의 예시적인 실시예들에서, 설명된 기능들은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 임의의 조합으로 구현될 수 있다. 컴퓨터 프로그램 물건으로서 소프트웨어로 구현되는 경우, 상기 기능들은 컴퓨터-판독가능 매체 상의 하나 또는 그 초과의 명령들 또는 코드로서 저장될 수 있다. 컴퓨터-판독가능 매체는 한 장소에서 다른 장소로 컴퓨터 프로그램의 전달을 가능하게 하는 컴퓨터 저장 매체를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 한정이 아닌 예시에 의해, 이러한 컴퓨터-

판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장부, 자기 디스크 저장부 또는 다른 자기 저장 디바이스들, 또는 명령들 또는 데이터 구조들의 형태로 원하는 프로그램 코드를 저장하기 위해 사용될 수 있고 컴퓨터에 의해 액세스될 수 있는 임의의 다른 매체를 포함할 수 있다. 본원에 사용되는 디스크(disk) 및 디스크(disc)는 콤팩트 디스크(CD: compact disc), 레이저 디스크(laser disc), 광학 디스크(optical disc), 디지털 다기능 디스크(DVD: digital versatile disc), 플로피 디스크(floppy disk) 및 블루-레이 디스크(blu-ray disc)를 포함하며, 여기서 디스크(disk)들은 통상적으로 자기적으로 데이터를 재생하는 반면에 디스크(disc)들은 레이저들을 통해 데이터를 광학적으로 재생한다. 전술한 것들의 조합들이 또한 컴퓨터-판독가능 매체의 범위 내에 포함되어야 한다. 컴퓨터-판독가능 매체는, 일시적 전파 신호를 포함하지 않도록, 비-일시적일 수 있다.

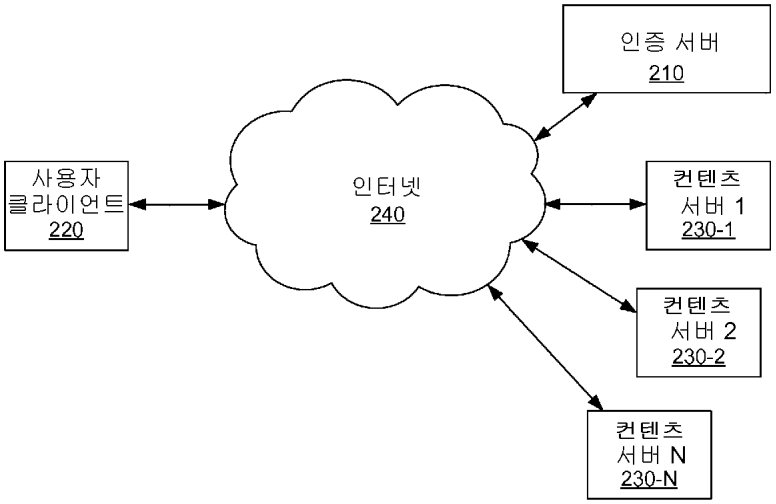
[0029] 개시된 실시예들의 이전의 설명은 임의의 당업자가 본 발명을 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 당업자들에게 용이하게 명백할 것이며, 본원에 정의된 일반 원리들은 본 발명의 범위 또는 사상을 벗어나지 않고 다른 실시예들에 적용될 수 있다. 그리하여, 본 발명은 본원에 나타낸 실시예들로 제한되는 것으로 의도되지 않고, 본원에 개시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에 부합할 것이다.

## 도면

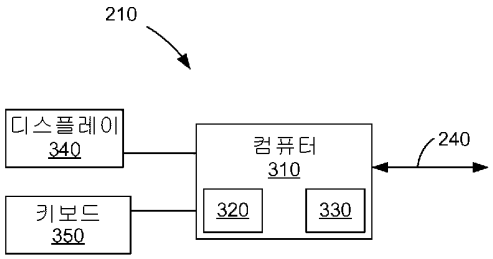
### 도면1



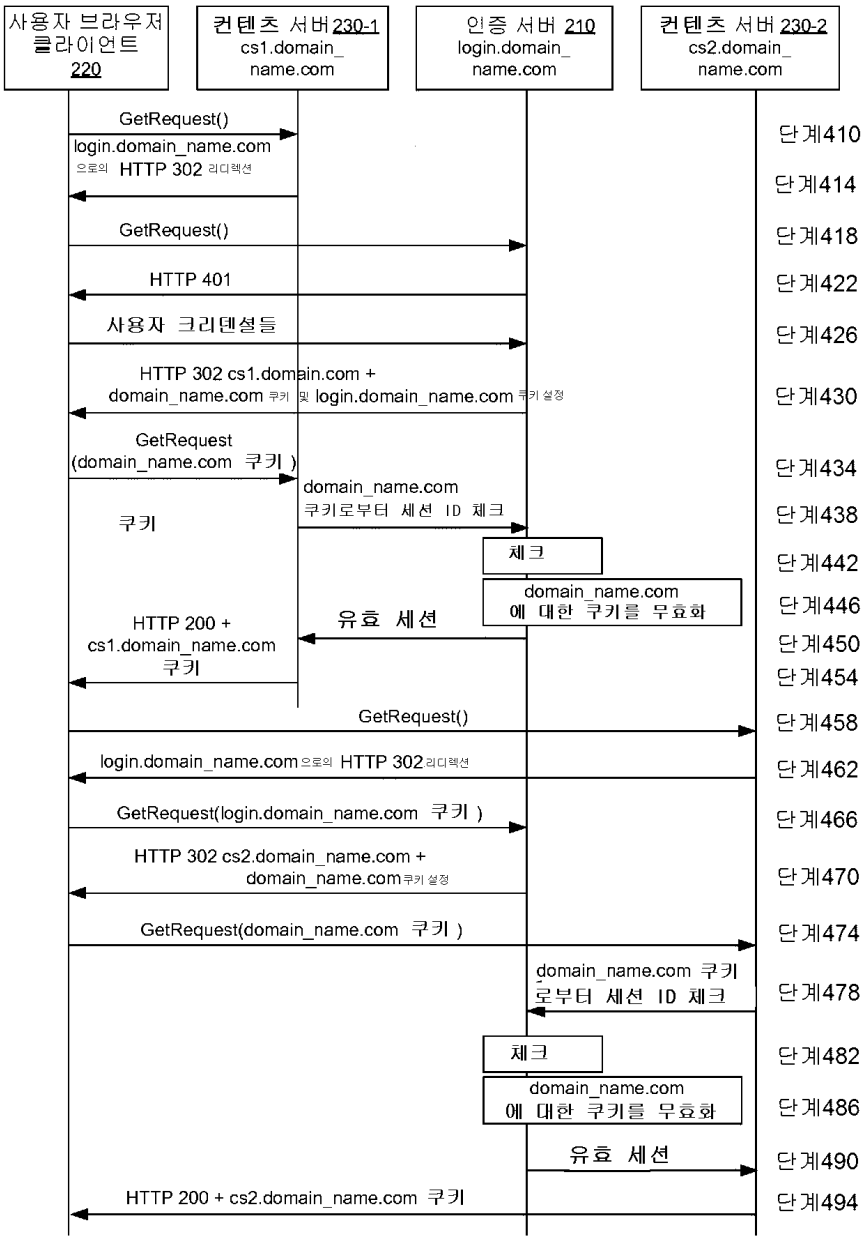
도면2


인증 서버
210
사용자
클라이언트
220
인터넷
240
컨텐츠
서버 1
230-1
컨텐츠
서버 2
230-2
컨텐츠
서버 N
230-N

도면3


210
디스플레이
340
키보드
350
컴퓨터
310
320
330
240

도면4


사용자 브라우저 클라이언트 220
컨텐츠 서버 230-1 cs1.domain_name.com
인증 서버 210 login.domain_name.com
컨텐츠 서버 230-2 cs2.domain_name.com
GetRequest()
login.domain_name.com 으로의 HTTP 302 리디렉션
단계410
단계414
GetRequest()
단계418
HTTP 401
단계422
사용자 크리덴셜들
단계426
HTTP 302 cs1.domain.com + domain_name.com 쿠키 및 login.domain_name.com 쿠키 설정
단계430
GetRequest (domain_name.com 쿠키 )
단계434
domain_name.com 쿠키로부터 세션 ID 체크
단계438
쿠키
체크
단계442
domain_name.com 에 대한 쿠키를 무효화
단계446
유효 세션
HTTP 200 + cs1.domain_name.com 쿠키
단계450
단계454
GetRequest()
단계458
login.domain_name.com 으로의 HTTP 302 리디렉션
단계462
GetRequest(login.domain_name.com 쿠키 )
단계466
HTTP 302 cs2.domain_name.com + domain_name.com 쿠키 설정
단계470
GetRequest(domain_name.com 쿠키 )
단계474
domain_name.com 쿠키 로부터 세션 ID 체크
단계478
체크
단계482
domain_name.com 에 대한 쿠키를 무효화
단계486
유효 세션
단계490
HTTP 200 + cs2.domain_name.com 쿠키
단계494