(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0053419
(43) 공개일자 2011년05월23일

(51) Int. Cl.
G06F 15/16 (2006.01)
(21) 출원번호 10-2011-7001682
(22) 출원일자(국제출원일자) 2009년06월17일
심사청구일자 없음
(85) 번역문제출일자 2011년01월21일
(86) 국제출원번호 PCT/US2009/047709
(87) 국제공개번호 WO 2010/011449
국제공개일자 2010년01월28일
(30) 우선권주장
12/258,787 2008년10월27일 미국(US)
61/083,474 2008년07월24일 미국(US)

(71) 출원인
프론트 포치 인크
미국 캘리포니아주 95370 소노라 모노 웨이 14520 스위트 200
(72) 발명자
브리톤 자카리 에드워
미국 캘리포니아주 95379 툴럼 요세미트 로드 18170
맥슨 데렉 스티븐
미국 캘리포니아주 95383 태인 하테 피오 박스 479
(뒷면에 계속)
(74) 대리인
신정건, 김태홍

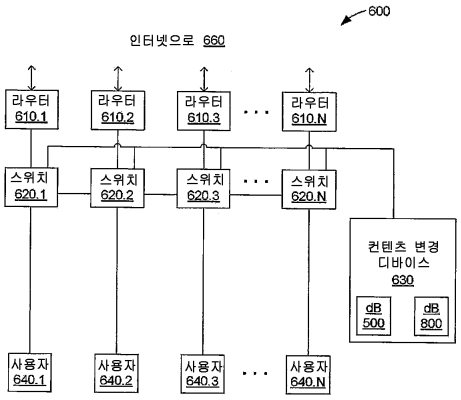
전체 청구항 수 : 총 21 항

(54) 인터넷 사용자의 프라이버시 명령을 실행하는 방법 및 장치

(57) 요 약

인터넷 사용자의 프라이버시 명령을 실행하는 방법이 개시되어 있다. 본 방법에서, 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링한다. 비순응 상태 정보를 포함한 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경한다. 대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷(replacement packet)을 수신하도록 대체 패킷(replacement packet)을 사용자 클라이언트에 전달한다. 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는다.

대 표 도 - 도6



(72) 발명자

블러처 브라이언 매튜

미국 캘리포니아주 95361 오크데일 알몬드크레스트 코트 774

플레쳐 타보 후세인

미국 캘리포니아주 95370 소노라 엘 푸마 서클 21748

스미스 스콧 케네스

미국 캘리포니아주 95355 모데스토 애시브룩 드라이브 2701

바즈퀘즈 카를로스 알버토

미국 캘리포니아주 91910 출라 비스타 텔레그라프 캐뇬 로드 #185 591

특허청구의 범위

청구항 1

인터넷 사용자의 프라이버시 명령을 실행하는 방법에 있어서,

사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링하는 것과,

비순응 상태 정보를 포함한 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하는 것과,

대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하는 것

을 포함하며,

상기 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 2

제1항에 있어서, 상기 상태 정보는 쿠키인 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 3

제1항에 있어서, 상기 상태 정보는 클라이언트 서버 상태 정보인 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 4

제1항에 있어서, 상기 복사된 패킷을 모니터링하는 것은

상기 상태 정보를 포함하는 웹 컨텐츠 요청이 타겟으로 되는 광고와 연관된 도메인을 갖고 있는지 여부를 결정하는 것과,

상기 타겟으로 되는 광고와 연관된 도메인과 사용자의 프라이버시 명령에 의해 커버된 도메인의 데이터베이스를 비교하는 것

을 포함하는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 5

제1항에 있어서, 상기 상태 정보를 변경하는 것은, 타겟으로 되는 광고 프로그램으로부터 사용자 클라이언트를 제거하도록 상기 상태 정보 내의 값을 설정하는 것을 포함하는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 6

제1항에 있어서, 사용자의 프라이버시 명령의 순응성은 상기 복사된 패킷 내에 포함된 인터넷 프로토콜(IP) 어드레스를 이용하여 결정되는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 7

제1항에 있어서, 상기 상태 정보를 변경하는 것은, 상기 상태 정보로부터 사용자의 프라이비트 엘리먼트(user private element)를 제거하는 것을 포함하는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 8

제1항에 있어서, 웹 컨텐츠 요청은 http get 커맨드인 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 9

제1항에 있어서, 웹 컨텐츠 요청은 http post 커맨드인 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 10

제1항에 있어서, 상기 모니터링하는 것, 상기 변경하는 것 및 상기 전달하는 것은 사용자 클라이언트에 비대칭 인터넷 액세스를 제공하는 서비스 네트워크에 의해 수행되는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 11

제1항에 있어서, 상기 복사된 패킷은 컨텐츠 변경 스테이션(station)으로 미러링된 패킷을 포함하는 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 12

제1항에 있어서,

상기 상태 정보는 사용자의 프라이버시 명령에 순응하도록 컨텐츠 변경 스테이션에 의해 변경되고,

상기 컨텐츠 변경 스테이션은 사용자 클라이언트와 타겟 서버 사이에서의 최초의 패킷의 경로에 있지 않은 것인 사용자의 프라이버시 명령을 실행하는 방법.

청구항 13

인터넷 사용자의 프라이버시 명령을 실행하는 장치에 있어서,

사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링하는 수단과,

비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하는 수단과,

대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하는 수단

을 포함하며,

상기 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는 것인 사용자의 프라이버시 명령을 실행하는 장치.

청구항 14

제13항에 있어서, 상기 상태 정보는 쿠키인 것인 사용자의 프라이버시 명령을 실행하는 장치.

청구항 15

제13항에 있어서, 상기 상태 정보는 클라이언트 서버 상태 정보인 것인 사용자의 프라이버시 명령을 실행하는 장치.

청구항 16

제13항에 있어서, 사용자의 프라이버시 명령의 순응성은 상기 복사된 패킷 내에 포함된 인터넷 프로토콜(IP) 어드레스를 이용하여 결정되는 것인 사용자의 프라이버시 명령을 실행하는 장치.

청구항 17

제13항에 있어서, 상기 복사된 패킷은 컨텐츠 변경 스테이션(station)으로 미러링된 패킷을 포함하는 것인 사용자의 프라이버시 명령을 실행하는 장치.

청구항 18

컴퓨터 프로그램 제품에 있어서,

컴퓨터 판독가능 매체를 포함하고,

상기 컴퓨터 판독가능 매체는,

컴퓨터로 하여금 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링하도록 하는 코드와,

컴퓨터로 하여금 비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하도록 하는 코드와,

컴퓨터로 하여금 대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하도록 하는 코드

를 포함하며,

상기 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는 것인 컴퓨터 프로그램 제품.

청구항 19

제18항에 있어서, 상기 상태 정보는 쿠키인 것인 컴퓨터 프로그램 제품.

청구항 20

제18항에 있어서, 상기 상태 정보는 클라이언트 서버 상태 정보인 것인 컴퓨터 프로그램 제품.

청구항 21

제18항에 있어서, 사용자의 프라이버시 명령의 순응성은 상기 복사된 패킷 내에 포함된 인터넷 프로토콜(IP) 어드레스를 이용하여 결정되는 것인 컴퓨터 프로그램 제품.

명 세 서

기 술 분 야

[0001] 본 발명은 인터넷 사용자 프라이버시에 관한 것으로, 보다 자세하게는, 원하지 않은 레이턴시를 발생시킴이 없이 인터넷 사용자의 프라이버시 명령을 실행하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 인터넷 사용자는 자신들이 웹사이트를 방문할 때 추적될 것에 대하여 점점더 우려하고 있다. 확장적으로 쿠키를 이용하는 사용자들 사이에서 광고 네트워크는 미래의 광고와 컨텐츠 개별화에 이용하기 위하여 사용자에 대한 정보를 기록한다. 이들 서비스를 탈퇴하기를 원하는 사용자들은 상당한 장애에 직면한다. 사용자의 탈퇴 선택을 유지하기 위해 쿠키를 이용하는 것은 지속적인 해결책은 아니다. 추가로, 수백개의 광고 네트워크와 수백만의 도메인이 존재하기 때문에, 사용자 선택의 지속성을 보장하는 것은 다루기가 힘들다.

[0003] 사용자의 탈퇴 선택은 다음 사건들 - 1) 새로운 컴퓨터의 구매, 또는 기존의 컴퓨터 상의 재로딩, 2) 새로운 웹 브라우저의 사용, 3) 인터넷에 액세스하는 동일한 컴퓨터 상의 다른 프로파일, 4) 기존의 쿠기가 비가역적으로 클리어됨, 5) 쿠키들이 보안 프로그램에 의해 클리어됨, 또는 6) 탈퇴 쿠키가 만료됨 - 중 어느 하나 이상으로 인해 손실될 수 있다. 대부분의 사용자는 자신들의 탈퇴 선택이 너무 쉽게 "잊혀질" 수 있음을 알지 못한다.

[0004] 또한, 인터넷 사용자를 답답하게 하는 것은 육백개 이상의 광고 네트워크가 현재 있으며, 이러한 네트워크가 모두 사용자가 탈퇴하는 것을 허용하는 것은 아니라는 것이다. 또한, 광고 네트워크에 의해 무슨 정보가 이미 수집되어 왔는지에 대하여 사용자가 아는 것도 어렵다.

[0005] 프라이버시 옹호자들은 전화 마켓팅에 대한 "수신 거부(Do Not Call)" 리스트와 유사하게, 목표로 되는 광고의 탈퇴를 위한 중앙 집중식 접근 방식을 생성할 것을 수개의 나라의 기관에 요청하였다. 현재, 정부 기관은 인터넷 사용자 프라이버시에 접근하기 위한 통일된 표준을 설정하지 않았으며, 광고 네트워크는 수입 감소 가능성으로 인해 탈퇴에 대한 간단한 액세스 기능을 제공하지 않으려 한다.

발명의 내용

해결하려는 과제

[0006] 따라서, 효율적이고 비용 효과적인 방식으로 인터넷 사용자의 프라이버시 문제를 해결하는 것이 필요하다. 본 발명은 이들 요구를 만족시킨다.

과제의 해결 수단

[0007] 본 발명의 일 양상은 인터넷 사용자의 프라이버시 명령을 실행하는 방법에 있을 수 있다. 본 방법에서, 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링한다. 비순응 상태 정보를 포함한 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경한다. 대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷(replacement packet)을 수신하도록 대체 패킷(replacement packet)을 사용자 클라이언트에 전달한다. 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는다.

[0008] 본 발명의 보다 자세한 양상에서는, 상태 정보가 쿠키와 같은 클라이언트-서버 상태 정보일 수 있다. 사용자의 프라이버시 명령의 순응성은 복사된 패킷 내에 포함된 인터넷 프로토콜(IP) 어드레스를 이용하여 결정될 수 있다. 웹 컨텐츠 요청은 http 겟 커맨드(get command) 또는 http 포스트 커맨드(post command)일 수 있다. 복사된 패킷은 컨텐츠 변경 스테이션(station)으로 미러링된 패킷을 포함할 수 있다.

[0009] 본 발명의 다른 보다 자세한 양상에서는, 복사된 패킷의 모니터링은 상태 정보를 포함하는 웹 컨텐츠 요청이 타겟으로 되는 광고와 연관된 도메인을 갖고 있는지 여부를 결정하는 것과, 타겟으로 되는 광고와 연관된 도메인과, 사용자의 프라이버시 명령에 의해 커버된 도메인의 데이터베이스를 비교하는 것을 포함한다. 또한, 상태 정보를 변경하는 것은, 타겟으로 되는 광고 프로그램으로부터 사용자 클라이언트를 제거하도록 상태 정보 내의 값을 설정하는 것과, 상태 정보로부터 사용자 프라이비트 엘리먼트(user private element)를 제거하는 것을 포함할 수 있다. 상태 정보는 사용자의 프라이버시 명령에 순응하도록 컨텐츠 변경 스테이션에 의해 변경될 수 있다. 컨텐츠 변경 스테이션은 사용자 클라이언트와 타겟 서버 사이에서의 최초의 패킷의 경로에 있지 않을 수 있다. 모니터링, 변경, 및 전달 단계는 사용자 클라이언트에 비대칭 인터넷 액세스를 제공하는 서비스 네트워크에 의해 수행될 수 있다.

[0010] 본 발명의 다른 양상은 인터넷 사용자의 프라이버시 명령을 실행하는 장치에 있을 수 있다. 본 장치는, 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링하는 수단과, 비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하는 수단과, 대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하는 수단을 포함하며, 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는다.

[0011] 본 발명의 또 다른 양상은 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품에 있을 수 있으며, 컴퓨터로 하여금 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들에 기초하는 복사된 패킷을 모니터링하도록 하는 코드와, 컴퓨터로 하여금 비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하도록 하는 코드와, 컴퓨터로 하여금 대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하도록 하는 코드를 포함하며, 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션을 갖는다.

발명의 효과

[0012] 원하지 않은 레이턴시를 발생시킴이 없이 인터넷 사용자의 탈퇴 명령을 실행하게 하여 인터넷 사용자의 프라이버시 침해를 보호할 수 있다.

도면의 간단한 설명

[0013] 첨부된 도면은 본 발명의 실시예들을 설명하며, 상세한 설명과 함께 본 발명의 원리를 설명하는 것을 돕는다.

도 1은 예시적인 쿠키 구조를 나타내는 스크릿 샷(shot)을 나타낸다.

도 2는 쿠키 변경 프로세스를 나타내는 흐름도이다.

도 3은 패킷 변경 프로세스를 나타내는 흐름도이다.

도 4는 본 발명에 따른 예시적인 대체 쿠키를 나타낸다.

도 5는 쿠키 변경 파라미터를 저장하는 예시적인 도메인 데이터베이스를 나타낸다.

도 6은 컨텐츠 변경 디바이스를 이용하여 비대칭 라우팅 네트워크에 대한 네트워크 도면을 나타낸다.

도 7은 컨텐츠 변경 디바이스에 의해 발생된 예시적인 대체 패킷을 나타낸다.

도 8은 프라이버시 명령과 같은 사용자 서비스 파라미터를 저장하기 위한 예시적인 사용자 데이터베이스를 나타낸다.

도 9는 본 발명에 따라 사용자의 프라이버시 명령을 실행하는 방법을 나타내는 흐름도이다.

도 10은 본 발명에 따라 사용자의 프라이버시 명령을 실행하는 트랜잭션들을 보여주는 개략도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명은 원하지 않는 레이턴시를 일으키지 않고 네트워크 디바이스를 통한 한번의 클릭으로 많은 광고 및 개인화 서비스에 대한 웹 사용자의 프라이버시 명령을 관리하는 방법 및 장치를 제공한다. 탈퇴를 위하여 광고 네트워크 도메인 및 쿠키의 데이터베이스가 유지된다. 데이터베이스는 탈퇴를 지원하지 않는 네트워크 뿐만 아니라 탈퇴를 지원하는 광고 네트워크를 포함한다.

[0015] 웹 사용자 프라이버시 선택 및 명령이 중요시되는지 여부를 결정하기 위하여, 도메인 및 쿠키 컨텐츠에 대하여 착신 HTTP 요청을 조사한다. 컨텐츠 변경 디바이스에 의해 레이턴시가 사실상 유도되지 않기 때문에 인터넷과 사용자 클라이언트 사이의 네트워크가 전속력으로 연속하게끔 허용하는 미러 포트 또는 탭과 같은 디바이스에 의해 컨텐츠 변경 디바이스에 발신 TCP 포트 80 트래픽을 전달할 수 있다.

[0016] 컨텐츠 변경 디바이스는 최초에 요청된 웹 서버의 IP 어드레스를 획득하여 하나 이상의 패킷을 발신 컴퓨터 및 서비스 네트워크에 직접 전송함으로써, HTTP 트랜잭션을 변경할 수 있다. 새로운 패킷은 서비스 네트워크 상의 발신 컴퓨터에 예정되고, 웹 서버의 IP 어드레스로부터 전송될 것으로 나타난다. TCP 시퀀스 값(SEQ)은 HTTP 요청을 포함한 패킷으로부터의 확인 응답 수이며, TCP 확인응답 값(ACK)은 HTTP 요청을 포함한 패킷의 SEQ에, 스푸프 프레임(spoof frame) 내의 TCP 데이터의 길이를 더한 값이다. 애플리케이션 계층에서의 HTTP 응답은 표준 HTTP 302 리디렉션에 쿠키에 대한 임의의 변경 추가를 더한 것이다. 이 변경은 탈퇴를 유지하도록 새로운 쿠키 엘리먼트의 삽입 또는 쿠키 제거 명령을 포함할 수 있다. 리디렉션은 HTTP를 통하여 전송될 수 있는 임의의 컨텐츠를 포함한 임의의 서버에 형성될 수 있다. 컨텐츠 변경 디바이스는 이 패킷 삽입을, 웹 서버로부터의 응답 전에 도달하도록 매우 신속하게 수행할 수 있어야 한다.

[0017] 네트워크 어플라이언스는 도메인 네임 또는 IP 어드레스에 의해 수신된 HTTP 트랜잭션을 평가한다. 도메인 또는 IP 어드레스가 도메인 데이터베이스 내의 기록과 매칭하면, 사용자의 프라이버시 명령의 어떠한 위반에 대해 쿠키를 관찰한다. 어떤 프라이비트 정보의 위반 또는 식별의 이벤트에서, 새로운 HTTP 응답은 위반한 쿠키 엘리먼트를 제거하도록 그리고 필요에 따라 탈퇴 기준을 쿠키 내에 설정하도록 구성될 수 있다.

[0018] 본 방법은 완전한 가정용 또는 국부 네트워크에 대해 모든 관련 쿠키들에 대해 지속적인 탈퇴 명령을 제공한다. 추가로, 네트워크 서비스 제공자는 개개의 사용자 쿠키 관리를 위한 클라이언트 측 소프트웨어 제품을 통하기보다 네트워크 서버 측 솔루션을 통하여 탈퇴 서비스를 사용자에게 제공한다.

[0019] 도 1을 참조하여 보면, 사용자 브라우저 쿠키 테이블(100)의 예시적인 디스플레이는 사용자 브라우저 인스탄스에 대한 쿠키의 대응 리스트(120)에 대한 도메인 리스트(110)를 보여준다. 각각의 쿠키 130.1 및 130.2는 컨텐츠, 도메인, 경로, 전송 및 만료와 같은 파라미터를 갖는다. 이 인스탄스에서, 하나의 쿠키(140)는 사용자가 탈퇴하였음을 표시하는 탈퇴 엘리먼트를 나타낸다. 이 예에서, 사용자가 탈퇴하였음(엘리먼트(140))에도 불구하고, 특정 프라이버시 엘리먼트가 제거되지 않았음을 중요시 해야 한다.

[0020] 도 2를 참조하여 보면, 쿠키는 사용자의 프라이버시 선택 또는 명령에 순응하도록 변경될 수 있다. 도 2를 나타

냄에 있어, 1) 인터넷 사용자는 사용자에 의해 이루어진 요청을 수신할 수 있는 컨텐츠 변경 디바이스를 갖는 네트워크 서비스 제공자의 서비스 네트워크를 통하여 인터넷에 연결되는 것으로 본다. 인터넷 사용자는 웹 페이지에 대한 HTTP 요청과 같은, 원격으로 위치된 서버로부터의 컨텐츠 요청을 생성한다. 도 3의 HTTP 변경 프로세스에 의해 입력을 수신한다(단계 210). 평가를 위하여 패킷을 수신한다(단계 220). 도 5에 나타낸 도메인 데이터베이스를 이용함으로써 HTTP 요청에 대한 도메인을 식별한다(단계 230). 도메인이 테이블 내의 기록과 매칭하면(단계 240), 프로세스는 단계 250로 진행하고, 그렇지 않으면, 프로세스는 패킷 또는 메타데이터에 대한 어떠한 변경 없이 부모 프로세스(도 3)로 리턴한다(단계 245). 또한 도메인 데이터베이스를 참조하여, 쿠키 내의 탈퇴 엘리먼트를 식별한다(단계 250). 탈퇴 엘리먼트가 쿠키 내에 없다면, 탈퇴 엘리먼트를 추가하도록 쿠키를 변경한다. 탈퇴의 부분이 아닌 쿠키 내에서 찾아지는 임의의 다른 기준을 식별하기 위해 쿠키를 평가한다(단계 260). 프라이비트 기준을 찾으면, 쿠키로부터 프라이비트 명령을 제거하라는 삭제 명령을 대체 쿠키 데이터에 추가한다(단계 265). 단계 250 및 단계 260의 결과를 평가하고, 이들 중 어느 단계가 긍정 결과를 발생시키면(단계 270), 변경된 쿠키를 도 3의 부모 프로세스에 리턴한다(단계 280). 그렇지 않으면, 루틴은 변경없이 리턴된다(단계 245).

[0021] 도 3을 참조하여 보면, HTTP 패킷을 컨텐츠 변경 디바이스에 의해 수신한다(단계 310). IP 어드레스, 포트, 및 L7 데이터와 같은 네트워크 엘리먼트를 결정하기 위해 패킷을 검사한다(단계 320). 패킷 내에서 찾아진 IP 어드레스를 도 8에 나타낸 사용자 데이터베이스에 대해 비교한다(단계 330). IP 어드레스가 찾아지지 않으면, 패킷은 변경에 대해 적합하지 않아 폐기된다(단계 390). IP 어드레스가 찾아지면, 요청에서의 쿠키 데이터가 존재하는지를 평가하도록 패킷에 대해 평가한다.(단계 340). 요청에서의 쿠키 데이터가 존재하는 패킷이라면, 패킷을 도 2의 쿠키 평가 프로세스로 전송한다(단계 350). 패킷이 요청에서의 쿠키 데이터를 포함하지 않는다면, 패킷을 폐기한다(단계 390). 쿠키 평가 프로세스로부터의 응답을 평가한다(단계 360). 응답이 변경되지 않으면, 패킷을 폐기한다(단계 390). 응답이 변경되면, 대체 또는 스푸프 응답 패킷을 구성한다(단계 370). 그 후, 원하는 웹 서버로 다시 보내라는 302의 응답을 패킷 라우팅 정보 내에 캡슐화하고, 스푸프된 패킷을 요청자에 전달될 네트워크 상에 되전송한다(단계 380).

[0022] 도 4는 본 발명에 따른 예시적인 대체 쿠키(400)를 나타낸다. 쿠키 내의 파라미터의 특성들이 변할 수 있지만, 구조는 쿠키의 구조를 기술하는 IETF RFC 2109에 일치한다. Set-Cookie에 대한 커맨드(410)를 채택하여, 웹 브라우저에 쿠키를 수락할 것을 명령한다. 쿠키는 탈퇴를 위해 속성 및 값이 변경되는데(420), 여기서 예시적인 속성은 NAI이고, 예시적인 값은 OPT_OUT이다. 경로 430가 표시된다. 이 예에서, 경로는 전체 도메인이다. 쿠키의 만료 시간 440이 설정된다.

[0023] 도 5는 적용가능한 도메인에 대한 쿠키 변경 파라미터를 저장하는 예시적인 도메인 데이터베이스(500)를 나타낸다. 데이터베이스의 이용은 도 2와 관련하여 위에 설명되어 있다. 참여 데이터베이스(500; participant database)는, 1) 쿠키 변경이 수행될 수 있는 임의이 도메인들에 대한 도메인 네임을 포함한 도메인 필드(510)와, 2) 대체 쿠키에 대한 탈퇴 키 속성을 포함하는 탈퇴 키 필드(520)와, 3) 속성에 기인하는 값을 포함하는 탈퇴 값 필드(530)를 갖는다.

[0024] 도 6은 본 발명에 따른 컨텐츠 변경 디바이스를 이용하여 비대칭 라우팅 네트워크에 대한 예시적인 네트워크 도면을 나타낸다. 도 6을 나타냄에 있어, 다음과 같은 것으로 본다. 1) 비대칭 방법을 이용하여 구성되고 인터넷에 대한 하나 이상의 연결을 각각 갖는 복수의 라우터들이 존재한다(비대칭 방법에서는, 동일한 플로우에 관련된 패킷들이 임의의 라우터를 통하여 수신되고 임의의 라우터를 통하여 국부 네트워크를 나갈 수 있다); 2) TCP 흐름은 라우터(610.1)를 통하여 라우팅될 수 있고 라우터(610.3)에 의해 원격 호스트로 진행하며 수신될 수 있다(스위칭된 네트워크는 패킷이 자신의 의도된 수신지에 도달하는 것을 보장할 것이다); 3) 컨텐츠 변경 디바이스(630)가 존재한다; 그리고 인터넷 사용자는 웹 페이지에 대한 HTTP 요청과 같은, 원격으로 위치된 서버로부터의 컨텐츠 요청을 생성한다.

[0025] 인터넷 사용자(640)는 웹 브라우저에서 도메인을 선택함으로써 웹 페이지를 요청한다. 컴퓨터의 TCP 스택은 스위칭된 네트워크(620)에 전송된 일련의 패킷을 구성시킨다. 이들 패킷의 복사본은 미러링 포트, 탭 또는 다른 유사한 방법을 통하여 컨텐츠 변경 디바이스(630)에 전송된다. 컨텐츠 변경 디바이스에 전송된 패킷들은, 패킷 내의 다른 수신지 포트로서 포트(80) 및 다른 HTTP 포트를 이용하여 이들 패킷들이 TCP 패킷임을 요청하는 규칙에 의해 필터링될 수 있다. 인터넷(660)으로부터 리턴된 패킷은 임의의 라우터(610)에 의해 수신되어 사용자 클라이언트(640)으로의 임의의 경로 상에 전송될 수 있고, 인터넷으로부터의 이들 패킷은 컨텐츠 변경 디바이스에 의해 요구되지 않는다. 컨텐츠 변경 디바이스는 도메인 데이터베이스(500)와 사용자 데이터베이스(800)를 포함

할 수 있거나 또는 이들 데이터베이스에 액세스할 수 있다.

[0026] 도 7은 컨텐츠 변경 디바이스에 의해 발생된 예시적인 대체 패킷(700)을 나타낸다. IP 헤더(710)가 변경되며, 여기서 소스 어드레스는 최초의 요청의 수신지였던 서버의 IP 어드레스이며, 수신지 어드레스는 발신 컴퓨터 디바이스의 IP 어드레스로 설정된다. 옵션 및 체크섬(checksum)과 같은 다른 필요한 IP 헤더들(720)은 표준 인터넷 프로토콜(RFC 791)에 따라 적절하게 설정된다. TCP 헤더(730)가 변경되며, 여기서 소스 포트는 최초의 요청에서의 수신지 포트로 설정된다. 수신지 포트는 최초의 요청의 소스 포트로 설정된다. TCP SEQ 및 ACK 수(740)가 변경되며, 여기서 이들 값은 전송 제어 프로토콜(RFC 675, 등)에 따라 설정된다. TCP 체크섬(750)이 표준의 전송 제어 프로토콜에 따라 계산된다. HTTP 응답(760)이 설정되고, 여기서 대체 쿠키는 동일한 또는 상이한 수신지일 수 있는 수신지로의 리디렉션으로 전송된다. 응답은 컴퓨터로 하여금 새로운 컨텐츠에 대한 새로운 HTTP 요청을 발생시키도록 하는 사용자의 컴퓨터로 전송되어 변경이 완료하게 된다.

[0027] 도 8은 사용자의 서비스 파라미터를 저장하는 예시적인 사용자 데이터베이스(800)를 보여준다. 데이터베이스의 이용은 도 3과 관련하여 위에 설명되어 있다. 참여 데이터베이스(800; participant database)는, 1) 컨텐츠 변경 디바이스(630)로부터 서비스들을 수신할 수 있는 사용자의 현재 IP 어드레스들을 포함하는 IP 어드레스 필드(810)와; 2) 대체될 쿠키의 유형들에 대응하는 하나 이상의 선택적 서비스 유형들을 포함하는 서비스 유형 필드(820)를 갖는다. 서비스 유형 필드는 프라이버시 명령을 나타내는 값(1, 2, 3)을 가질 수 있다. 이 값은 요청된 프라이버시의 레벨을 증가시키는 것에 대응할 수 있다.

[0028] 도 9 및 도 10을 참조하여 보면, 본 발명의 일 양상은 인터넷 사용자의 프라이버시 명령을 실행하는 방법(900)에 있을 수 있다. 본 방법에서, 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트(640)로부터 전송된 최초의 패킷들(1010)에 기초하는 복사된 패킷(1020)을 모니터링한다(단계 910). 비순응 상태 정보를 포함한 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시(단계 920), 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경한다(단계 930). 대응하는 최초의 패킷의 타겟 서버(660)로부터 응답 패킷(1040)을 수신하기 전에 사용자 클라이언트가 대체 패킷(1030; 도 7에서의 700)을 수신하도록 대체 패킷(1030)을 사용자 클라이언트에 전달한다. 대체 패킷은 변경된 상태 정보(400)를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션(1050)을 갖는다.

[0029] 상태 정보는 쿠키(140)와 같은 클라이언트-서버 상태 정보일 수 있다. 사용자의 프라이버시 명령의 순응성은 복사된 패킷(1020) 내에 포함된 인터넷 프로토콜(IP) 어드레스(810)를 이용하여 결정될 수 있다. 웹 컨텐츠 요청은 http get 커맨드(command) 또는 http post 커맨드일 수 있다. 복사된 패킷은 컨텐츠 변경 스테이션(station) 또는 디바이스(630)로 미러링된 패킷을 포함할 수 있다.

[0030] 복사된 패킷(1020)의 모니터링은 상태 정보를 포함하는 웹 컨텐츠 요청이 타겟으로 되는 광고와 연관된 도메인을 갖고 있는지 여부를 결정하는 것과, 타겟으로 되는 광고와 연관된 도메인과, 사용자의 프라이버시 명령에 의해 커버된 도메인(510)의 데이터베이스를 비교하는 것을 포함한다. 또한, 상태 정보를 변경하는 것은, 타겟으로 되는 광고 프로그램으로부터 사용자 클라이언트를 제거하도록 상태 정보 내의 값(530)을 설정하는 것과, 상태 정보로부터 사용자 프라이비트 엘리먼트(user private element)를 제거하는 것을 포함할 수 있다. 상태 정보는 사용자의 프라이버시 명령에 순응하도록 컨텐츠 변경 스테이션(630)에 의해 변경될 수 있다. 바람직하게는, 컨텐츠 변경 스테이션은 사용자 클라이언트(640)와 타겟 서버(660) 사이에서의 최초의 패킷의 경로에 있지 않을 수 있다. 모니터링, 변경, 및 전달 단계는 사용자 클라이언트에 비대칭 인터넷 액세스를 제공하는 네트워크 서비스 제공자의 서비스 네트워크에 의해 수행될 수 있다.

[0031] 본 발명의 다른 양상은 인터넷 사용자의 프라이버시 명령을 실행하는 장치에 있을 수 있다. 본 장치는, 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트(640)로부터 전송된 최초의 패킷들(1010)에 기초하는 복사된 패킷(1020)을 모니터링하는 수단(630)과, 비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하는 수단(630)과, 대응하는 최초의 패킷의 타겟 서버(660)로부터 응답 패킷(1040)을 수신하기 전에 사용자 클라이언트가 대체 패킷(1030)을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하는 수단(620 및 630)을 포함하며, 대체 패킷은 변경된 상태 정보를 포함한, 갱신된 웹 컨텐츠 요청(760)을 갖는 리디렉션(1050)을 갖는다.

[0032] 본 발명의 또 다른 양상은 컴퓨터 판독가능 매체를 포함하는 컴퓨터 프로그램 제품에 있을 수 있으며, 컴퓨터로 하여금 사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트(640)로부터 전송된 최초의 패킷들(1010)에 기초하는 복사된 패킷(1020)을 모니터링하도록 하는 코드와, 컴

퓨터로 하여금 비순응 상태 정보를 포함하는 웹 컨텐츠 요청을 갖는 복사된 패킷의 검출시, 사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경하도록 하는 코드와, 컴퓨터로 하여금 대응하는 최초의 패킷의 타겟 서버(660)로부터 응답 패킷(1040)을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷(1030)을 사용자 클라이언트에 전달하도록 하는 코드를 포함하며, 대체 패킷은 변경된 상태 정보(400)를 포함한, 갱신된 웹 컨텐츠 요청(760)을 갖는 리디렉션(1050)을 갖는다.

[0033] 당해 기술 분야의 숙련된 자는 정보와 신호가 여러 가지 서로 다른 기술 및 기법 중 어느 것을 이용하여 나타내어질 수 있음을 이해할 것이다. 예를 들어, 상술한 설명 전반에 걸쳐 참조될 수 있는, 데이터, 명령, 커맨드, 정보, 신호, 비트, 심볼, 및 칩들은 전압, 전류, 전자기파, 자기장, 또는 자기입자, 광학장 또는 광학 입자, 또는 이들의 임의의 조합에 의해 나타내어질 수 있다.

[0034] 당해 기술 분야의 숙련된 자는 또한, 본 명세서에 설명된 실시예와 연결된 여러 예시적인 논리 블록, 모듈, 회로 및 알고리즘 단계가, 전자 하드웨어, 컴퓨터 소프트웨어, 또는 이들의 조합으로서 구현될 수 있음을 알 것이다. 하드웨어 및 소프트웨어의 상호교환성을 명확히 설명하기 위하여, 다양한 예시적인 컴포넌트, 블록, 모듈, 회로 및 단계들은 일반적으로 그들의 기능성 관점에서 위에서 설명되었다. 이러한 기능성이 하드웨어로 구현되든 소프트웨어로 구현되든 간에, 특정 애플리케이션에 의존하며, 전체 시스템에 설계 구속요건이 부여된다. 당해 기술 분야의 숙련된 자는 각각의 특정 애플리케이션에 대한 다양한 방식으로 설명된 기능성을 구현할 수 있지만, 이러한 구현 결정은 본 발명의 범위로부터 벗어나게 하는 것으로 해석되어서는 안된다.

[0035] 본 명세서에 설명된 실시예들과 연결되어 설명된 여러 예시적인 논리 블록, 모듈, 및 회로는 범용 프로세서, 디지털 신호 처리기(DSP), 응용 주문형 집적 회로(ASIC), 필드 프로그래밍가능 게이트 어레이(FPGA) 또는 다른 프로그래밍가능한 논리 디바이스, 별도의 게이트, 또는 트랜지스터 로직, 별도의 하드웨어 컴포넌트 또는 본 명세서에 설명된 기능을 수행하도록 설계된 이들의 임의의 조합으로 구현될 수 있거나 수행될 수 있다. 범용 프로세서는 마이크로프로세서일 수 있지만, 대안으로서, 프로세서는 임의의 통상의 프로세서, 컨트롤러, 마이크로컨트롤러, 또는 스테이틱 머신일 수 있다. 프로세서는 컴퓨팅 디바이스의 조합, 예를 들어, DSP, 및 DSP 코어 또는 이러한 임의의 다른 구성과 결합한 마이크로프로세서, 복수의 마이크로프로세서, 하나 이상의 마이크로프로세서의 조합으로서 또한 구현될 수도 있다.

[0036] 본 명세서에 설명된 실시예들과 결합하여 설명된 방법 또는 알고리즘 단계는 하드웨어로, 프로세서에 의해 실행된 소프트웨어 모듈로 또는 이 둘의 조합으로 직접 구현될 수 있다. 소프트웨어 모듈은 RAM 메모리, 플래시 메모리, ROM 메모리, EPROM 메모리, EEPROM 메모리, 레지스터, 하드디스크, 탈착가능 디??, CD-ROM, 또는 당해 기술에 알려진 임의의 다른 형태의 저장 매체에 존재할 수 있다. 예시적인 저장 매체는 프로세서에 연결되어, 프로세서가 저장 매체로부터 정보를 읽을 수 있고 저장 매체에 정보를 기록할 수 있도록 한다. 대안으로서, 저장 매체는 프로세서와 일체형일 수 있다. 프로세서와 저장 매체는 ASIC 내에 존재할 수 있다. ASIC은 사용자 단말에 존재할 수 있다. 대안으로서, 프로세서 및 저장 매체는 사용자 단말 내의 별도의 컴포넌트로서 존재할 수 있다.

[0037] 하나 이상의 예시적인 실시예에서, 설명된 기능은 하드웨어, 소프트웨어, 펌웨어, 또는 이들의 임의의 조합으로 구현될 수 있다. 컴퓨터 프로그램 제품으로서 소프트웨어로 구현되면, 컴퓨터 판독가능 매체 상에 하나 이상의 명령 또는 코드상에 함수가 저장될 수 있거나 또는 코드를 통하여 함수가 전달될 수 있다. 컴퓨터 판독가능 매체는 하나의 위치에서 다른 위치로 컴퓨터 프로그램의 전달을 용이하게 하는 임의의 매체를 포함하는 컴퓨터 저장 매체 및 통신 매체 양쪽 모두를 포함한다. 저장 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 이용가능한 매체일 수 있다. 예들 들어, 비제한적으로, 이러한 컴퓨터 판독가능 매체는 RAM, ROM, EEPROM, CD-ROM 또는 다른 광학 디스크 저장 장치, 자기 디스크 저장 장치 또는 다른 자기 저장 디바이스, 또는 컴퓨터에 의해 액세스될 수 있고 명령 또는 데이터 구조의 형태로 원하는 프로그램 코드를 전달 또는 저장하는데 이용될 수 있는 임의의 다른 매체를 포함할 수 있다. 또한, 임의의 연결부는 컴퓨터 판독가능 매체로 적절하게 불린다. 예를 들어, 소프트웨어가 웹사이트, 서버, 또는 다른 원격 소스로부터 동축 케이블, 광섬 유 케이블, 트위스티드 페어, 디지털 가입자 회선(DSL), 또는 적외선, 무선, 마이크로웨이브와 같은 무선 기술을 이용하여 전달되면, 동축 케이블, 광섬유 케이블, 트위스티드 페어, DSL, 또는 적외선, 무선, 마이크로웨이브와 같은 무선 기술은 매체의 정의 내에 포함된다. 여기에 이용된 disk 또는 disc는 컴팩트 디스크(CD), 레이저 디스크, 광 디스크, DVD(digital versatile disc), 플로피 디스크, 및 블루레이 디스크를 포함하며, 여기서 disk는 통상 데이터를 자기적으로 재생하는 한편 disc는 통상 레이저로 광학적으로 데이터를 재생한다. 위의 조합이 또한 컴퓨터 판독가능 매체의 범위 내에 포함될 수 있다.

[0038] 개시된 실시예의 이전 설명은 당해 기술 분야의 숙련된 자가 본 발명을 이용 및 형성하도록 제공된다. 이들 실시예에 대한 여러 변형이 당해 기술 분야의 숙련된 자에게 쉽게 명백해질 것이며, 본 명세서에 정의된 일반 원리는 본 발명의 범위 또는 사상에 벗어남이 없이 다른 실시예들에도 적용될 수 있다. 따라서, 본 발명은 본 명세서에 설명된 실시예들로 제한되도록 의도되지 않으며, 본 명세서에 개시된 신규의 특징 및 원리에 부합하는 가장 넓은 범위로 적응되어야 한다.

부호의 설명

[0039] 610: 라우터

620: 스위치

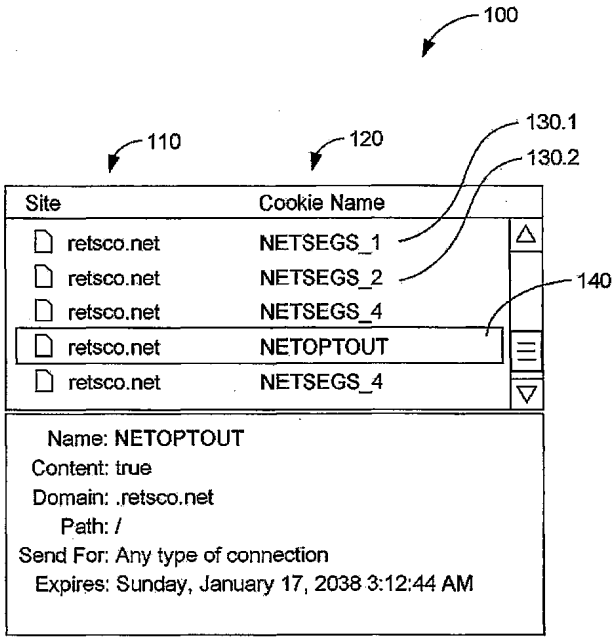
630: 컨텐츠 변경 디바이스

640: 사용자 클라이언트

660: 웹 서버

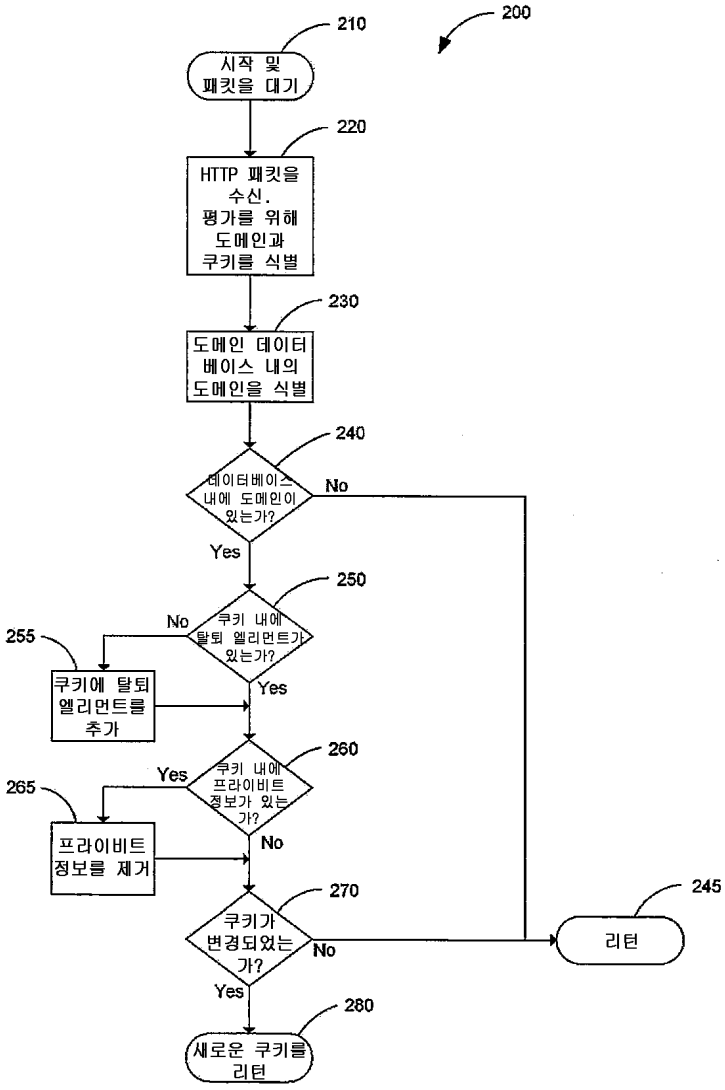
도면

도면1

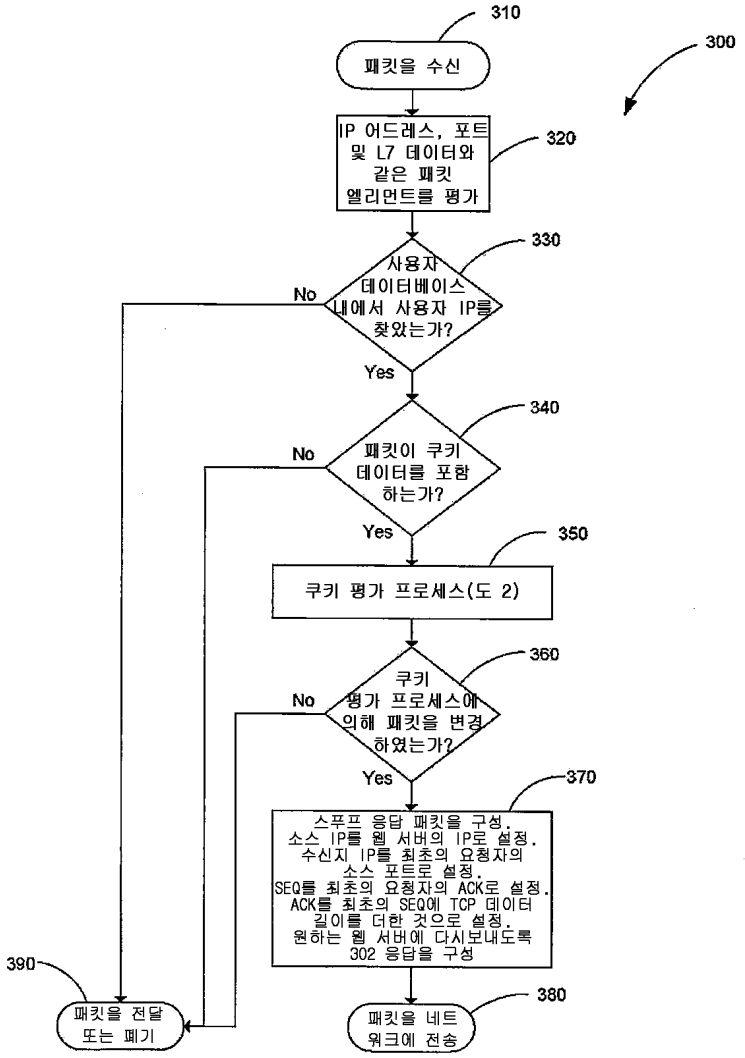


(종래 기술)

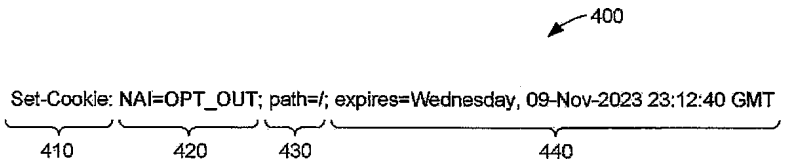
도면2


200
210
시작 및 패킷을 대기
220
HTTP 패킷을 수신. 평가를 위해 도메인과 쿠키를 식별
230
도메인 데이터 베이스 내의 도메인을 식별
240
데이터베이스 내에 도메인이 있는가?
No
Yes
250
쿠키 내에 탈퇴 엘리먼트가 있는가?
No
255
쿠키에 탈퇴 엘리먼트를 추가
Yes
260
쿠키 내에 프라이비트 정보가 있는가?
Yes
265
프라이비트 정보를 제거
No
270
쿠키가 변경되었는가?
No
245
리턴
Yes
280
새로운 쿠키를 리턴

도면3


310
패킷을 수신
300
IP 어드레스, 포트 및 L7 데이터와 같은 패킷 엘리먼트를 평가
320
330
사용자 데이터베이스 내에서 사용자 IP를 찾았는가?
No
Yes
340
패킷이 쿠키 데이터를 포함하는가?
No
Yes
350
쿠키 평가 프로세스(도 2)
360
쿠키 평가 프로세스에 의해 패킷을 변경하였는가?
No
Yes
370
스푸프 응답 패킷을 구성.
소스 IP를 웹 서버의 IP로 설정.
수신지 IP를 최초의 요청자의 소스 포트로 설정.
SEQ를 최초의 요청자의 ACK로 설정.
ACK를 최초의 SEQ에 TCP 데이터 길이를 더한 것으로 설정.
원하는 웹 서버에 다시보내도록 302 응답을 구성
380
패킷을 네트워크에 전송
390
패킷을 전달 또는 폐기

도면4

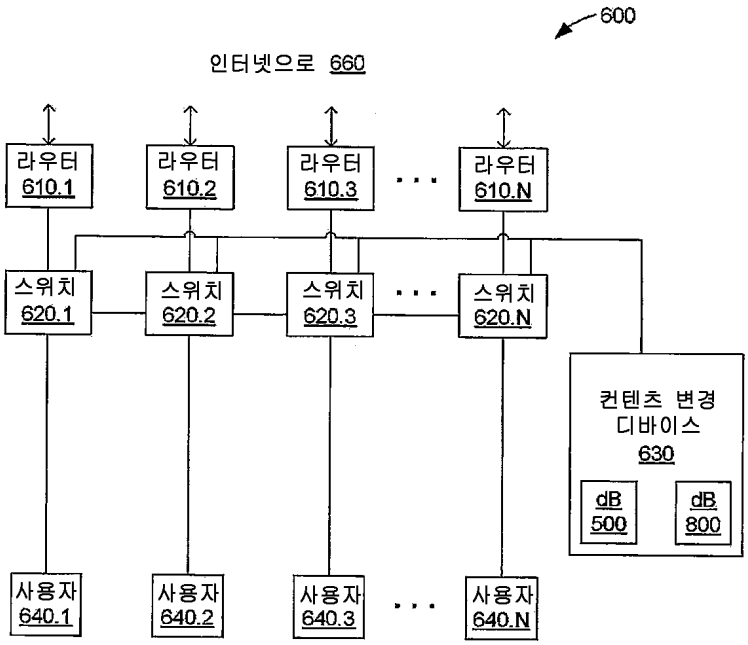

400
Set-Cookie: NAI=OPT_OUT; path=/; expires=Wednesday, 09-Nov-2023 23:12:40 GMT
410
420
430
440

도면5

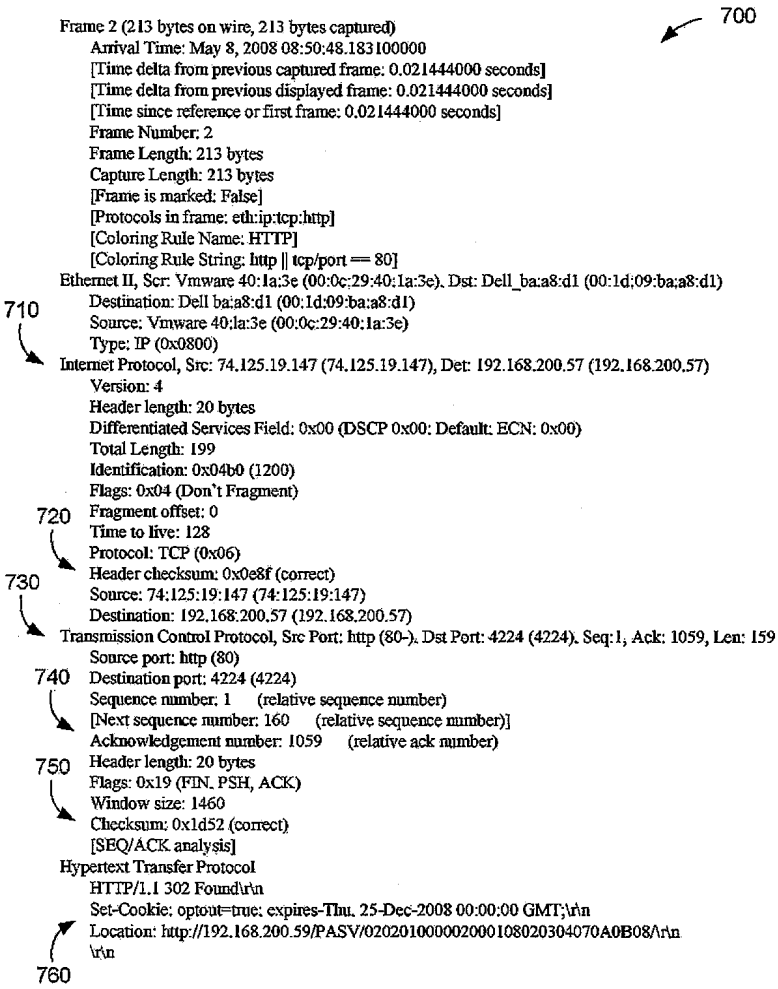
500

510	520	530
도메인	탈퇴 키	탈퇴 값
.retsco.net	NETOPTOUT	TRUE
.adrotator.com	NAI	OPT_OUT
.spclick.net	NAI	1
.togada.net	TID	togaoptout
.google.com		

도면6



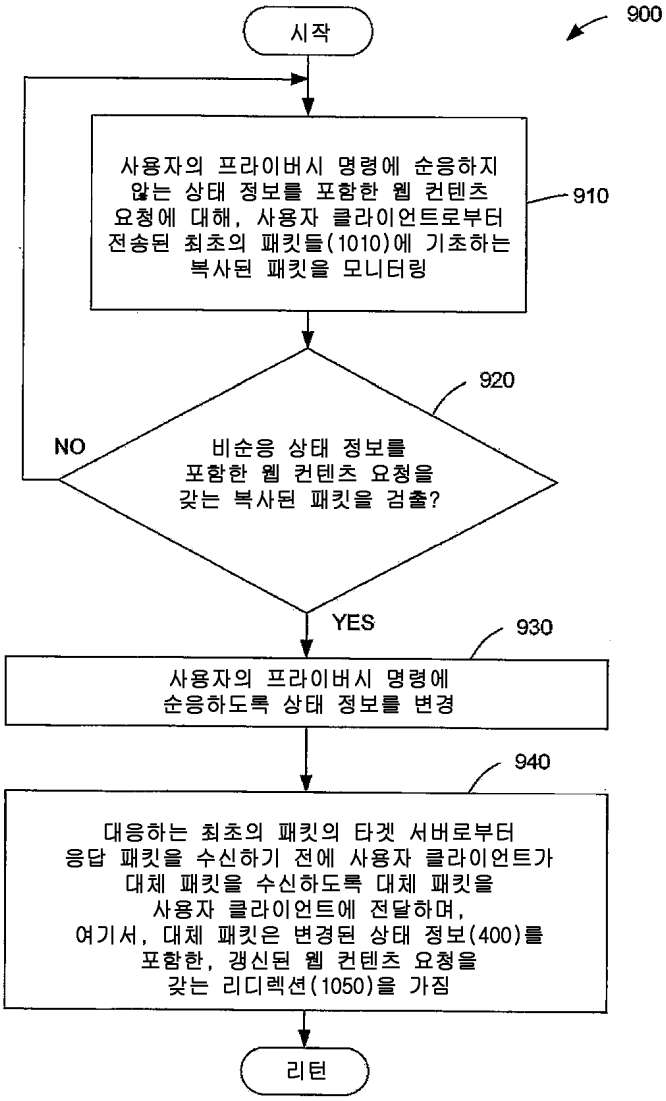
도면7



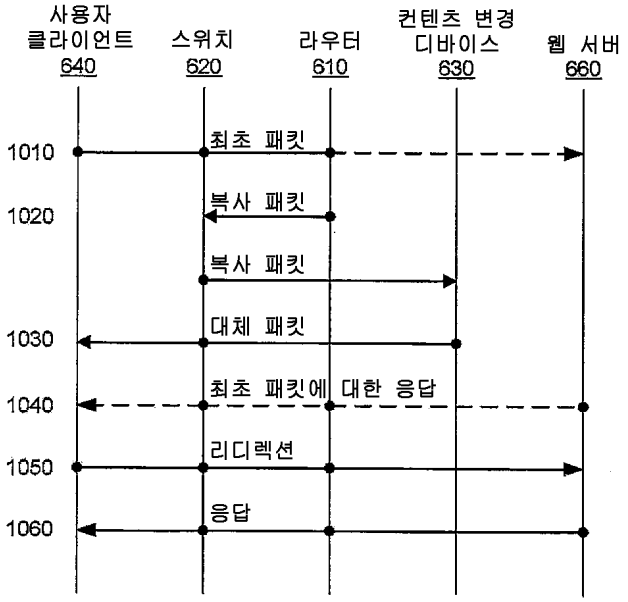
도면8

810 IP 어드레스	820 서비스 유형
10.10.10.1	1
10.10.10.2	2
10.10.10.3	2
10.10.10.4	1
10.10.10.5	3

도면9


900
시작
사용자의 프라이버시 명령에 순응하지 않는 상태 정보를 포함한 웹 컨텐츠 요청에 대해, 사용자 클라이언트로부터 전송된 최초의 패킷들(1010)에 기초하는 복사된 패킷을 모니터링
910
920
NO
비순응 상태 정보를 포함한 웹 컨텐츠 요청을 갖는 복사된 패킷을 검출?
YES
930
사용자의 프라이버시 명령에 순응하도록 상태 정보를 변경
940
대응하는 최초의 패킷의 타겟 서버로부터 응답 패킷을 수신하기 전에 사용자 클라이언트가 대체 패킷을 수신하도록 대체 패킷을 사용자 클라이언트에 전달하며, 여기서, 대체 패킷은 변경된 상태 정보(400)를 포함한, 갱신된 웹 컨텐츠 요청을 갖는 리디렉션(1050)을 가짐
리턴

도면10


사용자
클라이언트
640
스위치
620
라우터
610
컨텐츠 변경
디바이스
630
웹 서버
660
1010
최초 패킷
1020
복사 패킷
복사 패킷
1030
대체 패킷
1040
최초 패킷에 대한 응답
1050
리디렉션
1060
응답