(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년10월10일
(11) 등록번호 10-1071132
(24) 등록일자 2011년09월30일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2003-0082077
(22) 출원일자 2003년11월19일
심사청구일자 2008년10월24일
(65) 공개번호 10-2004-0044375
(43) 공개일자 2004년05월28일
(30) 우선권주장
60/428,152 2002년11월20일 미국(US)
10/459,863 2003년06월12일 미국(US)
(56) 선행기술조사문헌
US05757920 A1
US4972472 A
JP11272614 A
KR1019980070202 A
전체 청구항 수 : 총 25 항

(73) 특허권자
마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이
(72) 발명자
브레이스웰샤운데릭
미국98019워싱턴주두발284번사이클엔이14008
워드리차드비.
미국98053워싱턴주레드몬드261번애비뉴엔이8565
(뒷면에 계속)
(74) 대리인
제일특허법인

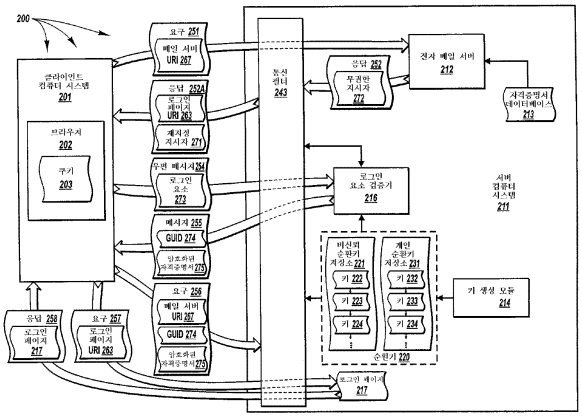
심사관 : 이형일

(54) 클라이언트 컴퓨터 시스템에서 리소스에 액세스할 권한을 부여받는 데에 사용되는 클라이언트측 자격 증명서를 보증하는 방법, 사용자 자격 증명서를 보존하는 방법, 사용자 자격 증명서의 유효성을 결정하는 방법 및 컴퓨터 판독가능 기록 매체

(57) 요 약

본 발명은 리소스에 웹 기반으로 액세스하기 위하여 사용되는 클라이언트 자격 증명서를 안전하게 처리하는 방법을 제공한다. 사용자 자격 증명서를 입력하기 위한 인터페이스를 구비하는 로그인 페이지가 클라이언트에 제공되고, 입력된 사용자 자격 증명서는 서버로 송신된다. 사용자 자격 증명서의 수신에 응답하여, 서버는 클라이언트에 대한 고유 세션 식별자를 생성한다. 서버는 또한 순환 키 저장소의 최근의 키 및 고유 세션 식별자에 기초하여 사용자 자격 증명서를 위한 전자 서명을 추출한다. 서버는 이어서 최근의 키와 고유 세션 식별자로부터 추출된 암호화 키에 기초하여 전자 서명 및 사용자 자격 증명서를 암호화한다. 암호화된 자격 증명서가 다시 클라이언트에게 수신될 때, 순환 키 저장소로부터의 키들이 자격 증명서의 검증을 시도하는 데에 사용된다. 사용자 자격 증명서가 검증되지 않으면, 사용자는 다시 로그인 페이지를 제공받는다.

대 표 도



(72) 발명자

심프손제알.러셀리

미국98034워싱턴주키클랜드79번플레이스엔이11136

베티스카림미첼

미국98117워싱턴주시애틀마비애비뉴엔더블유9214

특허청구의 범위

청구항 1

서버 컴퓨터 시스템의 리소스(resource)로의 웹 기반 액세스를 시도하는 클라이언트 컴퓨터 시스템에서, 상기 리소스에 액세스할 권한을 부여받는 데에 사용되는 클라이언트측 자격 증명서(credentials)를 보증하는(secure) 방법에 있어서,

상기 클라이언트 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 제1 요구(request)를 송신하는 단계;

상기 클라이언트 컴퓨터 시스템이 로그인 페이지(login page)로 재지정되고(redirected), 상기 로그인 페이지는 사용자 자격 증명서를 수용하기 위한 인터페이스를 제공하는 단계;

상기 클라이언트 컴퓨터 시스템이 상기 로그인 페이지를 이용하여 사용자 자격 증명서를 상기 서버 컴퓨터 시스템에 제출하는 단계;

상기 클라이언트 컴퓨터 시스템이 상기 제출된 사용자 자격 증명서 및 시간 의존 서명(time-dependent signature)의 적어도 일부분을 나타내는 암호화된 정보를 수신하고, 상기 시간 의존 서명은 상기 제출된 사용자 자격 증명서 및 서명 시간 의존 키(signature time-dependent key)의 적어도 일부분으로부터 추출되며, 상기 암호화된 정보는 암호화 시간 의존 키(encryption time-dependent key)를 사용하여 암호화되고, 상기 서명 시간 의존 키 및 상기 암호화 시간 의존 키의 양쪽 모두는 순환 키 저장소(rotating key store)의 키로부터 추출되는 단계; 및

상기 클라이언트 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제2 요구를 송신하고, 상기 제2 요구는 상기 암호화된 정보를 포함하는 단계

를 포함하는 방법.

청구항 2

삭제

청구항 3

삭제

청구항 4

제1항에 있어서, 상기 클라이언트 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제1 요구를 송신하는 상기 단계는, 전자 메일 서버의 전자 메일 리소스로의 웹 기반 액세스를 요구하는 HTTP 메시지를 송신하는 단계를 포함하는 방법.

청구항 5

제1항에 있어서, 상기 클라이언트 컴퓨터 시스템이 상기 제출된 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 수신하는 상기 단계는, 고유 세션 식별자와 함께 상기 암호화된 정보를 수신하는 단계를 포함하는 방법.

청구항 6

제5항에 있어서, 상기 클라이언트 컴퓨터 시스템의 대응하는 쿠키(cookies)에 상기 수신된 암호화된 정보 및 상기 수신된 고유 세션 식별자를 저장하는 단계를 더 포함하는 방법.

청구항 7

제1항에 있어서, 상기 클라이언트 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제2 요구를 송신하는 상기 단계는, 고유 세션 식별자와 함께 상기 암호화된 정보를 송신하는 단계를 포함하는 방법.

청구항 8

제1항에 있어서, 상기 클라이언트 컴퓨터 시스템이 상기 로그인 페이지를 이용하여 사용자 자격 증명서를 서버 컴퓨터 시스템에 제출하는 상기 단계는, 상기 클라이언트 컴퓨터 시스템이 상기 로그인 페이지를 이용하여 안전한, 상호 인증된 연결(secure, mutually authenticated connection)을 통하여 사용자 자격 증명서를 상기 서버 컴퓨터 시스템에 제출하는 단계를 포함하는 방법.

청구항 9

클라이언트 컴퓨터 시스템으로부터 서버 컴퓨터 시스템의 리소스로의 웹 기반 액세스를 요구하는 요구를 수신하는 서버 컴퓨터 시스템에서, 상기 리소스에 액세스할 권한을 부여받는 데에 사용되는 클라이언트측 자격 증명서를 보증하는 방법에 있어서,

상기 서버 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 제1 요구를 수신하고, 상기 제1 요구는 상기 클라이언트 컴퓨터 시스템에 의하여 송신되는 단계;

상기 서버 컴퓨터 시스템이 상기 제1 요구에 응답하여 상기 클라이언트 컴퓨터 시스템을 로그인 페이지로 재지정하고, 상기 로그인 페이지는 상기 클라이언트 컴퓨터 시스템이 사용자 자격 증명서를 입력할 수 있도록 하는 단계;

상기 서버 컴퓨터 시스템이 상기 로그인 페이지에서 제출된 사용자 자격 증명서를 수신하는 단계;

상기 서버 컴퓨터 시스템이 상기 제출된 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 송신하고, 상기 시간 의존 서명은 상기 제출된 사용자 자격 증명서 및 서명 시간 의존 키의 적어도 일부분으로부터 추출되며, 상기 암호화된 정보는 암호화 시간 의존 키를 사용하여 암호화되고, 상기 서명 시간 의존 키 및 상기 암호화 시간 의존 키의 양쪽 모두는 순환 키 저장소의 키로부터 추출되는 단계; 및

상기 서버 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제2 요구를 수신하고, 상기 제2 요구는 상기 클라이언트 컴퓨터 시스템으로부터 송신되며 상기 암호화된 정보를 포함하는 단계

를 포함하는 방법.

청구항 10

삭제

청구항 11

삭제

청구항 12

제9항에 있어서, 상기 서버 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 제1 요구를 수신하는 상기 단계는, 전자 메일 서버의 전자 메일 리소스로의 웹 기반 액세스를 요구하는 HTTP 메시지를 수신하는 단계를 포함하는 방법.

청구항 13

제9항에 있어서, 상기 서버 컴퓨터 시스템이 상기 제출된 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 송신하는 상기 단계는, 고유 세션 식별자와 함께 상기 암호화된 정보를 송신하는 단계를 포함하는 방법.

청구항 14

제9항에 있어서, 상기 서버 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제2 요구를 수신하는 상기 단계는, 고유 세션 식별자와 함께 상기 암호화된 정보를 수신하는 단계를 포함하는 방법.

청구항 15

서버 컴퓨터 시스템 - 상기 서버 컴퓨터 시스템은 클라이언트 컴퓨터 시스템으로부터 상기 서버 컴퓨터 시스템의 리소스로의 웹 기반 액세스를 요구하는 요구를 수신함 - 에서, 상기 리소스에 액세스할 권한을 부여받는 데(to become authorized)에 사용되는 클라이언트측 자격 증명서(client-side credentials)를 보증(securing)하

는 방법에 있어서,

상기 서버 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 제1 요구를 수신하는 단계 - 상기 제1 요구는 상기 클라이언트 컴퓨터 시스템에 의하여 송신됨 -;

클라이언트측 자격 증명서가 악의적인 사용자에게 리소스로의 권한 없는 액세스를 제공할 기회를 감소시키도록, 순환 키 저장소로부터의 키를 사용하여 상기 클라이언트측 자격 증명서를 보증하는 단계 - 상기 순환 키 저장소의 키는 서명 시간 의존 키(signature time-dependent key) 및 암호화 시간 의존 키(encryption time-dependent key)를 추출하는데 이용되고, 상기 암호화 시간 의존 키는 상기 클라이언트 컴퓨터 시스템으로 송신될 암호화된 정보를 암호화하는데 이용되며, 상기 암호화된 정보는 시간 의존 서명 및 상기 클라이언트측 자격 증명서의 적어도 일부분을 나타내고, 상기 시간 의존 서명은 상기 클라이언트측 자격 증명서 및 상기 서명 시간 의존 키의 적어도 일부분으로부터 추출됨 - ; 및

상기 서버 컴퓨터 시스템이 상기 리소스로의 웹 기반 액세스에 대한 제2 요구를 수신하는 단계 - 상기 제2 요구는 상기 클라이언트 컴퓨터 시스템으로부터 송신되고 상기 암호화된 정보를 포함함 - 를 포함하는 방법.

청구항 16

클라이언트 컴퓨터 시스템에서, 서버 컴퓨터 시스템의 리소스에 웹 기반으로 액세스하기 위하여 사용되는 사용자 자격 증명서를 보존하는 방법에 있어서,

상기 클라이언트 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 요구를 송신하고, 상기 요구는 고유 세션 식별자와, 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 포함하며, 상기 시간 의존 서명은 상기 사용자 자격 증명서 및 서명 시간 의존 키의 적어도 일부분으로부터 추출되고, 상기 암호화된 정보는 암호화 시간 의존 키를 사용하여 암호화되고, 상기 서명 시간 의존 키 및 상기 암호화 시간 의존 키의 양쪽 모두는 순환 키 저장소의 키로부터 추출되는 단계;

상기 클라이언트 컴퓨터 시스템이 갱신된 고유 세션 식별자 및 리프레시된 암호화된 정보와 함께 상기 요구된 리소스를 클라이언트측 브라우저에서 수신하고, 상기 리프레시된 암호화된 정보는 상기 사용자 자격 증명서 및 리프레시된 시간 의존 서명의 적어도 일부분을 나타내며, 상기 시간 의존 서명은 상기 사용자 자격 증명서 및 리프레시된 서명 시간 의존 키의 적어도 일부분으로부터 추출되고, 상기 암호화된 정보는 리프레시된 암호화 시간 의존 키를 사용하여 암호화되며, 상기 리프레시된 서명 시간 의존 키 및 상기 리프레시된 암호화 시간 의존 키의 양쪽 모두는 상기 순환 키 저장소의 가장 최근의 키로부터 추출되는 단계; 및

상기 클라이언트 컴퓨터 시스템이 상기 클라이언트의 대응하는 쿠키에 상기 갱신된 세션 식별자 및 상기 리프레시된 암호화된 정보를 저장하는 단계

를 포함하는 방법.

청구항 17

제16항에 있어서, 상기 클라이언트 컴퓨터 시스템이 리소스로의 웹 기반 액세스에 대한 요구를 송신하는 상기 단계는, 전자 메일 서버의 전자 메일 리소스로의 웹 기반 액세스를 요구하는 HTTP 메시지를 송신하는 단계를 포함하는 방법.

청구항 18

제16항에 있어서, 상기 클라이언트 컴퓨터 시스템이 갱신된 고유 세션 식별자 및 리프레시된 암호화된 정보와 함께 상기 요구된 리소스를 클라이언트측 브라우저에서 수신하는 상기 단계는, 상기 암호화된 정보의 생성에 사용된 키가 순환 키 저장소의 가장 최근의 키가 아닌 결과, 갱신된 세션 식별자 및 리프레시된 암호화된 정보를 수신하는 단계를 포함하는 방법.

청구항 19

제16항에 있어서, 상기 클라이언트 컴퓨터 시스템이 상기 클라이언트의 대응하는 쿠키에 상기 갱신된 고유 세션 식별자 및 상기 리프레시된 암호화된 정보를 저장하는 상기 단계는, 상기 갱신된 고유 세션 식별자 및 상기 리프레시된 암호화된 정보가 브라우저 메모리의 고유 세션 식별자 및 암호화된 정보에 겹쳐 쓰는(overwrite) 단계를 포함하는 방법.

청구항 20

서버 컴퓨터 시스템에서, 상기 서버 컴퓨터 시스템의 리소스에 웹 기반으로 액세스하기 위하여 사용되는 사용자 자격 증명서의 유효성을 결정하는 방법에 있어서,

상기 서버 컴퓨터 시스템이 클라이언트 컴퓨터 시스템으로부터 상기 서버의 리소스로의 웹 기반 액세스에 대한 요구를 수신하는 단계,

-상기 요구는:

고유 세션 식별자, 및

사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 포함하며, 상기 시간 의존 서명은 상기 사용자 자격 증명서 및 서명 시간 의존 키의 적어도 일부분으로부터 추출되고, 상기 클라이언트 컴퓨터 시스템으로부터 수신된 상기 암호화된 정보는 상기 서버 컴퓨터 시스템의 순환 키 저장소로부터 획득된 적어도 하나의 키 및 암호화 시간 의존 키를 사용하여 암호화되고, 상기 서명 시간 의존 키 및 상기 암호화 시간 의존 키의 양쪽 모두는 상기 서버 컴퓨터 시스템의 순환 키 저장소의 키로부터 추출되고, 상기 서버 컴퓨터 시스템에 있는 키 생성 모듈은, 상기 클라이언트 컴퓨터 시스템에 전달되는, 순환 키 저장소를 위한 키들을 생성함-;

상기 서버 컴퓨터 시스템이 순환 키 저장소의 가장 최근의 키를 사용하여 상기 사용자 자격 증명서의 적어도 일부분의 검증을 시도하고 상기 사용자 자격 증명서의 적어도 일부분이 상기 순환 키 저장소의 가장 최근의 키를 사용하여 검증될 수 없음을 결정하는 단계;

상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 다른 키들을 사용하여 상기 사용자 자격 증명서의 적어도 일부분의 검증을 시도하는 단계;

상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 가장 최근의 키 이외의 상기 순환 키 저장소의 키를 이용하여 상기 사용자 자격 증명서를 검증하는 단계;

상기 서버 컴퓨터 시스템이 상기 요구된 리소스로의 웹 기반 액세스를 제어하는 모듈로 상기 요구를 재전송하는 단계; 및

상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 가장 최근의 키 이외의 키로 상기 사용자 자격 증명서를 검증하는 것에 대한 응답으로, 상기 서버 컴퓨터 시스템이 상기 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야함을 결정하는 단계

를 포함하는 방법.

청구항 21

제20항에 있어서, 상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 가장 최근의 키 이외의 상기 저장소의 키를 사용하여 상기 사용자 자격 증명서를 검증하는 단계는, 상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 이전에 생성된 키에 기초하여 상기 사용자 자격 증명서의 적어도 일부분이 유효하다는 것을 결정 - 상기 이전에 생성된 키는 상기 가장 최근의 키보다 먼저 상기 순환 키 저장소에 삽입된 것임 - 하는 단계를 포함하는 방법.

청구항 22

제20항에 있어서, 상기 서버 컴퓨터 시스템이 상기 사용자 자격 증명서 및 시간 의존 서명의 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야함을 결정하는 상기 단계는, 상기 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야 한다는 것을 결정하는 단계를 포함하는 방법.

청구항 23

제22항에 있어서, 상기 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야함을 결정하는 상기 단계는, 상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 이전에 생성된 키에 기초하여 상기 사용자 자격 증명서의 적어도 일부분을

검증하였다는 것을 결정 - 상기 이전에 생성된 키는 상기 가장 최근의 키보다 먼저 상기 순환 키 저장소로 삽입된 것임 - 하는 단계를 포함하는 방법.

청구항 24

제22항에 있어서, 상기 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야함을 결정하는 상기 단계는, 상기 서버 컴퓨터 시스템이 상기 순환 키 저장소의 임의의 키로 상기 사용자 자격 증명서의 적어도 일부분을 검증할 수 없었다는 것을 결정하는 단계를 포함하는 방법.

청구항 25

제24항에 있어서, 상기 서버 컴퓨터 시스템이 상기 클라이언트 컴퓨터 시스템을 사용자 자격 증명서를 수신하기 위한 인터페이스를 제공하는 로그인 페이지로 재지정하는 단계를 더 포함하는 방법.

청구항 26

제20항에 있어서, 상기 서버 컴퓨터 시스템이 상기 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보가 상기 순환 키 저장소의 가장 최근의 키로부터 추출되어야함을 결정하는 상기 단계는, 리프레시된 암호화된 정보 및 시간 의존 서명을 상기 순환 키 저장소의 가장 최근의 키로부터 추출하는 단계를 포함하는 방법.

청구항 27

제26항에 있어서, 상기 서버 컴퓨터 시스템이 상기 요구된 리소스, 갱신된 고유 세션 식별자, 및 리프레시된 암호화된 정보를 상기 클라이언트 컴퓨터 시스템으로 송신하는 단계를 더 포함하는 방법.

청구항 28

서버 컴퓨터 시스템에서의 사용을 위한 컴퓨터 판독가능 기록 매체로서, 제20항에 따른 방법을 구현하기 위한 컴퓨터 판독가능 기록 매체.

청구항 29

제20항에 있어서, 상기 순환 키 저장소는 그 내부에 복수의 키를 보존하며, 따라서 상기 키 생성 모듈에 의해 새로운 키가 생성되었을 때, 상기 새로이 생성된 키는 상기 키 저장소 내로 순환되어 넣어지고(rotated into) 오래된 키는 상기 키 저장소로부터 제거되는(rotated out of) 방법.

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

[0023] 본 출원은 2002년 11월 20일 출원되고 발명의 명칭이 "쿠키 기반 인증 시스템 및 방법(System and Method For Cookie Based Authentication)"인 미국 가출원 제60/428,152호에 대한 우선권을 주장하는 것으로, 상기 가출원은 본 명세서에서 참조로서 모두 포함된다.

[0024] 본 발명은 컴퓨터 네트워크에 관한 것으로, 특히 리소스(resource)에 웹 기반으로 액세스하기 위하여 사용되는 클라이언트 자격 증명서(client credential)를 안전하게 처리하는 것에 관한 것이다.

[0025] 컴퓨터 시스템 및 연관 기술은 사회의 많은 면에 영향을 미친다. 참으로, 정보를 처리하는 컴퓨터 시스템의 능력은 우리가 생활하고 일하는 방식을 바꾸었다. 이제 컴퓨터 시스템은 그것의 출현 전에 수동으로 수행되었던 다수의 작업, 예를 들어 워드 프로세싱, 작업 관리(scheduling) 및 데이터베이스 관리를 일반적으로 수행한다. 최근에, 컴퓨터 시스템은 다른 컴퓨터 시스템과 결합되어서, 데이터를 공유하기 위하여 전기적으로 통신할 수 있는 유선 및 무선 통신 네트워크를 형성하고 있다. 결과적으로, 컴퓨터에서 수행되는 다수의 작업, 예를 들어 음성 통신, 전자 메일 접속, 전자 회의, 웹 브라우징은 유선 및/또는 무선 컴퓨터 네트워크를 통한 하나 이상의 다른 컴퓨터 시스템과의 전자식 통신을 포함한다.

[0026] 특히, 전자 메일은 통신에 있어 중요한 방법이 되었다. 일반적으로 전자 메일 시스템은 전자 메일 클라이언트 구성 요소 및 전자 메일 서버 구성 요소를 포함한다. 일반적으로 이들 구성 요소는 컴퓨터 시스템, 예를 들어 서버, PC, 랩탑(laptop) 및 PDA에서 수행되도록 구성된 소프트웨어 애플리케이션이다. 일반적으로 전자 메일 클라이언트 구성 요소 및 전자 메일 서버 구성 요소는 다른 구성 요소와의 특정 작업을 위하여 설계되고 구성된다. 일반적으로 전자 메일 클라이언트 구성 요소 및 전자 메일 서버 구성 요소는 원격 프로시저 호출(Remote Procedure Calls; RPC)과 같은 전용 프로토콜(proprietary protocol)을 사용하여 서로 통신을 하고, 이 프로토콜로 인하여, 예를 들어 클라이언트 컴퓨터 시스템의 애플리케이션 프로그램이 서버 컴퓨터 시스템 상에서 프로그램을 실행할 수 있다. 예를 들어, 전자 메일 클라이언트 구성 요소는 적당한 인수(argument)와 함께 메시지를 전자 메일 서버 구성 요소로 송신할 수 있고, 전자 메일 서버 구성 요소는 전자 메일 메시지를 반환한다.

[0027] 몇몇 종류의 전자 메일 서버는, 예를 들어 전용 전자 메일 클라이언트보다는 웹 브라우저가 있는 클라이언트 컴퓨터 시스템과 같은 "제로-터치(zero-touch)" 클라이언트를 통한 전자 메일 액세스를 허용하도록 구성된다. 이런 종류의 전자 메일 서버에서, 웹 브라우저는 전자 메일 서버와 상호 작용하고, 클라이언트 시스템에서 수행되도록 요구되는 임의의 기능은 웹 브라우저를 통하여 수행된다. 예를 들어, 클라이언트 컴퓨터 시스템은 웹 브라우저가 전자 메일 서버와 적당히 상호 작용하는 것을 가능하게 하는 HTML(HyperText Markup Language) 명령어와, Active Server Page와 같은 기술에 의하여 동적으로 생성된 스크립트(script)를 다운로드할 수 있다. 그러므로, 제로-터치 브라우저 기반 클라이언트는 사용자가 공통 네트워크, 예를 들어 WWW(World Wide Web)에 연결된 임의의 서버 시스템으로부터 전자 메일 및 다른 메일 관련 정보, 예를 들어, 달력 및 공유 폴더를 제로-터치 브라우저 기반 클라이언트로 액세스하는 것을 허용한다. 따라서, 예를 들어 WWW상의 다른 웹 기반 컨텐츠를 액세스하기 위하여 사용되는 HTTP(HyperText Transfer Protocol)와 같은 프로토콜은 또한 전자 메일 및 다른 메일 관련 정보를 액세스하기 위하여 사용될 수 있다.

[0028] 그러나, 또한 전자 메일 및 다른 메일 관련 정보에 대한 브라우저 기반 액세스 용이성(accessibility)은 잠재적인 보안 문제를 유발하는데, 몇몇 보안 문제는 웹 브라우저 메모리에 사용자 자격 증명서를 캐싱(caching)하는 것에 연관되어 있다. 웹 환경에서, 일반적으로 컨텐츠(content) 및 컨텐츠에 대한 요구는 HTTP를 사용하여 전송된다. 예를 들어, 컨텐츠를 액세스하려는 HTTP 요구는 브라우저 기반 클라이언트에서의 사용자로부터 발생하고, 그후 네트워크를 통하여 브라우저 기반 클라이언트로부터 전송된다. 그 후 요구는, 브라우저 기반 클라이언트의 사용자가 요구된 컨텐츠를 액세스할 권한이 있는지를 결정하기 위하여 요구를 처리하는 서버 컴퓨터 시스템의 웹 서버에서 수신된다. 사용자가 요구된 컨텐츠를 액세스할 권한이 있으면, 웹 서버는 HTTP 메시지로 컨텐츠를 웹 기반 클라이언트에게 전송할 것이다.

[0029] HTTP의 몇몇 버전, 예를 들어 HTTP/1.0은 상태를 저장할 수 없다(stateless). 즉, HTTP를 통한 통신, 예를 들어 전자 메일 메시지에 대한 요구는 서버에 의한 임의의 이전 통신, 예를 들어 전자 메일 메시지에 대한 다른 이전의 요구를 알지 못하고 수행된다. 예컨대, 이 버전의 HTTP는 사용자가 "로그인" 또는 "로그아웃" 하였는지에 관한 "세션(session)" 의 개념을 지원하지 않는다. 다른 버전의 HTTP, 예를 들어, HTTP/1.1는 HTTP 연결을 유지하는 것을 시도하기 위하여 클라이언트와 서버간에 송신되는 "킵-얼라이브(keep-alive)" 메시지를 지원한다. 그러나, 킵-얼라이브 메시지의 사용은 신뢰할 수 없고, 심지어 킵-얼라이브 메시지가 사용될 때, HTTP 연결이 유지될 수 있다는 아무런 보장이 없다. 또한, 흔히 클라이언트 요구는 다수의 사용자간에 킵-얼라이브 링크를 공유하는 중간의 프락시 서버를 통하여 흐르기 때문에, 수신된 요구가 이미 인증된 클라이언트에 의하여 송신되었는지를 서버가 결정하는 아무런 방법이 없을 수 있다. 따라서, HTTP 통신이 상태를 저장하지 못하거나 킵-얼라이브 메시지를 사용하던지 간에, HTTP를 통하여 전송되는 컨텐츠를 액세스하는 각각의 요구(이하, "HTTP 요구"라 함)는 적당한 HTTP 인증 정보를 포함하여야 한다.

[0030] 따라서, HTTP 인증 정보는 WWW 권한 헤더(WWW-Authorization header)라 불리고 "WWW-Authorization: [Authentication-Type][Credentials]" 포맷을 갖는 특수한 헤더를 통하여 HTTP 요구에 포함될 수 있다. 처음으로 웹 브라우저가 인증, 예를 들어 사용자 입력 자격 증명서 제출을 요구하는 컨텐츠를 액세스 하는 것을 시

도할 때, 웹 서버는 일반적으로 요구된 컨텐츠를 제공하는 것을 거부하고 대신 상태 코드 401 Unauthorized을 갖는 HTTP 메시지를 반환한다. HTTP 응답 메시지는 "WWW-Authenticate: [Authentication method][realm=realm value][Optional information]" 포맷의 헤더를 포함한다.

[0031] 웹 브라우저에서 수신되면, HTTP 응답 메시지는 웹 브라우저가, 예를 들어 사용자명 및 패스워드와 같은 자격 증명서를 요구하는 대화 상자를 제시하도록 한다. 사용자가 자격 증명서를 입력한 후에, 웹 브라우저는 입력된 자격 증명서를 포함하는 HTTP WWW 권한 헤더와 함께 원래의 HTTP 요구를 재전송한다. 웹 서버가 사용자 입력 자격 증명서를 유효하다고 수락하고, 요구된 컨텐츠, 예를 들어 전자 메일 메시지를 반환하면, 웹 브라우저는 브라우저 메모리에 사용자 입력 자격 증명서를 캐싱한다. 그러므로, 동일한 URL(Uniform Resource Locator) 또는 동일한 컨텐츠와 연관된 대응하는 파생된 상대적인 URL에 후속하는 요구에, 캐싱된 자격 증명서는 브라우저 메모리로부터 추출되고, 대응하는 HTTP WWW 권한 헤더에 포함된다. 따라서, HTTP가 상태를 저장하지 못할지라도, 사용자는 동일한 또는 대응하는 파생된 상대적인 URL에 대한 각각의 요구에 대하여 자격 증명서를 다시 입력할 필요가 없다.

[0032] 유감스럽게도, 웹 브라우저 프로그램을 종료하거나, 컴퓨터 시스템 또는 클라이언트 장치를 재부팅하거나 꺼서 웹 브라우저가 종료될 때까지 실질적으로 무한히, 캐싱된 자격 증명서를 브라우저 메모리에 보통 유지한다. 그러므로, 보호된 컨텐츠를 액세스한 인증된 사용자의 자격 증명서는 사용자가 웹 브라우저를 더 이상 사용하지 않게 된 후에도 브라우저 메모리에 캐싱될 수 있다. 그 후 인증된 사용자가 컴퓨터 시템으로부터 떠나면, 다른 인증되지 않은 사용자가 와서 보호된 컨텐츠를 액세스하는 것을 시도하기 위하여 브라우저의 백-버튼 또는 히스토리 특징을 사용할 수 있다. 인증된 사용자의 자격 증명서가 브라우저 메모리에 여전히 캐싱되어 있기 때문에, 웹 브라우저는 캐싱된 자격 증명서를 추출하고, 보호된 컨텐츠를 액세스하기 위하여 인증되지 않은 사용자의 요구와 함께 이것을 제출할 것이다. 그러므로, 인증되지 않은 사용자는 웹 브라우저에서 적당한 자격 증명서를 입력할 필요 없이 보호된 컨텐츠를 액세스할 수 있다.

[0033] 캐싱된 자기 증명서는 공용 컴퓨터를 갖는 장소 및/또는 웹 브라우저를 종료하는 것이 허용되지 않는 컴퓨터 시스템에서 특히 문제가 될 수 있다. 이러한 컴퓨터 시스템의 예에는 Internet Kiosk가 있다. Internet Kiosk는 흔히, 공중에게 인터넷에 대한 액세스를 제공하기 위하여, 예를 들어 도서관, 인터넷 카페 및 회의 센터와 같은 공용 장소에 위치한다. Internet Kiosk는 kiosk에 다가가는 사용자가 웹 브라우저를 발견하고 구동시킬 필요 없이 빠르게 인터넷에 액스세할 수 있도록 설계된다. 그러므로, 다수의 Internet Kiosk는 웹 브라우저가 항상 활성화되고 종료될 수 없도록 구성된다.

[0034] 이러한 점이 인터넷에 대하여 효율적인 액세스를 제공하지만, 이는 또한 브라우저 메모리에 실질적으로 무한히 남아 있는 캐싱된 자격 증명서를 잠재적으로 유발한다. 예를 들어, 인증된 사용자가 Internet Kiosk에서, 예를 들어 보호된 컨텐츠를 액세스하기 위하여 자격 증명서를 입력하면, 인증된 사용자의 자격 증명서는 브라우저 메모리에 캐싱된다. 웹 브라우저는 종료될 수 없기 때문에, 공용 Kiosk의 전원을 제거하지 않고서 캐싱된 자격 증명서를 제거하는 방법이 실질적으로 없다. 그러므로, 인증된 사용자가, 예를 들어 웹 브라우저를 종료함으로써 캐싱된 자격 증명서를 제거하는 방법을 안다고 하더라도, 그렇게 할 수 없다.

[0035] 보호된 컨텐츠를 액세스하기 위하여 캐싱된 자격 증명서를 사용하는 것은 브라우저 기반 전자 메일 애플리케이션에서 특히 관심 사항이다. 예를 들어, 인증되지 않은 사용자는, 사적인 데이터를 포함할 수 있는 인증된 사용자의 전자 메일 메시지에 액세스하기 위하여 페이지 백(page back) 할 수 있다. 인증된 사용자의 전자 메일을 액세스하는 것 이외에, 캐싱된 자격 증명서는 또한 인증되지 않은 사용자가 인증된 사용자 역할을 하는 것을 가능하게 할 수 있다. 예를 들어, 인증되지 않은 사용자는 인증된 사용자와 연관된 계정으로부터 전자 메일 메시지를 송신할 수 있다.

[0036] 이러한 문제점에 대한 한 가지 가능한 해결책은 컨텐츠가 요구될 때마다 사용자에게 재인증을 요구하는 것이다. 그러나, 이것은 사용자가 컨텐츠를 액세스하는 각각의 HTTP 요구에 대하여 수동으로 인증 정보를 재입력할 것을 요구한다. 웹 사이트와의 전형적인 상호 작용은 수십 또는 심지어는 수백개의 HTTP 요구로 이루어질 수 있기 때문에, 이것은 사용자가 수십 또는 수백된 자격 증명서를 다시 입력하게 할 수 있다. 그러므로, 각각의 HTTP 요구에 대하여 자격 증명서를 다시 입력하는 것은 컨텐츠를 액세스하기 위하여 필요한 시간 및 데이터 입력의 양을 증가시킬 것이다. 이러한 해결책은 자격 증명서를 세션 당 단지 한번 입력하기를 선호하는 대부분의 사용자에게 매우 귀찮은 일이다. 그러므로, 웹 기반 리소스를 액세스하기 위하여 사용되는 클라이언트 자격 증명서를 안전하게 처리하기 위한 시스템, 방법, 컴퓨터 프로그램 제품이 유용할 것이다.

발명이 이루고자 하는 기술적 과제

[0037] 상술한 종래기술에 따른 문제점은 본 발명의 원리에 의해 극복되며, 본 발명은 리소스에 웹 기반으로 액세스하기 위하여 사용되는 클라이언트 신분을 안전하게 처리하기 위한 방법, 시스템, 컴퓨터 프로그램 제품 및 데이터 구조를 포함하는 컴퓨터 판독 가능 매체에 적용될 수 있다. 클라이언트 컴퓨터 시스템(이하 "클라이언트"라 함) 및 서버 컴퓨터 시스템(이하 "서버"라 함)은 예를 들어 인터넷과 같은 일반 네트워크로 접속된다. 서버는 전자 메일 메시지 및 관련 메일 데이터와 같은 리소스로의 웹 기반 액세스가 가능하도록 구성된다. 클라이언트는 웹 기반 리소스로의 액세스를 요구하고 클라이언트의 사용자에게 웹 기반 리소스를 제공하는 브라우저로 구성된다.

발명의 구성 및 작용

[0038] 클라이언트는 서버의 리소스에 액세스하기 위하여 제1 요구(request)을 송신한다. 예를 들어, 클라이언트는 서버에 저장된 전자 메일 메시지에 액세스하기 위하여 요구를 송신한다. 서버는 상기 제1 요구를 수신하고, 클라이언트가 인증되지 않았으므로 서버는 제1 요구의 수신에 응답하여 클라이언트를 로그인 페이지로 재지정한다(redirect). 클라이언트를 재지정하는 것은, 서버가 클라이언트에게 로그인 페이지로의 URI와 함께 재지정 지시자, 예를 들어 상태 코드 302 Moved Temporarily를 갖는 HTTP 메시지를 포함하는 응답을 송신하는 것을 포함할 수 있다. 로그인 페이지는, 사용자 자격 증명서를 입력하기 위하여 클라이언트의 사용자에게 인터페이스를 제공하는 ASP(Active Server Pages) 페이지일 수 있다. 클라이언트는 로그인 페이지에 액세스하고, 로그인 페이지를 사용하여 서버에 사용자 자격 증명서를 제출한다. 클라이언트는 HTTP 포스트를 보호하기 위하여 예를 들어 SSL(Secure Sockets Layer)을 사용하여 자격 증명서를 제출할 수 있다.

[0039] 서버는 제출된 자격 증명서를 수신한다. 서버는 사용자 자격 증명서 및 시간 의존 전자 서명(time-dependent digital signature)을 나타내는 암호화된 정보를 송신한다. 서버는, 제출된 자격 증명서에 대해 인증이 되었음을 검증한 후, 암호화된 정보를 송신한다. 서버는 순환 키 저장소(rotating key store)로부터의 키를 사용하여 암호화된 데이터를 생성한다. 순환 키 저장소의 각 키는 특정 시간 간격, 예를 들어 10분이 경과한 후에 자동적으로 폐기된다. 특정 시간 간격이 경과한 후에, 서버는 새로운 키를 순환 키 저장소로 순환하여 넣고, 폐기된 키를 순환 키 저장소에서 제외시킨다. 순환 키 저장소에 보유되는 키의 수 및 특정 시간 간격은 관리자에 의해 정해질 수 있다.

[0040] 사용자 자격 증명서가 수신되면, 서버는 사용자 자격 증명서를 고유 식별자, 예를 들어 전 세계적 단일 식별자(Globally Unique Identifier; GUID)와 연관시킨다. 서버는 서명 키(signature key)를 얻는데, 서명 키는 순환 키 저장소의 가장 최근의 키, 고유 식별자 및 제1 상수 스트링(a first constant string)의 조합을, 예를 들어 SHA-1 또는 MD-5 해싱 알고리즘을 사용하여 해싱(hashing)함으로써 데이터를 디지털로 나타내는 데에 사용될 수 있다. 이어서, 서버는 서명 키를 사용하여 고유 식별자 및 사용자 자격 증명서의 조합으로부터 전자 서명, 예를 들어 Hashed Message Authentication Code(HMAC)를 추출한다.

[0041] 서버는 또한 암호화 키(encryption key)를 추출하는데, 이 암호화 키는 순환 키 저장소의 가장 최근의 키, 고유 식별자 및 제2 상수 스트링의 조합을 해싱함으로써 데이터를 암호화하는데 사용될 수 있다. 이어서, 서버는 암호화 키를 사용하여 전자 서명과 사용자 자격 증명서의 조합을 암호화하여 암호화된 정보를 만들 수 있다. 서버는 고유 식별자 및 암호화된 정보를 클라이언트로 송신한다. 클라이언트는 고유 식별자 및 암호화된 정보를 수신하고, 고유 식별자 및 암호화된 정보를 저장한다.

[0042] 클라이언트는 서버의 리소스에 액세스하기 위하여 제2 요구를 송신하며, 이 제2 요구는 고유 식별자 및 암호화된 정보를 포함한다. 서버는 제2 요구를 수신하고, 순환 키 저장소의 가장 최근의 키를 사용하여 사용자 자격 증명서의 검증을 시도한다. 서버는 순환 키 저장소의 가장 최근의 키, 고유 식별자, 및 제2 상수 스트링의 조합을 해싱함으로써 암호화된 키를 추출하며, 이 암호화된 키는 데이터를 복호화하는데 사용될 수 있다. 서버는 복호화 키(decryption key)를 사용하여 암호화된 정보를 복호화하고, 그럼으로써 전자 서명 및 사용자 자격 증명서가 드러난다. 서버는 순환 키 저장소의 가장 최근의 키, 고유 식별자 및 제1 상수 스트링의 조합을 해싱함으로써 검증 키(validation key)를 얻으며, 이 검증 키는 데이터를 인증하기 위하여 사용될 수 있다. 서버는 검증 서명 키(validation signature key)를 사용하여 고유 식별자와 사용자 자격 증명서의 조합으로부터 검증 전자 서명을 추출한다.

[0043] 서버는 검증 전자 서명(validation digital signature)을 전자 서명(digital signature)과 비교한다. 검증 전자 서명과 전자 서명이 일치하면 사용자 자격 증명서가 검증된다. 한편, 검증 전자 서명과 전자 서명이 일치하

지 않으면 자격 증명서가 검증되지 않는다. 순환 키 저장소의 가장 최근의 키를 사용하여 사용자 자격 증명서가 검증되지 않으면, 순환 키 저장소의 그 다음 최근의 키, 예를 들어 복호화 키 및 검증 전자 서명을 생성하기 위한 그 다음의 최근 키를 사용하여 사용자 자격 증명서의 검증을 시도한다. 서버는 순환 키 저장소의 각 키를 사용하여 사용자 자격 증명서의 검증을 시도할 수 있다. 검증된 사용자 자격 증명서는 요구된 리소스, 예를 들어 전자 메일 메시지로의 액세스를 제어하는 모듈, 예를 들어 전자 메일 서버로 보내진다.

[0044] 순환 키 저장소의 가장 최근의 키가 아닌 키로 사용자 자격 증명서가 검증된 경우, 서버는 리플레시된 암호화된 정보를 추출해야 한다고 결정할 수 있다. 서버는, 예를 들어 가장 최근의 키로부터 리플레시된 암호화 키 및 리플레시된 전자 서명을 추출함으로써, 리플레시된 암호화된 정보를 얻는 데에 순환 키 저장소의 가장 최근의 키를 사용한다. 검증된 사용자 자격 증명서가 적절한 경우, 요구된 리소스와 리플레시된 암호화된 정보가 클라이언트에게 반환된다. 클라이언트는 리소스 및 임의의 리플레시된 암호화된 정보를 수신한다. 클라이언트는 임의의 리플레시된 암호화된 정보를 저장하고, 고유 식별자에 대응하는 이전의 암호화된 정보를 덮어쓴다. 순환 키 저장소의 임의의 키를 사용하여 사용자 자격 증명서가 검증되지 않는 경우, 클라이언트는 다시 로그인 페이지로 보내지며, 여기서 새로운 사용자 자격 증명서를 입력할 수 있다.

[0045] 몇몇 실시예에 있어서, 로그인 페이지는, HTTP 메시지가 처리되는 방법을 변경할 수 있는 통신 특성, 예를 들어, gzip 압축을 위한 지원, 클라이언트 컴퓨터 시스템이 사적인 것인지 신용할 수 없는 클라이언트인지, 클라이언트가 단순한 컨텐츠를 선호하는 숙련된 클라이언트인지 등을 선택하기 위한 인터페이스를 포함한다. 통신 특성은 로그인 페이지에서 선택되고, 클라이언트와의 HTTP 통신이 처리되는 방법을 통신 필터로 지시하기 위하여 통신 필터로 송신된다. 선택된 통신 특성은 서버에서 수신된다.

[0046] 선택된 통신 특성이 클라이언트에 의하여 지원이 되는지를 결정하고, 다른 관련 통신 특성을 식별하기 위하여, 서버는 클라이언트에게 문의한다. 서버는 클라이언트에 의하여 지원되는 선택된 통신 특성 및 식별된 다른 관련 통신 특성에 따라 클라이언트와의 HTTP 통신을 처리하기 위하여 통신 필터를 구비한다. 비보안(non-secure) 위치에 있는 클라이언트에 기초하여, 서버는 더 짧은 순환 간격을 가지고 감소된 수의 키를 보유하는 다른 순환 키 저장소를 사용할 수 있다.

[0047] 본 발명의 추가적인 특징 및 장점은 이하의 상세한 설명에서 설명하며, 일부는 설명으로부터 명백할 것이며, 본 발명의 실시에 의하여 알 수 있다. 본 발명의 특징 및 장점은 특히 첨부된 청구항에서 지적된 기구 및 조합에 의해 실현되고 획득된다. 본 발명의 이러한 특징 및 다른 특징은 이하의 설명 및 첨부된 청구항으로부터 충분히 명백해질 것이며, 이하에서 설명하는 발명의 실시에 의해 얻어질 것이다.

[0048] **실시예**

[0049] 본 발명의 상술한 장점 및 특징과 다른 장점 및 특징이 얻어질 수 있는 방법을 설명하기 위하여, 위에서 간략하게 설명한 본 발명에 대하여 첨부된 도면에 도시된 특정 실시예를 참조하여 보다 구체적으로 설명한다. 첨부된 도면은 단지 본 발명의 일반적인 실시예를 나타내는 것이며, 따라서 본 발명의 범위를 제한하는 것으로 해석되어서는 안 된다. 본 발명에 대하여 첨부된 도면을 사용하여 추가적인 특수성 및 세부사항을 설명한다.

[0050] 본 발명의 원리는 리소스에 웹 기반으로 액세스하기 위하여 사용되는 클라이언트 자격 증명서를 안전하게 처리하는 방법을 제공한다. 서버는 하나 이상의 키를 포함하는 적어도 하나의 순환 키 저장소를 보유한다. 순환 키 저장소의 각 키는 특정 시간 간격, 예를 들어 10분이 경과한 후 자동으로 폐기된다. 특정 시간 간격이 경과한 후, 서버는 순환 키 저장소에 새로운 키를 순환하여 넣고, 폐기된 키를 순환 키 저장소에서 제거한다. 순환 키 저장소에서 보유하는 키의 수 및 특정 시간 간격은, 예를 들어 3개의 키를 보유하고 키를 5분마다 교체하는 식으로, 관리자에 의하여 정해질 수 있다. 서버는 사용자 자격 증명서를 위한 전자 서명을 생성하고, 순환 키 저장소의 키에 기초하여 사용자 자격 증명서를 암호화하여 사용자 자격 증명서를 보호한다.

[0051] 사용자 자격 증명서를 입력하기 위한 인터페이스를 구비한 로그인 페이지가 클라이언트에 표시된다. 클라이언트에서 입력된 사용자 자격 증명서는 서버로 송신된다. 서버는 사용자 자격 증명서의 수신에 응답하여, 클라이언트에 대한 고유 세션 식별자(unique session identifier)를 생성한다. 서버는 순환 키 저장소의 가장 최근의 키 및 고유 세션 식별자에 기초하여 사용자 자격 증명서를 위한 전자 서명을 추출한다. 이어서, 서버는 순환 키 저장소의 가장 최근 키로부터 추출된 암호화 키 및 고유 세션 식별자에 기초하여 전자 서명 및 사용자 자격 증명서를 암호화한다. 암호화된 자격 증명서가 클라이언트에서 다시 수신된 경우, 자격 증명서의 검증을 시도하기 위하여 순환 키 저장소로부터의 키가 사용된다. 사용자 자격 증명서를 암호화하기 위하여 본래 사용된 순환 키 저장소로부터의 키가 순환 키 저장소에서 제거되었으면, 클라이언트는 새로운 자격 증명서를 입력하도록

로그인 페이지로 재지정된다.

[0052] 본 발명의 범위에 속하는 실시예는 컴퓨터 실행 가능한 명령 또는 이에 저장된 데이터 구조를 실행하거나 포함하는 컴퓨터 판독 가능한 매체를 포함한다. 이러한 컴퓨터 판독 가능한 매체는 임의의 사용 가능한 매체일 수 있으며, 이 매체는 범용 또는 특수 컴퓨터 시스템에 의하여 액세스할 수 있다. 예를 들어, 이러한 컴퓨터 판독 가능한 매체는 RAM, ROM, EPROM, CD-ROM, 또는 다른 광 디스크 저장 장치, 자기 디스크 저장 장치 또는 다른 자기 저장 장치와 같은 물리적 저장 매체나, 컴퓨터 실행 가능한 명령, 컴퓨터 판독 가능한 명령 또는 데이터 구조의 형태의 원하는 프로그램 코드 수단을 실행하거나 저장하고 범용 또는 특수 컴퓨터 시스템에 의하여 액세스할 수 있는 임의의 다른 매체로 구성될 수 있다. 그러나, 이에 국한되는 것은 아니다.

[0053] 상세한 설명 및 이하의 청구항에 있어서, "네트워크"는 컴퓨터 시스템 및/또는 모듈 간의 전자 데이터의 송신을 가능하게 하는 하나 이상의 데이터 링크로 정의된다. 정보가 네트워크 또는 다른 통신 커넥션, 즉 배선(hardwired), 무선 또는 배선과 무선의 결합을 통해 컴퓨터 시스템으로 송신되거나 제공되면, 이러한 커넥션은 컴퓨터 판독 가능한 매체로 보여질 수 있다. 따라서, 임의의 이러한 커넥션은 컴퓨터 판독 가능한 매체라 함이 적절하다. 컴퓨터 실행 가능한 명령은, 예를 들어 범용 컴퓨터 시스템 또는 특수 컴퓨터 시스템이 일정한 기능 또는 기능 그룹을 수행하게 하는 명령 및 데이터로 구성된다. 컴퓨터 실행 가능한 명령은 예를 들어, 2진수, 어셈블리 언어와 같은 중간 형태의 명령이나 소스 코드일 수 있다.

[0054] 상세한 설명 및 이하의 청구항에 있어서, "컴퓨터 시스템"은 하나 이상의 소프트웨어 모듈, 하나 이상의 하드웨어 모듈, 또는 이들의 결합으로 정의되며, 이들은 전자 데이터에 관한 동작을 수행하기 위하여 함께 동작한다. 예를 들어, 컴퓨터 시스템의 정의는 퍼스널 컴퓨터의 운영 체제와 같은 소프트웨어 모듈뿐만 아니라 퍼스널 컴퓨터의 하드웨어 부품을 포함한다. 모듈의 물리적인 배치는 중요하지 않다. 컴퓨터 시스템은 네트워크를 통하여 결합된 하나 이상의 컴퓨터를 포함할 수 있다. 이와 유사하게, 컴퓨터 시스템은 하나의 물리적 장치, 예를 들어 휴대 전화 또는 개인 휴대 정보 단말기(PDA) 등을 포함할 수 있는데, 이 물리적 장치에서 메모리 또는 프로세서와 같은 내부 모듈은 전자 데이터에 관한 동작을 수행하기 위하여 함께 동작한다.

[0055] 본 발명은 퍼스널 컴퓨터, 랩톱 컴퓨터, 휴대용 장치, 멀티 프로세서 시스템, 마이크로프로세서 기판 또는 프로그래밍 가능한 소비자 가전제품, 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 휴대 전화, PDA, 페이저 등을 포함하는 많은 유형의 컴퓨터 시스템 구성을 구비한 네트워크 컴퓨팅 환경에서 실행될 수 있다는 것을 당업자라면 이해할 것이다. 본 발명은 로컬 및 원격 컴퓨터 시스템이 작업을 수행하는 분산 시스템 환경(distributed system environment)에서도 실행될 수 있으며, 로컬 및 원격 컴퓨터 시스템은 배선 데이터 링크, 무선 데이터 링크 또는 배선 및 무선 데이터 링크의 결합에 의해 네트워크를 통하여 링크되어 있다. 분산 시스템 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치에 모두 배치될 수 있다.

[0056] 도 1 및 이하의 논의는 본 발명이 구현될 수 있는 적절한 컴퓨팅 환경의 간략하고 일반적인 설명을 제공하기 위한 것이다. 반드시 요구되는 것은 아니지만, 본 발명은 컴퓨터 시스템에 의하여 실행되는 프로그램 모듈과 같은 컴퓨터 실행 가능한 명령의 일반적 내용에 따라 설명될 것이다. 일반적으로, 프로그램 모듈은 루틴, 프로그램, 객체, 구성요소, 데이터 구조 등을 포함하며, 이들은 특정 작업을 수행하거나 특정한 추상적인 데이터 유형을 구현한다. 데이터 구조와 관련된 컴퓨터 실행 가능한 명령 및 프로그램 모듈은 여기서 개시된 방법의 작동을 실행하기 위한 프로그램 코드 수단의 예를 나타낸다.

[0057] 도 1을 보면, 본 발명을 위한 예시적 시스템은 처리 장치(processing unit; 121), 시스템 메모리(122) 및, 처리 장치(121)에 시스템 메모리(122)와 같은 다양한 시스템 컴포넌트를 연결하는 시스템 버스(123)를 포함하는 컴퓨터 시스템(120)의 형태로 범용 컴퓨팅 장치를 포함한다. 처리 장치(121)는 본 발명의 특징을 포함하는 컴퓨터 시스템의 특징을 구현하도록 디자인된 컴퓨터 실행 가능 명령어를 실행할 수 있다. 시스템 버스(123)는 메모리 버스나 메모리 제어기, 주변 장치 버스, 및 다양한 버스 구조 중 임의의 것을 사용하는 로컬 버스를 포함하는 임의의 유형의 버스 구조일 수 있다. 시스템 메모리는 ROM(124) 및 RAM(125)을 포함한다. 예를 들어, 스타트업 동안에 컴퓨터 시스템내의 요소간의 정보 송신을 돕는 기본적 루틴을 포함하는 기본적 입출력 시스템(126; "BIOS")은 ROM(124)에 저장될 수 있다.

[0058] 컴퓨터 시스템(120)은 또한 자기 하드 디스크(139)에서의 기록 및 판독을 위한 자기 하드 드라이브(127), 이동 가능한 자기 디스크(129)에서의 기록 및 판독을 위한 자기 디스크 드라이브(128) 및 CD 롬 또는 다른 광 매체와 같은 이동 가능한 광 디스크에서 읽고 쓰기 위한 광 디스크 드라이브(131)를 포함한다. 자기 하드 디스크 드라이브(127), 자기 디스크 드라이브(128) 및 광 디스크 드라이브(130)는 하드 디스크 드라이브 인터페이스(132), 자기 디스크 드라이브 인터페이스(133) 및 광 디스크 인터페이스(134)에 의하여 각각 시스템 버스(123)에 접속

된다. 드라이브 및 관련 컴퓨터 판독 가능 매체는 컴퓨터 실행가능 명령어, 데이터 구조, 프로그램 모듈 및 컴퓨터 시스템(120)을 위한 다른 데이터의 비휘발성 기억매체를 제공한다. 여기에 설명된 예시적 환경은 자기 하드 디스크(139), 이동 가능한 자기 디스크(129) 및 이동 가능한 광 디스크(131)를 포함하지만, 자기 카세트, 플래시 메모리 카드, 디지털 다용도 디스크, 베르누이 카트리지, RAM, ROM 등과 같은 데이터 저장을 위한 여러 유형의 컴퓨터 판독 가능 매체가 사용될 수 있다.

[0059] 하나 이상의 프로그램 모듈을 포함하는 프로그램 코드 수단은, 운영체제(135), 하나 이상의 응용 프로그램(136), 다른 프로그램 모듈(137) 및 프로그램 데이터(138)를 포함하는 하드 디스크(139), 자기 디스크(129), 광학 디스크(131), ROM(124), RAM(125)에 저장될 수 있다. 사용자는 키보드(140), 포인팅 장치(142) 또는 마이크로폰, 조이스틱, 게임 패드, 스캐너 등의 다른 입력 장치(도시되지 않음)를 통하여 컴퓨터 시스템(120)에 명령 및 정보를 입력할 수 있다. 상기 및 다른 입력 장치는 시스템 버스(123)에 연결된 입출력 인터페이스(146)를 통하여 처리 장치(121)에 연결될 수 있다. 입출력 인터페이스(146)는, 예를 들어 시리얼 포트 인터페이스, PS/2 인터페이스, 패러럴 포트 인터페이스, USB 인터페이스 또는 IEEE(Institute of Electrical and Electronics Engineers) 1394 인터페이스(즉 FireWire 인터페이스)와 같은 넓은 범위의 다른 인터페이스 중 임의의 것을 논리적으로 나타내거나, 다른 인터페이스의 조합을 논리적으로 나타낼 수도 있다.

[0060] 모니터(147) 또는 다른 디스플레이 장치는 또한 비디오 어댑터(148)를 통하여 시스템 버스(123)에 연결될 수 있다. 스피커(169) 또는 다른 오디오 출력 장치는 또한 오디오 인터페이스(149)를 통하여 시스템 버스(123)에 연결될 수 있다. 또한 프린터와 같은 다른 주변 출력 장치(도시되지 않음)는 컴퓨터 시스템(120)에 연결될 수 있다. 컴퓨터 시스템(120)은, 예를 들어 사무실 기반 또는 기업 기반 컴퓨터 네트워크, 홈 네트워크, 인트라넷 및/또는 인터넷과 같은 네트워크에 접속 가능하다. 컴퓨터 시스템(120)은 원격 컴퓨터 시스템, 원격 응용 프로그램 및/또는 이러한 네트워크에 대한 원격 데이터베이스와 같은 외부 소스와 데이터를 교환할 수 있다.

[0061] 컴퓨터 시스템(120)은 네트워크 인터페이스(153)를 포함하고, 이를 통하여 컴퓨터 시스템(120)은 외부 소스로부터 데이터를 수신 및/또는 외부소스로 데이터를 송신한다. 도 1에서 설명하는 것처럼, 네트워크 인터페이스(153)는 링크(151)를 통하여 컴퓨터 시스템(183)에서의 데이터 교환을 촉진할 수 있다. 네트워크 인터페이스(153)는, 예를 들어 네트워크 인터페이스 카드 및 대응하는 네트워크 드라이버 인터페이스 사양(Network Driver Interface Specification; NDIS) 스택과 같은 하나 이상의 소프트웨어 또는/및 하드웨어 모듈을 논리적으로 나타낼 수 있다. 링크(151)는 네트워크의 일부, 예를 들어 인터넷 세그먼트를 나타내고, 원격 컴퓨터 시스템(183)은 네트워크의 노드를 나타낸다. 예를 들어, 원격 컴퓨터 시스템(183)은 전자 메일 메시지와 같은 리소스로의 웹 기반 액세스를 컴퓨터 시스템(120)에 제공하는 서버 컴퓨터 시스템일 수 있다. 반대로, 원격 컴퓨터 시스템(183)은 컴퓨터 시스템(120)으로부터 리소스로의 액세스하기 위하여 웹 기반 액세스를 사용하는 클라이언트 컴퓨터 시스템일 수 있다.

[0062] 이와 같이, 컴퓨터 시스템(120)은 입출력 인터페이스(146)를 포함할 수 있고, 이를 통하여 컴퓨터 시스템(120)은 외부 소스로부터 데이터를 수신 및/또는 외부 소스로 데이터를 송신한다. 입출력 인터페이스(146)는 링크(159)를 통하여 표준 모뎀, 케이블 모뎀 또는 디에스엘(DSL; digital subscriber line) 모뎀 등과 같은 모뎀(154)에 연결되고, 이를 통하여 컴퓨터 시스템(120)은 외부 소스로부터 데이터를 수신 및/또는 외부 소스로 데이터를 송신한다. 도 1에서 설명하는 것처럼, 입출력 인터페이스(146) 및 모뎀(154)은 링크(152)를 통하여 원격 컴퓨터 시스템(193)과의 데이터 교환을 촉진한다. 링크(152)는 네트워크의 일부를 나타내고, 원격 컴퓨터 시스템(193)은 네트워크의 노드를 나타낸다. 예를 들어, 원격 컴퓨터 시스템(193)은 컴퓨터 시스템(120)에 전자 메일 메시지와 같은 리소스로의 웹 기반 액세스를 제공하는 서버 컴퓨터 시스템일 수 있다. 반대로, 원격 컴퓨터 시스템(193)은 컴퓨터 시스템(120)으로부터 리소스로의 액세스하기 위하여, 웹 기반 액세스를 사용하는 클라이언트 컴퓨터 시스템일 수 있다.

[0063] 도 1은 본 발명에 적합한 동작 환경을 나타내고 있지만, 원칙적으로 본 발명은 본 발명의 원칙을 구현할 수 있고 필요하다면 적절한 변경을 가할 수 있는 임의의 시스템에서 사용될 수 있다. 도 1에 도시된 환경은 단지 예시적일 뿐 원칙적으로 본 발명에서 구현될 수 있는 다양한 환경의 일부분조차 나타내고 있지 못하다.

[0064] 관련 프로그램 데이터 및 본 발명의 모듈은 컴퓨터 시스템(120)과 연관된 임의의 컴퓨터 판독 가능 매체에서 저장되고 액세스될 수 있다. 예를 들어, 이러한 모듈 및 연관된 프로그램 데이터의 일부분은 시스템 메모리(122) 내에 저장되기 위한 운영체제(135), 응용 프로그램(136), 프로그램 모듈(137) 및/또는 프로그램 데이터(138)에 포함될 수 있다. 자기 하드 디스크(139)와 같은 범용 저장 장치가 컴퓨터 시스템(120)에 연결될 때, 이와 같은 모듈 및 연관된 프로그램 데이터는 또한 범용 저장 장치에 저장될 수 있다. 네트워킹된 환경에서 컴퓨터 시스

템(120)과 관련되어 설명되는 프로그램 모듈 또는 그 모듈의 부분은, 시스템 메모리 및/또는 원격 컴퓨터 시스템(183)과 연관된 범용 저장 장치 및/또는 원격 컴퓨터 시스템(193)과 같은 원격 메모리 저장 장치에 저장될 수 있다. 상기 모듈의 실행은 상술한 바와 같이 분산 환경에서 수행될 수 있다.

[0065] 도 2는 클라이언트가 서버의 리소스로의 액세스를 요구할 때, 클라이언트측 자격 증명서를 획득하는 것을 용이하게 하는 네트워크 구조(200)의 예를 도시한다. 클라이언트 컴퓨터 시스템(201) 및 서버 컴퓨터 시스템(211)은 LAN(local area network), WAN(wide area network) 또는 인터넷과 같은 공유 네트워크에 연결될 수 있다. 클라이언트 컴퓨터 시스템(201)은 리소스로의 웹 기반 액세스를 요구하고 클라이언트 컴퓨터 시스템(201)에서 현재 수신된 리소스를 제공하는 데에 사용될 수 있는 브라우저(202)를 포함할 수 있다. 쿠키(cookies; 203)는 서버 컴퓨터 시스템으로부터 이전에 수신된 데이터의 일부를 저장하는 하나 이상의 쿠키를 포함할 수 있다. 쿠키(203)에서의 데이터는 대응하는 서버 컴퓨터 시스템에 송신되어 서버 컴퓨터 시스템에 개인화된 정보 및 기호를 지시하고 저장된 정보의 일부를 수동으로 입력하여야 하는 것으로부터 사용자를 해방시킬 수 있다.

[0066] 서버 컴퓨터 시스템(211)은 전자 메일 서버(212)를 포함하고, 이것은 전자 메일 메시지, 어드레스 북 정보, 달력 정보와 같은 전자 메일 리소스에 접근할 수 있도록 한다. 전자 메일 서버(212)에 액세스할 수 있는 권한을 부여받기 위하여, 사용자는 전자 메일 서버(212)에 의하여 인증되도록 전자 메일 서버에 자격 증명서를 제공할 것을 요구받을 수 있다. 전자 메일 서버(212)는 수신된 자격 증명서를 자격 증명서 데이터 베이스(213)의 권한을 가진 자격 증명서들과 비교함으로써, 전자 메일 리소스로의 액세스하는 요구가 권한을 가지는 것인지를 결정한다. 사용자가 권한을 가질 때, 전자 메일 서버(212)는 요구한 클라이언트 컴퓨터 시스템으로 요구된 전자 메일 리소스를 반환할 수 있다. 사용자가 권한을 갖지 못할 경우, 전자 메일 서버(212)는 요구한 클라이언트 컴퓨터 시스템에 권한이 없다는 메시지, 예를 들어, 상태 코드 401 Unauthorized를 갖는 HTTP 메시지를 반환할 수 있다.

[0067] 서버 컴퓨터 시스템(211)은 또한 키 생성 모듈(214)을 포함한다. 키 생성 모듈(214)은 새로운 키를 생성하여 순환 키(220)로 순환시켜 넣을 수 있고, 순환 키(220)로부터 폐기된(expired) 키를 제거할 수 있다. 키 생성 모듈(214)은 하나 이상의 순환 키 저장소를 관리하기 위하여 배치될 수 있다. 예를 들어 네트워크 구조(200)에서, 키 생성 모듈(214)은 비신뢰(non-trusted) 순환 키 저장소(221) 및 개인 순환 키 저장소(231)를 관리할 수 있다.

[0068] 키가 순환될 때, 시간 간격을 지정하여 설정할 수 있다. 이것은, 생성된 키를 지정된 간격에서 순환 키 저장소로 새롭게 순환시켜 넣고, 지정된 간격에서 순환 키 저장소로부터 폐기된 키를 제거하도록 키 생성 모듈(214)이 배치될 수 있다는 의미이다. 예를 들어, 키 생성 모듈(214)은 매 10분마다 개인 순환 키 저장소(231)에 새로운 키를 삽입하고, 여기에서 폐기된 키를 제거할 수 있다. 순환 키 저장소에서 관리되는 키의 숫자도 설정 가능하다. 이는, 키 생성 모듈(214)이 순환 키 저장소에 지정된 숫자의 키를 관리하도록 설정될 수 있다는 것을 의미한다. 예를 들어, 키 생성 모듈(214)은 비신뢰 순환 키 저장소(221)에서 3개의 키를 관리하도록 설정될 수 있다.

[0069] 관리되는 키 및 명시된 간격의 수는 순환 키 저장소간에 차이가 있을 수 있다. 예를 들어, 키 생성 모듈(214)은 비신뢰 키 기억 장치(221)에서 지정된 5분 순환 간격으로 3개의 키를 관리하거나, 개인 키 기억 장치(231)에 지정된 1시간 순환 간격으로 4개의 키를 관리한다. 클라이언트 컴퓨터 시스템과 연관된 특성에 따라, 다른 키 기억 장치가 사용되어 본 발명의 원리를 구현할 수 있다. 순환 키 저장소에서 키 아래 나타난 화살표는 새로운 키가 추가되었을 때, 폐기된 키가 결국 순환 키 저장소로부터 제거될 때까지 키가 아래로 순환된다는 것을 지시한다. 예를 들어 새로운 키가 개인 순환 키 저장소(231)에 추가될 때, 키(232)는 키(233)의 위치로 순환할 것이다.

[0070] 서버 컴퓨터 시스템(211)은 또한 로그인 페이지(217)를 포함한다. 로그인 페이지(217)는 사용자 자격 증명서를 제출하고 클라이언트 컴퓨터 시스템과 연관된 통신 특성을 선택하기 위한 인터페이스를 제공하는 웹 페이지, 예를 들어 ASP 페이지일 수 있다. 로그인 페이지(217)에 대응하는 URI에 액세스하는 클라이언트 컴퓨터 시스템에 응답하여, 서버 컴퓨터 시스템(211)은 로그인 페이지(217)를 클라이언트 컴퓨터 시스템에 송신할 수 있다. 클라이언트 기반 브라우저는 클라이언트 컴퓨터 시스템에 로그인 페이지(217)를 제공할 수 있다. 로그인 페이지에서 제출된 사용자 자격 증명서 및 통신 특성 선택(communication property selection)은 서버 컴퓨터 시스템(211)으로 송신될 수 있다.

[0071] 서버 컴퓨터 시스템은 또한 통신 필터(243)를 포함한다. 통신 필터(243)는, 예를 들어 서버 컴퓨터 시스템(211)으로 송신되거나 상기 시스템으로부터 송신되는 요구, 응답 및 메시지와 같은 HTTP 통신을 가로챌 수

있다. 통신 필터(243)는, 예를 들어 HTTP 헤더를 변경함으로써 서버 컴퓨터 시스템(211)과 클라이언트 컴퓨터 시스템간의 HTTP 통신이 변경되어야 하는지를 결정하기 위하여 암호화된 쿠기에 포함된 클라이언트 상태 정보를 참조할 수 있다. 통신 필터(243)는 또한 사용자 자격 증명서를 복호화하고 검증하기 위하여 순환 키 저장소로부터의 키를 사용하여 암호화 알고리즘을 구현할 수 있다.

[0072] 서버 컴퓨터 시스템(211)은 또한 로그인 요소 검증기(216)를 포함한다. 로그인 요소 검증기(216)는 로그인 페이지(217)에서 입력되고 제출된 사용자 자격 증명서를 수신하고, 제출된 사용자 자격 증명서에 전자 서명하고 암호화하기 위하여 순환 키 저장소로부터 키를 사용하는 암호화 알고리즘을 구현한다. 로그인 요소 검증기(216)는 또한 서버 컴퓨터 시스템(211)의 리소스로의 웹 기반 액세스를 요구하는 클라이언트 컴퓨터 시스템을 위하여 Globally Unique Identifier(GUID)와 같은 고유 세션 식별자(unique session identifier)를 생성할 수 있다. 로그인 요소 검증기(216)는 고유 세션 식별자와, 사용자 자격 증명서 및 시간 의존 전자 서명을 포함하는 암호화된 정보를 송신한다. 예를 들어, 로그인 요소 검증기(216)는 쿠키(203)에 저장하기 위한 고유 세션 식별자 및 암호화된 사용자 자격 증명서를 클라이언트 컴퓨터 시스템(201)에 송신한다.

[0073] 도 3은 클라이언트가 서버의 리소스로의 액세스를 요구할 때 클라이언트측 자격 증명서를 획득하기 위한 방법(300)의 예시적인 플로우차트를 도시한다. 방법(300)은 도 2a에서 설명하는 클라이언트 컴퓨터 시스템 및 서버 컴퓨터 시스템과 관련하여 설명될 것이다. 방법(300)은 서버로 제1 요구를 송신하는 단계(301)를 포함한다. 단계(301)는 클라이언트 컴퓨터 시스템이 서버의 전자 메일 메시지와 같은 리소스로의 웹 기반 액세스에 대한 제1 요구를 송신하는 단계를 포함한다.

[0074] 예를 들어, 클라이언트 컴퓨터 시스템(201)은 메일 서버 URI(267)를 포함하는 요구(251)를 서버 컴퓨터 시스템(211)에 송신할 수 있다. 메일 서버 URI(267)는 전자 메일 서버(212)에 대응하는 URI가 될 수 있다. 이것은 전자 메일 서버에 의하여 관리되는 전자 메일 리소스로의 액세스를 원하는 사용자가 메일 서버 URI(267)에 액세스함으로써 전자 메일 리소스로의 웹 기반 액세스를 시도할 수 있다는 것을 의미한다. 따라서, 클라이언트 컴퓨터 시스템(201)에서 사용자가 브라우저(202)에 명령을 입력함으로써 클라이언트 컴퓨터 시스템(201)은 요구(251)를 송신할 수 있다.

[0075] 방법(300)은 클라이언트로부터 제1 요구를 수신하는 단계(306)를 포함할 수 있다. 단계(306)는 서버 컴퓨터 시스템이 서버의 리소스, 예를 들어 전자 메일 메시지로의 웹 기반 액세스에 대한 제1 요구를 수신하는 단계를 포함한다. 예를 들어, 서버 컴퓨터 시스템(211)은 메일 서버 URI(267)를 포함하는 요구(251)를 클라이언트 컴퓨터 시스템(201)으로부터 수신할 수 있다. 통신 필터(243)를 통과하는 점선에 의하여 도시되는 바와 같이, 통신 필터(243)는 요구(251)가 변경 없이 통과되도록 설정될 수 있다. 따라서, 요구(251)는 변경되지 않고 전자 메일 서버(212)로 재전송될 수 있다.

[0076] 방법(300)은 클라이언트측 자격 증명서를 보증하기 위한 기능적 결과 지향 단계(functional result-oriented step; 311)를 포함한다. 단계(311)는 클라이언트측 자격을 보증하기 위한 임의의 대응하는 단계를 포함할 수 있다. 그러나, 도 3에 도시된 예에서, 단계(311)는 제1 요구에 응답하여 클라이언트를 로그인 페이지로 재지정하는 대응 단계(307)를 포함한다. 단계(307)는 서버 컴퓨터 시스템이 제1 요구에 응답하여 로그인 페이지에 클라이언트 컴퓨터 시스템을 재지정하는 단계를 포함할 수 있다.

[0077] 요구(251)에 대응하여 전자 메일 서버(212)는 무권한 지시자(unauthorized indicator; 272)를 포함하는 응답(252)을 송신할 수 있다. 응답(252)은 사용자 자격 증명서를 포함하지 않는 요구(251)의 결과로서 반환되는 상태 코드 401 Unauthorized를 갖는 HTTP 메시지일 수 있다. 통신 필터(243)는 무권한 지시자를 포함하는 메시지를 가로채도록 설정될 수 있다. 따라서, 통신 필터(243)는 응답(252)을 가로챌 수 있다.

[0078] 통신 필터(243)는 응답(252)의 컨텐츠를 변경하여 클라이언트 컴퓨터 시스템(201)이 사용자 자격 증명서를 입력하기 위하여 인터페이스를 제공하는 로그인 페이지로 재지정되도록 할 수 있다. 예를 들어, 통신 필터(243)는 응답(252)으로부터 무권한 지시자(272)를 제거하고 응답(252)에 로그인 페이지 URI(263) 및 재지정 지시자(271)를 삽입할 수 있으며, 그 결과 응답(252a)이 된다. 응답(252a)은 상태 코드 302 Found를 갖는 HTTP 메시지일 수 있다. 로그인 페이지 URI(263)는 로그인 페이지(217)에 액세스하기 위하여 사용되는 URI일 수 있다. 따라서, 응답(252a)은 요구된 리소스, 예를 들어 전자 메일 메시지 대신 로그인 페이지 URI(263)가 액세스된다는 것을 클라이언트 컴퓨터 시스템(201)에게 지시할 수 있다.

[0079] 방법(300)은 로그인 페이지로 재지정되는 단계(302)를 포함한다. 단계(302)는 클라이언트 컴퓨터 시스템이 사용자 자격 증명서를 수용하기 위한 인터페이스를 제공하는 로그인 페이지에 재지정되는 단계를 포함한다. 예를

들어, 클라이언트 컴퓨터 시스템(201)은 로그인 페이지(217)로 재지정될 수 있다. 응답(252a)의 수신에 응답하여, 클라이언트 컴퓨터(201)는 서버 컴퓨터 시스템(211)에 로그인 페이지 URI(263)를 포함하는 요구(257)를 송신할 수 있다. 요구(257)에 응답하여, 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템에 로그인 페이지(217)를 포함하는 응답(258)을 송신한다. 로그인 페이지는 예를 들어 ASP 페이지와 같은 웹 페이지일 수 있다.

[0080] 브라우저(202)는 클라이언트 컴퓨터 시스템(201)에 로그인 페이지(217)를 제공할 수 있다. 도 6은 본 발명의 원칙에 따라 사용자 자격 및 통신 특성 선택을 받아들일 수 있는 로그인 페이지(600)의 예를 도시한다. 로그인 페이지(217)는 로그인 페이지(600)와 유사하다. 로그인 페이지(600)는 사용자 식별자를 받아들일 수 있는 필드(606) 및 대응하는 패스워드를 받아들일 수 있는 필드(607)를 포함한다.

[0081] 라디오 버튼(601)은 클라이언트측 브라우저가 "어드밴스트 클라이언트(Advanced Client)"라는 것을 지시하는 통신 특성 선택을 수용하도록 사용될 수 있다. 라디오 버튼(602)은 클라이언트측 브라우저가 "다운 레벨 클라이언트(Down Level Client)"라는 것을 지시하는 통신 특성 선택을 받아들이도록 사용될 수 있다. 어드밴스트 클라이언트는, 예를 들어 러닝 스크립트(running scripts) 또는 프리젠팅 멀티미디어 출력과 같은 더 발전된 처리를 수행하는 기능을 포함한다. 반대로, 다운 레벨 클라이언트는 발전된 처리를 수행하는 기능을 포함하지 않을 수 있다. 따라서, 서버로부터 반환되는 컨텐츠의 풍부함은 클라이언트측 브라우저의 용량에 따라서 적절히 조정될 수 있다. 어드밴스트 클라이언트가 감소된 대역폭 및/또는 다이얼 업 접속과 같은 지연이 높은 접속을 통하여 서버에 접속될 때, 다운 레벨 클라이언트를 선택함으로써 서버로부터 반환되는 컨텐츠의 양을 감소시킬 수 있다.

[0082] 라디오 버튼(603)은 클라이언트측 브라우저가 "비신뢰 클라이언트 컴퓨터 시스템(Non-Trusted Client Computer System)"에 있다는 것을 지시하는 통신 특성 선택을 수용하기 위하여 사용될 수 있다. 라디오 버튼(604)은 클라이언트측 브라우저가 "개인 클라이언트 컴퓨터 시스템(Private Client Computer System)"에 있다는 것을 지시하는 통신 특성 선택을 수용하기 위하여 사용될 수 있다. 개인 클라이언트 컴퓨터 시스템은 공개적 액세스를 제한하거나 아예 불허하는 홈 또는 기업 클라이언트 컴퓨터 시스템일 수 있다. 비신뢰 클라이언트 컴퓨터 시스템은, 예를 들어, 호텔 또는 공항의 Internet Kiosk와 같은 공개적 액세스가 많은 클라이언트 컴퓨터 시스템일 수 있다. 따라서, 서버로부터 반환되는 컨텐츠와 연관되는 보증은 클라이언트 컴퓨터 시스템의 신뢰 가치도에 따라 적절히 조정될 수 있다. 버튼(608)은 서버 컴퓨터 시스템에 입력된 사용자 자격 증명서 및 선택된 통신 특성을 송신하기 위하여 선택될 수 있다.

[0083] 도 5는 본 발명의 원칙에 따라 클라이언트와 연관된 통신 특성을 결정하기 위한 방법(500)의 예시적인 플로우차트를 도시한다. 방법(500)은 네트워크 구조(200)에서 설명된 클라이언트 컴퓨터 시스템 및 서버 컴퓨터 시스템과 관련하여 설명된다. 방법(500)은 클라이언트로 로그인 페이지를 송신하는 단계(501)를 포함한다. 단계(501)는 서버 컴퓨터 시스템이 HTTP 메시지가 처리되어야 할 방법을 변경할 수 있는 하나 이상의 통신 특성을 선택하기 위한 인터페이스를 포함하는 로그인 페이지를 송신하는 단계를 포함한다. 예를 들어, 서버 컴퓨터 시스템(211)은 로그인 페이지(600)를 클라이언트 컴퓨터 시스템(201)에 송신할 수 있다.

[0084] 방법(500)은 서버로부터 로그인 페이지를 수신하는 단계(505)를 포함한다. 단계(505)는 클라이언트 컴퓨터 시스템이 HTTP 메시지가 처리되어야 할 방법을 변경할 수 있는 하나 이상의 통신 특성을 선택하기 위한 인터페이스를 포함하는 로그인 페이지를 수신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 로그인 페이지(600)를 수신할 수 있다. 방법(500)은 클라이언트에서 로그인 페이지를 제공하는 단계(506)를 포함한다. 단계(506)는 클라이언트 컴퓨터 시스템의 브라우저가 클라이언트 컴퓨터 시스템에서 로그인 페이지를 제공하는 단계를 포함할 수 있다. 예를 들어, 브라우저(202)는 클라이언트 컴퓨터 시스템(201)에 로그인 페이지(600)를 제공할 수 있다.

[0085] 방법(500)은 하나 이상의 통신 특성 중 적어도 하나의 선택을 수신하는 단계(507)를 포함한다. 단계(507)는 클라이언트 컴퓨터 시스템이 로그인 페이지에서 적어도 하나 이상의 통신 특성의 선택을 수신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)에서의 사용자는 통신 특성 선택을 로그인 페이지(600)로 입력하기 위하여 입력 장치, 예를 들어 키보드 및/또는 마우스 등을 사용할 수 있다. 로그인 페이지(600)는 사용자 입력 선택을 수신할 수 있다. 예를 들어, 로그인 페이지(600)는 잠재적으로 필드(606, 607)에서 사용자 입력 자격 증명서를 수신함과 함께, 라디오 버튼(601) 또는 라디오 버튼(602)에 대한 사용자 입력 선택 또는 라디오 버튼(603) 또는 라디오 버튼(604)에 대한 사용자 입력 선택을 수신할 수 있다.

[0086] 방법(500)은 통신 특성 선택을 서버의 통신 필터로 송신하는 단계(508)를 포함한다. 단계(508)는 클라이언트 컴퓨터 시스템이 서버 컴퓨터 시스템의 통신 필터로 통신 특성 선택을 송신하는 단계를 포함할 수 있다. 예를

들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(211)에, 예를 들어 사용자 입력 자격 증명서와 함께 통신 특성 선택을 송신할 수 있다. 방법(500)은 클라이언트로부터 적어도 하나의 통신 특성 선택을 수신하는 단계(502)를 포함할 수 있다. 단계(502)는 서버 컴퓨터 시스템이 로그인 페이지로부터 적어도 하나 이상의 선택 가능한 통신 특성의 선택을 수신하는 단계를 포함할 수 있다. 예를 들어, 통신 필터(243)는 클라이언트 컴퓨터 시스템(201)으로부터, 예를 들어 로그인 페이지(600)에서 선택되는 하나 이상의 통신 특성의 선택을 수신할 수 있다.

[0087] 방법(500)은 클라이언트에 의하여 지원되는 다른 관련 통신 특성을 식별하기 위하여 뿐만 아니라 적어도 하나의 수신되는 통신 특성 선택이 지원되는지를 결정하기 위하여 클라이언트에게 문의하는 단계(503)를 포함한다. 단계(503)는 서버 컴퓨터 시스템이 수신된 통신 특성 선택이 지원되는지를 결정하고 클라이언트에 의하여 지원되는 다른 관련 통신 특성을 식별하기 위하여 클라이언트 컴퓨터 시스템에 문의하는 단계를 포함한다. 예를 들어, 서버 컴퓨터 시스템은 사용자-에이전트 HTTP 헤더 및 클라이언트 컴퓨터 시스템의 선행 지식을 사용하는 클라이언트 컴퓨터 시스템 용량을 결정할 수 있다. 클라이언트 컴퓨터 시스템의 추가적인 용량은 로그인 페이지를 통하여 및 클라이언트 컴퓨터 시스템에서 로그인 페이지 내에서 실행되는 스크립트, 예를 들어 자바 스크립트로부터 결정될 수 있다.

[0088] 반대로, 클라이언트 컴퓨터에 문의하는 단계는, 클라이언트 컴퓨터 시스템이 서버 컴퓨터 시스템에 설정 정보를 개시하도록 하는 클라이언트 컴퓨터로의 요구를 송신하는 단계를 포함한다. 예를 들어, 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템(201)으로 브라우저(202)의 설정을 요구하는 요구를 송신할 수 있다. 이에 대응하여, 브라우저(202)는, 예를 들어 버전 숫자 및 브라우저(202)가 gzip 압축과 같은 HTTP 압축을 지원하는지 여부 등의 설정 정보를 지시할 수 있다. 버전 숫자에 기초하여, 서버 컴퓨터 시스템(211)은 로그인 페이지(600)에서의 "어드밴스트 클라이언트"의 선택이 적절한 것인지를 결정할 수 있다. 예를 들어, 서버 컴퓨터 시스템은 브라우저(202)의 버전이 스크립트를 지원하지 않는다는 것을 결정할 수 있다. 따라서, "어드밴스트 클라이언트"가 선택되더라도 서버 컴퓨터 시스템은 클라이언트 컴퓨터 시스템(201)에 단순화된 컨텐츠를 제공할 수 있다.

[0089] 컨텐츠를 단순화하는 것은 클라이언트 컴퓨터 시스템에 전달된 컨텐츠의 합을 감소시키는 것을 포함할 수 있다. 예를 들어, 도움말 정보에 대한 다운 레벨 클라이언트 요구에 대응하여 서버 컴퓨터 시스템은 감소된, 즉 덜 장황한 도움말 정보를 반환할 수 있다. 반대로, 도움말 정보에 대한 어드밴스트 클라이언트 요구에 응답하여, 서버 컴퓨터 시스템은 증가된 도움말 정보를 반환할 수 있는데, 예를 들어 탐색 스크립트 및 다른 진보된 기능을 포함할 수 있다. 서버 컴퓨터 시스템은 또한 클라이언트 컴퓨터 시스템의 신용 가치도에 기초하여 전달되는 컨텐츠를 변경할 수 있다. 예를 들어, 서버 컴퓨터 시스템은 민감한 기업 데이터를 액세스하는 방법에 대한 도움말 정보를 개인 클라이언트 컴퓨터 시스템에 제공할 수 있지만, 같은 정보를 비신뢰 클라이언트 컴퓨터 시스템에 제공할 수는 없다.

[0090] 서버 컴퓨터 시스템(211)이 브라우저(202)를 검사하는 것은 통지된 특징이 적절하게 지원되는지 검증하기 위한 것이다. 예를 들어, 브라우저(202)가 gzip 압축에 대한 지원을 지시할 때, 서버 컴퓨터 시스템(211)은 브라우저(202)가 gzip 압축 컨텐츠를 적절히 처리하는지 결정하기 위하여 클라이언트 컴퓨터 시스템(201)에 gzip 압축된 컨텐츠를 송신할 수 있다. 클라이언트 컴퓨터 시스템(201)은 gzip 압축을 위한 지원을 지시하는 적절한 요구 헤더를 설정할 수 있다. 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(211)으로 송신되고 거기에서 수신되는 클라이언트 요구에 적절한 요구 헤더를 포함시킬 수 있다. 이에 대응하여 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템(201)이 적절하게 gzip 압축 컨텐츠를 캐싱하고 웹 기반 응용프로그램의 보안 및 무결성에 불리하게 영향을 미치지 않는 방법으로 gzip 압축 컨텐츠를 처리하는지를 결정하기 위하여 클라이언트 컴퓨터 시스템(201)에 문의할 수 있다.

[0091] 방법(500)은 선택 및 식별된 통신 특성에 따라 통신 필터를 설정하는 단계(504)를 포함한다. 단계(504)는 서버 컴퓨터 시스템이 임의의 선택된 통신 특성 및 클라이언트에 의하여 지원되는 식별된 다른 관련 특성에 따라 통신 필터가 클라이언트와 HTTP 통신을 처리하도록 설정하는 단계를 포함할 수 있다. 예를 들어, 서버 컴퓨터 시스템(211)은 통신 필터(243)가 통신 특성 선택, 예를 들어 어드밴스트 클라이언트 및 비신뢰 클라이언트 컴퓨터 시스템의 선택 및 브라우저(202)의 인식된 다른 관련 통신 특성, 예를 들어 HTTP 압축 지원 여부에 따라 클라이언트 컴퓨터 시스템(201)과 HTTP 통신을 처리하도록 통신 필터를 설정할 수 있다.

[0092] HTTP 메시지가 서버 컴퓨터 시스템(211)으로부터 클라이언트 컴퓨터 시스템(201)으로 송신될 때, 통신 필터(243)는 클라이언트 컴퓨터 시스템(201)에 대한 통신 특성에 부합하는 컨텐츠가 되도록, HTTP 메시지 헤더 및

HTTP 메시지의 컨텐츠를 변경할 수 있다. 예를 들어, 전자 메일 서버(212)가 클라이언트 컴퓨터 시스템(201)으로 압축되지 않은 전자 메일 정보를 갖는 메시지를 송신한다면, 통신 필터(243)는 메시지를 가로채고, 컨텐츠를 gzip 압축하고 전자 메일 정보가 gzip 압축되었다는 것을 지시하도록 메시지 헤더를 변경할 수 있다. 선택적으로, 예를 들어 인터넷 정보 서버(internet information server; IIS)와 같은 서버 컴퓨터 시스템의 다른 모듈이 gzip 압축을 구현할 수도 있다. 따라서 컨텐츠는 클라이언트 컴퓨터 시스템의 용량을 최고로 사용하는 방식 및 사용자의 요구에 따라 클라이언트 컴퓨터 시스템에 제공된다.

[0093] 서버 컴퓨터 시스템(211)이 클라이언트측 브라우저가 "개인 클라이언트 컴퓨터 시스템"에 있다고 지시하는 선택을 수신할 때, 예를 들어 개인 키 저장소(231)와 같은 개인 순환 키 저장소가 사용자 자격 증명서를 보증하기 위하여 사용될 수 있다. 반대로 서버 컴퓨터 시스템(211)이 클라이언트측 브라우저가 "비신뢰 클라이언트 컴퓨터 시스템"에 있다는 것을 지시하는 선택을 수신할 때, 비신뢰 키 저장소(221)와 같은 비신뢰 순환 키 저장소가 사용자 자격 증명서를 보증하기 위하여 사용될 수 있다.

[0094] 도 3을 다시 보면, 방법(300)은 서버에 자격 증명서를 제출하기 위하여 로그인 페이지를 이용하는 단계(303)를 포함한다. 단계(303)는 클라이언트 컴퓨터 시스템이 서버 컴퓨터 시스템에 자격 증명서를 제출하기 위하여 로그인 페이지를 이용하는 단계를 포함한다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 잠재적으로 통신 특성 선택에 따라 로그인 페이지(217)를 이용하여 서버 컴퓨터 시스템(211)에 자격 증명서를 제출할 수 있다. 사용자 자격 증명서 및 통신 특성 선택은 로그인 요소 포맷 검증기에 제출되는 메일 메시지에 로그인 요소로서 포함될 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템에 로그인 요소(273)를 포함하는 메일 메시지(254)를 송신할 수 있다.

[0095] 방법(300)은 로그인 페이지에서 제출된 사용자 자격 증명서를 수신하는 단계(308)를 포함한다. 단계(308)는 서버 컴퓨터 시스템이 로그인 페이지에서 제출된 사용자 자격 증명서를 수신하는 단계를 포함한다. 예를 들어, 서버 컴퓨터 시스템(211)은 잠재적으로 통신 특성 선택을 따라 클라이언트 컴퓨터 시스템(201)으로부터 사용자 자격 증명서를 수신할 수 있다. 자격 및 통신 특성 선택은 우편 메시지(post message)의 로그인 요소로서 수신될 수 있다. 예를 들어, 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템(201)으로부터 로그인 요소(273)를 포함하는 우편 메시지(254)를 수신할 수 있다.

[0096] 통신 필터(243)를 통과하는 점선에 의하여 도시되는 바와 같이, 통신 필터(243)는 우편 메시지(254)가 변경 없이 통과될 수 있도록 한다. 따라서, 우편 메시지(254)는 변경 없이 로그인 요소 검증기(216)로 재전송될 수 있다. 적당한 경우, 예를 들어 Transport Layer Security(TLS) 또는 Secure Sockets Layer(SSL)를 사용하는 상호 인증된 연결(mutually authenticated connection)이 클라이언트 컴퓨터 시스템과 서버 컴퓨터 시스템 사이에 설립됨으로써, 패킷을 "알아채는(sniffing)" 악의적인 프로세스나 사용자가 생길 가능성과 중간자(middle-man)의 공격 가능성을 감소시킨다.

[0097] 로그인 요소 검증기(216)는 또한 클라이언트 컴퓨터 시스템(201)에 대하여 예를 들어 Globally Unique Identifier(GUID)와 같은 고유 식별자를 생성할 수 있다. 로그인 요소 검증기(216)는, 예를 들어 로그인 요소(273)에 포함되어 수신되는 사용자 자격 증명서를 보증하기 위하여 전자 서명 및 암호화 알고리즘을 사용할 수 있다. 예를 들어, 로그인 요소 검증기(216)는 수신된 사용자 자격 증명서를 검증하는 데에 사용되는 전자 서명을 생성할 수 있다. 로그인 요소 검증기(216)는 서명 키를 추출할 수 있으며, 상기 서명 키는, 예를 들어 SHA1 또는 MD-5 해싱 알고리즘을 사용하여 순환 키 저장소의 가장 최근의 키, 생성된 고유 식별자, 및 제1 상수 스트링의 조합을 해싱함으로써, 데이터에 전자 서명하는 데에 사용될 수 있다. 일부 실시예에서, 전자 서명은 Hashed Message Authentication Code로서 나타날 수 있다. 따라서, 서명 키는 공식 1에 의하여 추출될 수 있다.

[0098] $$K_{SIG} = SHA\text{-}1(K_{MOST\ CURRENT\ ROTATING}, GUID, HMACKeyString)$$

[0099] 공식 1

[0100] 공식 1에서, $K_{MOST\ CURRENT\ ROTATING}$은 적당한 순환 키 저장소의 가장 최근의 키를 나타낸다. 예를 들어, 브라우저(202)가 (예를 들어, 통신 특성 선택에 의하여 지시되는) "개인 클라이언트 컴퓨터 시스템"에 있을 때, $K_{MOST\ CURRENT\ ROTATING}$은 개인 순환 키 저장소(231)의 가장 최근의 키, 예를 들어 키(232)를 나타낸다. GUID는 클라이언트 컴퓨터 시스템(201)에 대응하는 고유 식별자를 나타낸다. HMACKeyString은 텍스트 상수 스트링을 나타낸다. K_{SIG}로부터, Hashed Message Authentication Code는 공식 2에 의하여 생성될 수 있다.

[0101] $$\text{Digital Signature} = \text{HMAC}(K_{SIG},(\text{GUID},\{\text{username:password}\},\text{Flags}))$$

[0102] 공식 2

[0103] 공식 2에서, HMAC은, 예를 들어 Request For Comments("RFC"; 2104)에서 설명되는 바와 같은 Hashed Message Authentication Code 알고리즘을 나타낸다. 공식 2의 (GUID,{username:password},Flags) 부분은 통신 GUID, 사용자 자격 증명서, 및 통신 특성 선택을 나타내는 플래그들이 Hashed Message Authentication Code 알고리즘에 입력되는 텍스트로서 포함됨을 나타낸다. 적당한 경우, 사용자 자격 증명서는 Hashed Message Authentication Code 알고리즘과의 호환성을 위하여, 예를 들어 상기 사용자 자격 증명서를 64 베이스로 인코딩함으로써 텍스트 포맷으로 변환될 수 있다. Hashed Message Authentication Code 알고리즘을 사용하여 설명되었지만, 전자 서명을 생성하는 데에 사용되는 알고리즘은 중요하지 않으며, 사실상 임의의 전자 서명, 다이제스트(digest), 또는 인증 코드 알고리즘이 사용될 수 있다.

[0104] 로그인 요소 검증기(216)는 또한 암호화 키를 추출할 수 있으며, 상기 암호화 키는 순환 키 저장소의 가장 최근의 키, 고유 식별자, 및 제2 상수의 조합을 해싱함으로써, 데이터를 암호화하는 데에 사용될 수 있다. 따라서, 암호화 키는 공식 3에 따라 추출될 수 있다.

[0105] $$K_{ENC} = \text{SHA-1}(K_{\text{MOST CURRENT ROTATING}}, \text{GUID}, \text{EncryptKeyString})$$

[0106] 공식 3

[0107] 공식 3에서, $K_{\text{MOST CURRENT ROTATING}}$는 서명 키의 생성에 사용되었던 순환 키 저장소로부터의 가장 최근의 키를 나타낸다. 따라서, 만일 키(232)가 K_{SIG}를 생성하는 데에 사용되었다면, 키(232)는 K_{ENC}를 생성하는 데에도 사용될 수 있다. GUID는 클라이언트 컴퓨터 시스템(201)에 대응하는 고유 식별자를 나타낸다. EncryptKeyString은 HMACKeyString과 상이한 텍스트 상수 스트링을 나타낸다. 따라서, 암호화된 정보는 공식 4에 따라 생성될 수 있다.

[0108] $$\text{Encrypted Information}=K_{ENC}[\text{Digital Signature},\{\text{username:password}\},\text{Flags}]$$

[0109] 공식 4

[0110] 공식 4에서, Digital Signature는 공식 2에 의하여 생성되는 Digital Signature를 나타내고, {username:password}는 사용자 자격 증명서를 나타내며, Flags는 통신 특성 선택을 나타낸다.

[0111] 단계(311)는 사용자 자격 증명서 및 시간 의존 서명(time-dependent signature)의 적어도 일부분을 나타내는 암호화된 정보를 송신하는 단계의 대응 단계(309)를 포함한다. 단계(309)는 서버 컴퓨터 시스템이 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 클라이언트 컴퓨터 시스템으로 송신하는 단계를 포함할 수 있다. 예를 들어, 로그인 요소 검증기(216)는 GUID(274) 및 암호화된 자격 증명서(275)를 포함하는 메시지(255)를 클라이언트 컴퓨터 시스템(201)으로 송신할 수 있다. 통신 필터(243)를 통과하는 점선에 의하여 도시되는 바와 같이, 통신 필터(243)는 메시지(255)가 변경 없이 통과될 수 있도록 구성될 수 있다. 따라서, 메시지(255)는 변경 없이 클라이언트 컴퓨터 시스템(201)으로 재전송될 수 있다.

[0112] 방법(300)은 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 수신하는 단계(304)를 포함한다. 단계(304)는 클라이언트 컴퓨터 시스템이 서버 컴퓨터 시스템으로부터, 사용자 자격 증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 수신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(211)으로부터 GUID(274) 및 암호화된 자격 증명서(275)를 포함하는 메시지(255)를 수신할 수 있다. 메시지(255)는 클라이언트 컴퓨터 시스템(201)이 쿠키(203)에 GUID(274) 및 암호화된 자격 증명서(275)를 저장하게 하도록 구성된다. 예를 들어, 메시지(255)는 다음과 같이 구성된다.

[0113] Set-Cookie:sessionid={GUID};path=/

[0114] Set-Cookie:creddata={Encrypted Information};path=/

[0115] 방법(300)은 암호화된 정보를 포함하는 요구를 송신하는 단계(305)를 포함한다. 단계(305)는 클라이언트 컴퓨터 시스템이 제1 요구에서 요구된 전자 메일 메시지와 같은 리소스로의 웹 기반 액세스에 대한 제2 요구를 송신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(211)으로 메일

서버 URI(267), GUID(274), 및 암호화된 자격 증명서(275)를 포함하는 요구(256)를 송신할 수 있다. 방법(300)은 암호화된 정보를 포함하는 제2 요구를 수신하는 단계(310)를 포함할 수 있다. 단계(310)는 서버 컴퓨터 시스템이 제1 요구에서 요구된 전자 메일 메시지와 같은 리소스에 대한 웹 기반 액세스에 대한 제2 요구를 수신하는 단계를 포함할 수 있다. 예를 들어, 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템(201)으로부터 메일 서버 URI(267), GUID(274), 및 암호화된 자격 증명서(275)를 포함하는 요구(256)을 수신할 수 있다.

[0116] 일부 실시예에서, 클라이언트 컴퓨터 시스템은 이전에 브라우저 메모리 내에 GUID 및 암호화된 정보를 가진 대응하는 쿠키를 저장하고 있다. 저장된 GUID 및 암호화된 정보는 서버의 전자 메일 데이터와 같은 리소스로의 웹 기반 액세스를 요구할 때 사용될 수 있다. 도 2b는 본 발명에 따라 서버의 리소스를 액세스하기 위하여 보증된 클라이언트측 자격 증명서를 이용하는 것을 용이하게 하는 네트워크 구조의 예를 도시한다. 도 4는 본 발명에 따라 서버의 리소스에 액세스하기 위하여 보증된 클라이언트측 자격 증명서를 이용하는 방법(400)의 흐름도를 도시한다. 방법(400)은 도 2b에 도시된 클라이언트 컴퓨터 시스템 및 서버 컴퓨터 시스템에 대하여 설명될 것이다.

[0117] 방법(400)은 서버의 리소스로의 웹 기반 액세스에 대한, 세션 식별자 및 암호화된 사용자 자격 증명서를 포함하는 요구를 송신하는 단계(401)를 포함한다. 단계(401)는 클라이언트 컴퓨터 시스템이 서버 컴퓨터 시스템의 리소스로의 웹 기반 액세스에 대한 요구를 송신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(211)으로 메일 서버 URI(267), GUID(274), 및 암호화된 자격 증명서(275)를 포함하는 요구(291)을 송신할 수 있다. 메일 서버 URI(267)은 전자 메일 서버(212)에 의하여 제어되는 전자 메일 리소스로의 액세스를 제공하는 URI를 나타낸다. GUID(274)는 이전에 서버 컴퓨터 시스템(211)으로부터 클라이언트 컴퓨터 시스템(201)으로 송신된 고유 세션 식별자를 나타낸다. 암호화된 자격 증명서(275)는 이전에 서버 컴퓨터 시스템(211)으로부터 클라이언트 컴퓨터 시스템(201)으로 송신된 암호화된 사용자 자격 증명서 및 시간 의존 서명을 나타낸다. 암호화된 자격 증명서(275)는 적당한 순환 키 저장소의 키로부터 생성되었을 수도 있다.

[0118] 방법(400)은 서버의 리소스로의 웹 기반 액세스에 대한, 세션 식별자 및 암호화된 사용자 자격 증명서를 포함하는 요구를 수신하는 단계(404)를 포함한다. 단계(404)는 서버 컴퓨터 시스템이 서버 컴퓨터 시스템의 리소스로의 웹 기반 액세스에 대한 요구를 수신하는 단계를 포함할 수 있다. 예를 들어, 서버 컴퓨터 시스템(211)은 클라이언트 컴퓨터 시스템(201)으로부터, 메일 서버 URI(267), GUID(274), 및 암호화된 자격 증명서(275)를 포함하는 요구(291)를 수신할 수 있다.

[0119] 방법(400)은 순환 키 저장소의 가장 최근의 키를 사용하여 암호화된 사용자 자격 증명서의 검증을 시도하는 단계(405)를 포함한다. 단계(405)는 서버 컴퓨터 시스템이 순환 키 저장소의 가장 최근의 키를 사용하여 적어도 사용자 자격 증명서의 일부분의 검증을 시도하는 단계를 포함할 수 있다. 예를 들어, 브라우저(202)가 개인 클라이언트 컴퓨터 시스템에 있을 때, 서버 컴퓨터 시스템은 키(232)를 사용하여 암호화된 자격 증명서(275)의 검증을 시도할 수 있다. 반면, 브라우저(202)가 비신뢰 클라이언트 컴퓨터 시스템에 있을 때, 서버 컴퓨터 시스템은 키(222)를 사용하여 암호화된 자격 증명서(275)의 검증을 시도할 수 있다. 자격 증명서(237)는 적당한 순환 키 저장소로부터의 가장 최근의 키, 고유 세션 식별자, 및 암호화 키를 추출할 때 사용되는 제2 상수 스트링의 조합을 해싱함으로써, 데이터를 복호화하는 데에 사용될 수 있는 복호화 키(decryption key)를 추출할 수 있다. 따라서, 복호화 키는 공식 5에 의하여 추출될 수 있다.

[0120] $$K_{DCR} = \text{SHA-1}(K_{\text{MOST CURRENT ROTATING}}, \text{GUID}, \text{EncryptKeyString})$$

[0121] 공식 5

[0122] 공식 5에서, $K_{\text{MOST CURRENT ROTATING}}$은 적당한 순환 키 저장소의 가장 최근의 키, 예를 들어 키(232) 또는 키(222)를 나타낸다. GUID는 클라이언트 컴퓨터 시스템(201)에 대응하는 고유 식별자를 나타낸다. EncryptKeyString은 K_{ENC}를 추출하는 동안 사용되는 상수 스트링을 나타낸다. 따라서, 자격 증명서 검증기(237)는 공식 6에 따라 Digital Signature, 사용자 자격 증명서, 및 통신 특성 선택을 나타내는 Flags을 드러내기 위하여 암호화된 정보를 복호화할 수 있다.

[0123] $$\text{Digital Signature},\{\text{username:password}\},\text{Flags} = K_{DCR}[\text{Encrypted information}]$$

[0124] 공식 6

[0125] 자격 증명서 검증기(237)는 적당한 순환 키 저장소의 가장 최근의 키, 고유 식별자, 및 제1 상수 스트링의 조합

을 해싱함으로써, 검증 전자 서명을 생성하는 데에 사용될 수 있는 검증 키(validation key)를 추출할 수 있다. 일부 실시예에서, 검증 전자 서명은 Hashed Message Authentication Code로서 나타난다. 따라서, 검증 키는 공식 7에 의하여 추출될 수 있다.

[0126] $$K_{VAL} = SHA\text{-}1(K_{MOST\ CURRENT\ ROTATING}, GUID, HMACKeyString)$$

[0127] 공식 7

[0128] 공식 7에서, $K_{MOST\ CURRENT\ ROTATING}$은 적당한 순환 키 저장소의 가장 최근의 키를 나타낸다. GUID는 클라이언트 컴퓨터 시스템(201)에 대응하는 고유 식별자를 나타낸다. HMACKeyString은 서명 키를 추출할 때 사용되는 텍스트 상수 스트링을 나타낸다. K_{VAL}로부터, 그리고 공식 6으로부터 드러나는 사용자 자격 증명서 및 Flags를 사용하여, Hashed Message Authentication Code는 공식 8에 의하여 생성될 수 있다.

[0129] $$Validation\ Digital\ Signature=HMAC(K_{VAL},(GUID,\{username{:}password\},Flags))$$

[0130] 공식 8

[0131] 공식 8에서, HMAC은 Hashed Message Authentication Code 알고리즘을 나타낸다. 공식 8의 (GUID,{username:password},Flags) 부분은 GUID, 사용자 자격 증명서, 통신 특성 선택을 나타내는 플래그가 Hashed Message Authentication Code 알고리즘에 입력되는 텍스트로서 포함됨을 나타낸다. Hashed Message Authentication Code 알고리즘에 대하여 설명되었지만, 검증 전자 서명을 생성하는 데에 사용되는 알고리즘은 중요하지 않으며, 사실상 임의의 전자 서명, 다이제스트, 또는 인증 코드 알고리즘이 사용될 수 있다.

[0132] 검증 전자 서명이 전자 서명과 일치할 때, 암호화된 자격 증명서(275)에 나타나는 사용자 자격 증명서는 검증된다. 따라서, 통신 필터(243)는 검증된 사용자 자격 증명서를 포함하는, 예를 들어 HTTP 권한 헤더와 같은 권한 헤더를 생성한다. 통신 필터(243)는 리소스로의 웹 기반 액세스에 대한 요구에 권한 헤더를 삽입할 수 있다. 예를 들어, 통신 필터(243)는 요구(291)로부터 암호화된 자격 증명서(275)를 제거하고, 요구(291)에 자격 증명서(289)를 삽입하여, 요구(291A)가 생성하도록 할 수 있다.

[0133] 검증 전자 서명이 전자 서명과 일치하지 않을 때, 사용자 자격 증명서는 검증되지 않는다. 따라서, 자격 증명서 검증기(237)는 적당한 순환 키 저장소 내의 그 다음 최근의 키에 기초하여 공식 5, 6, 7, 및 8의 기능을 반복한다. 예를 들어, 개인 클라이언트 컴퓨터 시스템에서의 클라이언트측 브라우저에 대하여, 자격 증명서 검증기(237)는 키(233)를 사용할 수 있다. 한 편, 비신뢰 클라이언트의 클라이언트측 브라우저에 대하여, 자격 검증기(237)는 키(223)를 사용할 수 있다. 자격 증명서 검증기는 적당한 순환 키 저장소의 각각의 키를 사용하여 사용자 자격 증명서의 검증을 시도할 수 있다. 검증된 사용자 자격 증명서는 적당한 권한 헤더에 포함될 수 있다.

[0134] 일부 실시예에서, 암호화된 자격 증명서의 검증을 시도하는 데에 사용되는 순환 키, 예를 들어 전에 자격 증명서를 암호화하는 데에 사용되었던 순환 키를 지시하기 위한 인덱스가 암호화된 자격 증명서와 함께 포함된다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 요구(291)에서, 비신뢰 순환 키 저장소(221) 또는 개인 순환 키 저장소(231)에서의 순환 키를 식별하는 인덱스를 포함할 수 있다. 인덱스는 사용되는 순환 키의 생성을 식별하는 0, 1, 2 등과 같은 숫자일 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)이 개인 클라이언트 컴퓨터 시스템일 때, 인덱스 0은 키(232)를 식별하기 위하여 사용될 수 있다. 마찬가지로, 클라이언트 컴퓨터 시스템(201)이 비신뢰 클라이언트 컴퓨터 시스템일 때, 인덱스 2는 키(224)를 식별할 수 있다. 따라서, 인덱스의 사용은 검증 절차의 능률을 향상시킬 수 있다. 자격 증명서가 인덱스에 의하여 식별되는 순환 키로 검증되지 않을 때, 대응하는 순환 키 저장소 내의 다른 키가 자격 증명서의 검증을 시도하는 데에 사용될 수 있다.

[0135] 방법(400)은 요구된 리소스로의 웹 기반 엑세스를 제어하는 모듈로 요구를 재전송하는 단계(406)를 포함한다. 단계(406)는 서버 컴퓨터 시스템이 요구된 리소스로의 웹 기반 엑세스를 제어하는 모듈로 요구를 재전송하는 단계를 포함할 수 있다. 예를 들어, 통신 필터(243)는 전자 메일 서버(212)로 메일 서버 URI(267) 및 암호화된 자격 증명서(275)로부터 드러난 자격 증명서(289)를 포함하는 요구(291A)를 재전송할 수 있다. 전자 메일 서버(212)는 요구되는 전자 메일 리소스로의 웹 기반 액세스가 권한을 가진 것인지를 결정하기 위하여 자격 증명서(289)를 자격 증명서 데이터 베이스(213)와 비교할 수 있다.

[0136] 방법(400)은 리프레시된 암호화된 사용자 자격 증명서가 순환 키 저장소의 가장 최근의 키로부터 추출되어야 하는지를 결정하는 단계(407)를 포함한다. 단계(407)는 서버 컴퓨터 시스템이 사용자 자격 증명서 및 시간 의존

서명을 나타내는 리프레시된 암호화된 사용자 자격 증명서가 순환 키 저장소의 가장 최근의 키로부터 추출되어야 하는지를 결정하는 단계를 포함할 수 있다. 사용자 자격 증명서가 순환 키 저장소로부터의 가장 최근의 키가 아닌 키로 검증될 때, 서버는 리프레시된 암호화된 정보가 추출되어야 한다고 결정한다. 예를 들어, 만일 자격 증명서 검증기(237)가 암호화된 자격 증명서를 키(224)로 검증하면, 통신 필터(243)는 암호화된 자격 증명서로 나타나는 사용자 자격 증명서에 대하여 리프레시된 암호화된 자격 증명서가 추출되어야 한다고 결정할 수 있다.

[0137] 따라서, 점선 화살표에 의하여 도시되는 바와 같이, 통신 필터(243)는 선택적으로 로그인 요소 검증기(216)로 쿠키 리프레시 요구(294)를 송신할 수 있다. 로그인 요소 검증기(216)는, 예를 들어 가장 최근의 키로부터 리프레시된 전자 서명 및 리프레시된 암호화 키를 추출함으로써, 리프레시된 암호화된 정보를 추출하는 데에 적당한 순환 키 저장소의 가장 최근의 순환 키를 사용할 수 있다. 로그인 요소 검증기(216)는 갱신된 GUID 및 리프레시된 암호화된 자격 증명서를 통신 필터(243)로 반환할 수 있다. 예를 들어, 점선 화살표에 의하여 도시되는 바와 같이, 로그인 요소 검증기(216)는 갱신된 GUID 및 리프레시된 암호화된 자격 증명서를 포함하는 메시지(295)를 통신 필터(243)로 반환한다.

[0138] 자격 증명서(289)가 전자 메일 서버(212)의 전자 메일 리소스로의 웹 기반 액세스에 대하여 적절할 경우, 전자 메일 서버(212)는 요구(291A)에 응답하여 전자 메일 리소스를 반환할 수 있다. 예를 들어, 전자 메일 서버(212)는 전자 메일 메시지와 같은 리소스(293)를 포함하는 응답(292)을 통신 필터(243)로 반환할 수 있다. 반면, 자격 증명서(289)가 전자 메일 서버(212)에서의 전자 메일 리소스로의 웹 기반 액세스에 대하여 적절하지 않을 경우, 전자 메일 서버(212)는 요구(291A)에 응답하여 무권한 지시자를 반환할 수 있다. 예를 들어, 점선 화살표에 의하여 도시되는 바와 같이, 전자 메일 서버(212)는 무권한 지시자(272)를 포함하는 응답(294)을 통신 필터(243)로 반환할 수 있다. 통신 필터(243)가 무권한 지시자를 수신할 때, 통신 필터(243)는 클라이언트 컴퓨터 시스템(201)을 로그인 페이지(217)로 재지정할 수 있다.

[0139] 검증된 사용자 자격 증명서가 적절할 경우, 통신 필터(243)는 요구된 리소스를 클라이언트 컴퓨터 시스템(201)으로 송신할 수 있다. 예를 들어, 암호화된 자격 증명서(275)가 적당한 순환 키 저장소로부터의 가장 최근의 키로 검증될 경우, 리소스(293)를 포함하는 응답(292)이 통신 필터(243)에서 수신된다. 통신 필터(243)는 응답(292)을 클라이언트 컴퓨터 시스템으로 재전송할 수 있다. 따라서, 리소스(293)는 브라우저(202)에서 제공될 수 있다.

[0140] 검증된 사용자 자격 증명서가 적절할 경우, 통신 필터(243)는 또한 리소스와 함께 리프레시된 암호화된 자격 증명서 및 갱신된 GUID를 클라이언트 컴퓨터 시스템(201)으로 송신할 수 있다. 예를 들어, 암호화된 자격 증명서(275)가 순환 키 저장소의 가장 최근의 키가 아닌 키로 검증될 때, 리소스(293), 갱신된 GUID(296), 및 리프레시된 암호화된 자격 증명서(297)가 통신 필터(243)에서 수신될 수 있다. 점선 화살표에 의하여 도시되는 바와 같이, 통신 모듈(243)은 리소스(293), 갱신된 GUID(296), 및 리프레시된 암호화된 자격 증명서(297)를 포함하는 응답(276)을 클라이언트 컴퓨터 시스템(201)으로 송신할 수 있다.

[0141] 방법(400)은 갱신된 세션 식별자 및 리프레시된 암호화된 사용자 자격 증명서와 함께 요구된 리소스를 클라이언트측 브라우저에서 수신하는 단계(402)를 포함한다. 단계(402)는 클라이언트 컴퓨터 시스템이 갱신된 세션 식별자, 사용자 자격 증명서 및 리프레시된 시간 의존 서명의 적어도 일부분을 나타내는 리프레시된 암호화된 정보와 함께, 요구된 리소스를 수신하는 단계를 포함할 수 있다. 예를 들어, 클라이언트 컴퓨터 시스템(201)은 서버 컴퓨터 시스템(201)으로부터 리소스(293), 갱신된 GUID(293), 및 리프레시된 암호화된 자격 증명서(297)를 포함하는 응답(276)을 수신할 수 있다.

[0142] 방법(400)은 대응하는 쿠키에 갱신된 세션 식별자 및 리프레시된 암호화된 사용자 자격 증명서를 저장하는 단계(403)를 포함한다. 단계(403)는 클라이언트 컴퓨터 시스템이 클라이언트 컴퓨터 시스템의 대응 쿠키에 갱신된 세션 식별자 및 리프레시된 암호화된 정보를 저장하는 단계를 포함할 수 있다. 예를 들어, 갱신된 GUID(296) 및 리프레시된 암호화된 자격 증명서(297)는 GUID(274) 및 암호화된 자격 증명서(275)를 겹쳐 쓰면서 쿠키들(203) 중 대응하는 쿠키에 저장될 수 있다. 리소스(293)는 브라우저(202)에서 제공될 수 있다.

발명의 효과

[0143] 본 발명은 리소스에 웹 기반으로 액세스하기 위하여 사용되는 클라이언트 신분을 안전하게 처리하기 위한 방법, 시스템, 컴퓨터 프로그램 제품 및 데이터 구조를 포함하는 컴퓨터 판독 가능 매체를 제공한다.

[0144] 본 발명은 본 발명의 사상 또는 필수적인 특성으로부터 벗어나지 않으면서 다른 특정 형태로 구현될 수 있다.

설명된 실시예는 예시로서만 간주되어야 하며, 본 발명을 제한하는 것으로 간주되어서는 안 된다. 따라서, 본 발명의 범위는 전술된 설명보다는 첨부된 특허청구범위에 의하여 지시된다. 특허청구범위와 등가의 의미 및 범위 내에 오는 모든 변형은 본 발명의 범위 내에 포함된다.

도면의 간단한 설명

[0001] 도 1은 본 발명에 따른 적절한 동작 환경을 도시한 도면.

[0002] 도 2a는 본 발명에 따라 클라이언트가 리소스로의 액세스를 요구하는 경우 클라이언트측 자격 증명서의 보증을 용이하게 하는 네트워크 구조의 예를 도시한 도면.

[0003] 도 2b는 본 발명에 따라 서버의 리소스에 액세스하기 위하여 보증된 클라이언트측 자격 증명서의 사용을 용이하게 하는 네트워크 구조의 예를 도시한 도면.

[0004] 도 3은 본 발명에 따라 클라이언트가 서버의 리소스로의 액세스를 요구하는 경우 클라이언트측 자격 증명서를 보증하기 위한 방법을 예시한 흐름도.

[0005] 도 4는 본 발명에 따라 서버의 리소스에 액세스하기 위하여 보증된 클라이언트측 자격 증명서를 사용하는 방법을 예시한 흐름도.

[0006] 도 5는 본 발명에 따라 클라이언트와 관련된 통신 특성을 결정하기 위한 방법을 예시한 흐름도.

[0007] 도 6은 본 발명에 따라 자격 증명서 및 통신 특성 선택을 입력받을 수 있는 로그인 페이지를 예시한 도면.

[0008] <도면의 주요 부분에 대한 부호의 설명>

[0009] 201: 클라이언트 컴퓨터 시스템

[0010] 202: 브라우저

[0011] 203: 쿠기

[0012] 211: 서버 컴퓨터 시스템

[0013] 212: 전자 메일 서버

[0014] 213: 자격 증명서 데이터 베이스

[0015] 214: 키 생성 모듈

[0016] 216: 로그인 요소 검증기

[0017] 217: 로그인 페이지

[0018] 220: 순환지

[0019] 251, 256, 257: 요구

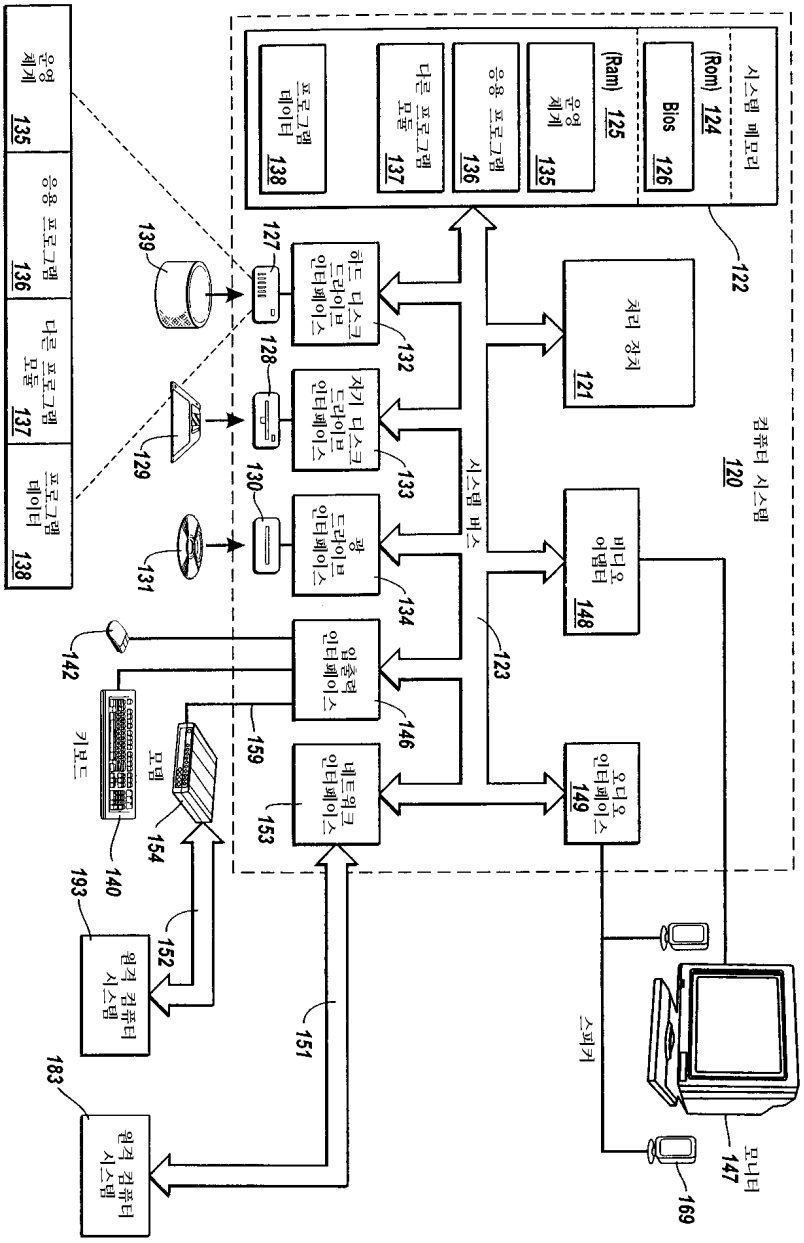
[0020] 252, 252A, 258: 응답

[0021] 254: 우편 메시지

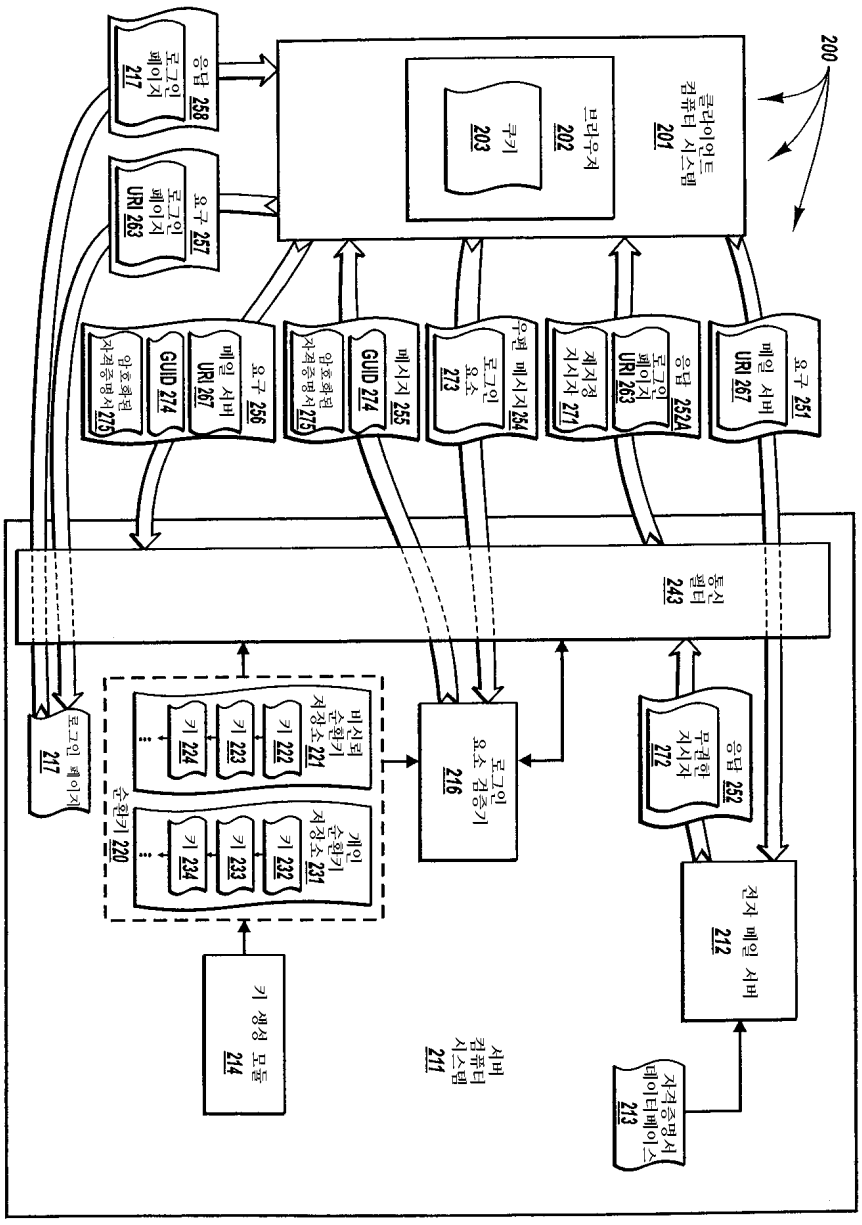
[0022] 255: 메시지

도면

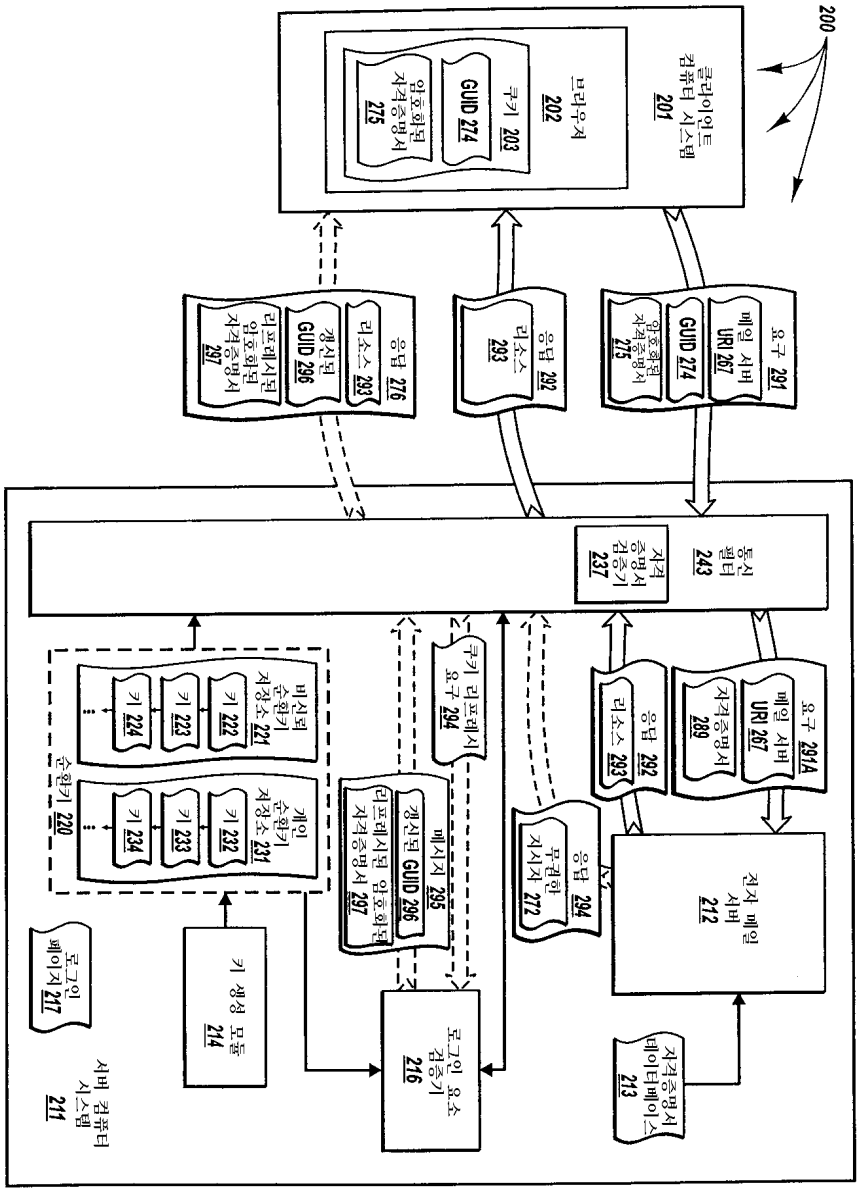
도면1


시스템 메모리
(Rom) 124
Bios 126
(Ram) 125
운영 체계 135
응용 프로그램 136
다른 프로그램 모듈 137
프로그램 데이터 138
122
처리 장치 121
컴퓨터 시스템 120
시스템 버스
하드 디스크 드라이브 인터페이스 132
자기 디스크 드라이브 인터페이스 133
광 드라이브 인터페이스 134
입출력 인터페이스 146
네트워크 인터페이스 153
비디오 어댑터 148
오디오 인터페이스 149
123
159
127
128
130
139
129
131
142
키보드 140
모뎀 154
193
152
원격 컴퓨터 시스템
183
151
스피커
모니터 147
169
운영 체계 135
응용 프로그램 136
다른 프로그램 모듈 137
프로그램 데이터 138

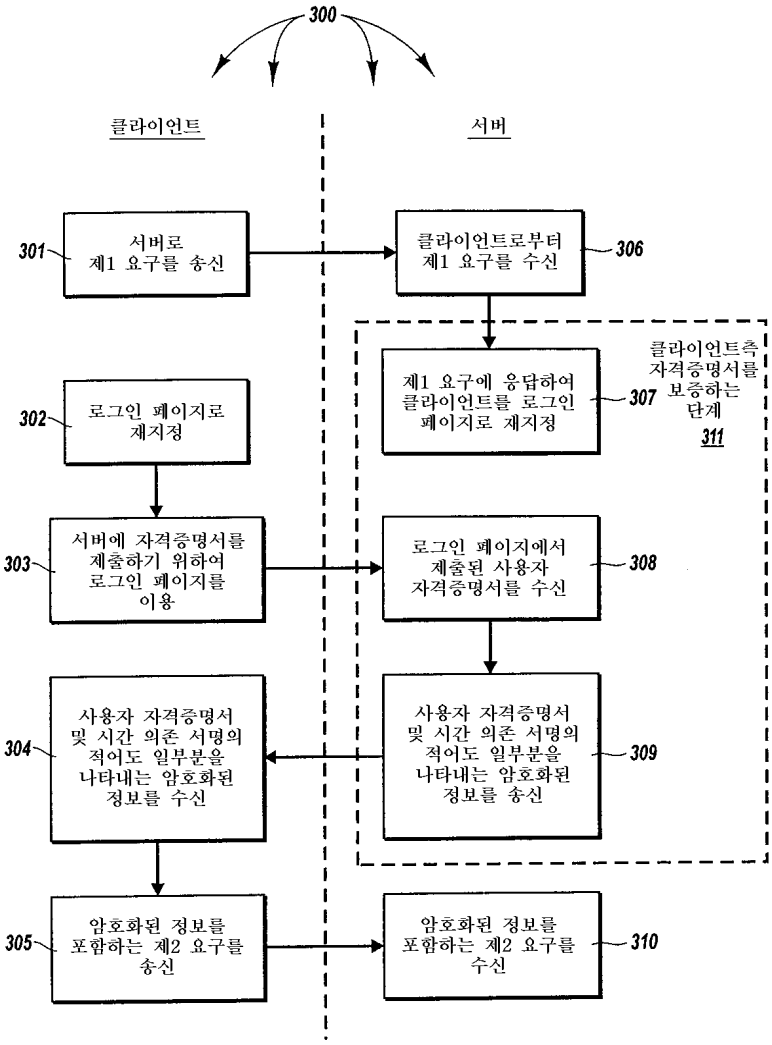
도면2a


200
클라이언트 컴퓨터 시스템 201
브라우저 202
쿠키 203
요구 251
메일 서버 URI 267
응답 252A
로그인 페이지 URI 263
재지정 지시자 271
우편 메시지 254
로그인 요소 273
메시지 255
GUID 274
암호화된 자격증명서 275
요구 256
메일 서버 URI 267
GUID 274
암호화된 자격증명서 275
요구 257
로그인 페이지 URI 263
응답 258
로그인 페이지 217
통신 필터 243
응답 252
무결한 지시자 272
로그인 요소 검증기 216
전자 메일 서버 212
자격증명서 데이터베이스 213
서버 컴퓨터 시스템 211
키 생성 모듈 214
비신뢰 순환키 저장소 221
키 222
키 223
키 224
개인 순환키 저장소 231
키 232
키 233
키 234
순환키 220
로그인 페이지 217

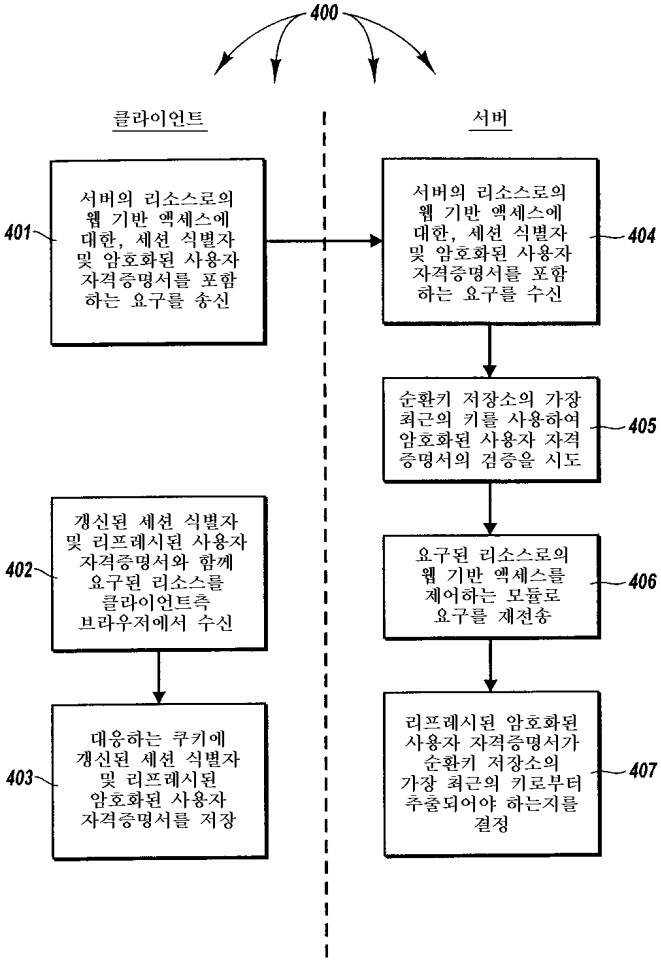
도면2b


200
클라이언트 컴퓨터 시스템 201
브라우저 202
쿠키 203
GUID 274
암호화된 자격증명서 275
요구 291
메일 서버 URI 267
GUID 274
암호화된 자격증명서 275
응답 292
리소스 293
응답 276
리소스 293
갱신된 GUID 296
리프레시된 암호화된 자격증명서 297
통신 필터 243
자격 증명서 검증기 237
요구 291A
메일 서버 URI 267
자격증명서 289
응답 292
리소스 293
쿠키 리프레시 요구 294
메시지 295
갱신된 GUID 296
리프레시된 암호화된 자격증명서 297
무권한 지시자 272
응답 294
전자 메일 서버 212
자격증명서 데이터베이스 213
로그인 요소 검증기 216
키 생성 모듈 214
로그인 페이지 217
서버 컴퓨터 시스템 211
비신뢰 순환키 저장소 221
키 222
키 223
키 224
개인 순환키 저장소 231
키 232
키 233
키 234
순환기 220

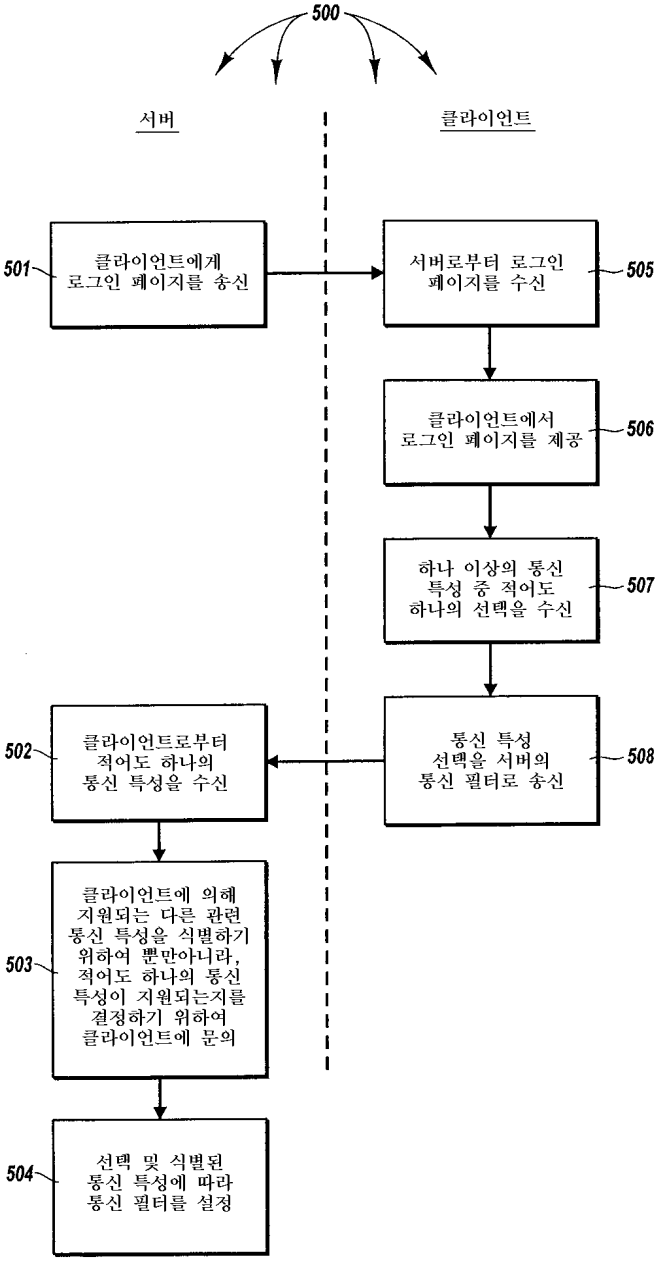
도면3


300
클라이언트
서버
301
서버로 제1 요구를 송신
306
클라이언트로부터 제1 요구를 수신
302
로그인 페이지로 재지정
307
제1 요구에 응답하여 클라이언트를 로그인 페이지로 재지정
클라이언트측 자격증명서를 보증하는 단계
311
303
서버에 자격증명서를 제출하기 위하여 로그인 페이지를 이용
308
로그인 페이지에서 제출된 사용자 자격증명서를 수신
304
사용자 자격증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 수신
309
사용자 자격증명서 및 시간 의존 서명의 적어도 일부분을 나타내는 암호화된 정보를 송신
305
암호화된 정보를 포함하는 제2 요구를 송신
310
암호화된 정보를 포함하는 제2 요구를 수신

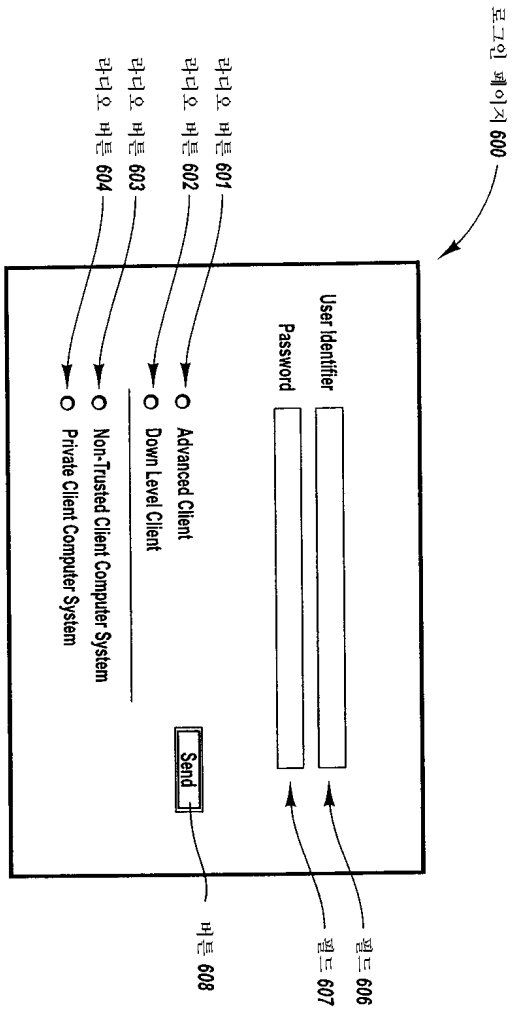
도면4


400
클라이언트
서버
서버의 리소스로의 웹 기반 액세스에 대한, 세션 식별자 및 암호화된 사용자 자격증명서를 포함하는 요구를 송신
401
서버의 리소스로의 웹 기반 액세스에 대한, 세션 식별자 및 암호화된 사용자 자격증명서를 포함하는 요구를 수신
404
순환키 저장소의 가장 최근의 키를 사용하여 암호화된 사용자 자격증명서의 검증을 시도
405
요구된 리소스로의 웹 기반 액세스를 제어하는 모듈로 요구를 재전송
406
리프레시된 암호화된 사용자 자격증명서가 순환키 저장소의 가장 최근의 키로부터 추출되어야 하는지를 결정
407
갱신된 세션 식별자 및 리프레시된 사용자 자격증명서와 함께 요구된 리소스를 클라이언트측 브라우저에서 수신
402
대응하는 쿠키에 갱신된 세션 식별자 및 리프레시된 암호화된 사용자 자격증명서를 저장
403

도면5


500
서버
클라이언트
501
클라이언트에게 로그인 페이지를 송신
505
서버로부터 로그인 페이지를 수신
506
클라이언트에서 로그인 페이지를 제공
507
하나 이상의 통신 특성 중 적어도 하나의 선택을 수신
508
통신 특성 선택을 서버의 통신 필터로 송신
502
클라이언트로부터 적어도 하나의 통신 특성을 수신
503
클라이언트에 의해 지원되는 다른 관련 통신 특성을 식별하기 위하여 뿐만아니라, 적어도 하나의 통신 특성이 지원되는지를 결정하기 위하여 클라이언트에 문의
504
선택 및 식별된 통신 특성에 따라 통신 필터를 설정

도면6


로그인 페이지 600
라디오 버튼 601
라디오 버튼 602
라디오 버튼 603
라디오 버튼 604
User Identifier
Password
Advanced Client
Down Level Client
Non-Trusted Client Computer System
Private Client Computer System
Send
필드 606
필드 607
버튼 608