(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 9/30

(11) 공개번호 특2003-0088855
(43) 공개일자 2003년11월20일

(21) 출원번호 10-2003-0022923
(22) 출원일자 2003년04월11일

(30) 우선권주장 10/146,686 2002년05월15일 미국(US)

(71) 출원인 마이크로소프트 코포레이션
미국 워싱턴주 (우편번호 : 98052) 레드몬드 원 마이크로소프트 웨이

(72) 발명자 구오,웨이-쿠앙엠.
미국98006워싱턴주벨레뷰원헌드레드써티써드애비뉴에스이4616

호워드,존에이치.
미국98074워싱턴주삼마미스엔이에이틴쓰스트리트25025

찬,콕더블유
미국98007워싱턴주벨레뷰엔이피프티세븐쓰스트리트14552

(74) 대리인 주성민
백만기
이중희

심사청구 : 없음

(54) 세션 키 보안 프로토콜

요약

멀티-사이트 인증 시스템에서 사용하기 위한 보안 프로토콜이 제공된다. 사용자를 인증한 후에, 인증 서버는 사용자와 관련된 정보를 포함하는 티켓을 생성한다. 인증 서버는 제휴 서버와 공유되는 대칭 키를 사용해서 티켓의 내용을 암호화한다. 제휴 서버는 인증 서버가 공유 키를 암호화하기 위해 사용하는 공개 키를 가진다. 인증 서버는 티켓 상에 서명을 생성하기 위해 개인 키를 가진다. 제휴 서버는 그것의 개인 키로 공유 키를 해독하고 그 후 해독된 공유 키를 사용해서 티켓의 내용을 해독한다. 제휴 서버는 인증 서버의 공개 키로 서명을 유효하게 한다.

대표도

도 3

색인어

공개 키, 개인 키, 공유 키, 보안 프로토콜, 인증 시스템

명세서

도면의 간단한 설명

도 1은 본 발명이 이용되는 대표적인 네트워크 환경을 설명하는 블록도.

도 2 및 도 3은 클라이언트 컴퓨터의 사용자가 제휴 서버에 접속하려고 할 때 도 1의 클라이언트 컴퓨터, 제휴 서버, 및 인증 서버 사이의 상호작용을 설명하는 대표적인 흐름도.

도 4는 도 1의 시스템에서의 이용을 위한 컴퓨터의 구성요소를 설명하는 블록도.

대응하는 참조 부호는 도면을 통해서 대응하는 부분을 가리킨다.

<도면의 주요 부분에 대한 부호 설명>

12 클라이언트 컴퓨터 시스템 26 인증 데이터베이스

14 네트워크 78 ROM

16 제휴 서버 76 시스템 버스

24 인증 서버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 컴퓨터 네트워크 환경 분야에 관한 것이다. 특히, 본 발명은 세 션 키 보안 프로토콜을 사용함으로써 멀티-사이트 사용자 인증 시스템(multi-site user authentication system)에서 향상된 보안에 관한 것이다.

웹사이트, 또는 인터넷 사이트는, 매우 자주 정보, 제품, 서비스, 또는 그와 같은 것을 그것의 사용자에게 제공한다. 많은 웹사이트는 그것의 웹 서버가 사용자에게 접속을 승인하기 전에 사용자에게 '등록'하기를 요구한다. 등록 동안, 사용자는 일반적으로 사용자명, 계좌 번호, 주소, 전화번호, 이-메일 주소, 컴퓨터 플랫폼, 나이, 성별, 및/또는 취미와 같은 개인 정보를 등록 웹사이트에 제공한다. 등록 정보는 거래(예, 상업 또는 금융 거래)를 완료하기 위해서 필요할 수 있다. 일반적으로, 정보는 또한 웹사이트가 예를 들어, 특별 판매, 신상품, 또는 새로운 웹사이트 특징을 알리기 위해 직접(예, 이-메일을 통해서) 사용자에 접촉하는 것을 허용한다. 추가적으로, 웹사이트는 자주 사용자 정보를 수집해서 웹사이트 운영자는 더 낫게 미래 마케팅 활동을 목표로 할 수 있거나 사이트에 의해 제공되는 내용을 조정할 수 있다.

처음으로 사용자를 등록할 때, 웹사이트는 일반적으로 사용자가 로그인 ID 및 관련된 패스워드를 선택하도록 요구한다. 로그인 ID는 웹사이트가 다음번에 사용자가 웹사이트를 방문하는 동안 사용자를 확인하고 사용자의 정보를 추출하는 것을 허용한다. 일반적으로, 로그인 ID는 웹사이트에 유일해야 하기 때문에 어떤 두 사용자도 동일한 로그인 ID를 갖지 않는다. 로그인 ID와 관련된 패스워드는 웹사이트가 웹사이트에 대한 다음 번 방문 동안 사용자를 인증하는 것을 가능하게 한다. 패스워드는 또한 다른 사람(패스워드를 모르는 사람)이 사용자의 로그인 ID를 사용해서 웹사이트에 접속하는 것을 막는다. 웹사이트가 금융 정보 또는 의료 기록과 같은 사용자에 대한 개인적 또는 비밀 정보를 저장하고 있다면 이 패스워드 보호는 특히 중요하다.

만약 사용자가 여러 다른 웹사이트를 방문하면, 각 웹사이트는 사용자 이름, 우편 주소, 및 이-메일 주소와 같은 사용자에 관한 유사한 등록 정보의 입력을 요구한다. 짧은 시간 동안 다수의 웹사이트를 방문할 때 이 동일한 데이터의 반복된 입력은 번거로운 일이다. 많은 웹사이트는 사용자에게 사이트 상에서 제공되는 임의의 정보에 접근하기 전에 등록하기를 요구한다. 그러므로, 사용자는 사이트가 관심 있는 임의의 정보를 포함하고 있는지 결정할 수 있기 전에 요구되는 등록 정보를 먼저 입력해야 한다.

다수의 웹사이트에 등록한 후에, 사용자는 각각의 웹사이트 또는 다른 인터넷 서비스에서 사용되는 특정 로그인 ID와 패스워드를 기억해야 한다. 로그인 ID와 패스워드가 정확하지 않다면, 사용자는 등록 정보를 다시 입력해야 한다. 특정 사용자는 다른 웹사이트 상에 다른 로그인 ID 및 관련된 패스워드를 가질 수 있다. 예를 들어, Bob Smith라는 사용자는 특정 사이트에 대해 그의 로그인 ID로 'smith'를 선택할 수 있다. 만약 그 사이트가 이미 'smith'라는 로그인 ID를

가진 사용자가 있거나 로그인 ID가 최소 여섯 자 이상이어야 한다고 요구하면, 그러면 사용자는 다른 로그인 ID를 선택해야 한다. 다수의 웹사이트에 등록한 후에, Bob Smith는 smith, smith1, bsmith, smithb, bobsmith, bob_smith 및 smithbob와 같은 서로 다른 로그인 ID의 집합을 가질 수 있다. 또한, 서로 다른 웹사이트의 다른 패스워 드 요건(예, 패스워드의 길이 요건 또는 각각의 패스워드가 적어도 하나의 숫자 및/또는 적어도 하나의 대문자를 포함하여야 한다는 요건) 때문에 서로 다른 패스워드는 서로 다른 로그인 ID와 관련이 있을 것이다. 그러므로, Bob Smith는 그가 정기적으로 방문하는 모든 웹사이트에 대해 웹사이트, 로그인 ID, 및 관련된 패스워드의 리스트를 유지해야 한다.

현재 이용 가능한 멀티-사이트 사용자 인증 시스템이 웹 사용자가 다수의, 제휴 웹 서버(affiliated web servers) 또는 서비스에 접근하기 위해 하나의 사용자 ID(및 관련된 패스워드)를 유지하는 것을 허용함에도 불구하고, 그 이상의 향상이 요구된다. 예를 들어, 인증 데이터는 일반적으로 사실상 민감하고 보호되어야 한다. 그러므로, 다수의 제휴 웹 서버 및 인증을 수행하는 인증 서버 상에서 보안을 유지하는 것은 중요하다.

Kerberos 인증과 같은 현재 이용 가능한 네트워크 보안 프로토콜은, 네트워크에 로그온 하려는 사용자의 신원을 인증하기 위해 그리고 그들의 통신을 암호화하기 위해 공유 또는 하나의 키(shared or single key)를 채용한다. 간혹 대칭 키 암호화(symmetric key encryption)라고 하는 공유 키의 사용은 새로운 웹 서비스가 인증 서비스를 이용하기 위해 키 인증 프로세스를 요구한다. Kerberos 시스템에서, 인증 서버(즉, Kerberos 서버, 또는 키 배포 센터(KDC))는 그것의 인증 서비스를 이용하는 각 제휴 서버에 공유 키를 배포해야 하고 정기적으로 키를 갱신해야 한다. KDC는 자주 우편으로 키를 발행한다. 불행히도, 공유 키를 제공해야 한다면, 새로운 웹 서비스에 대한 등록 및 계속되는 유지(예, 주기적 키 개정)를 행함 에 있어 상당한 복잡성이 생긴다. 또한 다수의 인증 서비스 제공자를 포함하는 연합 환경에서, 키 배포는 훨씬 더 복잡해진다.

제휴 사이트가 둘 또는 다수의 독립 KDC로부터 '구속(kerb)' 티켓을 수용하기로 결정할 때 키 배포는 더 복잡해진다. 또한, 제휴를 위한 키는 두 KDC에 모두 구성되어야 한다. 바꾸어 말하면, 제휴 사이트가 지원하는 KDC가 많아질수록, 키 배포 프로세스는 더 복잡해진다. 추가적으로, KDC가 서로 연합하면, 그것들은 키 배포 복잡성을 가중시키면서, 모든 키를 공유해야 한다.

키는 또한 KDC 또는 제휴 사이트 중의 하나에서 도난 당할 위험이 있고, 그것은 보안 프로토콜의 각 끝에서 키 타협(key compromise)의 위험을 제공한다. 예를 들어, 인증 서비스에 대한 사람의 침입은 각 제휴 서버에 대한 모든 키를 잠재적으로 훔칠 수 있다. 제휴 서버의 모든 네트워크 상에서 대한 모든 키를 갱신하기 위해 필요한 시간 때문에 이것은 실질적으로 인증 서비스를 폐쇄시킬 수 있다.

공개 키 기반 구조(public key infrastructure)(PKI)는 디지털 서명뿐만 아니라 암호화를 지원하기 위해 또한 사용될 수 있다. 공개 키 암호화는 듀얼 키(dual keys), 즉 하나의 공개 키 및 하나의 개인 키를 채용한다. 공개 키에 의해 암호화되는 데이터는 개인 키에 의해서만 해독될 수 있고, 반대의 경우도 마찬가지이다. PKI가 인증 및 디지털로 서명한 문서에 유용한 프로토콜을 제공함에도 불구하고, 확장 가능/이종 플랫폼 인증 시스템(scalable/cross-platform authentication system)에서는 잘 동작하지 않는다. 예를 들어, PKI 시스템은 일반적으로 훨씬 긴 키(일반적으로, 512비트 및 그 이상, 여기서 공유 키는 200비트 보다 작은 길이를 사용한다)를 요구하기 때문에 대용량 데이터를 처리할 때 매우 느리게 동작한다. 키가 길어질수록, 암호 및 해독하기 위해 더 많은 계산 능력이 요구된다.

또한, PKI는 키가 동기화 되는 것을 요구한다. PKI는 두 개의 키(공개 키 및 개인 키)를 가지고 있고 이 두개의 키는 동기화 되어 유지되어야 한다. 그러한 쌍(pair) 및 새로운 쌍을 생성하는 것을 무효로 하기 위한 잘 확립된 프로토콜/프로세스가 있다.

발명이 이루고자 하는 기술적 과제

이러한 이유로, 확장가능/이종 플랫폼 인증 시스템에서 특히 사용하기 위한 공유 대칭 키 프로토콜에서의 문제를 최소화하는 향상된 보안 프로토콜이 요구된다.

발명의 구성 및 작용

본 발명은 멀티-사이트 사용자 인증 시스템에서 향상된 보안을 제공함으로써 상기한 필요를 만족시키고 선행 기술의 하나 또는 다수의 결점을 극복한다. 유리하게는, 본 발명은 공개 키 기반 구조(PKI)의 특징과 보안을 접합함으로써 확장가능/이종 플랫폼 인증 시스템을 만드는 것의 복잡성을 감소시킨다. 이것은 공유 대칭 키 프로토콜의 고유한 문제를 최소화하고 이미 적당한 레가시 시스템(legacy system)/소프트웨어의 사용을 허가하는데, 이것은 상당한 비용 절감을 제공하고 산업에 의한 광범위한 채용을 촉진시킨다.

누군가가 인증 서비스의 개인 키를 절도할지라도, 본 발명에 따른 향상된 보 안 프로토콜은 인증 서비스가 잔여의 신뢰되는 제휴점을 중단시키지 않고 빨리 그것의 개인 키를 갱신할 수 있게 하다. 유사하게, 목적지 서비스(즉, 제휴 웹 서버)에서 개인 키가 도난 당하면, 목적지 서비스(destination service)는 인증 서비스가 새로운 키를 발행하기를 기다리기 보다, 그 자신의 개인 키 및 공개 키를 갱신하는 프로세스를 독립적으로 초기화할 수 있다.

본 발명은 또한 보안 위험을 격리시키기 위해 목적지 서비스가 다수의 개인/공개 키 쌍(예, 그것이 신뢰하는 인증 서비스 당 하나)을 갖는 것을 허용한다. 본 발명은 PKI 개념을 공유 키 인증 프로토콜에 적용하고, 인증 서비스에서 키 타협과 관련된 보안 위험이 제거되기 때문에, 프로토콜을 강하게 한다. 또한, 여기에서 설명되는 본 발명의 특징은 경제적으로 실현할 수 있고 상업적으로 실시될 수 있을 뿐만 아니라 현재 이용 가능한 기술보다 구현하기에 덜 귀찮고 더 쉽다.

간단하게 설명하면, 본 발명의 태양을 실시하는 방법은 데이터 통신 네트워크에 연결된 제1 및 제2 네트워크 서버를 포함하는 멀티-사이트 인증 시스템에서 정보 보안을 제공한다. 그 방법은 제1 네트워크 서버로부터 인증 티켓을 생성하고 티켓의 내용을 암호화하는 것을 포함한다. 그 티켓은 데이터 통신 네트워크에 또한 연결된 클라이언트 컴퓨터의 사용자와 관련된 정보를 포함한다. 제1 네트워크 서버는 제1 및 제2 네트워크 서버에 의해 공유되는 대칭 키를 사용해서 티켓 내용을 암호화한다. 그 방법은 제2 네트워크 서버와 관련된 공개 키를 사용해서 공유 키를 암호화하고 제1 네트워크 서버로부터 제2 네트워크 서버로의 티켓을 따라 클라이언트 컴퓨터를 지시하는 것을 더 포함한다.

본 발명의 또 다른 태양은 멀티-사이트 사용자 인증 시스템과 관련이 있는 인증 서버를 포함하는 시스템에 의해 실시된다. 인증 서버는 사용자를 인증하기 위해 클라이언트 컴퓨터의 사용자로부터 로그인 정보를 추출한다. 인증 서버는 사용자를 인증한 후에 인증 티켓을 또한 생성한다. 그 티켓은 클라이언트 컴퓨터의 사용자와 관련된 정보를 포함한다. 인증 서버는 티켓의 내용을 암호화하기 위해 제휴 서버와 공유되는 대칭 키를 사용한다. 제휴 서버는 인증 서버가 공유 키를 암호화하기 위해 사용하는 공개 키를 가지고 있다.

그러나 본 발명의 또 다른 실시예는 제1 네트워크 서버로부터 인증 티켓을 생성하고 제1 네트워크 서버와 관련이 있는 개인 키를 사용해서 티켓을 위한 서명을 생성하는 것을 포함하는 방법을 목적으로 한다. 티켓은 클라이언트 컴퓨터의 사용자와 관련된 정보를 가지고 있고 서명은 제2 네트워크 서버에 대한 주소 정보를 가지고 있다. 그 방법은 프라이버시-향상 프로토콜(privacy-enhanced protocol) 상에서 제1 네트워크 서버로부터 제2 네트워크 서버로의 티켓을 따라 클라이언트 컴퓨터를 지시하는 것과, 제2 네트워크 서버에 의해, 서명을 유효하게 하기 위해 서명 속의 그 자신의 주소 정보를 확인하는 것을 포함한다.

본 발명의 태양을 실시하는 보안 프로토콜은 공유 대칭 키, 공개 키, 및 개인 키를 포함한다. 제1 네트워크 서버 및 제2 네트워크 서버는 공유 키를 공유한다. 공유 키를 사용해서, 제1 네트워크 서버는 인증 티켓의 내용을 암호화한다. 제1 네트워크 서버는 공개 키를 사용해서 공유 키를 또한 암호화하고, 그것은 제2 네트워크 서버와 관련이 있다. 그것의 개인 키를 사용해서, 제2 네트워크 서버는 암호화된 공유 키를 해독하고 그리고 나서 해독된 공개 키를 사용해서 티켓의 내용을 해독한다.

다른 예로, 본 발명은 다양한 다른 방법 및 장치를 포함할 수 있다.

다른 특징은 이하에서 부분적으로 명확하고 부분적으로 지적될 것이다.

도면을 참조하면, 도 1은 본 발명이 이용되는 대표적인 네트워크 환경을 설명한다. 클라이언트 컴퓨터 시스템(12)은 데이터 통신 네트워크(14)에 연결되어 있다. 이 예에서, 네트워크(14)는 인터넷(또는 월드 와이드 웹)이다. 그러나, 본 발명의 교시는 임의의 데이터 통신 네트워크에 적용될 수 있다. 다수의 제휴 서버(16, 18, 및 20)는 또한 네트워크(14)에 연결되어 있다. 차례대로, 클라이언트 컴퓨터 시스템(12)은 네트워크(14)를 통해서 제휴 서버(16, 18, 및 20)에 접속할 수 있다. 제휴 서버(16, 18, 및 20)는 또한 '웹 서버' 및 '네트워크 서버'라 하기도 한다. 네트워크(14)에 연결된 인증 서버(24)는 그것 자신 및 클라이언트 컴퓨터 시스템(12) 및 웹 서버(16, 18, 및 20) 사이의 통신을 허용한다. '인증 서버'라는 하지만, 설명되는 실시예에서의 인증 서버(24)는 또한 웹 브라우저 및 다른 웹 서버와 상호작용 할 수 있는 웹 서버이다. 이 예에서, 인터넷 상에서 정보를 교환하기 위해 자주 사용되는 프로토콜, 하이퍼텍스트 전송 프로토콜(HTTP)을 사용해서 데이터는 인증 서버(24), 클라이언트 컴퓨터 시스템(12), 및 웹 서버(16, 18, 20) 사이에서 전달된다.

인증 데이터베이스(26)는 인증 서버(24)에 연결된다. 인증 데이터베이스(26)는 클라이언트 컴퓨터 시스템(12)의 사용자(또한 네트워크 상의 다른 사용자)를 인증하기 위해 필요한 정보를 포함하고 사용자가 제휴 서버에 접속할 때 사용자 프로파일 중 어떤 요소가 특정 제휴 서버에 제공되어야 하는지를 또한 확인한다. 인증 데이터베이스(26)가 인증 서버(24)와 떨어져서 도시되어 있지만, 본 발명의 다른 실시예에서, 인증 데이터베이스(26)는 인증 서버(24) 내에 포함될 수 있다는 것을 이해해야 한다. 연합 환경에서, 예를 들어, 다수의 인증 서버(24)는 인증 서비스를 제공하기 위해 이용될 수 있다(가상선으로 도시된 인증 서버(24)를 참조).

아래에서 설명되는 바와 같이, 인증 서버(24)는 제휴 서버(16, 18, 20) 중의 특정한 하나에 접속하려고 하는 클라이언트 컴퓨터(12)의 사용자를 인증한다. 인증 서버(24)는 먼저 사용자 로그인 ID와 패스워드와 같은, 사용자로부터 인증 정보를 요구한다. 만약 사용자가 성공적으로 인증되면, 인증 서버(24)는 사용자에게 원하는 서비스를 수행하기 위해 적당한 제휴 서버로 클라이언트 컴퓨터(12)의 루트를 정한다.

사용자 인증 프로세스의 일부로서, 인증 서버(24)는 사용자의 이-메일 주소, 사용자 선호, 및 클라이언트 컴퓨터(12) 상에 설치된 인터넷 브라우저의 종류와 같은, 특정 사용자 프로파일 정보를 제휴 서버에 제공할 수 있다. 이 사용자 프로파일 정보는 사용자의 로그인 ID와 연관이 있어서 사용자가 특정 제휴 서버에 접속할 때마다, 연관된 사용자 프로파일 정보가 제휴 서버에 이용 가능하다. 이 사용자 프로파일은 사용자가 한 번 정보를 입력하고 새로운 제휴 서버에 다음에 로그인하는 동안 그 정보를 이용하는 것을 허용한다.

일 실시예에서, '제휴 서버'는 '등록'했거나 또는 만약 그렇지 않으면 인증 서버(24)와 관계 또는 제휴를 확립한 웹 서버이다. 각 제휴 서버(16, 18, 및 20)는 사용자(그는 또한 인증 서버에 등록했다)가 제휴 서버에 접속을 요청할 때 제휴 서버가 인증 서버(24)와 통신하는 것을 허용하는 코드 시퀀스(도시되지 않음)를 포함한다. 인증 프로세스 및 클라이언트 컴퓨터(12), 제휴 서버(16, 18, 20), 및 인증 서버(24) 사이의 상호 작용을 주시하는 추가적인 세부 사항은 아래에서 제공된다.

본 발명은 도 1에 도시된 멀티-사이트 사용자 인증 시스템에 대해 향상된 보안을 제공한다. 유리하게는, 본 발명은 듀얼 키 암호화 시스템의 특징과 보안 프로토콜을 적응시킴으로써 확장가능/이종 플랫폼 인증 시스템을 구성하는 것의 복잡성을 감소시킨다. 이것은 공유 대칭 키 프로토콜에서의 근본적인 문제를 최소화시키고 이미 적당한 레가시 시스템/소프트웨어의 이용을 허용하고, 그것은 산업에 의한 광범위한 채용을 촉진한다.

아래에서 설명된 인증 프로세스를 실행하기 전에, 클라이언트 컴퓨터 시스템(12)의 사용자 및 제휴 서버(16, 18, 20)의 운영자는 인증서버(24)에 '등록'한다. 이 등록은 인증 서버에 필요한 정보를 제공하는 한 번의 프로세스이다. 예를 들어, 사용자 이름, 우편 주소, 및 이-메일 주소, 및/또는 사용자 또는 클라이언트 컴퓨터에 대한 다른 정보를 제공하는 것에 의해, 클라이언트 컴퓨터 시스템(12)의 사용자는 인증 서버(24)에 등록한다. 사용자 등록 과정의 일부로서, 사용자는 로그인 ID를 할당(또는 선택) 받으며, 그것은 임의의 제휴 서버(예, 서버(16, 18, 20))에 접속하기 위해 사용되는, 일반적인 로그인 ID이다. 로그인 ID는 또한 여기에서 '사용자명' 또는 '로그인 명'으로 언급된다. 추가적으로, 사용자는 인증 목적으로 사용되는 로그인 ID와 관련이 있는 패스워드를 선택한다. 인증 서버에 등록하고 로깅을 한 후에, 사용자는 임의의 추가적인 인증을 요구하는 것 없이 그리고 관련된 사용자 프로파일에 이미 포함된 사용자 정보를 입력하는 것 없이 임의의 제휴 서버(즉, 동일 인증 서버에 또한 등록된 제휴 서버)를 방문할 수 있다.

제휴 서버(16, 18, 20)의 운영자는 제휴 서버에 관한 정보를 제공함으로써(예, 서버 명 및 인터넷 주소) 인증 서버(24)에 등록한다. 추가적으로, 각 제휴 서버(16, 18, 20)는 그것의 인증 요건을 고려하는 정보를 제공한다. 인증을 위한 요건은 마지막 로그인 및 사용자에 의한 인증 정보의 입력 이후에 허용된 최대 시간에 대한 것으로 규정될 수 있다. 이 요건은 사용자에 의한 인증 정보의 마지막 '갱신' 이후 허용된 최대 시간에 의해 또한 규정될 수 있다.

인증 정보를 갱신하는 것은 적절한 사용자가 여전히 클라이언트 컴퓨터 시스템(12)을 동작하고 있다는 것을 확실히 하기 위해 사용자에게 패스워드를 다시 입력하게 하는 프로세스를 의미한다. 사용자가 인증 서버(24)를 로그 아웃하지 않고 자신의 컴퓨터 시스템을 떠남으로써, 또 다른 개인이 예전 사용자의 로그인 ID를 사용해서 제휴 서버(16, 18, 및 20)를 접속하는 것을 허용하면, 인증 정보의 이 주기적 갱신은 유용하다. 만약 사용자가 최대 허용 시간이 경과한 후에 제휴 서버(16, 18, 및 20) 중 하나에 접속을 요청하면, 인증 서버(24)는 사용자를 재인 증(즉, 갱신) 한다. 그러므로, 중앙 인증 서버(24)가 있음에도, 제휴 서버(16, 18, 20)는 그 자신의 인증 요건이 인증 서버에 의해 강제되도록 확립할 수 있다. 인증 서버(24)에 등록한 후에, 제휴 서버(16, 18, 20)는 인증 서버를 사용해서 인증 서버에 또한 등록한 임의의 사용자를 인증할 수 있다.

상기에서 설명된 바와 같이, 공유 대칭 키 보안 프로토콜(예, Kerberos)은 인증 서비스 및 목적지 서비스 사이의 인증을 수행하기 위해 사용될 수 있다. 이 예에서, 인증 서비스는 일반적으로 사용자명/패스워드(또는 패스워드와 동등한 것)를 받아들일 수 있다. 사용자명/패스워드의 확인 후에, 인증 서비스는 목적지 서비스에 대한 티켓을 준다. 단지 인증 서비스 및 목적지 서비스에 알려진, 공유 대칭 키는 티켓을 암호화했기 때문에, 티켓은 사용자의 신원의 목적지 서비스를 단독으로 보증한다. 이 프로토콜은 티켓이 신뢰되는 목적지 서비스에 의해 단지 사용 가능한 인증 서비스 및 티켓이 신뢰되는 출처(즉, 인증 서비스)로부터 온 목적지 서비스에 단독으로 보증을 제공한다. 또한, 그 프로토콜은 내용이 누구에게도 보이지 않는다고 인증 서비스 및 목적지 서비스 모두를 보증한다. 이 보증의 모두는 동일한 내용을 암호화하고 해독하는 유일한 방법은 공유 대칭 비밀 키에 대한 정보를 아는 것이라는 사실에 근거한다. 일반적으로, 각각의 목적지 서비스는 그 자신의 키를 가지고 있어서, 인증 서비스는 키의 모두를 알지만 각 목적지 서비스는 단지 자신의 키를 안다.

당해 기술 분야에서 능숙한 자는 공개 키 기반 구조(PKI)는 키가 동기화 되는 것을 요구하는 것을 이해한다. PKI는 두

개의 키(공개 키 및 개인 키)를 가지 고 있고 이 두 개의 키는 동기화 되어야 한다. 그러한 쌍 및 새로운 쌍을 생성하는 것을 무효화하는 잘 확립된 프로토콜/프로세스가 있다. 본 발명은 키 쌍 권한 및 키의 사용자에게 이 문제를 위임하고, 그러므로, 공유 키 인증 시스템으로부터 키 배포를 제거한다. 본 발명의 이 태양은 아래에서 더 상술된다.

다수의 암호화 알고리즘(예, 3DES 및 HMAC-RC4)은 키에 대한 지식 없이 암호화된 덩어리(blob)의 내용을 해독하는 것은 거의 불가능하다고 산업계에서 충분히 인정된다. 그러므로, 키를 보호하는 것은 보안 프로토콜의 매우 중요한 면이다. 상기에서 설명된 바와 같이, 선행 기술 공유 키 시스템에서는, 인증 서비스는 목적지 서비스에 안전하게 키를 전달해야 한다. 그 프로토콜은 또한 키를 정기적으로 갱신하는 조치를 취해야 하며, 키가 도난 당한 경우에도, 피해가 최소화될 것이다. 유감스럽게도, 이것은 과도하게 멀티-사이트 사용자 인증 시스템에서 보안을 복잡하게 한다. 또한, 목적지 서비스가 동일한 프로토콜을 통해서 하나의 인증 서비스 이상의 것을 신뢰하도록 선택하면, 그 후 공유 대칭 키는 모든 인증 서비스 사이에서 또한 공유되어야 한다. 이것은 공유 대칭 키의 배포 및 갱신에 심한 복잡성을 가중시킨다.

본 발명의 일 실시예에서, 랜덤하게 생성된, 단일-사용 세션 키가 공유 키를 대체한다. 인증 서버(24)는 목적지 서비스(즉, 제휴 서버(16, 18, 20) 중 하나)의 공개 키로 세션 키를 암호화한다. 인증 서버(24)는 또한 내용을 서명하기 위해 개인 키를 사용한다. 이러한 방법으로, 본 발명은 그것의 결점이 아니라 공유 대칭 키의 보안 특성을 유지한다. 본 발명의 세션 키 보안 프로토콜은 (a)인증 티켓은 특정 제휴 서버(16, 18, 또는 20)에서 단지 사용될 수 있다; (b)내용은 올바른 출처(즉 인증 서버(24))로부터 온다; (c)티켓의 내용은 출처 및 목적지(즉, 각각, 인증 서버 및 제휴 서버)에 의해 단지 알려진다; 및 (d)제휴 서버는 그것의 서명을 거절할 수 없다 는 것을 보증한다. 티켓이 단지 인증 정보만 포함하고 있고 개인 사용자 정보를 포함하고 있지 않다면 티켓의 내용은 출처 및 목적지에 제한될 필요는 없다. 이 예에서, 내용은 임의의 다른 장소에서 사용될 수 없고, 그러므로 보호될 필요가 없다. 당해 기술 분야에서 능숙한 자는 서명된 데이터 중에서, 잘 알려진, 미리 정의된 식별자(pre-defined identifier)인 서명 알고리즘을 포함하는 실시에 익숙하다. 본 발명의 일 실시예로, 이것은 포함될 것이고, 또한 일반적인 알고리즘은 인증 서버(24) 및 사이트(16) 모두에 의해 가정된다.

보안 소켓 층(secure socket layer)(SSL) 또는 그와 같은 것을 통해 인증 티켓을 전송하는 것은 출처 및 목적지 만이 인증 프로토콜에 복잡성을 더하지 않고 티켓의 내용을 안다는 것을 보증한다는 것을 이해해야 한다.

본 발명의 이 실시예의 세션 보안 프로토콜은 공개 키 암호화 시스템(예, 신뢰되는 상대방을 확인하기 위해 디지털 증명서를 사용하는 공개 키 기반 구조(PKI))의 개념을 공유 키 환경에 적용한다. 일반적으로, 공개 키 시스템은 하나의 키는 공개 키이고 또 다른 키는 개인 키인 쌍 키 또는 듀얼 키 암호화를 이용한다. 예를 들어, 공개 키는 메시지를 암호화하고 그 후 수신 측의 개인 키는 메시지를 해독한다. 공개 키에 의해 암호화된 데이터는 개인 키에 의해서만 해독될 수 있고, 그 반대의 경우도 마찬가지이다. 추가적으로, 주어진 쌍에서 공개 및 개 인 키는 서로 다른 값을 가져서 하나의 키에 대한 지식은 다른 키를 알려주지 않는다. 그러므로, 인증 서버(24)는 보안 위험을 생성하지 않고 제3 자에게 공개 키를 발행할 수 있다. PKI는 SSL과 같은 프로토콜로 증명서와 연결되어 자주 이용된다.

바람직하게는, 본 발명은 공유 대칭 키 프로토콜의 기본적인 특징을 유지한다. 즉, 본 발명은 티켓 내용 및 내용의 관련된 해석의 모두를 변경하지 않는다. 일반적으로, 인증 서버(24)가 티켓 내용을 암호화하려고 할 때, 그것인 랜덤 세션 키(공유 대칭 키로서 동일한 암호문 강도/길이의)를 생성할 것이다. 인증 서버(24)는 공유 대칭 키 시스템에 있는 것과 같이 동일한 암호화 알고리즘을 사용해서 티켓 내용을 암호화하기 위해 랜덤 키를 이용한다. 그리고 나서 인증 서버(24)는 목적지(즉, 제휴 서버(16, 18, 또는 20))의 공유 키로 랜덤 세션 키를 암호화한다.

또한, 인증 서버(24)는 그것의 개인 키를 사용해서 아래의 계산에 의한 서명을 생성한다: Encrypt(Digest(티켓 내용)).

도 2는 본 발명의 구현 및 클라이언트 컴퓨터 시스템의 사용자가 제휴 서버에 접속하려고 할 때 클라이언트 컴퓨터 시스템(12), 적어도 하나의 제휴 서버(16), 및 인증 서버(24) 사이의 상호작용을 설명하는 대표적인 흐름도이다. 간단하게, 원칙이 제휴 서버(18, 20), 및 본 발명의 멀티-사이트 사용자 인증 시스템을 사용하는 임의의 다른 제휴된 웹 서비스에 적용됨에도 불구하고 아래의 설명은 제휴 서버(16)를 목적으로 한다.

도 2에서 설명된 예는 클라이언트 컴퓨터 시스템(12)의 사용자가 제휴 서버(16)에 아직 로그온을 하지 않았고 아직 인증 서버(24)에 의해 인증 받지 않은 상황을 설명한다. 본 발명의 일 실시예에서, 다수의 인증 서버(24)는 연합된 환경을 제공한다. 'A'내지 'G'라고 붙여진 도 2의 선은 인증 프로세스 동안 정보 및 활동의 흐름을 나타낸다. 선상의 화살표는 프로세스 흐름의 방향을 가리킨다. 부호 'A'는 프로세스의 시작을 나타내고 부호 'G'는 프로세스의 끝을 나타낸다. 도 3은 도 2의 프로세스와 관련이 있는 대표적인 흐름도이다.

도 2 및 도 3의 대표적인 프로세스 흐름에서, 클라이언트 컴퓨터 시스템(12)의 사용자는 제휴 서버(16)를 통해서 이용 가능한 포털 서비스(예, http://www.msn.com에서 인터넷 서비스의 MSN?네트워크)에 접속하기 위해 32에서 시

작한다. 32에서, 사용자는 포털을 통해서 이용 가능한 서비스의 하나를 선택한다. 예를 들어, 사용자는 링크(예, http://eshop.msn.com)를 클릭함으로써 포털을 통해서 이용 가능한, 온라인 쇼핑 서비스, 또는 또 다른 웹 서비스에 접속한다. (A를 참조).

34 및 36에 나아가면서, 제휴 서버(16)는 먼저 사용자에게 사인-인 인터페이스(sign-in interface)(예, '로그인하기 위해 여기를 클릭 하시오')를 제공한다. 그리고 나서 사용자가 사인-인 인터페이스를 클릭할 때 제휴 서버(16)의 포털 서비스는 클라이언트 컴퓨터 시스템(12)을 인증 서버(24)(예, Microsoft?패스포트 사인-인 서비스)에 의해 제공되는 멀티-사이트 사용자 인증 시스템으로 리다이렉트한다(redirect). (B를 참조). 도 2 및 3의 예에서, 제휴 서버(16)는 클라이언트 컴퓨터 시스템(12)을 login.authsite.com으로 리다이렉트하고 클라이언트 컴퓨터 시 스템(12)은 36에서 포털에 의해 발행되는 리다이렉트 명령을 따른다.

40에서, 인증 서버(24)는 사용자가 이미 인증이 되었는지 가리키는 *.authsite.com 도메인 하에서 인증 쿠키(cookie)가 있는지를 결정한다. 없다면, 인증 서버(24)의 login.authsite.com에서의 사용자 인터페이스 모듈은 사용자명/패스워드를 받는 사용자 인터페이스 페이지와 48에서 반응한다. (C를 참조). 사용자는 그의 사용자명/패스워드를 50에서 입력하고 그 정보를 login.authsite.com에서 인증 서버(24)에 알려준다. (D를 참조). 그리고 나서 인증 서버(24)는 52에서 사용자에 의해 제공되는 사용자명/패스워드를 확인한다. (E를 참조).

52에서 일어나는 확인이 성공적이면, 인증 서버(24)는 원하는 웹 서비스 위치를 검색하고 클라이언트 컴퓨터 시스템(12)을 암호화된 티켓/프로파일 정보로 적당한 서비스(예, http://eshop.msn.com/)로 리다이렉트한다. (F를 참조). 바꾸어 말하면, 인증 서버(24)는 인증 데이터베이스(26)로부터 적당한 위치 정보를 추출해서 선택된 서비스를 제공하는 서버(16 또는 18 또는 20)의 위치를 확인하다. 본 발명의 일 실시예로, 보안 프로토콜은 티켓의 메시지 내용(예, 사용자명 및 패스워드)을 암호화하기 위해 일반적 세션 키를 채용한다. 차례대로, 인증 서버(24)는 제휴 서버(16)의 공개 키를 사용해서 세션 키를 암호화하고 그 후 그 자신의 개인 키를 사용해서 티켓을 사인한다.

그리고 나서 클라이언트 컴퓨터(12)는 제휴 서버(16)(예, http://eshop.msn.com)에서 웹 서비스로 60에서 리다이렉트를 따르고 인증된다. (G를 참조). 이 예에서, 제휴 서버(16)는 그것의 공개 키 및 서명을 근거로 티켓 의 내용을 검증한다. 그리고 나서 제휴 서버(16)는 그것의 개인 키를 사용해서 세션 키를 해독하고, 차례로, 세션 키를 사용해서 인증 티켓의 메시지 내용을 해독한다. 선택적으로, 인증 서버(24)가 특정 웹 서비스의 공개 키를 가지고 있지 않다면 보안 소켓 층의 이용을 확실히 하기 위해 http://eshop.msn.com에 리다이렉트를 따른다.

52로 돌아가면, 사용자가 입력한 정보가 정확하지 않으면(즉, 그것이 인증 데이터베이스(26)에 저장되어 있는 정보와 일치하지 않는다면), 인증 서버(24)는 사용자에게 로그인 ID와 패스워드 조합이 정확하지 않다는 것을 가리키는 웹 페이지를 생성하고 전달한다. 사용자명 및/또는 패스워드 실패의 경우에, 예를 들어, 보안 관심은 사용자가 로그인을 시도할 수 있는 횟수에 제한을 둘 수 있다.

이 실시예에서, 인증 서버(24)는 램덤 키에 의해 암호화되지 않은 티켓의 부분으로 둘 다 암호화된 랜덤 키 및 서명을 추가한다. 인증 서버(24)는 목적지 서비스(즉, 제휴 서버(16, 18, 20) 중의 하나)의 공개 키로 세션 키를 암호화한다. 인증 서버(24)는 또한 내용을 서명하기 위해 개인 키를 사용한다. 이러한 방법으로, 본 발명은 그것의 결점이 아니라 공유 대칭 키의 보안 특성을 유지한다. 본 발명의 세션 키 보안 프로토콜은 인증 서버(24)에게 단지 특정 제휴 서버(16)가 인증 티켓을 사용할 수 있다는 것을 보증한다. 비슷하게, 본 발명은 목적지 서비스(즉, 제휴 서버(16))에게 티켓이 올바른 출처(즉, 인증 서버(24))로부터 왔다는 것을 보증한다. 이것은 인증 서비스의 공개 키로 서명을 유효하게 함으로써 이루어진다. 추가적으로, 단지 출처 및 목적지(즉, 각각, 인증 서버 및 제휴 서버)은 티 켓의 내용을 안다.

예를 들어, 티켓은 $t = Encrypt_{sessionkey}$ (사용자명 + ...)$PKIEncrypt_{PP3}$ (세션 키)$PKISignature_{PVP}$ (전체 내용)의 형태를 취하고 아래 문자 PP3는 제3 자 공개 키를 나타내고 아래 문자 PVP는 인증 서버(24)의 공개 키를 나타낸다.

티켓이 단지 인증 정보를 포함하고 개인 사용자 정보를 포함하지 않는다면 티켓의 내용에 대한 지식은 출처 및 목적지에 제한될 필요는 없다. 예를 들어, 내용은 임의의 다른 위치에서 사용될 수 없고 제3자 공격자에게 가치가 거의 없거나 하나도 없다. 세션 키 보안 프로토콜의 일 실시예로, 티켓 내용의 지식을 인증 서버(24) 및 제휴 서버(16)에 한정하기 위한 필요는 목적지의 공개 키의 지식을 요구하지 않는 것에 의해 완화될 수 있다. 보안 티켓은 간단히 암호화되지 않는다. 티켓이 다른 목적지에 의해 사용되지 않는 것을 보증하기 위해, 티켓은 서명의 일부로 목적지의 주소(예, 도메인 명)를 포함한다. 그러므로, 목적지 서비스는 그것을 사용하기 전에 그 자신의 도메인 명으로 서명을 확인할 수 있다.

예를 들어, 티켓은 $t = \{ PUID + sign\ in\ time + ... + siteID_{3} (siteDomain_{3}) \}$ 서명의 형태를 취하고 여기서 PUID는 인증 서버(24)에 의해 성립되는 유일한 동일 증명이고 아래 문자 3은 제3자를 나타낸다.

SSL/TLS와 같은 함부로 변경하지 못하고, 프라이버시 향상된 프로토콜 상으로 암호화되지 않은 인증 티켓을 전송하는 것은 단지 출처 및 목적지만이 티켓의 내용을 안다는 것을 보증한다는 것을 이해해야 한다. 인증 서버(24)는 제휴 서버(16)의 공개 키를 알 필요가 없기 때문에 본 발명의 이 실시예는 키 제공 시스템을 또한 간단하게 한다.

도 3의 흐름도는 Microsoft?패스포트 사인-인 서비스와 같은 인증 서비스에 대한 세션 키 보안 프로토콜의 태양을 설명한다. 이 태양은 Kerberos 프로토콜에 또한 적용 가능하다는 것이 이해되어야 한다. 부록 A는 분산된, 멀티-사이트 사용자 인증 시스템(예, Microsoft?패스포트 사인-인 서비스)에 의해 이용되는 '패스포트' 프로토콜에 적용되고 Kerberos 프로토콜에 적용되는 세션 키 보안 프로토콜의 특정 예를 제공한다.

도 4는 컴퓨터(70)의 형태로 범용 컴퓨팅 장치(general purpose computing device)의 하나의 예이다. 본 발명의 일 실시예로, 컴퓨터(70)와 같은 컴퓨터는 클라이언트 컴퓨터 시스템(12), 인증 서버(24), 사용자 인터페이스 서버(28), 또는 제휴 서버(16, 18, 및 20) 중 임의 것에서의 사용에 적당하다.

설명된 실시예에서, 컴퓨터(70)는 하나 또는 다수의 프로세서 또는 처리 장치(72) 및 시스템 메모리(74)를 구비한다. 설명된 실시예에서, 시스템 버스(76)는 시스템 메모리(74)를 포함하는 다양한 시스템 구성 요소를 프로세서(72)에 연결한다. 버스(76)는 메모리 버스 또는 메모리 제어기, 주변 장치 버스, 가속된 그래픽 포트, 및 프로세서 또는 다양한 버스 구조 중 임의의 것을 사용하는 로컬 버스를 포함하면서, 다양한 형태의 버스 구조의 임의의 것 중 하나 또는 다수를 나타낸다. 제한하지 않는 예로서, 그러한 구조는 업계 표준 구조(ISA) 버스, 마이크로 채널 구조(MCA) 버스, 향상된 ISA(EISA) 버스, 비디오 전자 공학 표준 협회(VESA) 로컬 버스, Mezzanine라고 또한 알려진 주변 장치 구성 요소 상호 연결(PCI) 버스를 포함한다.

컴퓨터(70)는 일반적으로 컴퓨터 판독 가능 매체의 적어도 약간의 형태를 포함한다. 휘발성 및 비휘발성 매체, 분리성 및 비분리성 매체를 포함하는 컴퓨터 판독 가능 매체는 컴퓨터(70)에 의해 접근될 수 있는 임의의 가용 매체일 수 있다. 제한하지 않는 예로, 컴퓨터 판독 가능 매체는 컴퓨터 저장 매체 및 통신 매체를 포함한다. 컴퓨터 저장 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 다른 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리성 및 비분리성 매체를 포함한다. 예를 들어, 컴퓨터 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 다른 메모리 기술, CD-ROM, 디지털 비디오 디스크(DVD) 또는 다른 광 디스크 저장, 자기 카세트, 자기 테이프, 자기 디스크 저장 또는 다른 자기 저장 장치, 또는 컴퓨터(70)에 의해 접근될 수 있는 원하는 정보를 저장하기 위해 사용될 수 있는 임의의 다른 매체를 포함한다. 통신 매체는 일반적으로 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파(carrier wave) 또는 다른 전송 메커니즘과 같은 변조된 데이터 신호로 된 다른 데이터를 포함하고 임의의 정보 전달 매체를 포함한다. 당해 기술 분야에서 능숙한 자는 변조된 데이터 신호에 익숙하며, 그것은 그러한 방법으로 설정되거나 변경된 그것의 특징을 하나 또는 다수 가지고 있어서 신호 내의 정보를 암호화한다. 유선 네트워크(wired network) 또는 직접 유선 연결(direct-wired connection)과 같은 유선 매체, 및 음향, RF, 적외선, 및 다른 무선 매체와 같은 무선 매체는 통신 매체의 예이다. 상기의 임의의 조합은 또한 컴퓨터 판독 가능 매체의 범위 내에서 포함된다.

시스템 메모리(74)는 분리성 및/또는 비분리성, 휘발성 및/또는 비휘발성 메모리의 형태로 컴퓨터 저장 매체를 포함한다. 설명된 실시예에서, 시스템 메모리(74)는 ROM(read only memory)(78) 및 RAM(random access memory)(80)을 포함한다. 기동시 동안과 같이 컴퓨터(70) 내의 요소 사이에서 정보 전달을 돕는 기본적인 루틴를 포함하는, 기본 입력/출력 시스템(82)(BIOS)은, 일반적으로 ROM(78)에 저장된다. RAM(80)은 일반적으로 처리 장치(72)에 의해 현재 수행되고 있고 그리고/또는 즉시 접근 가능한 데이터 프로그램 모듈 및/또는 데이터를 포함한다. 제한하지 않는 예로, 도 4는 운영 체제(84), 애플리케이션 프로그램(86), 다른 프로그램 모듈(88), 및 프로그램 데이터(90)를 설명한다.

컴퓨터(70)는 또한 다른 분리성/비분리성, 휘발성/비휘발성 컴퓨터 저장 매체를 포함한다. 예를 들어, 도 4는 비분리성, 비휘발성 자기 매체로부터 읽거나 쓰는 하드디스크 드라이브(94)를 설명한다. 도 4는 또한 분리성, 비휘발성 자기 디스크(98)로부터 읽거나 쓰는 자기 디스크 드라이브(96), 및 CD-ROM 또는 다른 광 매체와 같은 분리성, 비휘발성 광 디스크(102)로부터 읽거나 쓰는 광 디스크 드라이브(102)를 도시한다. 대표적인 운영 환경에서 이용될 수 있는 다른 분리성/비분리성, 휘발성/비휘발성 컴퓨터 저장 매체는, 자기 테이프 카세트, 플래시 메모리 카드, 디지털 비디오 디스크(digital versatile disks), 디지털 비디오 테이프, 고체 RAM(solid state RAM), 고체 ROM(solid state ROM), 및 그와 같은 것을 포함하 지만, 그것에 한정되지는 않는다. 하드디스크 드라이브(84), 및 자기 디스크 드라이브(96) 및 광 디스크 드라이브(100)는 일반적으로 인터페이스(106)와 같은 비휘발성 메모리 인터페이스에 의해 시스템 버스(76)에 연결된다.

상기에서 논의되고 도 4에서 설명된 드라이브 또는 다른 대용량 저장 장치 및 그것의 연관된 컴퓨터 저장 매체는, 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 및 컴퓨터(70)를 위한 다른 데이터의 저장을 제공한다. 도 4에서, 예를 들어, 하드디스크 드라이브(94)는 운영 체제(110), 애플리케이션 프로그램(112), 다른 프로그램 모듈(114), 및 프로그램 데이터(116)을 저장하는 것으로 설명된다. 이 구성 요소는 운영 체제(84), 애플리케이션 프로그램(86), 다른 프로그램 모듈(88), 및 프로그램 데이터(90)와 동일하거나 다를 수 있다는 점을 주목해야 한다. 운영 체제(110), 애플

리케이션 프로그램(112), 다른 프로그램 모듈(114), 및 프로그램 데이터(116)는 최소한 그들이 다른 사본이라는 것을 설명하기 위해 여기서 다른 숫자로 주어져 있다.

사용자는 키보드(120) 및 다른 포인팅 장치(122)(예, 마우스, 트랙볼, 펜, 또는 터치패드)와 같은 입력 장치를 통해서 컴퓨터(70)에 명령 및 정보를 입력할 수 있다. 다른 입력 장치(도시되지 않음)는 마이크로폰, 조이스틱, 게임 패드, 위성 접시, 스캐너, 또는 그와 같은 것을 포함할 수 있다. 이것 및 다른 입력 장치는 시스템 버스(76)에 연결된 사용자 입력 인터페이스(124)를 통해서 처리 장치(72)에 연결되지만, 병렬 포트, 게임 포트, 또는 범용 시리얼 버스(USB)와 같은, 버스 구조 및 다른 인터페이스에 의해 연결될 수 있다. 모니터(128) 또는 다 른 종류의 디스플레이 장치는 비디오 인터페이스(130)와 같은 인터페이스를 통해서 시스템 버스(76)에 또한 연결된다. 모니터(128)에 추가해서, 컴퓨터는 자주 프린터 및 스피커와 같은 다른 주변 출력 장치(도시되지 않음)를 포함하고, 그것은 출력 주변 장치 인터페이스(도시되지 않음)를 통해서 연결될 수 있다.

컴퓨터(70)는 원격 컴퓨터(134)와 같은 하나 또는 다수의 원격 컴퓨터에 논리적 연결을 가지는 네트워크 환경에서 동작할 수 있다. 원격 컴퓨터(134)는 퍼스널 컴퓨터, 서버, 라우터, 네트워크 PC, 피어 장치(peer device) 또는 다른 일반적인 네트워크 노드를 포함할 수 있고, 일반적으로 컴퓨터(70)에 관하여 상기에서 설명된 요소의 다수 또는 전부를 포함한다. 도 4에서 도시된 논리적 회로는 근거리 통신망(LAN)(136) 및 원거리 통신망(WAN)(138)을 포함하지만, 또는 다른 네트워크를 포함하지 않을 수 있다. 그러한 네트워킹 환경은 사무실, 기업 범위 컴퓨터 네트워크(enterprise-wide computer networks), 인트라넷, 및 세계 컴퓨터 네트워크(global computer network)(예, 인터넷)에서 흔하다.

근거리 네트워킹 환경에서 사용될 때, 컴퓨터(70)는 네트워크 인터페이스 또는 어댑터(140)를 통해서 LAN(136)에 연결된다. 원거리 네트워킹 환경에서 사용될 때, 컴퓨터(70)는 인터넷과 같은 WAN(138) 상에서 통신을 성립하기 위한 다른 수단 또는 모뎀(142)을 일반적으로 포함한다. 내부 또는 외부일 수 있는 모뎀(142)은 사용자 입력 인터페이스(134), 또는 다른 적당한 메커니즘을 통해서 시스템 버스(76)에 연결된다. 네트워크 환경에서, 컴퓨터(70)에 대해 설명된 프로그램 모듈, 또는 그것의 일부는 원격 메모리 저장 장치(도시되지 않음)에 저장될 수 있다. 제한하지 않는 예로, 도 4는 메모지 장치 상에 거주하는 것으로 원격 애플리케이션 프로그램(144)을 설명한다. 도시된 네트워크 연결은 대표적이고 컴퓨터 사이의 통신 링크를 성립하는 다른 수단이 사용될 수 있다는 것이 인정될 것이다.

일반적으로, 컴퓨터(70)의 데이터 프로세서는 컴퓨터의 다양한 컴퓨터 판독 가능 저장 매체에서 다른 시기에 저장된 명령어에 의해 프로그램 된다. 프로그램 및 운영 체제는 예를 들어, 플로피 디스크 또는 CD-ROM으로 일반적으로 배포된다. 그것으로부터, 그것은 컴퓨터의 부차적 기억 장치(secondary memory)에 인스톨되거나 로드된다. 그러한 매체가 마이크로 프로세서 또는 다른 데이터 프로세서와 함께 아래에서 설명되는 단계를 구현하기 위한 프로그램 또는 명령어를 포함할 때 여기에서 설명된 발명은 이것 및 다양한 컴퓨터 판독 가능 저장 매체를 포함한다. 아래에서 설명되는 기술 또는 방법에 따라 프로그램 될 때 발명은 컴퓨터 그 자체를 또한 포함한다.

설명의 목적으로, 프로그램 및 운영 체제와 같은 다른 실행 가능한 프로그램 구성 요소는, 분리된 블록으로 여기서 설명된다. 그러나, 그러한 프로그램 및 구성 요소는 컴퓨터의 다른 저장 구성 요소에서 다양한 시기에 상주하고, 컴퓨터의 데이터 프로세서(들)에 의해 실행된다는 것을 인식해야 한다.

컴퓨터(70)를 포함해서, 대표적인 컴퓨팅 시스템 환경과 연결되어 설명했지만, 본 발명은 다수의 다른 범용 또는 특별한 목적의 컴퓨팅 시스템 환경 또는 구성과 함께 동작할 수 있다. 컴퓨팅 시스템 환경은 본 발명의 기능성 및 이용의 범위에 어떠한 제한을 가하기 위한 목적은 아니다. 또한, 컴퓨팅 시스템 환경은 대 표적인 운영 환경에서 설명된 구성 요소의 임의의 하나 또는 조합과 관련하여 임의의 요건 또는 의존을 가진 것으로 해석되어서는 안 된다. 본 발명과 함께 이용하기에 적합할 수 있는 구성, 환경 , 및/또는 잘 알려진 컴퓨팅 시스템의 예는, 퍼스널 컴퓨터, 서버 컴퓨터, 핸드헬드(hand-held) 또는 휴대용 컴퓨터, 멀티프로세서 시스템, 마이크로프로세서 기반 시스템, 셋 톱 박스(set top boxes), 프로그래머블 가전 제품(programmable consumer electronics), 네트워크 PC, 미니컴퓨터, 메인프레임 컴퓨터, 상기 시스템 및 장치의 임의의 것을 포함하는 분산 컴퓨팅 환경, 및 그와 같은 것을 포함하지만, 그것에 한정되지는 않는다.

본 발명은 하나 또는 다수의 컴퓨터 또는 다른 장치에 의해 실행되는, 프로그램 모듈과 같은 컴퓨터 실행 가능 명령어의 일반적인 문맥으로 설명될 것이다. 일반적으로, 프로그램 모듈은 특정 작업을 수행하거나 특정 추상 데이터 형식을 구현하는 데이터 구조, 컴포넌트, 객체, 프로그램, 및 루틴을 포함하지만, 그것에 한정되지는 않는다. 본 발명은 작업이 통신 네트워크를 통해 연결된 원격 처리 장치에 의해 수행되는 분산 컴퓨팅 환경에서 또한 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 메모리 저장 장치를 포함하는 원격 및 근거리 컴퓨터 저장 매체에 위치할 수 있다.

본 발명은 듀얼 키 시스템에 기반한 세션 키 보안 프로토콜과 함께 공유 대칭 키 프로토콜에 고유한 문제를 본래 제거한다. 이롭게, 세션 키 프로토콜은 이미 적당한 매우 많은 양의 레가시 시스템/소프트웨어와 함께 경제적 이용을 허용한다. 또한, 프로토콜은 산업에 의해 널리 퍼진 채택을 촉진하는 원리를 이용한다.

또한, 본 발명은 프로토콜의 어느 쪽 끝에 타협되어 있는 키의 위험이 제거되는 강력한 프로토콜을 제공한다. 예를 들어, 인증 서비스에 대한 사람의 침입은 잠재적으로 각 제휴 서버에 대한 키의 모두를 훔칠 수 있다. 제휴된 서버의 모든 네트워크를 통해 키의 모두를 갱신하는데 필요한 시간 때문에 이것은 인증 서버를 실질적으로 폐쇄시킬 수 있다. 반대로, 본 발명의 보안 프로토콜은 인증 서비스가 신뢰되는 상대방의 다른 것을 두절시키지 않고 그것의 도난 당한 개인 키를 빨리 대체하게 한다. 유사하게, 목적지 서비스에서 개인 키가 도난 당하면, 목적지 서비스는, 인증 서비스가 새로운 키를 발행하는 것을 기다리기 보다, 그 자신의 개인 키 및 공개 키를 갱신하는 프로세스를 독립적으로 초기화한다. 또한, 본 발명은 목적지 서비스가 보안 위험을 분리시키기 위해 다수의 개인/공개 키 쌍(예, 그것이 신뢰하는 인증 서비스 당 하나)을 갖는 것을 허용한다. 본 발명의 요소 또는 그것의 실시예를 소개할 때, 관사 '하나(a, an)', '그(the)', 및 '상기(said)'는 요소가 하나 또는 다수 있다는 것을 나타내기 위한 의도이다. 문구 '포함하는(comprising, including, 및 having)'은 열거된 요소 외에 추가적인 요소가 있을 수 있다는 것을 의미하고 포함하기 위한 의도이다.

상기에서 본 바와 같이, 본 발명의 다양한 목적은 이루어지고 다른 이로운 결과가 얻어짐을 알 수 있을 것이다.

본 발명의 범위를 벗어나지 않고 다양한 변경이 상기 구성 및 방법에 만들어질 수 있기 때문에, 상기 설명에 포함되고 첨부된 도면에 도시된 모든 내용은 예시적이고 제한하는 의미가 아니라는 것을 의도한다.

발명의 효과

본 발명은 멀티-사이트 사용자 인증 시스템에서 향상된 보안을 제공함으로써 상기한 필요를 만족시키고 선행 기술의 하나 또는 다수의 결점을 극복한다. 이롭게, 본 발명은 공개 키 기반 구조(PKI)의 특징과 보안을 접합함으로써 확장가능/이종 플랫폼 인증 시스템을 만드는 것의 복잡성을 감소시킨다. 이것은 공유 대칭 키 프로토콜의 고유한 문제를 최소화하고 이미 적당한 레가시 시스템(legacy system)/소프트웨어의 사용을 허가하는데, 이것은 상당한 비용 절감을 제공하고 산업에 의한 광범위한 채용을 촉진시킨다.

누군가가 인증 서비스의 개인 키를 절도할지라도, 본 발명에 따른 향상된 보안 프로토콜은 인증 서비스가 잔여의 신뢰되는 제휴점을 중단시키지 않고 빨리 그것의 개인 키를 갱신할 수 있게 하다. 유사하게, 목적지 서비스(즉, 제휴 웹 서버)에서 개인 키가 도난 당하면, 목적지 서비스(destination service)는 인증 서비스가 새로운 키를 발행하기를 기다리기 보다, 그 자신의 개인 키 및 공개 키를 갱신하는 프로세스를 독립적으로 초기화할 수 있다.

본 발명은 또한 보안 위험을 격리시키기 위해 목적지 서비스가 다수의 개인/공개 키 쌍(예, 그것이 신뢰하는 인증 서비스 당 하나)을 갖는 것을 허용한다. 본 발명은 PKI 개념을 공유 키 인증 프로토콜에 적용하고, 인증 서비스에서 키 타협과 관련된 보안 위험이 제거되기 때문에, 프로토콜을 강하게 한다. 또한, 여기에서 설명되는 본 발명의 특징은 경제적으로 실현할 수 있고 상업적으로 실시될 수 있을 뿐만 아니라 현재 이용 가능한 기술보다 구현하기에 덜 귀찮고 더 쉽다.

[부록 A]

예1

분산된, 멀티-사이트 사용자 인증 시스템(예, Microsoft?패스포트 사인-인 서비스)에 의해 이용되는 '패스포트' 프로토콜에 적용되는 세션 키 보안 프로토콜의 예.

패스포트 티켓의 구조:

Ticket = {

memberidLow integer

memberidHigh integer

lastRefresh integer

lastLogin integer

currentTime integer

}

내용 모두는 공유 키를 통해서 패스포트 2.1에 암호화된다.

(1)목적지 공개 키의 지식 없이, 사이트 정보 및 서명은 티켓의 일부로서 추가될 수 있다:

Ticket = {

memberidLow integer

memberidHigh integer

lastRefresh integer

lastLogin integer

currentTime integer

siteID integer

siteDomain(optional)

signature

}

서명은 아래와 같은 패스포트 개인 키에 기초한다:

Encrypt (Digest(서명 자체를 제외한 티켓 내용))

티켓 내용이 제3자에 의해 보여지지 않는다는 것을 보증하기 위해, 이 티켓 내용은 단지 SSL/TLS 네트워크 프로토콜을 통해서 전달될 것이다. 인증 서비스가 memberid가 보호하기에 중요하지 않다고 결정하면, SSL/TLS는 요구되지 않는다.

최근의 웹 표준에 따르기 위해, 이 실시예에서의 패스포트 구현은 티켓 구조를 xml 문서 형식으로 변환한다.

(2)목적지 공개 키의 지식으로, 티켓은 아래와 같이 암호화될 수 있다:

Ticket = {

EncryptedContent{

memberidLow integer

memberidHigh integer

lastRefresh integer

lastLogin integer

currentTime integer

}

EncryptedSessionKey

Signature

}

EncryptedSessionKey = 목적지 공개 키로 Encrypt(랜덤 세션 키)

Signature = 패스포트 개인 키로 Encrypt(Digest(서명을 제외한 티켓)

EncryptedContent는 세션 키를 통한다.

예2

Kerberos 프로토콜에 적용되는 세션 키 보안 프로토콜의 예

Kerberos 서비스 티켓 구조:

Ticket ::= [APPLICATION 1] SEQUENCE{

tkt-vno[0] INTEGER

realm[1] Realm,

sname[2] PrincipalName,

enc-part[3] EncryptedData, -- EncTicketPart

extensions[4] TicketExtensions OPTIONAL

}

현재, EncryptedData는 공유 키를 사용해서 암호화된다. 일 실시예에서, 티켓 확장(ticket extension)은 ticketkey를 보유하기 위해 추가되고, ticketkey는 EncryptedData를 암화화하기 위해 이용된다. PKI-Ticket-Extension은 목적지(sname)의 공개 키에 의해 암호화된 ticketkey를 포함한다. 티켓이 신뢰되는 KDC로부터 온다는 것을 입증하기 위해, PKI-Ticket-Extension은 또한 KDC에 의한 EncryptedData의 서명을 포함한다.

PKI-Ticket-Extension: {

te-type[0] INTEGER

te-TicketKey[1]

te-Signature[2]

}

te-Ticket = 목적지의 공개 키로 Encrypt (TicketKey)

te-Signature = kdc의 개인 키로 Encrypt (Digest (EncryptedData))

(57) 청구의 범위

청구항 1.

멀티-사이트 인증 시스템에서 정보 보안을 위한 방법에 있어서,

제1 네트워크 서버로부터 인증 티켓을 생성하는 단계 - 상기 티켓은 클라이언트 컴퓨터의 사용자와 관련이 있는 정보를 포함, 상기 제1 네트워크 서버 및 상기 클라이언트 컴퓨터는 데이터 통신 네트워크에 연결되어 있음 - ;

공유 대칭 키를 사용해서, 제1 네트워크 서버에 의해, 상기 티켓의 내용을 암호화하는 단계 - 상기 공유 키는 제1 네트워크 서버 및 제2 네트워크 서버에 의해 공유됨, 상기 제2 네트워크 서버는 데이터 통신 네트워크에 또한 연결되어 있음 - ;

제2 네트워크 서버와 관련이 있는 공개 키를 사용해서, 제1 네트워크 서버에 의해, 공유 키를 암호화하는 단계; 및

제1 네트워크 서버로부터 제2 네트워크 서버로의 티켓을 따라 클라이언트 컴퓨터를 지시하는 단계

를 포함하는 정보 보안을 위한 방법.

청구항 2.
제1항에 있어서,

제2 네트워크 서버와 관련된 개인 키를 사용해서, 제2 네트워크 서버에 의해, 암호화된 공유 키를 해독하는 단계; 및

해독된 공유 키를 사용해서, 제2 네트워크 서버에 의해, 티켓의 내용을 해독 하는 단계

를 더 포함하는 정보 보안을 위한 방법.

청구항 3.
제1항에 있어서, 제1 네트워크 서버와 관련된 개인 키를 사용해서 티켓을 위한 서명을 생성하는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 4.
제3항에 있어서, 티켓은 공유 키에 의해 암호화된 내용, 공유 키, 및 서명을 포함하는 정보 보안을 위한 방법.

청구항 5.
제3항에 있어서, 서명은 제2 네트워크 서버를 위한 주소 정보를 포함하고 있고, 제2 네트워크 서버에 의해, 서명을 유효하게 하기 위해 서명내의 그 자신의 주소 정보를 확인하는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 6.
제1항에 있어서, 상기 공유 키는 램덤하게 생성된, 단일-사용 세션 키를 포함하는 정보 보안을 위한 방법.

청구항 7.
제1항에 있어서, 프라이버시 향상된(privacy-enhanced) 프로토콜을 통해 제1 네트워크 서버로부터 제2 네트워크 서버로의 티켓을 전달하는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 8.
제1항에 있어서, 제1 네트워크 서버는 멀티-사이트 사용자 인증 시스템과 관련이 있는 인증 서버이고 티켓을 생성하기 전에 사용자를 인증하기 위해 사용자로부터 로그인 정보를 추출하는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 9.
제8항에 있어서, 티켓의 내용이 추출된 로그인 정보를 포함하고 있는 정보 보안을 위한 방법.

청구항 10.
제8항에 있어서, 추출된 로그인 정보가 로그인 ID 및 로그인 ID와 관련된 패스워드를 포함하고 있는 정보 보안을 위한 방법.

청구항 11.
제8항에 있어서, 사용자를 인증하기 전에, 사용자가 이미 인증되었는지를 결정하고, 사용자가 이미 인증되지 않았으면, 사용자로부터 로그인 정보를 추출하고 로그인 정보를 인증 서버와 연결된 데이터베이스에 저장된 인증 정보와 비교하여 사용자를 인증 서버로 인증하는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 12.
제1항에 있어서, 클라이언트 컴퓨터의 브라우저를 통해서 사용자로부터, 제2 네트워크 서버로부터 제공될 선택된 서비스를 위한, 요구를 받아들이는 단계를 더 포함하는 정보 보안을 위한 방법.

청구항 13.
제1항에 있어서, 제2 네트워크 서버는 데이터 통신 네트워크에 연결된 하나 또는 다수의 다른 네트워크 서버에 의해 제공되는 서비스에 대한 출입구를 사용자에게 제공하기 위한 포털인 정보 보안을 위한 방법.

청구항 14.
제1항에 있어서, 네트워크 서버는 웹 서버이고 데이터 통신 네트워크는 인터넷인 정보 보안을 위한 방법.

청구항 15.
제1항의 방법을 수행하기 위한 컴퓨터 실행 가능 명령어를 갖는 컴퓨터 판독 가능 매체.

청구항 16.
멀티-사이트 사용자 인증 시스템과 관련된 인증 서버를 포함해서 정보를 보안하는 시스템으로서, 상기 인증 서버는 사용자를 인증하기 위해 클라이언트 컴퓨터의 사용자로부터 로그인 정보를 추출하고, 상기 인증 서버는 사용자를 인증한 후에 인증 티켓을 더 생성하고, 상기 티켓은 클라이언트 컴퓨터의 사용자와 관련된 정보를 포함하고, 상기 인증 서버는 티켓의 내용을 암호화하기 위한 공유 대칭 키를 가지고, 상기 공유 키는 인증 서버와 제휴 서버에 의해 공유되고, 상기 제휴 서버는 공개 키를 가지고 있고 상기 인증 서버는 공개 키를 사용해서 공유 키를 암호화하는 정보 보안을 위한 시스템.

청구항 17.
제16항에 있어서, 제휴 서버는 암호화된 공유 키를 해독하기 위한 개인 키를 가지고 있고, 상기 제휴 서버는 해독된 공유 키를 사용해서 티켓의 내용을 해독하 는 정보 보안을 위한 시스템.

청구항 18.
제16항에 있어서, 인증 서버는 티켓을 위한 서명을 생성하기 위한 개인 키를 갖는 정보 보안을 위한 시스템.

청구항 19.
제18항에 있어서, 상기 티켓은 공유 키에 의해 암호화되는 내용, 공유 키, 및 서명을 포함하는 정보 보안을 위한 시스템.

청구항 20.
제18항에 있어서, 서명은 제휴 서버를 위한 주소 정보를 포함하고, 상기 제휴 서버는 서명 내의 그 자신의 주소 정보를 확인하는 것에 의해 서명을 유효하게 하는 정보 보안을 위한 시스템.

청구항 21.
제16항에 있어서, 공유 키는 랜덤하게 생성된, 단일-사용 세션 키를 포함하는 정보 보안을 위한 시스템.

청구항 22.
제16항에 있어서, 인증 서버와 연결된 데이터베이스를 더 포함하고, 상기 데이터베이스는 사용자로부터 추출한 로그인 정보와 비교하기 위한 사용자 정보를 저장하는 정보 보안을 위한 시스템.

청구항 23.
제16항에 있어서, 클라이언트 컴퓨터의 브라우저를 더 포함하고, 상기 제휴 서버는 제휴 서버에 의해 제공될 선택된 서비스를 위해 브라우저를 통해서 사용자로부터 요구를 받는 정보 보안을 위한 시스템.

청구항 24.
제16항에 있어서, 제휴 서버는 사용자에게 데이터 통신 네트워크에 연결된 하나 또는 다수의 네트워크 서버에 의해 제공되는 출입구를 제공하기 위한 포탈인 정보 보안을 위한 시스템.

청구항 25.
제16항에 있어서, 제휴 서버는 웹 서버이고 데이터 통신 네트워크는 인터넷인 정보 보안을 위한 시스템.

청구항 26.
멀티-사이트 인증 시스템에서 정보 보안을 위한 방법에 있어서,

제1 네트워크로부터 인증 티켓을 생성하는 단계 - 상기 티켓은 클라이언트 컴퓨터와 관련된 정보를 포함하고, 상기 제1 네트워크 서버 및 상기 클라이언트 컴퓨터는 데이터 통신 네트워크에 연결되어 있음 - ;

제1 네트워크 서버와 관련된 개인 키를 사용해서 티켓을 위한 서명을 생성하는 단계 - 상기 서명은 제2 네트워크 서버를 위한 주소 정보를 포함하고, 상기 제2 네트워크 서버는 데이터 통신 네트워크에 또한 연결되어 있음 - ;

프라이버시 향상된 프로토콜을 통해 제1 네트워크 서버로부터 제2 네트워크 서버의 티켓을 따라 클라이언트 컴퓨터를 지시하는 단계; 및

제2 네트워크 서버에 의해, 서명을 유효하게 하기 위해 서명 내의 그 자신의 주소 정보를 확인하는 단계

를 포함하는 정보 보안을 위한 방법.

청구항 27.
제26항에 있어서, 프라이버시 향상된 프로토콜은 보안 소켓 층(secure socket layer)인 정보 보안을 위한 방법.

청구항 28.
멀티-사이트 인증 시스템에서 이용하기 위한 보안 프로토콜에 있어서,

제1 네트워크 서버 및 제2 네트워크 서버에 의해 공유되는 공유 대칭키 - 상기 제1 네트워크 서버는 공유 키를 사용해서 클라이언트 컴퓨터의 사용자와 관련된 정보를 포함하는 인증 티켓의 내용을 암호화하고, 상기 제1 및 2 네트워크 서버와 상기 클라이언트 컴퓨터는 데이터 통신 네트워크에 연결됨 - ;

제2 네트워크 서버와 관련이 있는 공개 키 - 상기 제1 네트워크 서버는 공개 키를 사용해서 공유 키를 암호화함 - ; 및

제2 네트워크 서버와 관련이 있는 개인 키 - 상기 제2 네트워크 서버는 개인 키를 사용해서 암호화된 공유 키를 해독하고 해독된 공유 키를 사용해서 티켓의 내용을 해독함 -

를 포함하는 보안 프로토콜.

청구항 29.
제28항에 있어서, 제1 네트워크 서버와 관련된 개인 키를 더 포함하고, 상기 네트워크 서버는 그것의 개인 키를 사용해서 티켓을 위한 서명을 생성하는 보안 프 로토콜.

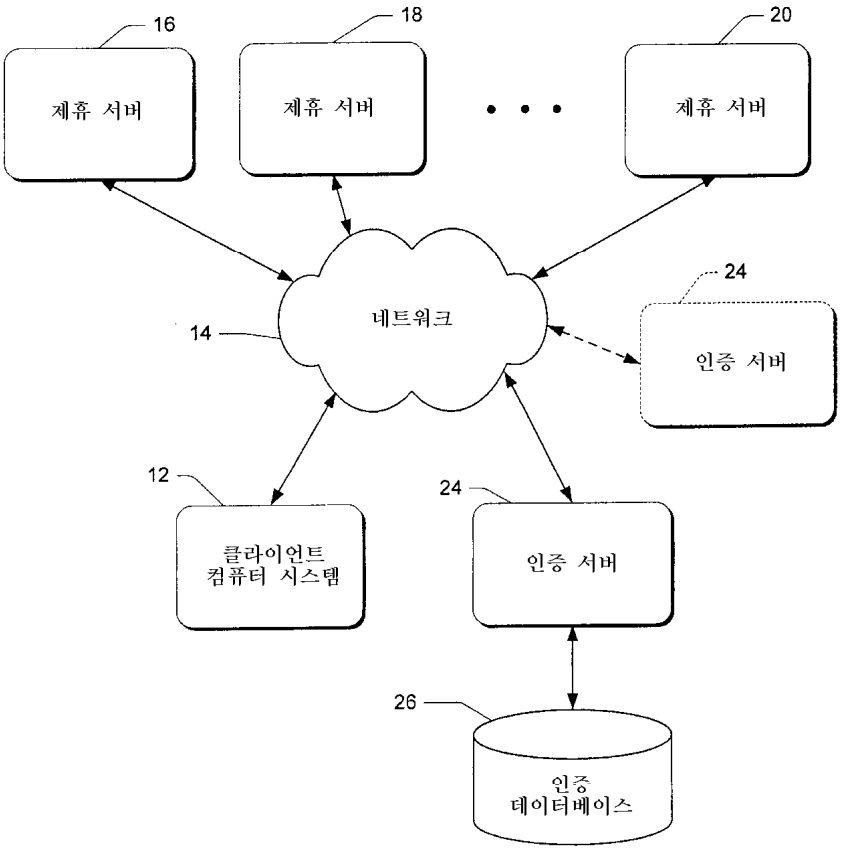
청구항 30.
제29항에 있어서, 티켓은 공유 키에 의해 암호화된 내용, 공유 키, 및 서명을 포함하는 보안 프로토콜

청구항 31.
제29항에 있어서, 서명은 제2 네트워크 서버를 위한 주소 정보를 포함하고 제2 네트워크 서버는 서명 내의 그 자신의 주소 정보를 확인함으로써 서명을 유효하게 하는 보안 프로토콜.

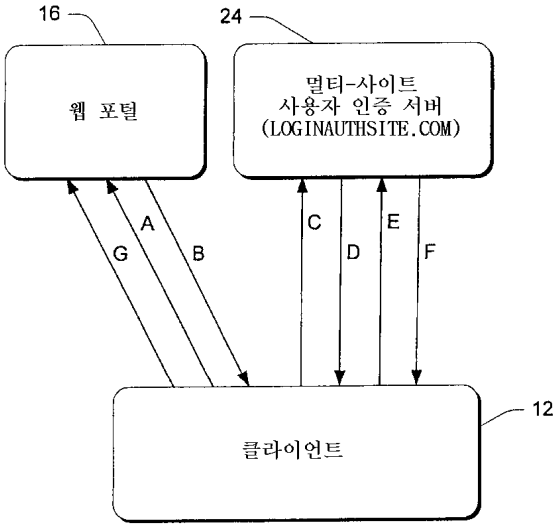
청구항 32.
제28항에 있어서, 공유 키는 램덤하게 생성된, 단일-사용 세션 키를 포함하는 보안 프로토콜.

도면

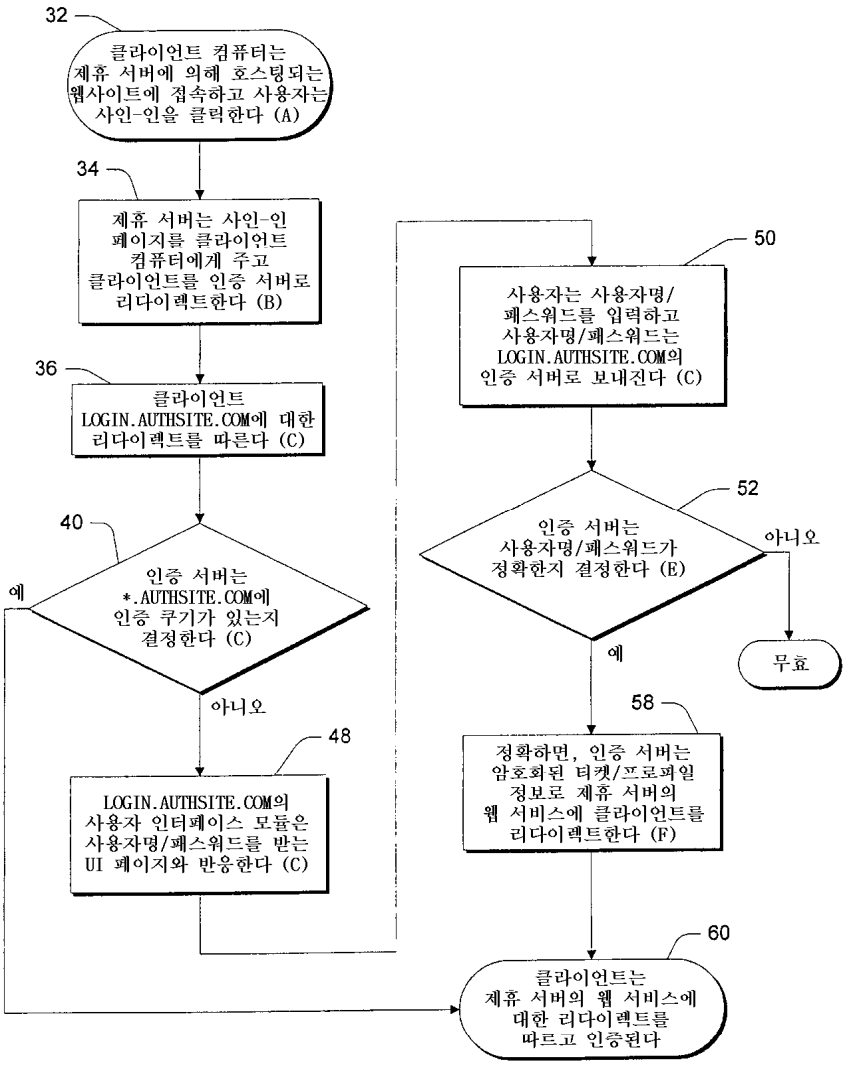
도면1


16
제휴 서버
18
제휴 서버
20
제휴 서버
네트워크
14
24
인증 서버
12
클라이언트
컴퓨터 시스템
24
인증 서버
26
인증
데이터베이스

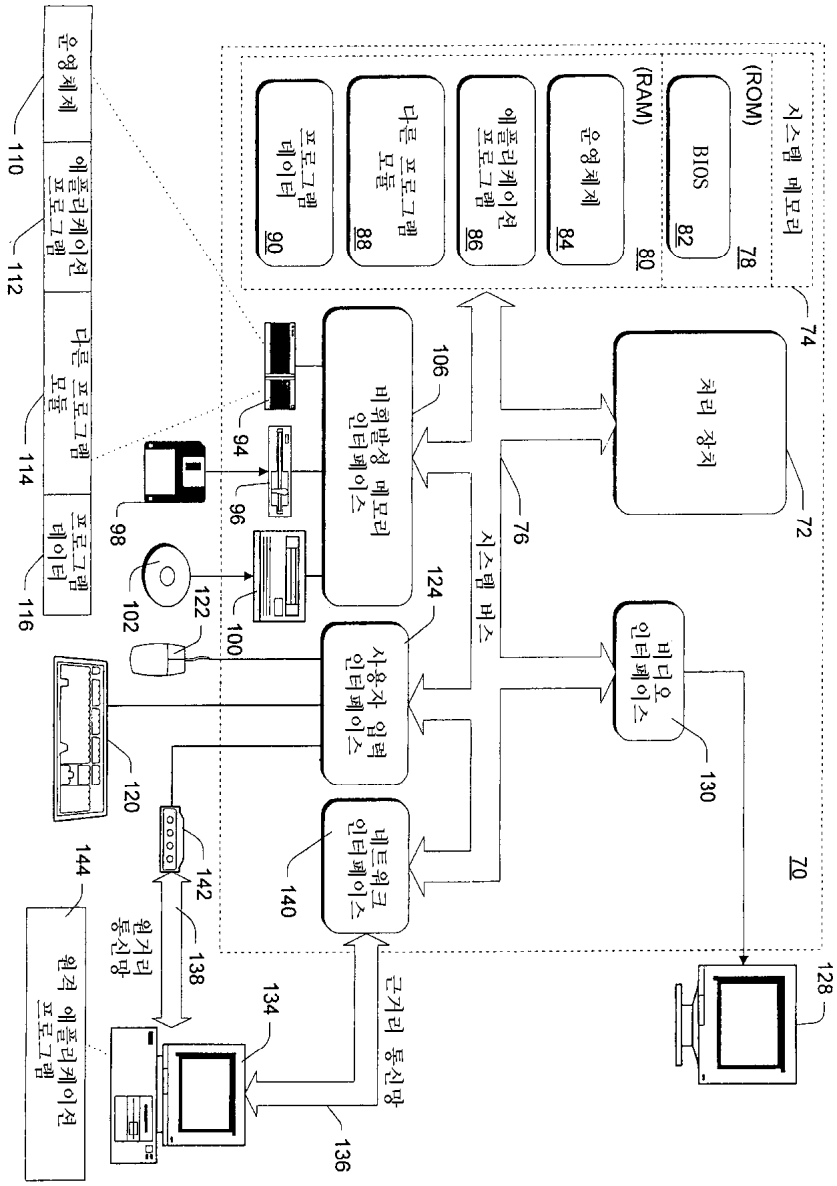
도면2


16
웹 포털
24
멀티-사이트
사용자 인증 서버
(LOGINAUTHSITE.COM)
A
B
C
D
E
F
G
12
클라이언트

도면3


32
클라이언트 컴퓨터는 제휴 서버에 의해 호스팅되는 웹사이트에 접속하고 사용자는 사인-인을 클릭한다 (A)
34
제휴 서버는 사인-인 페이지를 클라이언트 컴퓨터에게 주고 클라이언트를 인증 서버로 리다이렉트한다 (B)
36
클라이언트 LOGIN.AUTHSITE.COM에 대한 리다이렉트를 따른다 (C)
40
인증 서버는 *.AUTHSITE.COM에 인증 쿠키가 있는지 결정한다 (C)
예
아니오
48
LOGIN.AUTHSITE.COM의 사용자 인터페이스 모듈은 사용자명/패스워드를 받는 UI 페이지와 반응한다 (C)
50
사용자는 사용자명/ 패스워드를 입력하고 사용자명/패스워드는 LOGIN.AUTHSITE.COM의 인증 서버로 보내진다 (C)
52
인증 서버는 사용자명/패스워드가 정확한지 결정한다 (E)
아니오
무효
예
58
정확하면, 인증 서버는 암호화된 티켓/프로파일 정보로 제휴 서버의 웹 서비스에 클라이언트를 리다이렉트한다 (F)
60
클라이언트는 제휴 서버의 웹 서비스에 대한 리다이렉트를 따르고 인증된다

도면4


시스템 메모리
(ROM) 78
BIOS 82
(RAM) 80
운영체제 84
에플리케이션 프로그램 86
다른 프로그램 모듈 88
프로그램 데이터 90
74
처리 장치
72
시스템 버스
76
비휘발성 메모리 인터페이스
106
비디오 인터페이스
130
사용자 입력 인터페이스
124
네트워크 인터페이스
140
70
128
94
96
98
100
102
120
122
142
138
144
원거리 통신망
원격 에플리케이션 프로그램
134
136
근거리 통신망
운영체제
110
에플리케이션 프로그램
112
다른 프로그램 모듈
114
프로그램 데이터
116