(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년03월10일
(11) 등록번호 10-0946110
(24) 등록일자 2010년02월26일

(51) Int. Cl.
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
H04L 12/22 (2006.01)
(21) 출원번호 10-2006-7000100
(22) 출원일자 2004년07월09일
심사청구일자 2007년09월28일
(85) 번역문제출일자 2006년01월02일
(65) 공개번호 10-2006-0032625
(43) 공개일자 2006년04월17일
(86) 국제출원번호 PCT/EP2004/051435
(87) 국제공개번호 WO 2005/015872
국제공개일자 2005년02월17일
(30) 우선권주장
10/621,927 2003년07월17일 미국(US)
(56) 선행기술조사문헌
WO0200111451 A1
WO0200027089 A1
WO02002039237 A1
전체 청구항 수 : 총 9 항

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
애쉴리 폴 안토니
오스트레일리아 4065 퀸스랜드 바던 바우만 파라데 49
무피디 스리드하르
미국 78759 텍사스주 오스틴 야우폰 드라이브 6623
반덴바우버 마크
미국 78681 텍사스주 라운드 록 휘트워스 레인 8013
(74) 대리인
김원준, 김창세, 장성구

심사관 : 남기영

(54) 기존 SSL 세션을 브레이킹하지 않고 인증서-기반 인증으로 스텝 업하는 방법 및 시스템

(57) 요 약

본 발명은 인증 동작을 수행하는 방법에 관한 것이다. 클라이언트가 서버로부터 자원을 요청하면, 서버와 클라이언트 사이에서 비 인증서 기반 인증 동작이 수행된다. 클라이언트가 또 다른 자원을 요청하면, 서버는 보다 제한적인 인증 수준으로 보안을 강화하고, 인증서 기반 인증 동작을 이행하기 이전의 SSL 세션을 빠져 나가거나 재조정하지 않으며 그 SSL 세션을 통해 인증서 기반 인증 동작이 수행된다. 인증서 기반 인증 동작 중에, 실행 가능한 모듈이 SSL 세션을 hxd해 서버로부터 클라이언트로 다운로드되고, 그 후에 서버는 클라이언트에서 디지털 인증서를 사용하여 실행 가능한 모듈에 의해 생성된 디지털 서명을 SSL 세션을 통해 수신한다. 서버에서 디지털 서명을 성공적으로 검증한 것에 응답하여, 서버는 요청 자원에 대한 액세스를 제공한다.

특허청구의 범위

청구항 1

인증 동작을 수행하는 방법으로서,

서버와 클라이언트 사이에서 SSL(Secure Sockets Layer) 세션을 통해 비 인증서 기반 인증 동작(non-certificate-based authentication operation)을 수행하는 단계(402)와,

상기 비 인증서 기반 인증 동작을 수행한 후에,

상기 SSL 세션을 통해 실행 가능한 모듈을 상기 서버로부터 상기 클라이언트로 다운로드하는 단계(406)와,

상기 클라이언트에서 디지털 인증서를 이용하여 상기 실행 가능한 모듈에 의해 생성된 디지털 인증서를 상기 서버에서 수신하는 단계(410)와,

상기 서버와 상기 클라이언트 간의 상기 SSL 세션을 통해 인증서 기반 인증 동작을 수행하되, 상기 인증서 기반 인증 동작의 완료 이전에는 상기 SSL 세션을 빠져나가거나 재조정하지 않는 단계를 포함하는

인증 동작 수행 방법.

청구항 2

제 1 항에 있어서,

상기 SSL 세션의 재조정에서는 상기 클라이언트로부터의 제 1 디지털 인증서를 사용하고,

상기 인증서 기반 인증 동작에서는 상기 클라이언트로부터의 제 2 디지털 인증서를 사용하며,

상기 제 1 디지털 인증서 및 상기 제 2 디지털 인증서는 동일하지 않은

인증 동작 수행 방법.

청구항 3

제 2 항에 있어서,

상기 비 인증서 기반 인증 동작과 연관되어 있는 서버에 의해서 클라이언트에게 제 1 자원에 대한 액세스를 제공하는 단계를 더 포함하는 인증 동작 수행 방법.

청구항 4

삭제

청구항 5

제 3 항에 있어서,

상기 인증서 기반 인증 동작과 연관되어 있는 서버에 의해서 클라이언트에게 제 2 자원에 대한 액세스를 제공하는 단계를 더 포함하는 인증 동작 수행 방법.

청구항 6

삭제

청구항 7

삭제

청구항 8

제 1 항 내지 제 3 항 및 제 5 항 중 어느 한 항에 있어서,

상기 인증서 기반 인증 동작과 연관되어 있는 클라이언트에서, 상기 서버에 있는 제 2 자원에 대한 액세스를 획득하는 단계를 더 포함하는

인증 동작 수행 방법.

청구항 9

제 8 항에 있어서,

상기 제 2 자원에 대한 액세스를 획득하는 단계는,

상기 SSL 세션을 통해 상기 클라이언트로부터 상기 서버로 제 2 자원 요청을 전송하는 단계와,

상기 SSL 세션을 통해 상기 서버로부터 상기 클라이언트에서 실행 가능한 모듈 - 상기 실행 가능한 모듈은 인증서 기반 인증 동작을 수행하기 위한 기능을 포함함 - 을 수신하는 단계와,

상기 클라이언트에서 디지털 인증서를 이용하여 상기 실행 가능한 모듈에 의해서 생성된 디지털 서명을 상기 SSL 세션을 통해 상기 서버로 전송하는 단계와,

상기 클라이언트에서 상기 서버로부터의 제 2 자원 응답을 수신하는 단계를 더 포함하는

인증 동작 수행 방법.

청구항 10

제 8 항에 있어서,

상기 제 2 자원에 대한 액세스를 획득하는 단계는,

상기 SSL 세션을 통해 상기 클라이언트로부터 상기 서버로 제 2 자원 요청을 전송하는 단계와,

상기 클라이언트에서, 상기 SSL 세션을 통해 상기 서버로부터 콘텐츠 및 이와 연관된 콘텐츠 유형 표시자를 갖는 응답 메세지를 수신하는 단계와,

상기 콘텐츠의 콘텐츠 유형을 결정하는 것에 응답하여, 상기 클라이언트에서 다운로드 가능한 소프트웨어 모듈을 실행하는 단계와,

상기 클라이언트에서 디지털 인증서를 이용하여 상기 실행 가능한 모듈에 의해 생성된 디지털 서명을 상기 SSL 세션을 통해 상기 서버로 전송하는 단계와,

상기 클라이언트에서 상기 서버로부터의 제 2 자원 응답을 수신하는 단계를 더 포함하는

인증 동작 수행 방법.

청구항 11

인증 동작을 수행하는 장치로서,

서버와 클라이언트 사이에서 SSL(Secure Sockets Layer) 세션을 통해 비 인증서 기반 인증 동작을 수행하는(402) 수단과,

상기 SSL 세션을 통해 실행 가능한 모듈을 상기 서버로부터 상기 클라이언트로 다운로드하는(406) 수단과,

상기 클라이언트에서 디지털 인증서를 이용하여 상기 실행 가능한 모듈에 의해 생성된 디지털 인증서를 상기 서버에서 수신하는(410) 수단과,

상기 비 인증서 기반 인증 동작을 수행한 후에, 상기 서버와 상기 클라이언트 간의 상기 SSL 세션을 통해 인증서 기반 인증 동작을 수행하되, 상기 인증서 기반 인증 동작의 완료 이전에는 상기 SSL 세션을 빠져나가거나 재조정하지 않는(416) 수단을 포함하는

인증 동작 수행 장치.

청구항 12

인증 동작을 수행하는 데이터 처리 시스템에서 사용하기 위한 컴퓨터 프로그램 제품을 가지는 컴퓨터로 판독 가능한 매체로서,

상기 컴퓨터 프로그램 제품은,

서버와 클라이언트 사이에서 SSL(Secure Sockets Layer) 세션을 통해 비 인증서 기반 인증 동작을 수행하는(402) 수단과,

상기 SSL 세션을 통해 실행 가능한 모듈을 상기 서버로부터 상기 클라이언트로 다운로드하는(406) 수단과,

상기 클라이언트에서 디지털 인증서를 이용하여 상기 실행 가능한 모듈에 의해 생성된 디지털 인증서를 상기 서버에서 수신하는 수단과,

상기 비 인증서 기반 인증 동작을 수행한 후에, 상기 서버와 상기 클라이언트 간의 상기 SSL 세션을 통해 인증서 기반 인증 동작을 수행하되, 상기 인증서 기반 인증 동작의 완료 이전에는 상기 SSL 세션을 빠져나가거나 재조정하지 않는(416) 수단을 포함하는

컴퓨터로 판독 가능한 매체.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

삭제

청구항 17

삭제

청구항 18

삭제

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 향상된 데이터 처리 시스템에 관한 것이고, 보다 구체적으로는, 멀티컴퓨터 데이터 전송 방법 및 장치에 관한 것이다. 보다 더 세부적으로 본 발명은, 암호화를 이용하는 멀티컴퓨터 통신 방법 및 장치를 제공한다.

배 경 기 술

[0002] 전자 상거래(E-commerce) 웹 사이트 및 웹 애플리케이션은 사용자를 위해서 컴퓨터 네트워크 상에서 거래를 행한다. 사용자는 보안을 위해 적절한 수준의 확실한 것에 대해 자신의 신원을 제공하는 인증 절차를 거치기도 한다.

[0003] 다수의 컴퓨터 시스템에서는 서로 다른 수준의 보안을 위해 서로 다른 유형의 인증을 한다. 예컨대, 사용자가 올바른 사용자명 및 패스워드 조합을 제공하는 제 1 수준의 인증을 성공적으로 완료한 후, 시스템은 웹 싸이트 상의 특정 자원 집합에 대한 액세스를 제공할 수 있다. 제 2 수준의 인증은 사용자가 하드웨어 토큰, 예를 들면, 스마트카드를 제출할 것을 필요로 하는데, 이러한 하드웨어 토큰을 제공한 후, 보다 강력히 제어된 웹 사이트 상의 자원들에 대해 접근이 가능하다. 제 3 수준의 인증은 사용자가 어떤 형태의 생체인식 데이터(biometric data)를 예를 들어, 지문 스캔 또는 망막 스캔을 통해서 제공할 것을 필요로 하는데, 이러한 생체인식 데이터를 제공한 후, 시스템이 매우 민감하거나 기밀성인 웹 사이트상의 자원에 대해 액세스를 제공한다.

[0004] 어떤 인증 수준에서 다음 레벨로 옮겨가는 처리를 "단계별 인증(set-up authentication)"이라 한다. 즉, 시스템이 보다 민감한 자원에 대한 이득 액세스를 필요로 하면 사용자는 어떤 인증 수준을 보다 상위 수준으로 보안 수준을 강화한다.

[0005] 전자 상거래 웹 기반 환경에서, 컴퓨터 시스템은 웹 사이트를 액세스하기 위한 프런트 도어 또는 센트리 게이트

(sentry gate)의 형태로서 인증 서비스를 구현하기도 한다. 이러한 인증 서비스는 애플리케이션의 앞에, 즉, 사용자와 애플리케이션 사이에 배치되어 임의의 자원에 대한 액세스를 얻기 전에 사용자가 인증되도록 확보한다. 이러한 인증 서비스는 웹 서버 플러그인, 역 프록시 등의 기술로서 구현될 수 있다. 이러한 인증 서비스에서 잠재된 문제는 이들이 사용자명/패스워드 인증을 사용하여, 클라이언트 기반 인증서를 사용하는 인증 방법으로 옮아갈 수 없는 경우가 있다는 것이다. 일반적으로 인증서 기반 인증 절차는 사용자명/패스워드 기반 인증 절차에 비해 높은 수준의 보안을 달성하는 것으로 간주된다.

[0006] 인증서 기반 인증은 공개/개인 비동기식 암호키 쌍의 사용을 포함하며, 디지털 인증서는 증명된 사용자의 신원을 공개 암호키와 바인딩한다. 인증서 기반 인증 절차 중에, 사용자는 자신의 디지털 인증서를 인증 서비스에게로 제공하고, 그 공개키에 대응하는 개인 암호키에 대해 사용자가 액세스 권한이 있는지를 증명할 필요가 있다. 예를 들어, 인증 서비스는 검사 데이터(challenge data)를 사용자의 클라이언트 컴퓨터에게 제공하고, 그 후, 사용자의 클라이언트 컴퓨터는 그 검사 데이터를 사용자의 개인키를 이용하여 승인하고, 인증 서비스는 공개키를 이용하여 그 디지털 서명을 검증할 수 있다. 인증 서비스가, 사용자의 개인키로 그 검사 데이터가 올바르게 승인되었다고 판정하면, 인증서에 저장되어 있는 사용자에 의해서 키가 항상 비밀로 유지되어야 하기 때문에, 그 인증 서비스는 사용자의 신원을 높은 수준에 대해 검증했다.

[0007] 인증서 기반 절차로 보안 수준을 강화하는 동작이 불가능한 경우도 있다. 전형적으로는, 보다 낮은 수준의 비 인증서 기반 인증, 예컨대, 사용자명/패스워드 조합 인증을 위해 클라이언트와 서버 사이에 상호 인증된 SSL 세션이 이미 설정되었기 때문에, 문제가 발생한다. 인증서 기반 인증 절차를 필요로 하는 인증 서비스가 SSL 스택에 대한 제어를 하지 않으면 – 이는 상업적으로 가장 많이 이용되는 경우이며, 예를 들어, 이러한 제어는 어떤 방식으로 운영 체제 내에 내장될 수 있음 – 인증 서비스는 새로운 SSL 세션의 설정을 강요할 수 없다. 따라서, 인증 서비스는 활성 SSL 세션 상에서 이미 생긴 사용자명/패스워드 기반 인증 절차로부터 그 활성 SSL 세션을 유지하면서 인증서 기반 인증 절차로 옮겨갈 수가 없다.

[0008] 따라서, 어떤 이유로 인증 서비스에 의해서 필요로 하는 보다 높은 보안 수준을 확보하기 위해 이전에 설정된 SSL 세션을 빠져나가거나 재조정하지 않으며 비 인증서 기반 인증 절차로부터 인증서 기반 인증 절차로 옮겨갈 수 있는 방법 및 시스템이 있으면 유리할 것이다.

발명의 상세한 설명

[0009] 인증 동작을 수행하는 방법을 개시한다. 클라이언트가 서버로부터의 자원을 요청하면, 서버와 클라이언트 사이의 SSL(Secure Socket Layer) 세션을 통해 비 인증서 기반 인증 동작이 수행된다. 클라이언트가 또 다른 자원을 요청하면, 서버는 보다 높은 수준의 인증 단계로 보안 수준을 강화하도록 결정하고, 인증서 기반 인증 동작이 완료되기 전에는 SSL 세션을 빠져나가거나 재조정하지 않으며 그 SSL 세션을 통해 인증서 기반 인증 동작이 수행된다.

실 시 예

[0019] 일반적으로, 본 발명을 포함하는, 또는 본 발명에 관련된 장치는 다양한 데이터 처리 기술을 포함한다. 따라서, 본 발명을 설명하기에 앞서 배경 지식으로서, 분산형 데이터 처리 시스템 내의 통상적인 하드웨어 및 소프트웨어 구성요소의 조직에 대해 보다 상세히 설명한다.

[0020] 이제, 도면을 참조하면, 도 1a는 각각이 본 발명의 일부를 구현할 수 있는 데이터 처리 시스템의 전형적인 네트워크를 도시한다. 분산형 데이터 처리 시스템(100)은 분산형 처리 시스템(100) 내에서 함께 연결되는 각종 장치와 컴퓨터들간에 통신 링크를 제공하는 데 사용될 수 있는 매체인 네트워크(101)를 포함한다. 네트워크(101)는 영구 접속, 예컨대, 유선 또는 광섬유 케이블, 또는 전화나 무선 통신을 통해 이루어지는 임시 접속을 포함한다. 도시한 예에서, 서버(102) 및 서버(103)는 저장 유닛(104)과 함께 네트워크(101)에 연결되어 있다. 클라이언트(105~107)도 네트워크(101)에 연결되어 있다. 클라이언트(105~107) 및 서버(102~103)는 각종 컴퓨터 장치, 예를 들면, 본체(mainframe), PC, PDA 등으로 나타낼 수 있다. 분산형 데이터 처리 시스템(100)은 추가 서버, 클라이언트, 라우터 등의 장치와, 도시하지는 않은 피어 투 피어(peer-to-peer) 아키텍쳐를 포함할 수 있다.

[0021] 도시한 예에서, 분산형 데이터 처리 시스템(100)은 서로 통신하기 위해 각종 프로토콜, 예컨대, LDAP(Lightweight Directory Access Protocol), TCP/IP(Transport Control Protocol/Internet Protocol), HTTP(Hypertext Transport Protocol), WAP(Wireless Application Protocol) 등을 사용하는 게이트웨이와 네트

워크의 전세계에 걸친 집합체를 나타내는 네트워크(101)를 가지는 인터넷을 포함한다. 예를 들면, 분산형 데이터 처리 시스템(100)은 예컨대 인트라넷, LAN(local area network), 또는 WAN(wide area network)와 같은 다수의 서로 다른 유형의 네트워크도 포함한다. 예를 들어, 서버(102)는 무선 통신 링크를 포함하는 네트워크(110)와 클라이언트(109)를 직접 지원한다. 네트워크 인에이블형 전화(111)는 무선 링크(112)를 통해서 네트워크(110)에 접속하고, PDA(113)는 무선 링크(114)를 통해서 네트워크(110)에 접속한다. 전화(111) 및 PDA(113)는 블루투스 무선 기술과 같은 적절한 기술을 이용하여 무선 링크(115)를 거쳐서 이들간에 데이터를 직접 전송하여, 소위 PAN(personal area networks) 또는 사설 애드 혹 네트워크(personal ad-hoc networks)를 형성할 수도 있다. 이와 유사하게, PDA(113)도 무선 통신 링크(116)를 통해서 PDA(107)에 데이터를 전송할 수 있다.

[0022] 본 발명은 각종 하드웨어 플랫폼 상에서 구현될 수 있으며, 도 1a는 여러 컴퓨터 환경의 일 예일 뿐 본 발명을 이러한 구조에 제한하려는 것이 아니다.

[0023] 이제, 도 1b를 참조하면, 도면은 도 1a에 도시한 것과 같은, 본 발명이 구현될 수 있는 데이터 처리 시스템의 전형적인 아키텍처를 도시한다. 데이터 처리 시스템(120)은 RAM(random access memory)(124), ROM(read-only memory)(126), 및 내부 시스템 버스(123)에 연결된 하나 이상의 중앙 처리 장치(CPU)(122)를 포함하는데, 내부 시스템 버스(123)는 그프린터(130), 디스크 유닛(132) 또는 음성 출력 시스템 등과 같은, 도시하지 않은 기타 장치들을 지원하는 입출력 어댑터(128)를 상호 연결한다. 시스템 버스(123)는 통신 링크(136)에 대한 액세스를 제공하는 통신 어댑터(134)에도 연결된다. 사용자 인터페이스 어댑터(148)는 각종 사용자 장치, 예컨대, 키보드(140)와 마우스(142), 또는 터치 스크린, 스타일러스와 같은 도시하지 않은 다른 장치들을 연결한다.

[0024] 당업자라면, 도 1b의 하드웨어가 시스템 구현예에 따라 달라질 수 있다는 것을 이해할 수 있을 것이다. 예를 들어, 시스템은 하나 이상의 프로세서, 예컨대 Intel® Pentium® 기반 프로세서 및 디지털 신호 프로세서(DSP), 및 한가지 이상의 휘발성 및 비휘발성 메모리 유형을 포함할 수 있다. 도 1b에 도시한 하드웨어에 추가하여 또는 이 대신에 다른 주변 장치들이 사용될 수 있다. 도시한 예는 본 발명에 대한 구조적 제한을 암시하는 것이 아니다.

[0025] 본 발명은 각종 하드웨어 플랫폼 상에서 구현이 가능하고, 각종 소프트웨어 환경에서도 구현될 수 있다. 각각의 데이터 처리 시스템 내에서의 프로그램 실행을 제어하기 위해 통상적인 운영 체제를 사용할 수 있다. 예를 들어, 하나의 장치는 UNIX® 운영 체제를 실행하는 반면, 또 다른 장치는 간단한 Java® 실시간 환경을 포함한다. 대표적인 컴퓨터 플랫폼에는, 각종 포맷의 하이퍼텍스트 문서, 예컨대 그래픽 파일, 워드 프로세싱 파일, XML(Extensible Markup Language), HTML(Hypertext Markup Language), HDML(Handheld Device Markup Language), WML(Wireless Markup Language) 및 각종 다른 포맷 및 유형의 파일 액세스용으로 잘 알려져 있는 소프트웨어인 브라우저를 포함할 수 있다.

[0026] 본 발명은 도 1a 및 1b에 대해서 위에서 기술한 바와 같이, 각종 하드웨어 및 소프트웨어 플랫폼 상에서 구현될 수 있다. 그러나, 보다 구체적으로 본 발명은 향상된 인증 서비스에 관한 것이다. 이러한 향상된 인증 서비스에 대해 설명하기에 앞서, 통상적인 인증 서비스에 대해 설명한다.

[0027] 본 명세서에서 도면에 관한 설명에는 클라이언트 장치나 클라이언트 장치의 사용자 중 하나에 의한 어떤 동작이 포함된다. 당업자라면, 클라이언트에 대한 응답 및/또는 클라이언트로부터의 요청이 사용자에 의해서 개시되기도 하고, 다른 때에는 클라이언트의 사용자를 대신하여 클라이언트에 의해서 자동적으로 개시되기도 한다는 것을 이해할 수 있을 것이다. 따라서, 도면의 설명에서 클라이언트 또는 클라이언트의 사용자를 언급하는 경우, 용어 "클라이언트"와 "사용자"는, 기술하는 처리의 의미에 하등의 영향을 미치지 않으며 상호 교환될 수 있다는 것을 이해해야 한다.

[0028] 이제, 도 1c를 참조하면, 데이터 순서도는 클라이언트가 서버에 있는 보호 자원을 액세스하려 할 때 사용될 수 있는 전형적인 인증 처리를 나타낸다. 도시하는 바와 같이, 클라이언트 워크스테이션(150)에서의 사용자는 컴퓨터 네트워크상에서 클라이언트 워크스테이션 상에서 실행 중인 사용자의 웹 브라우저를 통해 서버(151) 상에 있는 보호 자원에 대해 액세스를 하려 한다. 보호 자원이란, 액세스가 제어되거나 제한되는 자원(애플리케이션, 객체, 문서, 페이지, 파일, 실행 가능 코드, 또는 기타 계산적 자원, 통신형 자원 등)이다. 보호 자원은 URL(Uniform Resource Locator)로, 또는 보다 일반적으로 인증되거나 승인된 사용자에 의해서만 액세스될 수 있는 URI(Uniform Resource Identifier)이다. 컴퓨터 네트워크는 도 1a나 도 1b에 도시한 바와 같이, 인터넷, 인트라넷 등의 네트워크일 수 있고, 서버는 WAS(web application server), 서버 애플리케이션, 서

브렛 프로세스 등일 수 있다.

[0029] 사용자가 서버측 보호 자원, 예를 들어, 도메인 "ibm.com" 내의 웹 페이지를 요청(단계 152)하면, 처리를 시작한다. 용어 "서버측" 및 "클라이언트측"이란, 네트워크 환경에서 서버 또는 클라이언트 각각에서의 동작이나 개체를 지칭한다. 웹 브라우저(또는 이와 연관되어 있는 애플리케이션이나 애플렛)는 도메인 "ibm.com"을 호스팅하는 웹 서버에 전송되는 HTTP 요청(단계 153)을 생성한다. 용어 "요청" 및 "응답"은, 특정 동작에 포함되어 있는 정보, 예컨대, 메세지, 통신 프로토콜 정보 등의 연관된 정보의 전달에 적합한 데이터 포맷을 포함하는 것으로 이해해야 한다.

[0030] 클라이언트에 대한 활성 세션을 포함하지 않는다고 판정(단계 154)해서, 클라이언트와 서버간의 정보의 복수 전송을 수반하여 서버와 클라이언트 사이에서 SSL(Secure Sockets Layer) 세션 설정을 개시하고 완료(단계 155)한다. SSL 세션이 설정된 후에, 그 SSL 세션 내에서 후속 통신 메세지가 전달되는데, 어떤 비밀 정보는 그 SSL 세션 내에서의 암호화된 통신 메세지로 인해 보안이 유지된다.

[0031] 그러나, 서버는 사용자가 보호 자원에 대한 액세스할 수 있게 하기 전에 사용자의 신분이 옳은지 결정할 필요가 있어서, 서버는 클라이언트에게 어떤 유형의 인증 검사를 전송(단계 156)함으로써, 사용자가 인증 처리를 수행하도록 요구한다. 인증 검사는 각종 포맷, 예컨대, HTML 형태일 수 있다. 그 후, 사용자는 요청하는 또는 요구하는 정보를, 예컨대, 사용자명, 또는 다른 유형의 사용자 식별자를 그와 연관된 패스워드 등의 비밀 정보와 함께 제공(단계 157)한다.

[0032] 인증 응답 정보가 서버로 전송(단계 158)되고, 이 시점에서 예를 들면, 이전에 제출된 등록 정보를 검색하고 제출된 인증 정보를 사용자의 저장된 정보와 매칭함으로써 서버가 사용자 또는 클라이언트를 인증(단계 159)한다. 인증이 성공적이면, 인증된 서버 또는 클라이언트를 위해 활성 세션이 설정된다.

[0033] 그 다음으로 서버는, 원시 요청 웹 페이지를 검색하고, HTTP 응답 메세지를 클라이언트에게 전송(단계 160)하여, 이로써, 보호 자원에 대한 사용자의 원시 요청이 완료된다. 이 시점에서, 사용자는 브라우저 윈도우 내의 하이퍼텍스트 링크를 클릭함으로써 "ibm.com" 내의 다른 페이지를 요청할 수 있고, 브라우저는 또 다른 HTTP 요청 메세지를 서버에게 전송(단계 162)한다. 이 시점에서, 서버는 사용자가 활성 세션을 가진다고 인식(단계 163)하고, 서버는 요청한 웹 페이지를 또 다른 HTTP 응답 메세지로 클라이언트에게 되전송(단계 164)한다.

[0034] 이제, 도 1d를 참조하면, 블록도는, 복수의 인증 서버를 포함하는, 전형적인 회사 도메인(170)용 데이터 처리 시스템을 도시한다. 전형적인 공동 컴퓨팅 환경 또는 인터넷 기반 컴퓨팅 환경에서와 같이, 회사 도메인(170)은 네트워크(174)를 통해서 예를 들면, 클라이언트 장치(173) 상의 브라우저 애플리케이션(172)을 이용함으로써, 사용자가 액세스할 수 있는 관리 자원을 호스팅한다. 애플리케이션 서버(176)는 각종 인증 메카니즘, 예컨대, 사용자명/패스워드, X.509 인증서 또는 보안 토큰을 지원한다. 회사 도메인(170)은 복수의 서버를 지원한다. 프록시 서버(177)는 회사 도메인(170)을 위한 폭넓은 기능을 수행한다. 프록시 서버(177)는,애플리케이션 서버로부터의 콘텐츠를 미러링하거나, 입력 데이터스트림 필터 유닛(179) 및 출력 데이터스트림 필터 유닛(180)을 통해 입력 및 출력되는 데이터스트림을 필터링하기 위해, 관리상 배치 파일 및 회사 방침 데이터베이스(178)를 통해 프록시 서버(177)의 기능, 예를 들면, 웹 페이지 캐싱을 제어하도록 구성될 수 있다. 입력 데이터스트림 필터 유닛(179)은 입력되는 요청에 대해 다중 검사를 행할 수 있고, 출력 데이터스트림 필터 유닛(180)은 출력되는 응답에 대해 다중 검사를 행할 수 있으며, 각 검사는 여러 가지 회사 방침 내에 명시되어 있는 목적 및 조건에 따라 수행될 수 있다

[0035] 회사 도메인(170)은 인증 서버(181)를 포함한다. 인증 서버(181)에 있는 인증 방침 관리 유닛(182)은 사용자 레지스트리(183) 및 ACL(access control list) 데이터베이스(184) 내의 정보를 관리한다. 방침 관리 유닛(182)은 사용자의 서비스 요청에 대한 방침을 검사함으로써 도메인(170) 내의 애플리케이션 서버(175)에 의해 제공되는 어떤 서비스를 액세스할 권한이 사용자에게 부여되는 지를 판정한다. 본 명세서에서의 예에서는, 사용자에게 권한이 부여된 후에는 모든 관리 자원을 액세스할 권한이 부여된다고 가정하지만, 본 발명의 여러 가지 실시예에서는 본 발명의 범주에 영향을 미치지 않으며 대안적인 인증 처리를 포함할 수 있다는 것을 이해해야 한다.

[0036] 위에서 언급한, 회사 도메인(170) 내의 개체들은 많은 컴퓨팅 환경에서의 통상적인 개체들을 나타낸다. 도 1c에서 도시한 바와 같이, 웹 기반 애플리케이션은 사용자로 하여금 HTML 서식 내에서 사용자명/패스워드 조합과 같은 인증 정보를 입력하게 하는 각종 수단을 이용할 수 있다. 도 1에 도시하는 예에서, 사용자(171)는 클라이

언트(173)가 자원에 대한 액세스 권한을 가지며, 그 클라이언트(173)가 자원에 대한 액세스 권한을 가지게 되면, 위의 도 1c에서 기술한 것과 유사한 방식으로 클라이언트를 위해 세션이 설정될 수 있다. 도 1d에서, 클라이언트(173)로부터 입력되는 요청을 수신한 후에, 입력 데이터스트림 필터 유닛(179)은 클라이언트(173)가 이미 세션을 설정했는 지를 판정할 수 있으며, 세션을 설정한 경우가 아니면, 사용자를 인증하기 위해서 인증 서버(176) 상의 인증 서비스가 호출될 수 있다. 클라이언트(173)가 이미 세션을 설정했으면, 관리 자원에 대한 액세스 권한을 부여하기 전에, 입력되는 요청에 대해 추가 검사를 행할 수 있는데, 이 추가 검사는 회사 인증 방침에 명시될 수 있다.

[0037] 이제, 본 발명에 초점을 맞추면, 어떤 시스템은 단계별 인증 절차를 행할 필요가 있다는 것을 특별히 언급했다. 그러나, 하위 수준 비 인증서 기반 인증 절차로부터 하위 수준 인증서 기반 인증 절차로의 보안 수준 강화 동작은 인증 서비스와 사용자의 브라우저 또는 이와 유사한 클라이언트 애플리케이션 사이에 상호 인증되어 활성화된 SSL 세션 – SSL 세션은, 하위 수준 비 인증서 기반 인증 절차, 예를 들면, 사용자명/패스워드 조합 인증 절차를 위해 클라이언트와 서버 사이에 설정되었음 – 을 유지하면서 이루어질 수 있는 것이 아니었다. 본 발명은, 서버측 인증 서비스가 기존의 SSL 세션을 통해 사용자나 사용자의 클라이언트 장치에 대한 인증서 기반 인증 절차를 수행하게 함으로써 이러한 문제에 대한 해결책을 제공한다. 아래에서 본 발명은 나머지 도면에 대해서 보다 상세히 설명한다.

[0038] 이제, 도 2를 참조하면, 블록도는, 본 발명에 따른 단계별 인증 처리를 포함하도록 확장된 인증 서비스를 도시한다. 도 1d에 대해서 위에서 기술한 것과 유사한 방식으로, 클라이언트(200)는 각종 웹 애플리케이션으로부터 자원 및 서비스를 액세스하기 위해 웹 브라우저 애플리케이션(202)이나 이와 유사한 클라이언트 애플리케이션을 실행시킨다. 브라우저(202)는 가상 머신을 포함할 수 있는 실시간 환경(204)을 지원하는데, 실시간 환경(204)은 여러 유형의 다운로드 가능하며 실행 가능한 소프트웨어 모듈, 예를 들면 애플렛이나 플러그인을 실행시킬 수 있다. 브라우저(202)와 지원형 애플렛/플러그인은 클라이언트가 사용자의 디지털 인증서 및/또는 암호키를 유지하는 키 데이터베이스(206)를 액세스할 수 있다. 또한, 브라우저(202)와 지원형 실행 가능 모듈은 클라이언트(200)에서 생성된 서명의 로그를 포함하는 서명 로그(208)를 액세스할 수 있다. 서명 로그(208)는 클라이언트(200)로부터의 서명 제출에 응답하여 웹 서버로부터 리턴된 서명 기록/수령증도 포함할 수 있다.

[0039] 도메인(210)은 애플리케이션 서버 및 인증 서버를 포함하는데, 이들 중 적어도 하나는 본 발명의 단계별 인증 기능을 구현하는 단계별 인증 처리 유닛(214)을 포함하는 인증 서비스(212)를 지원한다. 인증 서비스(212)는 클라이언트로부터 수신되는 디지털 서명을 검증하기 위한 디지털 서명 검증 유닛(216)과, 인증 서비스(212)로부터의 요구에 응답하여 클라이언트로부터 리턴된 수신한 서명의 기록을 저장하기 위한 서명 로그(218)도 지원하는데, 이들에 대해서는 아래에 보다 상세히 설명할 것이다.

[0040] 이제, 도 3을 참조하면, 순서도는 상호 인증되어 활성화된 SSL 세션을 유지하며 하위 수준 비 인증서 기반 인증 절차로부터 상위 수준 인증서 기반 인증 절차로의 보안 강화 방법을 나타낸다. 도 1c에 대해서 위에서 설명한 바와 같이, 전형적인 비 인증서 기반 인증 동작은 보호 자원에 대한 사용자의 요청을 수신(단계 302)하는 것에 응답하여, 예를 들면, 클라이언트 장치에서의 브라우저 애플리케이션에서의 사용자 동작에 응답하여 생성된 HTTP 요청 메세지의 형태의 웹 페이지 요청의 결과로서 서버에서 이루어질 수 있다. 클라이언트와 서버 사이에서 상호 인증된 SSL 세션을 설정한 후에, 서버는 그 SSL 세션을 통해서 비 인증서 기반 인증 동작, 예를 들면, 클라이언트/사용자가 유효한 사용자명/패스워드 조합이나 어떤 다른 비밀 정보를 제공하는 지에 대한 검사를 수행(단계 304)한다. 비 인증서 기반 인증 동작을 성공적으로 완료했다고 하면, 서버는 예를 들어 응답 메세지를 리턴하거나 어떤 다른 동작을 수행함으로써 원시 요청 자원을 클라이언트에게 제공(단계 306)한다.

[0041] 그러나, 도 3은 도 1c와 상이한데, 즉, 도 1c는 비 인증서 기반 인증 동작인 반면, 도 3은 본 발명이 인증서 기반 인증 동작에 의해 제공되는 보다 높은 보안 수준으로 보안을 강화하는 방법을 제공하는 방식을 설명한다.

[0042] 비 인증서 기반 인증 동작이 완료되었고, 이전의 비 인증서 기반 인증 동작에 의해 확보되는 클라이언트 세션 중에 서버가 보호 자원을 제공한 후의 어떤 시점에, 서버는 보다 상위 보안 수준으로 제어되는, 즉, 특정 자원에 대한 액세스가 보다 제한되는 보호 자원에 대한 요청을 수신(단계 308)한다. 이에 응답하여, 서버는 서버와 클라이언트 사이에서 이전에 설정된 SSL 세션을 통해, 현재의 SSL 세션을 중단하지 않으며, 현재의 SSL 세션을 재조정하거나, 현재의 SSL 세션을 빠져나가지 않으며 인증서 기반 인증 동작을 수행한다. 인증서 기반 인증 동작을 성공적으로 완료했다고 가정하면, 서버는 예를 들면, 응답 메세지를 리턴하거나 어떤 다른 동작을 수행함으로써 클라이언트에게 보다 제한형인 자원을 제공(단계 312)한다. 이러한 방식으로, 비 인증서 기반 인증 동작을 위해 이전에 사용된 것과 동일한 SSL 세션을 통해서 인증서 기반 인증 동작이 이루어진다.

[0043] 용어 "비 인증서 기반 인증 동작"은 사용자/클라이언트의 동일성을 판정하기 위한 제 1 인증 동작이 디지털 인증서를 사용하지 않는다는 사실을 나타낸다. 본 명세서에서 (비 인증서 기반 인증 동작에 사용되는 비밀 정보, 예컨대 패스워드를 안전하게 전달하기 위해 사용될 수 있는) SSL 세션을 설정하기 위해서 클라이언트측에서의 디지털 인증서를 사용하는 것은 비 인증서 기반 인증 동작에서의 인증서의 사용이 아닌 것으로 간주한다.

[0044] 이제, 도 4를 참조하면, 순서도는 본 발명의 일 실시예에 따라 단계별 인증서 기반 인증 동작을 위한, 서버측에서의 특정 처리의 세부사항들을 더 나타낸다. 도 4에 도시하는 처리는 주로 도 3의 단계(308~312)에 대해 보다 상세히 나타낸다. 도 4의 처리 단계들은 서버측 데이터 처리 시스템, 예를 들어, 도 2에 도시하는 분산형 데이터 처리 시스템과 유사한 시스템 내에서 발생하며, 설명을 쉽게 하기 위해서, 전체 처리가 하나의 서버 내에서 이루어지는 것처럼 나타내었으나, 처리는 복수의 서버, 애플리케이션 및/또는 장치들에 걸쳐서 구현될 수 있다. 본 예에서는 HTTP 메세지 및 HTML 페이지의 사용에 대해 기술하지만, 본 발명은 다른 프로토콜 및 메세지/문서 포맷을 지원하도록 구현될 수 있다.

[0045] 이러한 처리는 SSL 세션을 통해서 비 인증서 기반 인증 동작, 예컨대, 도 3의 단계(302~306)에서 도시하는 비 인증서 기반 인증 동작이 발생한 후에 서버가 클라이언트로부터 자원 요청을 수신하는 것으로 시작된다. 따라서, 서버가, 이미 그 서버와 함께 활성 세션을 설정한 클라이언트로부터 자원 요청을 수신했다고 인식하고, 도 1c와 다르게, 서버는 클라이언트가 인증 동작을 완료할 것을 즉시 요구하지 않고 요청에 대한 응답을 진행한다.

[0046] 그 후, 서버는 요청 자원에 대한 액세스가, 그 클라이언트와 함께 이전에 완료한 비 인증서 기반 인증 동작에 의해서 제공된 하위 보안 수준이 아닌 인증서 기반 인증 동작에 의해 제공될 수 있는 상위 보안 수준을 요구한다고 판단(단계 404)한다. 서버는 본 발명의 범주에 영향을 미치지 않으며 각종 처리를 통해 이러한 판정을 행할 수 있다. 일 예로서, 입력되는 자원 요청은 프록시 서버, 예컨대 도 2의 서버(177)에 의해 필터링되거나 스캔될 수 있다. 입력되는 요청 메세지로부터 요청 URI를 추출한 후에, 추출된 URI는 추출된 URI와 연관되어 있는 방침과 매칭을 한다. 연관되어 있는 방침은, URI에 대해 적절히 응답하도록 수행되어야 하는 적절한 동작을 나타내며, 임의의 인증 요구사항 등의 보안 절차를 포함한다. 이러한 방침에서, 요청에 대해 응답하기 전에 인증서 기반 인증 동작이 성공적으로 완료되어야 한다고 나타내고, 인증서 기반 인증 동작이 요청 중인 클라이언트와 함께 아직 완료되지 않았으면, 도 4에 도시되어 있는 처리의 나머지 단계에 나타내는 바와 같이 인증 수준을 강화하는 절차가 개시된다.

[0047] 그 후, 서버는 서버로부터 클라이언트로 소프트웨어 모듈을 다운로드 및/또는 클라이언트에서 소프트웨어 모듈의 실행을 트리거하도록 진행(단계 406)한다. 소프트웨어 모듈이 다운로드되거나 실행되도록 트리거되는 방식은 바뀔 수 있다. 제 1 실시예에서, 서버는 예를 들어, 클라이언트로부터의 원시 요청, 즉, 인증서 기반 인증 동작을 필요로 한다고 판정된 요청에 대해서 HTTP 응답 메세지의 콘텐츠 페이로드로서 리턴되는 HTML 웹 페이지 내에 Java 애플렛을 내장함으로써 애플렛이나 플러그인을 클라이언트 애플리케이션, 예컨대 브라우저로 다운로드한다. 이에 응답하여, 브라우저는 웹 페이지의 처리 및 그 정규 해석의 일부로서 애플렛을 로딩한다.

[0048] 다른 실시예에서, 서버는 자신이 특정 MIME형(다목적 인터넷 우편 확장자)을 갖는 콘텐츠를 포함한다고 나타내는 메세지를 클라이언트에게 리턴할 수 있다. 이에 응답하여, 클라이언트에 있는 브라우저 애플리케이션은 브라우저를 이용하여 그 특정 MIME형을 처리할 수 있기 때문에 이전에 등록한 적절한 플러그인을 로딩한다. 어떤 경우에, 브라우저는 사용자가 특정 MIME형에 대해 등록되지 않았으면 적절한 플러그인을 찾도록 한다. 이러한 방식으로, 브라우저는 후술하는 처리 단계들을 실행할 수 있는 소프트웨어 모듈을 이미 가질 수 있으므로, 그 서버가 클라이언트로 소프트웨어 모듈을 다운로드할 필요가 없게 된다.

[0049] 어떤 경우에, 보호 자원에 대한 요청을 전송하는 클라이언트 애플리케이션은 이전에 활성화된 SSL 세션도 유지중이며, 서버가 그 SSL 세션을 통해서 적절한 메세지를 클라이언트 애플리케이션에 전송하여 인증서 기반 인증 절차를 위한 클라이언트측 단계들을 실행하는 소프트웨어 모듈을 클라이언트 애플리케이션이 실행하게 한다. 어떤 경우에, 서버는 소프트웨어 모듈을 다운로드할 수도 있고, 다른 경우에는 그 소프트웨어 모듈이 이미 클라이언트에 존재할 수 있다. 본 발명은 표준 인터넷 관련 프로토콜 및 사양을 고수하기 때문에, 본 발명은 클라이언트 애플리케이션이 서버측 인증 요구사항에 응답하기 위한 기능을 형성하지 않았다고 가정하며 단계별 인증 동작을 제공한다. 잘 알려져 있는 인터넷 관련 및 WWW 관련 기술을 통해 브라우저 등의 클라이언트 애플리케이션을 확장시킴으로써 필요로 하는 기능을 소프트웨어 모듈에 제공할 수 있다.

[0050] 도 4와 연결하여 그 다음으로 서버는 소프트웨어 모듈에 의해 디지털 서명될 검사 데이터를 다운로드(단계 408)한다. 검사 데이터는 애플렛, 플러그인 또는 클라이언트의 다른 소프트웨어 모듈 내에서 검사 데이터에 대해

디지털 서명을 생성하는 디지털 서명 알고리즘에 대한 입력으로서 사용될 수 있는 어떤 유형의 데이터 아이템이다. 검사 데이터의 포맷은 사용되는 디지털 서명 알고리즘에 따라 달라질 수 있고, 본 발명은 하나 이상의 표준 또는 적절한 디지털 서명 알고리즘을 지원할 수 있다.

[0051] 서버는 다운로드하는 애플렛과 함께 검사 데이터를 다운로드할 수 있고, 또는 검사 데이터는 후속 메세지로 전송될 수 있다. 이와 다르게, 클라이언트에서 애플렛, 플러그인 등의 소프트웨어 모듈은 검사 데이터를 요청할 수 있고, 서버는 이에 응답하여 검사 데이터를 리턴한다. 이와 다르게, 클라이언트는 이미 검사 데이터를 가지고 있을 수 있고, 예를 들면, 서버에 의해서 클라이언트로 이전에 리턴된 캐시된 웹 페이지가 있을 수 있다.

[0052] 어떤 후속 시점에, 서버는 클라이언트로부터 디지털 서명을 수신(단계 410)하고, 서버는 사용자/클라이언트의 적절한 공개키 인증서를 이용하여 디지털 서명을 검증(단계 412)한다. 서버는 디렉토리로부터 공개키 인증서를 검색할 수 있고, 또는 공개 키 인증서는 클라이언트로부터의 디지털 서명을 가지고 있는 메세지를 덧붙이고 있을 수 있는데, 공개키 인증서의 인증은 인증서 인증 및 각종 인증서 파기 수단을 통해 확인이 가능하다. 디지털 서명이 검증되면, 클라이언트는, 비동기적 공개/개인 암호키 쌍으로 공개키에 대응하는 개인키를 가지고 있다고 나타내고, 이로써, 클라이언트/사용자의 신원확인 설정을 하는데, 이는, 유효한 공개키 인증서에 표시되는 개인/개체만이 그 공개키에 대응하는 개인키를 가지고 있어야 하기 때문이다. 디지털 서명이 성공적으로 검증되었다고 하면, 서버는 비복제를 목적으로 예를 들면, 디지털 서명의 복사본, 검증 가능한 타임스탬프 및 디지털 서명을 수신한 IP 어드레스를 이용하여 데이터베이스 레코드를 생성함으로써 디지털 서명의 수령증을 기록(단계 414)할 수 있다. 디지털 서명의 성공적인 검증은 인증서 기반 인증 동작을 완료하고, 그 결과, 서버는 서버가 인증서 기반 인증 동작을 시도하기 전에 클라이언트에 의해 요청된 자원에 대한 액세스 권한을 부여(단계 416)하여, 그 결과 도 4에 나타내는 처리로 된다.

[0053] 이제, 도 5를 참조하면, 순서도는 본 발명의 일 실시예에 따라 단계별 인증서 기반 인증 동작을 위한, 클라이언트에서의 처리를 나타낸다. 서버측 처리를 나타내는 도 4와 반대로, 도 5는 클라이언트측 처리를 나타낸다. 처리는, 클라이언트가 그 서버와 함께 SSL 세션을 이미 설정하고, 그 서버와 비 인증서 기반 인증 동작을 성공적으로 완료한 후에 서버에게 자원 요청 메세지를 전송(단계 502)하는 것으로 시작된다. 요청에 응답하여, 클라이언트는 소프트웨어 모듈을 포함하거나, 인증서 기반 인증 동작을 지원하는 소프트웨어 모듈의 실행을 트리거하는 응답 메세지를 수신(단계 504)한다. 클라이언트는 브라우저와 같은 클라이언트 애플리케이션에 의해 지원되는 가상 머신 내에서 실행 가능한 애플렛, 예컨대 Java 애플렛을 수신할 수 있다. 이와 다르게, 클라이언트는 특정 MIME형의 콘텐츠를 포함하는 메세지를 수신하고, 이로써, 클라이언트 애플리케이션이 표시한 MIME형을 갖는 대상물을 처리하는 플러그인을 시작하도록 트리거할 수 있다.

[0054] 또한, 클라이언트 애플리케이션은, 디지털 서명을 생성할 때 사용될 검사 데이터를 수신(단계 506)할 수 있다. 이와 다르게, 클라이언트 애플리케이션은, 디지털 서명 알고리즘에 대한 입력으로서 사용될 수 있는 데이터 아이템을 이미 가지고 있을 수 있다. 어떤 경우에는 입력 데이터에 대해서 생성되는 디지털 서명을 서버가 검증하도록 하기 위해서 클라이언트에 의해 사용되는 디지털 서명 알고리즘에 대한 입력 데이터를 서버가 알고 있어야 한다. 따라서, 디지털 서명 알고리즘에 대한 입력 데이터는 클라이언트에 의해 선택되고, 그 후, 예를 들면 SSL 세션을 통해서 생성된 디지털 서명과 함께 서버로 전달된다.

[0055] 디지털 서명을 생성하도록 트리거되거나, 디지털 서명을 생성하는 것으로 결정한 후의 어떤 시점에, 클라이언트 애플리케이션은 디지털 서명을 생성(단계 508)하고, 그 디지털 서명을 서버에게 전송(단계 510)한다. 또한, 클라이언트 애플리케이션은 타임스탬프 및 비복제 절차를 도울 수 있는 기타 정보와 함께 디지털 서명의 생성을 기록(단계 512)할 수 있다. 디지털 서명이 적절하게 생성되었다고 하면, 클라이언트는 이전에 설정된 SSL 세션을 통해서 단계별 인증서 기반 인증 동작을 연속적으로 완료하고, 그 후 클라이언트가, 예를 들면, 웹 페이지를 검색함으로써 요청 자원에 대한 액세스 권한을 수신(단계 514)하고, 클라이언트측 처리를 마친다.

[0056] 디지털 서명이 생성되고 검증되는 방식은 본 발명의 범주에 영향을 미치지 않으며 공지되어 있는 표준의 또는 적절한 처리에 따라 달라질 수 있다. 예를 들어, 클라이언트측 처리는 이전에 설정된 SSL 세션을 통해서 단계별 인증서 기반 인증 처리를 수행한다는 서버의 판정에 응답하여 클라이언트의 브라우저가 내장된 애플렛을 갖는 HTML 페이지를 수신하면 발생할 수 있다. 브라우저는 웹 페이지를 처리하고, 애플렛을 실행시킬 수 있는데, 이 애플렛은 클라이언트 상의 파일과 같은 키 데이터 저장소 식별자와, 이와 함께 키 데이터 저장소를 여는 패스워드를 사용자가 입력하게 할 수 있다. 애플렛이 사용자로 하여금 동작시키게 하는 수단은 본 발명의 구현예에 따라 달라질 수 있다. 애플렛은 진행 중인 요청에 대한 디지털 서명 생성이 필요한 지를 나타내는 웹 페이지를 브라우저 윈도우 내에서 사용자에게 나타내게 하고, 표시되는 웹 페이지는 사용자가 디지털 서명 요청을

승인하거나 승인 거부하게 하는 OK 버튼 및 취소 버튼을 가질 수 있다. 또한, 표시되는 웹 페이지는 서명되는 검사 데이터를 반복해서, 사용자가 검사 데이터를 검토할 수 있게 된다.

[0057] 전형적으로, 키 데이터 저장소가 비동기식 암호화 기능을 위한 개인/공개 키쌍 중 개인키를 유지한다. 키 데이터 저장소는 각종 개체, 예를 들면, 브라우저 애플리케이션, 애플렛 등 클라이언트 운영 체제 의해 관리될 수 있다. 브라우저는 암호화 정보의 사용에 관한 각종 기준을 고수할 수 있다. 예를 들어, "PKCS #7: Cryptographic Message Syntax", RFC(Request for commnets)2315, Internet Engineering Task Force(IETF)는 데이터에 부가되는 암호, 예컨대 디지털 서명 및 디지털 봉합을 가질 수 있는 데이터에 대한 일반적인 신텍스를 기술하는 PKCS(Public Key Cryptographic System) 사양이다. 또 다른 예로서, "PKCS # 11P: Cryptographic Tocken Interface Standard". RSA Security Inc.는 암호 정보를 유지하고 암호화 기능을 수행하는 장치를 위한 API(application programming interface)를 기술하는 PKCS 사양이다.

[0058] 사용자가 요청한 정보를 입력하고 사용자가 사용자의 개인키의 사용을 승인한다고 나타낸 후에, 애플렛은 디지털 서명을 바람직하게는 W3C(World Wide Web Consortium)에 의해 표준화된 XML 디지털 서명의 형태로 생성한다. 나중에 검증될 데이터 아이템의 세트, 소위 "서명된 정보"에 대해 적절한 서명 알고리즘을 적용함으로써 디지털 서명이 생성되며, 이러한 시나리오에서, 서명되는 데이터는 검사 데이터를 최소로 포함할 것이다. XML 서명은 또한 디지털 서명을 검증하기 위해 사용되어야 하는 사용자의 공개 키 인증서를 포함할 수 있는 "키 정보"를 포함한다. 그 후, 애플렛은 웹 서버에 XML 서명을 전송하고, 디지털 서명을 생성하는 처리를 완료한다.

[0059] 본 발명의 유리한 점은 위에서 제공하는 상세한 설명의 견지에서 명백하다. 본 발명은 SSL 세션이 하위 수준 비 인증서 기반 인증 절차, 예컨대 사용자명/패스워드 조합 인증 절차를 위해 클라이언트와 서버 사이에서 설정된, 상호 인증되어 활성화된 SSL 세션을 유지하면서, 하위 수준의 비 인증서 기반 인증 절차로부터 상위 수준의 인증서 기반 인증 절차로의 보안 강화 동작을 제공한다.

[0060] 본 발명은 서버측 인증 서비스가 기존의 SSL 세션을 통해서 사용자 또는 사용자의 클라이언트 장치에 대한 인증서 기반 인증 절차를 수행하게 함으로써 이러한 문제에 대한 해결책을 제공한다. 인증 서비스는 필요하면, 기존의 SSL 세션을 통해서 클라이언트로 실행 가능한 모듈을 다운로드한다. 그 후, 실행 가능하나 모듈은 클라이언트측 디지털 인증서를 이용하여 디지털 서명을 생성하고, 디지털 서명은 이전에 설정된 SSL 세션을 통해 리턴된다. 인증서 기반 인증 절차는, 인증 서비스가 디지털 서명을 검증한 후에 완료된다. 이러한 방식으로, 인증 서비스는 기존의 SSL 세션을 빠져나가거나 재조정할 필요 없이 인증서 기반 인증으로 보안을 강화할 수 있다.

[0061] 본 발명은 독립적으로 기능하는 데이터 처리 시스템의 문맥으로 기술되었으나, 당업자라면, 본 발명의 처리들이 실제로 분산을 수행하기 위해 사용되는 특정 유형의 신호 보유 매체와 상관없이 컴퓨터 판독 가능 매체 내의 인스트럭션의 형태 등의 형태로 분산될 수 있다는 것을 이해할 수 있을 것이다. 컴퓨터 판독 가능 매체의 예에는, EPROM, ROM, 테이프, 플로피 디스크, 하드 디스크 드라이브, RAM 및 CD-ROM 및 디지털 및 아날로그 통신 링크와 같은 전송 유형 매체가 있다.

[0062] 본 방법은 전체적으로 원하는 결과로 이르는 단계들의 자체 시퀀스인 것으로 구상된다. 이들 단계는 물리적 신호의 물리적 조작을 필요로 한다. 보통 이들 신호는 저장되거나, 전달되거나, 결합되거나, 비교되고, 그렇지 않으면 조작되는 전기 또는 자기 신호의 형태를 가진다. 일반적으로 이러한 신호를 가리키기 위해, 비트, 값, 파라미터, 아이템, 요소, 대상물, 심볼, 문자, 용어, 번호 등을 주로 사용하는 것이 편리하다. 그러나, 모든 이러한 용어 및 이와 유사한 용어는 적절한 물리적 신호와 연관되어 있으며, 이러한 신호에 붙여지는 편리한 라벨일 뿐임을 유념하라.

[0063] 본 발명의 상세한 설명은, 설명을 목적으로 제공되었을 뿐 개시한 실시예에 제한을 두려는 것이 아니다. 당업자에게는 다수의 수정 및 변형예가 자명할 것이다. 실시예는 본 발명의 원리와 그 실제 응용예를 설명하고, 당업자가 본 발명을 이해해서, 다른 구상 용도에 적합하게 각종 수정예를 이용하여 각종 실시예를 구현할 수 있도록 하기 위해 선택되었다.

도면의 간단한 설명

[0010] 본 발명의 신규한 특징으로 사료되는 특성은 이하 청구의 범위에 설정되어 있다. 다음 상세한 설명을 이하 도면과 연결하여 판독하면 본 발명과, 그 목적 및 이점을 보다 쉽게 이해할 수 있을 것이다.

[0011] 도 1a는 각각 본 발명을 구현할 수 있는 전형적인 데이터 처리 시스템의 네트워크를 도시하는 도면,

[0012] 도 1b는 본 발명이 구현될 수 있는 데이터 처리 시스템 내에서 사용할 수 있는 전형적인 컴퓨터 아키텍처를 도

시하는 도면,

[0013] 도 1c는 클라이언트가 서버에 있는 보호 자원을 액세스하려 할 때 사용할 수 있는 전형적인 컴퓨터 아키텍쳐를 도시하는 도면,

[0014] 도 1d는 복수의 인증 서버를 포함하는, 전형적인 기업 도메인용 데이터 처리 시스템을 도시하는 블록도,

[0015] 도 2는 본 발명에 따라 단계별 인증 처리를 포함하도록 확장된 인증 서비스를 나타내는 블록도,

[0016] 도 3은 상호 인증되어 활성화된 SSL 세션을 유지하며 하위 레벨 비 인증서 기반 인증 절차로부터 상위 레벨 인증서 기반 인증 절차로의 보안 강화 처리를 나타내는 순서도,

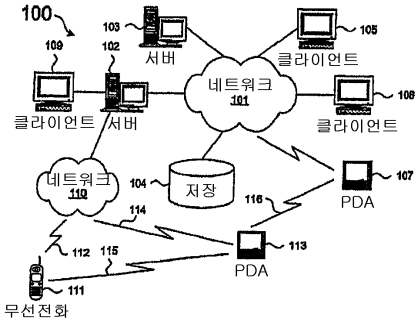
[0017] 도 4는 본 발명의 일 실시예에 따라, 단계별 인증서 기반 인증 동작을 위한 서버에서의 특정 절차에 대한 세부사항들을 더 나타내는 순서도,

[0018] 도 5는 본 발명의 일 실시예에 따라 단계별 인증서 기반 인증 동작을 위한 클라이언트에서의 처리를 나타내는 순서도.

도면

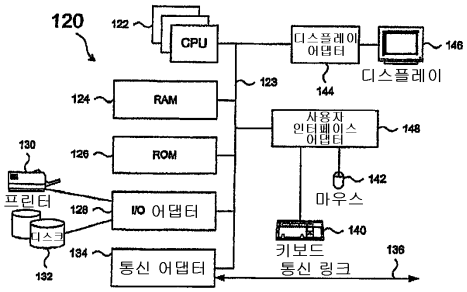
도면1a

(종래기술)



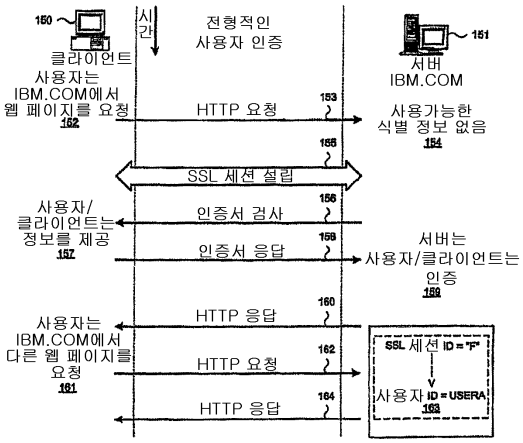
도면1b

(종래기술)



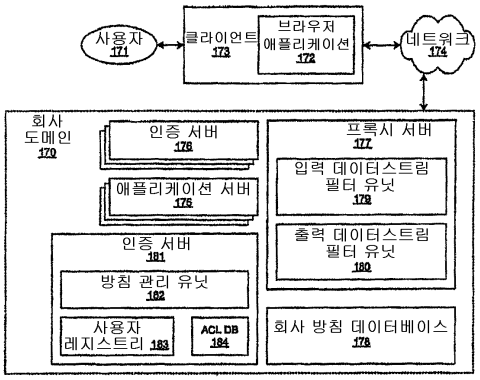
도면1c

(종래기술)

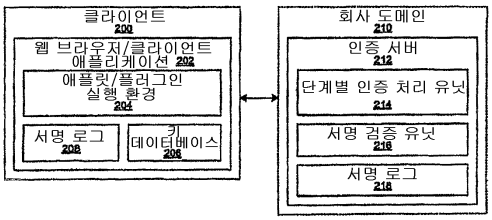


도면1d

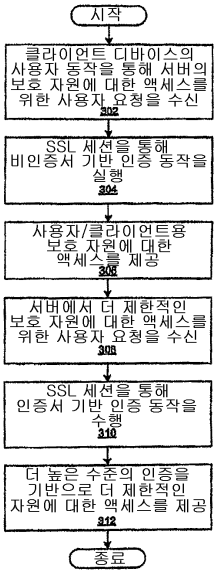
(종래기술)



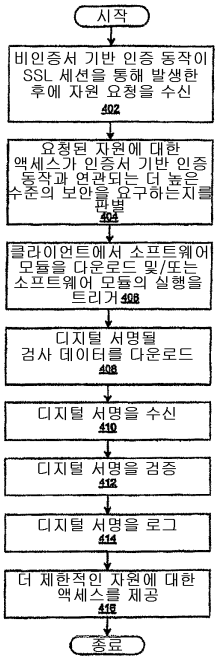
도면2



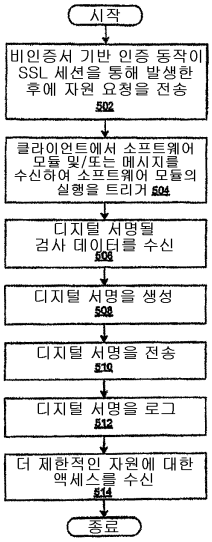
도면3


시작
클라이언트 디바이스의 사용자 동작을 통해 서버의 보호 자원에 대한 액세스를 위한 사용자 요청을 수신
302
SSL 세션을 통해 비인증서 기반 인증 동작을 실행
304
사용자/클라이언트용 보호 자원에 대한 액세스를 제공
306
서버에서 더 제한적인 보호 자원에 대한 액세스를 위한 사용자 요청을 수신
308
SSL 세션을 통해 인증서 기반 인증 동작을 수행
310
더 높은 수준의 인증을 기반으로 더 제한적인 자원에 대한 액세스를 제공
312
종료

도면4


시작
비인증서 기반 인증 동작이 SSL 세션을 통해 발생한 후에 자원 요청을 수신
402
요청된 자원에 대한 액세스가 인증서 기반 인증 동작과 연관되는 더 높은 수준의 보안을 요구하는지를 판별
404
클라이언트에서 소프트웨어 모듈을 다운로드 및/또는 소프트웨어 모듈의 실행을 트리거
408
디지털 서명될 검사 데이터를 다운로드
406
디지털 서명을 수신
410
디지털 서명을 검증
412
디지털 서명을 로그
414
더 제한적인 자원에 대한 액세스를 제공
416
종료

도면5


시작
비인증서 기반 인증 동작이 SSL 세션을 통해 발생한 후에 자원 요청을 전송
502
클라이언트에서 소프트웨어 모듈 및/또는 메시지를 수신하여 소프트웨어 모듈의 실행을 트리거
504
디지털 서명될 검사 데이터를 수신
506
디지털 서명을 생성
508
디지털 서명을 전송
510
디지털 서명을 로그
512
더 제한적인 자원에 대한 액세스를 수신
514
종료