(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2009년07월07일
(11) 등록번호 10-0906119
(24) 등록일자 2009년06월29일

(51) Int. Cl.
G06F 15/16 (2006.01) *G06F 15/00* (2006.01)
(21) 출원번호 10-2005-7018432
(22) 출원일자 2004년04월15일
심사청구일자 2006년12월29일
(85) 번역문제출일자 2005년09월29일
(65) 공개번호 10-2006-0015714
(43) 공개일자 2006년02월20일
(86) 국제출원번호 PCT/GB2004/001629
(87) 국제공개번호 WO 2004/104902
국제공개일자 2004년12월02일
(30) 우선권주장
10/443,675 2003년05월22일 미국(US)
(56) 선행기술조사문헌
URL:http://web.archive.org/web/20030404014033/http://msdn.microshoft.com/msdnmag/issues/0600/websecure/default.aspx
URL:http://web.archive.org/web/20030423074148/http://www.hypermedic.com/php/redicrect.htm
전체 청구항 수 : 총 10 항 심사관 : 조기덕

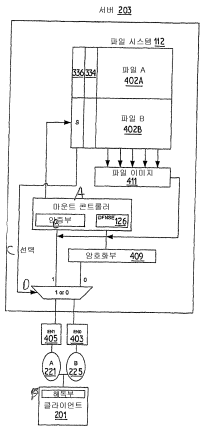
(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
케오한 수산 마리
미국 78704 텍사스주 오스틴 브랙켄릿지 스트리트 1911
맥브리어티 제랄드 프란시스
미국 78759 텍사스주 오스틴 베이릿지 코브 10709
(뒷면에 계속)
(74) 대리인
김원준, 김창세, 장성구

(54) 분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법및 시스템

(57) 요 약

네트워크화된 파일 시스템 상에서 감지 가능한 파일에 대한 액세스가 요구되는 경우 파일 시스템의 증강된 마운트(mount) 보안성을 동적으로 구현하는 보안성 프로토콜이 제공된다. 클라이언트 시스템의 사용자가 특별히 태그된 감지 가능한 파일을 액세스하도록 시도하는 경우, 파일 시스템을 호스트하는 서버는 현재의 마운트를 종료시키고, 서버 포트가 보다 안전한 포트를 통해 클라이언트로부터 리마운트(remount)를 채택하도록 재구성하는 소프트웨어 코드를 실행한다. 서버 포트를 재구성한 서버에는 클라이언트의 IP 어드레스가 제공되고 리마운트 동작 동안 IP 어드레스를 매칭시킨다. 인증된 사용자가 높은 비용의 암호화 및 다른 리소스 집약적인 보안 특성에 의해 서버에 부담주지 않고 감지 가능한 파일에 대한 액세스가 허용되도록 이음매 없는 방식으로 보안 마운트로의 스위칭이 완료된다. 사용자에게는 엄청난 지연이 경험되지 않는 한편, 클라이언트 시스템으로의 송신 동안 인증되지 않은 포착으로부터 감지 가능한 파일이 보호된다.

대 표 도



(72) 발명자

물렌 샤운 페트릭

미국 78610 텍사스주 부다 컨트리 오크스 39

무릴로 제시카 켈리

미국 78634 텍사스주 휴토 컨트리 로드 109 980

시에 조니 멩-한

미국 78731 텍사스주 오스틴 업벨리 런 5908

특허청구의 범위

청구항 1

적어도 하나의 제 1 파일의 송신을 위한 보안성을 제공하는 방법으로서, (1) 기설정된 액세스 승인부를 갖는 상기 적어도 하나의 제 1 파일이 저장되는 저장 매체와, (2) 데이터 프로세싱 시스템을 외부 클라이언트 시스템에 접속하는 적어도 제 1 표준 포트 및 제 2 보안 포트와, (3) 상기 제 1 표준 포트 및 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신을 선택적으로 라우팅(routing)하는 로직과, (4) 상기 클라이언트 시스템에 의한 마운트(mount)를 지원하기 위해 상기 제 1 표준 포트 및 상기 제 2 보안 포트를 구성하는 재구성 로직을 구비한 상기 데이터 프로세싱 시스템에서 이용하는 방법에 있어서,

상기 외부 클라이언트 시스템에 의해 상기 적어도 하나의 제 1 파일을 액세스하기 위한 요구에 응답하여, 상기 적어도 하나의 제 1 파일의 상기 기설정된 액세스 승인부를 체크하는 단계와,

보안 액세스를 나타내는 상기 적어도 하나의 제 1 파일의 상기 기설정된 액세스 승인부가 상기 적어도 하나의 제 1 파일에 대해 요구되는 경우, 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신을 외부 클라이언트 시스템에 동적으로 라우팅하는 단계를 포함하되,

상기 동적으로 라우팅하는 단계는,

상기 클라이언트 시스템으로부터 수신된 리마운트(remount) 동작을 지원하도록 상기 제 2 보안 포트를 처음 구성하는 단계와,

상기 클라이언트 시스템에 의해 상기 제 1 표준 포트 상에서 현재의 마운트를 종료시키는 단계와,

상기 제 2 보안 포트 상에서 세션의 이음매 없는 연속을 가능하게 하도록 상기 현재의 마운트의 세션 파라미터를 저장하는 단계를 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 2

청구항 2은(는) 설정등록료 납부시 포기되었습니다.

제 1 항에 있어서,

규칙적인 액세스를 나타내는 상기 기설정된 액세스 승인부가 충분한 경우 상기 제 1 표준 포트를 통해 상기 적어도 하나의 제 1 파일의 상기 송신을 라우팅하는 단계를 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 표준 포트를 통해 상기 데이터 프로세싱 시스템의 제 1 마운트(first mount)를 인에이블링하는 단계와,

상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하는 경우에만 상기 제 2 보안 포트를 통해 상기 데이터 프로세싱 시스템의 제 2 마운트(second mount)를 인에이블링하는 단계를 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 4

제 1 항에 있어서,

상기 데이터 프로세싱 시스템은 상기 제 2 보안 포트와 연관된 암호화 모듈을 더 포함하며,

상기 동적으로 라우팅하는 단계는 상기 암호화 모듈을 이용하여 상기 적어도 하나의 제 1 파일을 처음 암호화하는 단계를 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 5

제 4 항에 있어서,

상기 제 2 보안 포트를 처음 구성하는 단계 및 상기 현재의 마운트의 세션 파라미터를 저장하는 단계는,

상기 클라이언트 시스템의 IP 어드레스를 검색하는 단계와,

상기 제 2 보안 포트의 구성에 상기 IP 어드레스를 위치시키는 단계-상기 제 2 보안 포트는 상기 클라이언트 시스템으로부터의 리마운트 동작을 자동으로 인식하고, 상기 클라이언트 시스템과의 세션을 재확립함-를 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 6

청구항 6은(는) 설정등록료 납부시 포기되었습니다.

제 1 항에 있어서,

상기 기설정된 액세스 승인부는 상기 적어도 하나의 제 1 파일에 링크된 메타데이터 내의 비트이며,

상기 적어도 하나의 제 1 파일이 보안 액세스를 필요로 하는 지를 평가하도록 상기 비트의 값을 판독하는 단계를 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 7

청구항 7은(는) 설정등록료 납부시 포기되었습니다.

제 1 항에 있어서,

상기 기설정된 액세스 승인부는 보안 액세스를 통해 상기 적어도 하나의 제 1 파일을 액세스하도록 허용되는 특정 사용자의 식별을 포함하며,

상기 클라이언트 시스템의 임의의 사용자를 상기 적어도 하나의 제 1 파일을 액세스할 수 있도록 승인된 상기 특정의 사용자와 비교하는 단계와,

상기 임의의 사용자가 상기 특정 사용자 중 한 명인 경우, 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신 재라우팅(re-routing)을 자동으로 초기화하는 단계를 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 8

청구항 8은(는) 설정등록료 납부시 포기되었습니다.

제 1 항에 있어서,

상기 제 1 표준 포트는 제 1 비보안(unsecured) 네트워크를 통해 상기 클라이언트 시스템에 접속하고, 상기 제 2 보안 포트는 제 2 보안 네트워크를 통해 상기 클라이언트 시스템에 접속하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 9

제 1 항에 있어서,

상기 데이터 프로세싱 시스템은, 상기 제 1 표준 포트를 상기 클라이언트 시스템에 접속하는 제 1 서브네트(first subnet) 및 상기 제 2 보안 포트를 상기 클라이언트 시스템에 접속하는 제 2 서브네트(second subnet)를 갖는 네트워크 내의 서버이고,

상기 적어도 하나의 제 1 파일은 파일 시스템 내에 저장되며,

상기 체크 단계는 상기 파일 시스템을 액세스하고 상기 적어도 하나의 제 1 파일을 위치시키는 단계를 포함하고,

상기 라우팅 단계는, 상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하는 경우 상기 제 2 서브네트를 통해 상기 적어도 하나의 제 1 파일을 송신하고, 상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하지 않는 경우 상기 제 1 서브네트를 통해 상기 적어도 하나의 제 1 파일을 송신하는 단계를 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 방법.

청구항 10

적어도 하나의 제 1 파일의 송신에 대한 보안성을 제공하는 시스템으로서, (1) 기설정된 액세스 승인부를 갖는 상기 적어도 하나의 제 1 파일이 저장되는 저장 매체와, (2) 데이터 프로세싱 시스템을 외부 클라이언트 시스템에 접속하는 적어도 제 1 표준 포트 및 제 2 보안 포트와, (3) 상기 제 1 표준 포트 및 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신을 선택적으로 라우팅하는 로직을 구비하는 상기 데이터 프로세싱 시스템에서 이용하는 시스템에 있어서,

상기 외부 클라이언트 시스템에 의해 상기 적어도 하나의 제 1 파일을 액세스하기 위한 요구에 응답하여, 상기 적어도 하나의 제 1 파일의 상기 기설정된 액세스 승인부를 체크하는 로직과,

상기 클라이언트 시스템에 의한 마운트를 지원하도록 상기 제 1 표준 포트 및 상기 제 2 보안 포트를 구성하는 재구성 로직과,

보안 액세스를 나타내는 상기 적어도 하나의 제 1 파일의 상기 기설정된 액세스 승인부가 상기 적어도 하나의 제 1 파일에 대해 요구되는 경우, 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신을 외부 클라이언트 시스템에 동적으로 라우팅하는 로직을 포함하되,

상기 동적으로 라우팅하는 로직은,

상기 클라이언트 시스템으로부터 수신된 리마운트 동작을 지원하도록 상기 제 2 보안 포트를 처음 구성하는 로직과,

상기 클라이언트 시스템에 의해 상기 제 1 표준 포트 상에서 현재의 마운트를 종료시키는 로직과,

상기 제 2 보안 포트 상에서 세션의 이음매 없는 연속을 가능하게 하도록 상기 현재의 마운트의 세션 파라미터를 저장하는 로직을 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 11

청구항 11은(는) 설정등록료 납부시 포기되었습니다.

제 10 항에 있어서,

규칙적인 액세스를 나타내는 상기 기설정된 액세스 승인부가 충분한 경우 상기 제 1 표준 포트를 통해 상기 적어도 하나의 제 1 파일의 상기 송신을 라우팅하는 로직을 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 12

제 10 항에 있어서,

상기 제 1 표준 포트를 통해 상기 데이터 프로세싱 시스템의 제 1 마운트를 인에이블링하는 로직과,

상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하는 경우에만 상기 제 2 보안 포트를 통해 상기 데이터 프로세싱 시스템의 제 2 마운트를 인에이블링하는 로직을 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 13

제 10 항에 있어서,

상기 데이터 프로세싱 시스템은 상기 제 2 보안 포트와 연관된 암호화 모듈을 더 포함하며,

상기 동적으로 라우팅하는 로직은 상기 암호화 모듈을 이용하여 상기 적어도 하나의 제 1 파일을 처음 암호화하는 로직을 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 14

제 10 항에 있어서,

상기 제 2 보안 포트를 처음 구성하는 로직 및 상기 현재의 마운트의 세션 파라미터를 저장하는 로직은,

상기 클라이언트 시스템의 IP 어드레스를 검색하는 로직과,

상기 제 2 보안 포트의 구성에 상기 IP 어드레스를 위치시키는 로직-상기 제 2 보안 포트는 상기 클라이언트 시스템으로부터의 리마운트 동작을 자동으로 인식하고, 상기 클라이언트 시스템과의 세션을 재확립함-을 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 15

청구항 15은(는) 설정등록료 납부시 포기되었습니다.

제 10 항에 있어서,

상기 기설정된 액세스 승인부는 상기 적어도 하나의 제 1 파일에 링크된 메타데이터 내의 비트이며,

상기 적어도 하나의 제 1 파일이 보안 액세스를 필요로 하는지를 평가하도록 상기 비트의 값을 판독하는 것을 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 16

청구항 16은(는) 설정등록료 납부시 포기되었습니다.

제 10 항에 있어서,

상기 기설정된 액세스 승인부는, 보안 액세스를 통해 상기 적어도 하나의 제 1 파일을 액세스하도록 특정의 사용자가 허용되는 식별부를 포함하며,

상기 클라이언트 시스템의 임의의 사용자를 상기 적어도 하나의 제 1 파일을 액세스할 수 있도록 승인된 상기 특정의 사용자와 비교하는 단계와,

상기 임의의 사용자가 상기 특정의 사용자 중 한 명인 경우, 상기 제 2 보안 포트를 통해 상기 적어도 하나의 제 1 파일의 송신 재라우팅을 자동으로 초기화하는 로직을 더 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 17

청구항 17은(는) 설정등록료 납부시 포기되었습니다.

제 10 항에 있어서,

상기 제 1 표준 포트는 제 1 비보안 네트워크를 통해 상기 클라이언트 시스템에 접속하고, 상기 제 2 보안 포트는 제 2 보안 네트워크를 통해 상기 클라이언트 시스템에 접속하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 18

제 10 항에 있어서,

상기 데이터 프로세싱 시스템은, 상기 제 1 표준 포트를 상기 클라이언트 시스템에 접속하는 제 1 서브네트 및 상기 제 2 보안 포트를 상기 클라이언트 시스템에 접속하는 제 2 서브네트를 갖는 네트워크 내의 서버이고,

상기 적어도 하나의 제 1 파일은 파일 시스템 내에 저장되며,

상기 체크 로직은 상기 파일 시스템을 액세스하고 상기 적어도 하나의 제 1 파일을 위치시키는 수단을 포함하고,

상기 라우팅 로직은, 상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하는 경우 상기 제 2 서브네트를 통해 상기 적어도 하나의 제 1 파일을 송신하고, 상기 적어도 하나의 제 1 파일이 보안 액세스를 요구하지 않는 경우 상기 제 1 서브네트를 통해 상기 적어도 하나의 제 1 파일을 송신하는 수단을 포함하는

분배 파일 시스템 네트워크에 있어서의 보안성 제공 시스템.

청구항 19

삭제

청구항 20

삭제

명 세 서

기 술 분 야

<1> 본 발명은 전반적으로는 네트워크 시스템에 관한 것으로서, 구체적으로는, 분배 파일 시스템에 관한 것이다. 보다 구체적으로, 본 발명은 분배 파일 시스템에 대한 액세스를 위한 보안 특성에 관한 것이다.

배 경 기 술

<2> 유닉스 운영 체제(오퍼레이팅 시스템 : OS)의 지원 버전과 같은 범용 컴퓨팅 시스템에서, 애플리케이션은 파일 시스템을 포함하는 운영 체제 서비스 세트에 의해 디스크 드라이브 상에 저장된 데이터를 액세스할 수 있다(유닉스는 등록된 상표로서, 오픈 그룹(Open Group)을 통해 독점적으로 허가되어 있음). 파일 시스템은 파일의 큰 집합체를 개별적인 파일 및 파일 디렉토리로 구성하고 이들 파일을 디스크와 같은 저장 디바이스에 매핑하는 컴퓨터 시스템에 의해 채용될 수도 있다. 파일 시스템은 2개의 주요한 구성 요소로 이루어지는데, 즉, 파일의 물리적 표시를 제어하는 프로그램과, 디스크 상에 저장되는 파일 자체로 이루어진다.

<3> 분배 컴퓨팅 환경에서, 통신 네트워크 또는 다른 연결 설비에 의해 다수의 컴퓨팅 시스템이 상호 접속될 수 있고 분배 파일 시스템에 의해 파일을 공유할 수 있다. 파일 시스템 익스포터(exporter)는 통상적으로 서버 노드(파일 시스템 데이터를 포함하는 디스크에 대한 액세스를 제어하는 컴퓨팅 시스템) 상에서 실행되는 반면, 파일 시스템 임포터(importer)는 통상적으로 클라이언트 노드(디스크 상에서 파일을 액세스하도록 이용된 다른 컴퓨팅 시스템) 상에서 실행된다. 클라이언트 노드 상에서 사용자에 의해 이루어진 공유 파일에 대한 액세스는 "원격" 액세스로서 지칭된다. 서버 노드 상에서 사용자에 의해 이루어진 공유 파일에 대한 액세스는 "로컬(local)" 액세스로서 지칭된다.

<4> 네트워크 파일 시스템은 네트워크의 서버 또는 노드 상에서 공유되며, 서버 또는 노드는 통상적으로 네트워크에 원격 링크되는 클라이언트 터미널(즉, 사용자 컴퓨터)로부터 액세스 가능하다. 실질적인 링크는 표준 이더넷 기반 근거리 통신망(LAN)에서와 같은 유선 링크일 수도 있고, 블루투스(Bluetooth) 가상 전용 네트워크(VPN)와 같은 무선 링크일 수도 있다. 클라이언트 터미널을 거쳐서 파일 시스템을 액세스하는 프로세스는 "파일 시스템의 마운팅(mounting)"라고 지칭된다. 파일 시스템이 마운트(mount)되는 경우, 파일 시스템의 제어 프로그램은 파일 시스템 객체의 레이아웃에 관한 디스크로부터 특정의 정보를 판독한다. 이러한 정보로부터, 파일 시스템은 "가상 시스템" 또는 Vfs로서 알려진 데이터 구조를 구성한다. 파일이 오픈(open)되거나, 액세스 가능해질 때마다, 파일 시스템은 vfs에 연결되는 "vnode"로서 지칭되는 데이터 구조를 생성한다.

<5> 각각의 vnode는 주어진 파일에 관한 정보를 포함하고 물리적인 파일 시스템 데이터 구조에 대한 레퍼런스(references)를 포함한다. 물리적인 파일 시스템 데이터 구조는 파일의 소유자, 파일의 크기, 파일의 생성 날짜 및 시간, 디스크 상에서의 파일 블록의 위치와 같은 정보를 포함한다. 파일 시스템은 메타데이터(meta-

data)라 호칭되는 내부 데이터를 포함하여, 파일을 관리한다. 메타데이터는 파일의 각 데이터 블록이 어디에 저장되는지, 파일의 메모리 수정 버전이 어디에 저장되는지, 파일의 승인 및 소유자를 나타내는 데이터를 포함할 수 있다.

<6> 감지 가능한 정보를 갖는 일부 정보를 포함하는, 파일/문서를 전기적으로 저장하고 이후에 검색하기 위해 원격/네트워크 액세스 가능한 분배 파일 시스템을 이용하는 회사가 점점 증가함에 따라, 분배 파일 시스템의 보안성이 점점 중요성을 갖게 된다. 표준의 IP 보안성(IPSec) 스위트(suite)가 도입되어 2개의 주요한 보안 특성, 즉 인증성 및 암호화성을 제공한다. 즉, IPSec은 송신기 및 수신기 이들 기기가 실질적으로 요구하고자 하는 것을 보장하고, 데이터가 공중에서 스크램블링되도록 하여 방해를 받는 경우 IPSec은 데이터가 판독 불가능하도록 할 것이다.

<7> 따라서 대부분의 시스템은 통상 초기 마운트 동안 사용자 패스워드 등을 검증하는 것을 포함하는 사용자의 인증을 필요로 한다. 그러나, 패스워드 보호 및 유사한 보안 수단은 크래킹(cracking)에 노출되기 쉽다고 하는 단점이 널리 알려져 있고 용이하게 타협될 수 있으며, 당업계에서는 일단 파일 시스템에 대한 일반적인 액세스가 획득되면 패스워드 보호 시스템은 감지 가능한 파일에 대한 보호 기능을 거의 제공하지 않는 것으로 인식되고 있다.

<8> 보다 진보된 해커는, 허가된 마운트 동안 송신부에 태핑(tapping)하고 파일 시스템으로부터 클라이언트 시스템으로 송신되는 것처럼 데이터를 간단히 복제함으로써, 파일 시스템 상에 저장된 파일에 대해 액세스하는데 또한 장점을 갖고 있다. 이것은 대부분의 패스워드 보호 분배 파일 시스템에 의해, 일단 몇 가지 레벨의 보안 로그인(패스워드 검증 등)이 완료되면, 파일 시스템으로부터 파일의 실질적인 송신이 명확한 텍스트에서 발생하기 때문에, 생기는 것이다. 따라서, 송신부가 매우 감지 가능한 데이터를 포함하는 경우, 송신 동안 간단하게 파일을 복제함으로써 명확한 텍스트 데이터가 입수 가능하지 않도록 하는 것을 보장하도록, 별도의 보안 수단이 요구된다.

<9> 이러한 최근의 방법을 통해 감지 가능한 정보의 보안성이 타협될 수 있는 용이함은, 파일 시스템을 마운트/액세스하기 위해 허가된 사용자에 의해 이용되는 매체 상에 어느 정도는 의존한다. 예를 들면, 무선 액세스/송신은 통상 해당 와이어 풀(wired-full)(무선) 네트워크 매체를 도청하고 크래킹하는 것이 더 용이하다. 그러나, 표준 이더넷이라 하더라도 검출부 없이 용이하게 침해될 수 있고, 따라서, 표준 이더넷도 또한 감지 가능한 데이터를 라우팅(routing)하기 위해서는 안전하지 않은 옵션이다.

<10> 전술한 바와 같이, 당업계에서는 파일 시스템의 마운트 동안 모든 송신된 데이터에 대해 강하게 암호화성을 부여함으로써 송신 매체 상에서 보안을 위한 필요성이 증가하는 반응을 보여 왔다. 현재, 클라이언트 시스템/노드 및 파일 시스템을 호스팅하는 서버 사이의 송신을 위한 보안성(예를 들어, 무선 트랜스포트 층 보안성)을 제공하도록 설계된 몇 가지의 알고리즘 및 표준안이 존재한다. 강력한 암호화를 이용하는 것은 모든 트래픽에 대해 클라이언트 시스템 및 서버에 과중한 처리 부담이 가해질 것을 필요로 한다. 이들 파일 시스템에 대한 액세스를 위해 시스템 폭의 암호화를 구현하고자 하는 회사에 의해 시스템의 전체 성능이 저하하고, 막대한 비용이 초래된다. 트래픽의 대부분이 해당 레벨의 보안성(예를 들어, 감지 불가능한 정보/파일)을 필요로 하지 않을 수 있다 하더라도, 암호화는 통신 메커니즘에 내장되어 클라이언트 시스템 및 서버 사이의 모든 트래픽에 적용될 것이다.

<11> 회사가 모바일(mobile)일 수도 있는 사용자에 대한 원격 액세스를 제공하고 네트워크를 원격 접속하고자 함에 따라, 파일 시스템을 액세스하기 위한 무선 시스템의 이용이 증가하고 있다. 그러나, 무선 접속은 유선 접속보다 크래킹에 영향을 보다 쉽게 받는다. 몇몇 무선 사용자는 WTLS를 이용하지만, 이러한 보안 특성은, 보안 레벨이 상대적으로 약한 것으로 알려져 있다. 하나의 해결책에서는 클라이언트의 다수가 토크 링을 통해 파일 시스템을 액세스하고 있는 중일 때라도, 감지 가능한 데이터를 액세스하기 위해 가상 전용 네트워크(VPN) 데이터의 캡슐화/암호화를 필요로 한다. 이러한 VPN 데이터 캡슐화는, 또한 서버가 모든 데이터를 암호화하고 해독함에 따라 서버의 속도에 부정적으로 영향을 줄 수 있다.

<12> IP 어드레스 또는 서브네트를 인식하고 특정의 서브네트 상에서 암호화만을 필요로 하기 위해 VPN 또는 VPN 상의 서버를 구성하는 것이 또한 가능하다. 이러한 해결책에 의한 하나의 문제점은, 분배 파일 시스템 서버의 집행자가 네트워크 내에 있지 않은 모든 무선 노드를 반드시 인지하여야 한다는 것이다. 무선 네트워크가 이들의 디파트먼트(department) 내의 구성에 의해 셋업되는 경우, 서브네트가 IP 어드레스의 VPN 리스트에 부가되도록 서버 집행자는 무선 네트워크를 인지하도록 할 필요가 있다.

MSDN magazine(2000년 6월호)에 게재된 Keith Brown의 "Web Security: Putting Secure Front End on your COM+ Distributed Applications"에는 HTTPS 프로토콜이 사용될 것을 요구하는 IIS 메타베이스의 사용이 개시되어 있다. IIS 메타베이스는 클라이언트가 HTTPS 프로토콜을 사용할 것을 지시하는 데 사용된다.

<13> 전술한 관점에서, 본 발명은 분배 파일 시스템 상에서 감지 가능한 파일에 대한 액세스가 요구되는 경우 증강된 마운트 보안성을 동적으로 구현하는 방법, 시스템 및 데이터 프로세싱 시스템을 갖는 것이 바람직할 것이라는 것을 인지하여 이루어진 것이다. 진행 중인 세션 동안 감지 가능한 파일/데이터가 거의 액세스될 때마다 보안 마운트를 자동으로 제공하는 방법 및 시스템은 긍정적인 개선책이 될 것이다. 접속 해제 및 리마운트(re-mount) 인증 프로세스를 경험하지 않고 감지 가능한 파일에 대한 액세스를 허가된 사용자가 수신하는 한편, 보다 안전한 마운트를 통해 감지 가능한 파일을 라우팅함으로써 허가되지 않은 캡처(capture)로부터 감지 가능한 파일이 보호되도록 이음매 없는 방식으로 보안 마운트가 완료되는 경우 또한 바람직할 것이다.

<14>

발명의 상세한 설명

<15> 네트워크화된 파일 시스템 상에서 감지 가능한 파일에 대한 액세스가 요구되는 경우 파일 시스템의 증강된 마운트 보안성을 동적으로 구현하는 방법, 시스템 및 컴퓨터 프로그램 제품이 제공된다. 클라이언트 시스템은 파일 시스템의 파일에 대해 액세스를 위한 표준 마운트 및 인증 프로세스를 초기화한다. 클라이언트 시스템의 사용자가 특별히 태그된 감지 가능한 파일을 액세스하도록 시도하는 경우, 서버는 현재의 마운트를 종료시키는 소프트웨어 코드를 실행한다. 서버는 클라이언트와 연관된 IP 어드레스로부터 서버를 리마운트하기 위한 임의의 시도를 보안 포트에 대해 라우팅하도록 재구성된다. 세션이 서버에 의해서 종료되면, 클라이언트 시스템은 서버를 자동으로 리마운트하게끔 프로그래밍된다. 서버는 리마운트 동작 동안 클라이언트의 IP 어드레스를 인지하고 클라이언트를 보안 포트로 라우팅한다.

<16> 따라서 표준 마운트 상에서 초기화되는 진행 중인 세션 동안 감지 가능한 파일/데이터가 거의 액세스될 때마다 보안 마운트가 자동으로 제공된다. 그 다음에 허가된 사용자가, 사용자 초기화된 리마운트 및 인증 프로세스를 필요로 하는 막대한 지연 또는 가시적인 접속 해제를 경험하지 않고 감지 가능한 파일에 대한 액세스를 수신하도록 이음매 없는 방식으로 보안 마운트를 통한 라우팅이 완료된다. 한편으로 확립된 보다 안전한 마운트를 통해 감지 가능한 파일을 라우팅함으로써 허가되지 않은 캡처로부터 감지 가능한 파일이 보호된다.

<17> 본 발명은 이하 첨부 도면을 참조하여 기술되며, 단지 일례로서 기술될 것이다.

<18>

실 시 예

<25> 이하 첨부 도면, 특히 도 1의 (a)를 참조하면, 분배 파일 시스템을 호스트하는 서버나 분배 파일 시스템이 호스트되는 서버를 마운트하도록 이용된 클라이언트 시스템으로서 이용될 수 있는 컴퓨터 시스템의 블록도가 도시되어 있다. 컴퓨터 시스템(100)은 시스템 버스/상호배선(110)을 통해 접속된 프로세서(102) 및 메모리(104)를 포함한다. 컴퓨터 시스템(160)은 상호배선(110)에 결합되는 입/출력(I/O) 채널 콘트롤러(CC)(109)를 또한 포함한다. I/O CC(109)는 디스크의 리던던트 어레이(Redundant Array od Disk : RAID)(114)를 포함하여, I/O 디바이스(106)에 접속된다. RAID(114)는 프로세서에 의해 실행되는 애플리케이션에 의해 필요로 하는 바와 같이 메모리에 로드되는 인스트럭션 및 데이터를 저장한다. 예시적인 실시예에 따르면, RAID(114)는 파일 시스템(112)을 구성하는 복수의 파일에 대한 저장 매체를 제공한다.

<26> 컴퓨터 시스템(100)은 다른 디바이스 중에서, 유선 모뎀, 무선 모뎀, 이더넷 카드를 포함할 수 있는 네트워크 접속 디바이스(108)를 더 포함한다. I/O 디바이스(106) 및 네트워크 접속 디바이스(108)로/로부터의 액세스는, 필요로 하는 경우, 이하 더 기술되는 바와 같이, "보안" 경로/채널/포트를 통해 컴퓨터 시스템(100)으로/으로부터 마운트의 자동적인 재확립을 완료시키는 로직을 포함하는 I/O 채널 콘트롤러(I/O CC)(109)를 통해 라우팅된다.

<27> 컴퓨터 시스템(100)은 운영 체제(OS)(122), 파일 시스템 소프트웨어 애플리케이션(124), 마운트 코드(125), 분배 시스템 네트워크 보안성 확장부(DFNSE)(126)를 포함한다. 파일 시스템 소프트웨어 애플리케이션(124)은 파일 시스템(112)을 호스트하도록 컴퓨터 시스템(100)이 이용되는 경우, 파일 시스템(112)의 기본 액세스, 유지, 갱신을 제공한다.

<28> 클라이언트 시스템 내에서, 파일 시스템 소프트웨어 애플리케이션(124)은 마운트를 완료시키는 마운트 코드(125)의 클라이언트 버전 및 파일 시스템을 호스트하는 서버의 자동 리마운트를 포함한다. 예시적인 실시예에서, 자동 리마운트 프로세스는, 서버의 언마운트(unmount)를 완료시킨 클라이언트에 의하지 않고 서버에 의해 확립된 마운트가 파손/소실될 때마다 클라이언트 시스템에 의해 구현된다. 기술된 실시예에서, 서버는 현재의 마운트를 종료시키기 위한 FTN 커맨드를 송출할 수 있고 따라서 클라이언트로 하여금 서버의 리마운트를 초기화시키도록 한다. FTN 커맨드는 이후 보다 상세하게 설명되는 바와 같이, 특수한 보안성 보호를 필요로 하는 특정의 파일에 대한 액세스에 응답하여 송출된다.

<29> 다시 도 1의 (a)를 참조하여, 파일 시스템 소프트웨어 애플리케이션(124)을 설명하면, 서버 내에서 실행되는 경우, 파일 시스템 소프트웨어 애플리케이션(124)은 각종 사용자 및 클라이언트 시스템의 자격 정보를 수신하고, 유지하며, 검증하는 코드, 파일 시스템(112)을 유지하는 코드, 분배 파일 시스템 네트워크 보안 확장부(DFNSE)(126)라 불리우는, 보안성 소프트웨어 및 연관 응답을 선택적으로 초기화하는 코드를 포함한다. DFNSE(126)는 본 발명의 백본(backbone)이며, 도 3의 (a) 내지 (c) 및 도 4의 (a)를 참조하여 서버 상에서 DFNSE(126)의 실행이 기술된다. 기본 레벨에서, DFNSE(126)는 파일 시스템(112)의 특정 파일에 대해 어느 레벨의 보안 액세스가 승인/허가되는지, 및 본 발명의 증강된 보안 수단을 언제 초기화할 지를 결정한다.

<30> 이제 도 2를 참조하면, 분배 파일 시스템을 각각 호스트하거나 또는 액세스하는 서버 또는 클라이언트 기능을 제공하도록 유용하게 이용되는 도 1의 컴퓨터 시스템(100)과 유사하게 구성될 수 있는 다수의 상호 접속된 컴퓨터 시스템을 포함하는 일례의 네트워크가 도시되어 있다. 네트워크(200)는 3개 (이상의) 상호 접속된 서버(203) 상에서 호스트된 분배 파일 시스템(202)을 포함한다. 네트워크(200)는 네트워크 백본(210)을 거쳐 분배 파일 시스템(202)에 접속된 복수의 클라이언트 시스템(201)을 또한 포함한다. 네트워크 백본(210)은 이더넷 또는 토큰 링과 같은 네트워크 프로토콜에 따라 구성될 수 있는 하나 이상의 네트워크 접속 시스템(또는 서브네트워크)를 포함한다. 이들 서브네트워크는, 예를 들어, 유선이나 무선 근거리 통신망(LAN), 또는 인터넷과 같은 광역 네트워크(WAN)일 수도 있다. 부가적으로, 서브네트워크는 광 파이버 네트워크를 또한 포함할 수도 있다.

<31> 분배 파일 시스템(202)은 적어도 하나의 서버(203) 상에서 하나 이상의 포트(도시하지 않음)를 통해 네트워크 백본(210)에 직접 결합된다. 클라이언트 시스템(201)은 네트워크 백본(유선)에 직접 결합될 수도 있고, 또는 무선 안테나(207)로 도시된 무선 매체를 통해 통신 가능하게 접속될 수도 있다. 클라이언트 시스템(201)은 각각 상이한 레벨의 크래킹의 영향을 각각 받는, 각종 네트워크 구성 중 하나를 이용하는 각종 입수 가능한 매체 중 하나를 통해 분배 파일 시스템(202)을 액세스한다. 따라서, 클라이언트 시스템(201)은 비보안 무선 네트워크(227)를 통해 파일 시스템(203)을 액세스하여 마운트하거나, 혹은, 클라이언트 시스템(201)은 안전한 광 파이버 네트워크(225)를 이용하여 파일 시스템(252)을 마운트할 수도 있다. 본 발명을 간략하게 설명하기 위해, 무선 네트워크(227)는 암호화하지 않고, 표준의 비보안(non-secure) 네트워크로 가정되는 한편, 광 파이버 네트워크(225)는 암호화하고, 특수한 보안 접속으로 가정될 것이다. 각각의 접속은 파일 시스템(202)의 마운트가 지원되는 서버(203)에 대해 입수 가능한 포트 중 상이한 하나를 통해 라우팅된다.

<32> 도 1의 (b)는 파일 시스템(202)을 포함하는 파일을 보다 상세하게 도시한 파일 시스템(202)을 나타내는 블록도이다. 도시한 바와 같이, 파일 시스템(202)은 제어 블록(131) 및 복수의 파일(132a-n)을 포함하며, 이들 파일의 각각은 헤더/식별자 필드(334) 및 보안 필드(336)를 갖는 메타데이터 태그(112)를 포함한다. 헤더/ID 필드(334)는 파일 ID에 관한 정보 및 파일을 액세스하는 사용자를 포함한다. 보안 필드는 해당 파일에 기인하는 보안성의 레벨 및 그에 따라 승인된 사용자 액세스의 유형을 나타내는 단일 비트 필드이다. 예시적인 실시예에 따르면, 최고 레벨의 보안성을 필요로 하며 보안 마운트 상에서만 액세스되는 것으로 제한되는 특정의 파일(예를 들어, 파일 1 및 3)은 이들 제각각의 메타데이터의 보안 필드(336)에서 "1"로 태그된다. 그와 같이 태그되지 않은(즉, "0"으로 태그된) 다른 파일(예를 들어, 파일 2)은 정상이며 특수한 보안 마운트 없이 임의의 허가된 사용자에 의해 액세스될 수 있다.

<33> 전술한 바와 같이, 본 발명은 예시적인 실시예에서, DFNSE(분배 파일 시스템 네트워크 보안 확장부)로서 지칭되는, 증강된 보안성 메커니즘을 도입한다. DFNSE에 의해, 파일 시스템 서버는 특정의 사용자에 의해 파일을 액세스하는 경우 연관된 파일 승인으로부터 추정 가능하다. DFNSE는 서버 레벨 파일 시스템의 보안성 강화 애플리케이션 및/또는 프로시쥬어이다. 따라서, DFNSE에 의해, 서버에 의해 이용되는 네트워크 접속 또는 어댑터를 서버만이 인지하도록 요구된다.

<34> DFNSE를 구현하기 위해 파일 시스템에 마운트를 제공할 수 있는 각 서버 내에서 특정의 하드웨어, 로직 및 소프트웨어 요소가 제공된다. 도 4는 이들 요소의 일부를 도시하는 블록도이다. 도 4에 도시한 바와 같이, 서버

(203)에는 2개의 이더넷 네트워크 어댑터(또는 포트), 즉, 보안성을 갖는 En0(403), 보안성을 갖지 않는 En1(405)이 제공될 수 있다. 일 실시예에서, 이들 어댑터 다음의 네트워크 토폴로지(topology)는 일정하다. 즉, 선택된 서브네트워크 자체는 보안성을 제공하며, 서버는 요구된 보안성 레벨에 근거하여 서브네트워크들 사이를 동적으로 선택할 수 있다. 다른 실시예에서, 보안 어댑터 En0(403)에 별도의 암호화 또는 다른 보안 특성이 제공된다.

<35> En0(403)은 감지 가능한 모든 데이터를 라우팅하도록 이용되는 파이버 네트워크(225)에 접속하는 한편, En1(405)은 다른 모든(감지 불가능한) 데이터 통신을 라우팅하도록 이용되는 표준 이더넷 기반 와이어 네트워크(221)에 접속된다. En1(405)은 파일 시스템의 서버를 라우팅하는 디폴트(default) 포트이다. 예시적인 실시예에서는 검출부 없이 표준 이더넷이 침해될 수 있는 용이함으로 인해 이더넷이 감지 가능한 데이터를 라우팅하는 안전하지 않은 옵션이 되도록 하는 것으로 가정한다. 파일 시스템의 마운트 동안, 각각이 파일에 대해 파일 승인(334) 및 보안 레벨(336)을 상세하게 알고 있는 서버는 사용자 액세스를 추적하고, 액세스되는 파일 대신에 파일 승인부에 근거하여 언제 클라이언트가 보안 네트워크에 강제로 스위칭하도록 할 지를 판정한다. 예시적인 실시예에 따르면, 보안 및 비보안 라우팅에 대한 네트워크 토폴로지가 일정함에 따라 비보안 서브네트워크로부터 보안 서브네트워크로의 스위칭 동안 상이한 토폴로지에 대해 실행하도록 부가적인 하드웨어 및/또는 라우팅 프로토콜 업그레이드가 요구되지는 않는다.

<36> 도 4의 서버(203)는 파일 시스템(202)에 대해 통상적인 마운트 지원 및 언마운트 동작을 수행할 뿐만 아니라 본 발명의 원리에 따라 리마운트 구성을 수행하는 마운트 콘트롤러(407)를 또한 포함한다. 마운트 콘트롤러(407)는 DFNSE(126)를 포함하며 바람직하게는 서버(203) 상에서 실행하는 소프트웨어 코드로서 구현된다. DFNSE(126)는 마운트 콘트롤러(407)를 트리거하도록 동작하여 표준 포트 En1(405) 또는 보안 포트 En0(403)을 통해 마운트에 대한 요구를 라우팅한다. 암호화가 보안 포트 상에서 구현되는 경우, 서버(203)는 DFNSE(126) 및 En0(403)와 결합하여 이용되는 암호화 모듈(409)을 또한 포함한다.

<37> 파일 시스템 액세스 동안, 서버(203)에서 감지 가능한 동작을 액세스하기 위한 요구가 수신되는 경우, 마운트 콘트롤러(407)는 클라이언트의 IP 어드레스를, 감지 가능한 데이터에 대한 액세스를 필요로 하는 하나로서 마크한다. 그리고 나서 서버(203)는 현재의 접속을 차단한다(즉, 서버는 클라이언트에 FTN을 전송함). 클라이언트는 자동으로 재접속하도록 시도하고, 마운트 콘트롤러(407)는 리마운트 동안 클라이언트 IP 어드레스를 인지한다. 그 다음에 클라이언트의 세션은 보안 SSL 포트로 방향 설정된다. 따라서, 표준 포트를 통해 주요한 액세스가 제공되는 한편, 감지 가능한 데이터/파일에 대한 액세스가 요구되는 경우, 액세스는 SSL 보안 포트로 동적으로 스위칭된다.

<38> 이제 도 3의 (b)를 참조하면, 파일 시스템을 호스팅하는 서버의 상기 하드웨어/로직 구성 내에서 소프트웨어 구현된 DFNSE 보안 특성이 구현되는 프로세스의 플로우차트가 도시되어 있다. 프로세스는 블록(321)에서 도시한 바와 같이 클라이언트로부터 서버의 표준 포트에서 수신된 표준 마운트 요구로 개시한다. 사용자는 인증 데이터(패스워드 등)에 대해 프롬프트되고, 블록(323)에서 도시한 바와 같이 클라이언트 시스템의 IP 어드레스가 데이터 패킷으로부터 검색된다. 블록(325)에서 도시한 바와 같이 표준 포트 상에서 세션이 오픈되며 특정 세션에 링크된 파라미터 파일 내에서 IP 어드레스 및 사용자의 인증 데이터가 저장된다. 블록(327)에서 도시한 바와 같이 일단 세션이 확립되면, 즉, 액세스 승인 등과 연관된 서버 로직이 사용자의 상호 작용을 모니터링하고, 블록(329)에서 사용자가 감지 가능한 파일에 대한 액세스를 요구하고 있는지 여부에 대한 판정이 행해진다.

<39> 파일에 대한 클라이언트 요구를 충족하고 있는 서버는 액세스되는 파일의 승인 및 원격 클라이언트 상에서 사용자의 인증/자격으로 프로그래밍된다. 액세스되는 파일이 감지 불가능한 경우, 블록(331)에서 도시한 바와 같이 표준 포트 상에 사용자에게 규칙적인 액세스가 제공된다. 그러나, 클라이언트에 의해 요구되는 파일이, 액세스가 허여될 수 있기 전에 보다 안전한 채널을 필요로 하는 감지 가능한 파일인 경우, 블록(333)에서 사용자가 파일을 액세스하도록 적절하게 액세스를 승인하는지 여부에 대해 다음의 판정이 행해진다. 블록(335)에서 도시한 바와 같이 사용자가 적절한 액세스 승인부를 갖지 않은 경우, 요구는 금지된다. 그러나, 사용자의 자격이, 사용자가 특정의 파일을 액세스하도록 허가하는 것을 나타내는 경우, 블록(337)에서 도시한 바와 같이 DFNSE 보안성 프로토콜이 활성화된다. DFNSE의 활성화는 FTN을 클라이언트에 송출하고, 이와 동시에 보다 안전한 포트를 구성하여 세션 파라미터에 의해 저장된 IP 어드레스를 갖는 클라이언트로부터 리마운트를 채택함으로써 서버로 하여금 클라이언트의 언마운트를 강화시키도록 한다. 그 다음에 서버는 블록(339)에 도시한 바와 같이 보안 포트를 통해 파일에 보안 액세스를 제공한다.

<40> 도 3의 (a)는 사용자/클라이언트 시스템의 사시도로부터 본 발명의 구현에 수반되는 주요한 프로세스의 플로우

차트이다. 프로세스는, 블록(302)에서 도시한 바와 같이 사용자가 먼저 (클라이언트 시스템을 통해) 파일 시스템을 호스트하는 서버를 마운트하는 경우에 개시되고, 블록(304)에서 도시한 바와 같이 파일 시스템에 대한 액세스를 요구한다. 클라이언트는 NFS 파일 시스템을 초기에 마운트하고, 마운트는 디폴트에 의해 표준 TCP 접속을 통해 완료된다. 예를 들면, 접속부는 잘 알려진 2048의 NFS 포트일 수도 있다. 서버는 이러한 포트에 결합된 청취용 소켓을 가지며, 표준(비보안) 프로토콜에 따라 동작한다. 특히, 예시적인 실시예에서, 표준 프로토콜은 DFNSE 프로토콜에 의해 증강되며, 이는 감지 가능한 파일에 대한액세스가 요구되는 경우에 구현된다.

<41> 클라이언트로부터 접속이 요구되는 경우, 서버의 청취용 소켓은 기본적으로 그 자신을 복제하고, 접속부를 원격 클라이언트에 본딩한다. 그 다음에 청취용 소켓은 다른 접속 요구를 취급하도록 오픈된 상태로 유지된다. 블록(366)에서 도시한 바와 같이 클라이언트의 인증이 초기화되고, 블록(308)에서 클라이언트의 인증이 성공적이었는지 여부에 대한 판정이 행해진다. 클라이언트/사용자 인증 처리가 성공적이지 않은 경우, 블록(310)에서 도시한 바와 같이 파일 시스템에 대한 액세스가 금지되고 마운트가 접속 해제된다. 그리고 나서 프로세스는 블록(311)에서 도시한 바와 같이 종료된다. 한편, 블록(309)에서 도시한 바와 같이 세션이 오픈되고 사용자에게 파일 시스템에 대한 액세스가 제공된다.

<42> 클라이언트 시스템은 블록(312)에서 도시한 바와 같이 접속 해제를 위한 접속부를 모니터링하고 블록(314)에서 도시한 바와 같이 접속이 응답하지 않게 되거나 또는 수신기 측에서 너무 빨리 해제되는지(즉, 이상적으로는 FTN을 송출한 서버가 수신될 때) 여부를 판정한다. 접속이 응답하지 않게 되거나, 해제되는 경우, 블록(316)에서 도시한 바와 같이 클라이언트는 서버에 의해 표시된 포트에 대해 라우팅되는 리마운트를 초기화한다.

<43> 특히, 디스마운트(dismount)를 개시한 서버에 응답하는 재접속은, 클라이언트 시스템에서 실질적인 포트가 알려져 있지 않다 하더라도, 서버에서의 보안 포트 상으로 방향 설정된다. DFNSE의 보안 프로토콜을 이용하고, 그리고 어느 포트가 안전하며, 세션이 보안 포트를 필요로 하는 지에 대한 지식에 근거하여, 서버는 클라이언트가 보안 포트를 통해 리마운트하도록 요구할 수 있다. 예를 들어, 클라이언트는 보안 소켓 레이어(Secure Socket Layer)를 실행하는 포트를 이용하여 리마운트하도록 행해질 수도 있다. 특히, 사용자 액션은 리마운트 및 포트 스위칭 프로시쥬어를 완료시키도록 요구된다. 서버 측 언마운트 및 후속의 리마운트 모두에 대한 모니터링은 클라이언트 시스템에서 배경 프로세서로서 발생하고, 사용자(클라이언트)는 보다 안전한 포트로의 스위칭을 인지하지 못할 것이다.

<44> 도 3의 (c)의 플로우차트에 의해 서버 측에서 보다 안전한 포트를 통해 재라우팅하도록 요구된 내부 프로세싱의 보다 상세한 설명이 나타나 있다. 프로세스는 블록(351)에서 도시한 바와 같이 감지 가능한 파일에 대한 액세스가 DFNSE에 의해 식별되는 경우에 개시된다. 서버는 블록(352)에서 도시한 바와 같이 현재의 포트 보안성을 체크한다. (예시적인 실시예에서 파일의 보안성 비트를 판독함으로써 추론되는 파일이 얼마나 감지 가능한지에 따라) 현재의 포트 보안성이 요구된 파일을 액세스하는데 충분한지 여부에 대한 판정이 블록(354)에서 행해진다. 현재의 포트 보안성이 요구된 파일을 액세스하는데 충분한 경우, 블록(356)에서 도시한 바와 같이 액세스가 제공된다.

<45> 다른 일 실시예에서, 리마운트 기능은 선택적으로 자동화될 수 있으며, 프로세스는 자동 리마운트에 대한 특성이 가능한지 여부에 대해 다음의 판정을 필요로 한다. 이러한 다른 실시예에 의해, 자동 리마운트 능력이 가능하지 않은 경우, 사용자는 실질적으로 보안 마운트를 통해 리마운트하도록 프롬프트될 것이다.

<46> 도 3의 (c)의 예시된 실시예를 참조하면, 포트 보안성이 불충분한 경우, 서버는 블록(358)에서 도시한 바와 같이 세션에 대해 보다 안전한 포트(예를 들어, En0)를 선택함으로써 응답한다. 서버는 클라이언트의 IP 어드레스를 포함하여, 세션의 마운트 파라미터 및 인증의 스냅샷(snapshot)을 취하고, 이들 파라미터를 블록(360)에서 도시한 바와 같이 보다 안전한 포트의 제어 로직으로 전달한다. 전달은 매우 적은 레이턴시(latency)에 의해 발생하며, 따라서 보다 안전한 포트가 자동 구성되어 해당 클라이언트로부터 리마운트를 수신하고 세션을 진행하도록 연속적으로 지원한다. 보안 포트가 구성된 후에, 대응하는 포트 수는 클라이언트의 IP 어드레스와 함께 마운트 콘트롤러에 주어진다. 서버는 블록(362)에서 도시한 바와 같이 제 1 표준 포트 상에서 마운트를 종료시키고 클라이언트로부터 리마운트가 수신되는 경우 보다 안전한 포트를 통해 세션을 재확립한다.

<47> 특히, 초기화 마운트를 종료시키는 서버에 응답하여, 클라이언트는 제 2 보안 링크에 대해 사용자에 의해 방향 설정되는 리마운트를 초기화한다. 이것은 제 1 포트를 통해 클라이언트의 초기화 세션을 재확립한다. 접속을 재확립하는 것은 클라이언트 IP 어드레스를 체크하고, 이를, 해당 IP 어드레스로부터의 접속을 수신하도록 셋업(set up)되는 포트에 매칭시킨다. 전체 프로세스는 배경에서 발생하며, 따라서 사용자의 관점으로부터 포트의 이음매 없는 스위칭이 완료된다.

<48> 다른 일 실시예에서, 특정 파일에 기인하는 보안성의 레벨은 특정 파일에 대한 액세스가 제공되는 사용자(또는 선택된 클라이언트 시스템)에 의해 결정된다. 따라서, 파일 액세스 승인이 파일 시스템 집행자만으로 제한되는 경우, 보안 레벨은 하이(hjgh)로 되는 한편, 정규 고용인에 주어진 파일 액세스 승인은 요구된 보안성의 상대적으로 로우(low) 레벨을 표시한다. 파일에 대한 보안 레벨의 판정은, 사용자가 초기에 파일을 생성하고 액세스 승인을 해당 파일에 할당하는 경우에 완료된다. 일단 파일 시스템 내에서 파일이 위치하면, 파일은 적절한 위치에 위치하는 네트워크 보안성 보호를 자동으로 인계한다. 이러한 구현에 의해, 파일 시스템(예를 들어, 사용자, 그룹 등을 위한 유닉스 -rwx,rwx,rwx) 내의 파일 상의 현재의 파일 승인은 확장 시스템 집행 및 구성을 필요로 하지 않고 제공된 보안 모델에 폴딩(fold)된다. 따라서, 본 발명은 파일 단위로 현존의 파일 시스템을 재구성하기 위한 필요성을 없애 준다. 본 발명에 의하면, 보다 감지 가능한 파일을 안전한 서버로 이동시킬 필요가 또한 없다.

도면의 간단한 설명

<19> 도 1의 (a)는 본 발명의 특성이 구현될 수 있는 데이터 프로세싱 시스템의 블록도이고,

<20> 도 1의 (b)는 본 발명의 일 실시예에 따라 요구된 레벨의 보안성을 나타내는 보안성 태그를 갖는 도 1의 (a)의 파일 시스템 내의 파일을 나타내는 블록도이며,

<21> 도 2는 본 발명의 일 실시예에 따라 본 발명의 특성이 구현될 수 있는 분배 네트워크의 블록도이고,

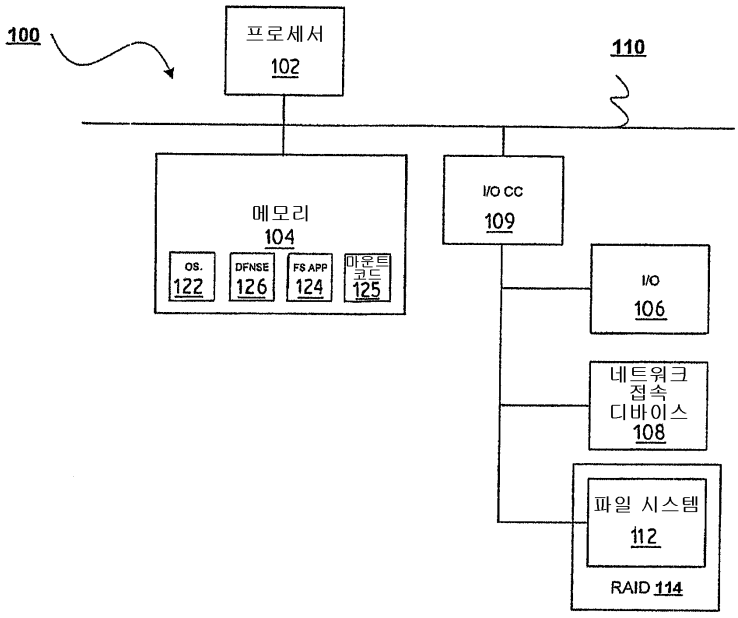
<22> 도 3의 (a)는 본 발명의 일 실시예에 따라 표준 마운트를 통해 액세스 동안 감지 가능한 파일에 대한 액세스가 클라이언트에게 제공되는 프로세스의 플로우차트이며,

<23> 도 3의 (b) 및 (c)는 본 발명의 일 실시예에 따라 보안 채널을 통해 이들 파일에 대한 액세스가 라우팅되는 것을 보장하도록 감지 가능한 파일 액세스에 대한 클라이언트 요구를 서버가 모니터링하고 제어하는 프로세스의 플로우차트이고,

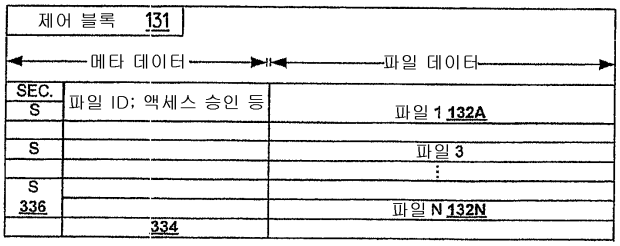
<24> 도 4는 본 발명의 일 실시예에 따라 하나의 연속적인 세션 동안 표준의 비보안(non-secured) 채널로부터 보안 채널까지 파일 시스템 상에서의 클라이언트 세션의 스위칭을 이음매 없이 완료시키는 논리 구성 요소를 도시하는 블록도이다.

도면

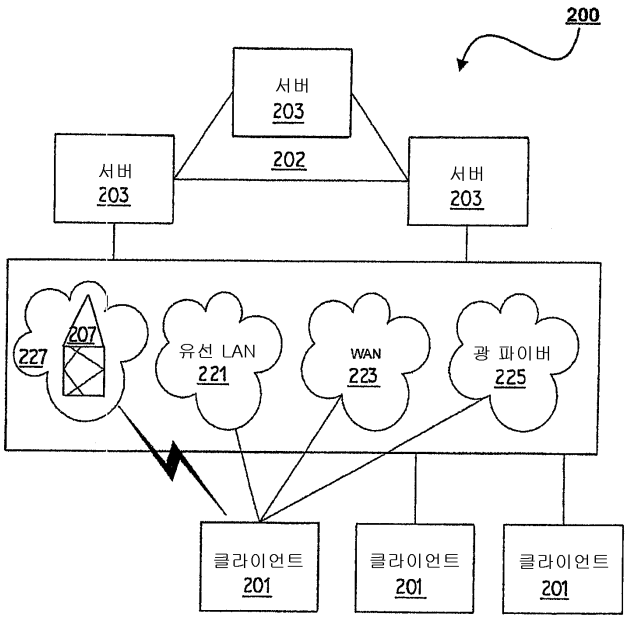
도면1a



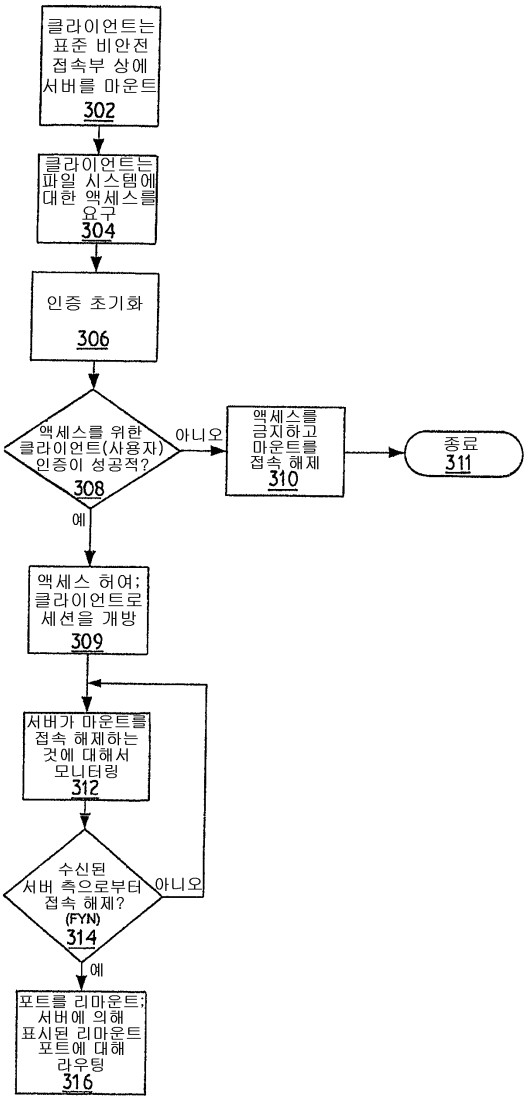
도면1b


제어 블록 131
메타 데이터
파일 데이터
SEC.
S
파일 ID; 액세스 승인 등
파일 1 132A
S
파일 3
S
336
파일 N 132N
334

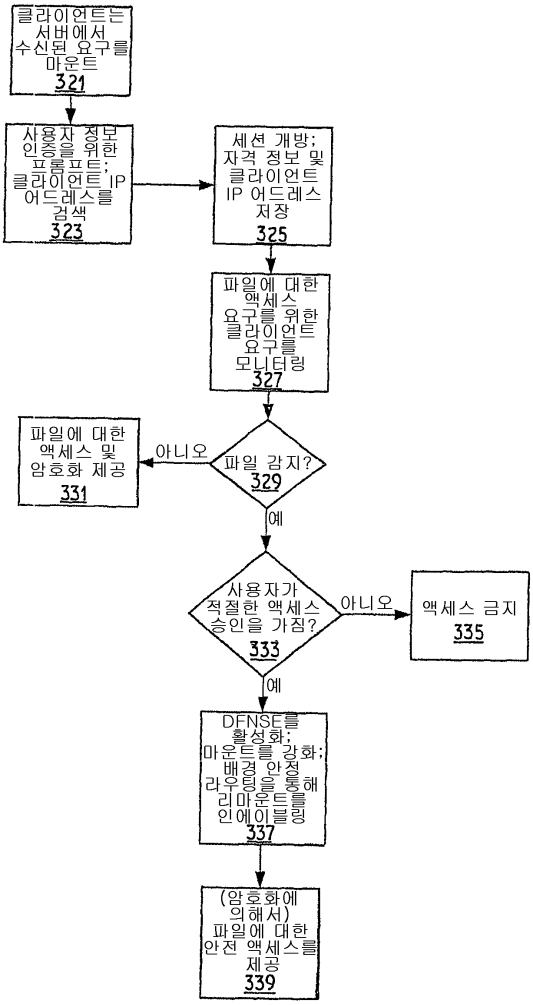
도면2


200
서버
203
202
서버
203
서버
203
207
227
유선 LAN
221
WAN
223
광 파이버
225
클라이언트
201
클라이언트
201
클라이언트
201

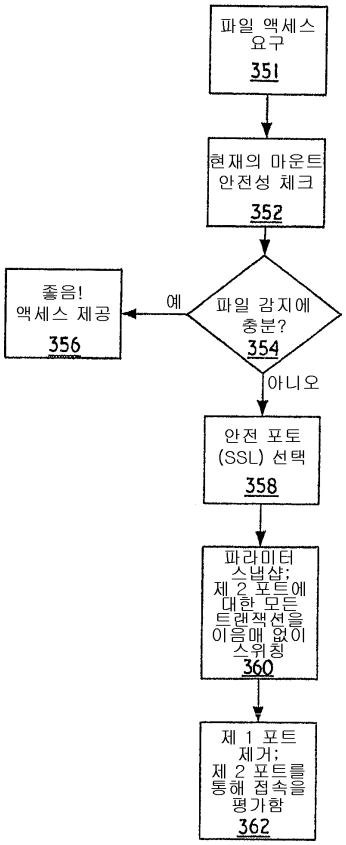
도면3a


클라이언트는 표준 비안전 접속부 상에 서버를 마운트
302
클라이언트는 파일 시스템에 대한 액세스를 요구
304
인증 초기화
306
액세스를 위한 클라이언트(사용자) 인증이 성공적?
308
아니오
액세스를 금지하고 마운트를 접속 해제
310
종료
311
예
액세스 허여; 클라이언트로 세션을 개방
309
서버가 마운트를 접속 해제하는 것에 대해서 모니터링
312
수신된 서버 측으로부터 접속 해제? (FYN)
314
아니오
예
포트를 리마운트; 서버에 의해 표시된 리마운트 포트에 대해 라우팅
316

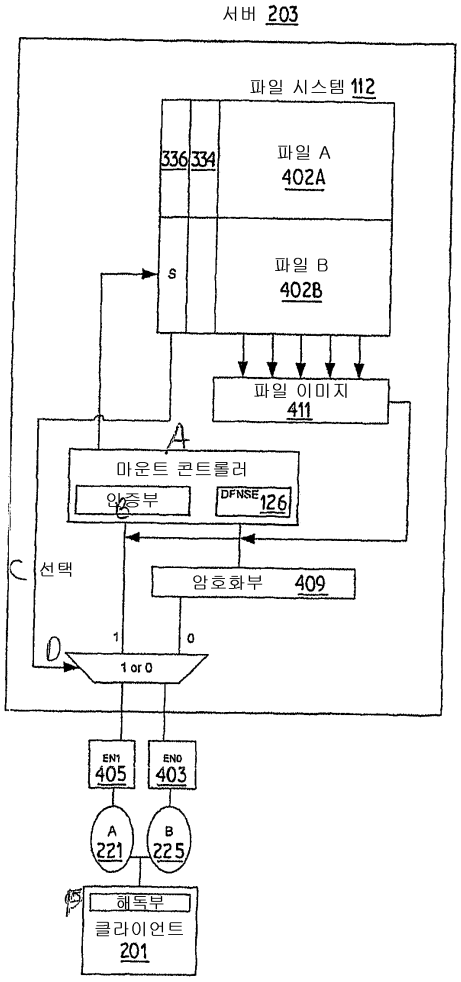
도면3b


클라이언트는 서버에서 수신된 요구를 마운트
321
사용자 정보 인증을 위한 프롬프트; 클라이언트 IP 어드레스를 검색
323
세션 개방; 자격 정보 및 클라이언트 IP 어드레스 저장
325
파일에 대한 액세스 요구를 위한 클라이언트 요구를 모니터링
327
파일 감지?
329
아니오
파일에 대한 액세스 및 암호화 제공
331
예
사용자가 적절한 액세스 승인을 가짐?
333
아니오
액세스 금지
335
예
DFNSE를 활성화; 마운트를 강화; 배경 안정 라우팅을 통해 리마운트를 인에이블링
337
(암호화에 의해서) 파일에 대한 안전 액세스를 제공
339

도면3c


파일 액세스 요구
351
현재의 마운트 안전성 체크
352
파일 감지에 충분?
354
예
좋음! 액세스 제공
356
아니오
안전 포토 (SSL) 선택
358
파라미터 스냅샵; 제 2 포트에 대한 모든 트랜잭션을 이음매 없이 스위칭
360
제 1 포트 제거; 제 2 포트를 통해 접속을 평가함
362

도면4


서버 203
파일 시스템 112
336
334
파일 A
402A
S
파일 B
402B
파일 이미지
411
A
마운트 콘트롤러
암증부
DFNSE 126
선택
암호화부 409
1
0
1 or 0
EN1
405
EN0
403
A
221
B
225
해독부
클라이언트
201