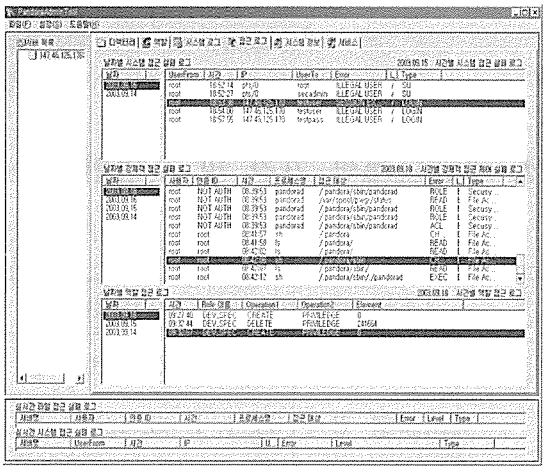
Cloud-Secu 서버 암호화 보안제품

해킹 원천 차단 -
서버 암/복호화 보안솔루션



(주)전유시스템 (대표 김규종) 의 Cloud-Secu 보안 운영체제는 국내 독자 기술로 개발된 서버 보안 운영체제 솔루션으로서, 시스템에서 기본으로 제공되는 접근 제어에 더하여 운영체제 수준에서 보다 세분화한 강제적인 역할 통제 기능을 제공한다. 이를 통해 시스템을 안전하게 보호하고 자료의 불법적인 유출을 차단하여 원천적으로 해킹을 차단할 수 있다. 또한 암호화 파일 시스템을 지원하여 파일 시스템 이하 수준에서 디스크에 대한 물리적인 접근을 통한 자료 유출을 차단한다. 그리고 GUI 기반의 관리 도구를 통해 여러 서버를 한곳에서 관리하도록 하여 관리의 편의성을 도모하였다.

Cloud-Secu 서버 암호화 보안솔루션은 과거의 네트워크 기반의 보안 시스템들의 단점을 극복한 시스템 기반의 보안을 제공하는 시스템이다. 과거의 네트워크 기반 보안 시스템들은 크게 침입 차단 시스템과 침입 탐지 시스템으로 나뉜다. 침입 차단 시스템은 내부 네트워크로부터의 침입에 대해 안전하지 못하다. 침입 탐지 시스템은 약 60% 정도의 침입만을 탐지하는 것으로 알려져 있다.

Cloud-Secu 서버 암호화 보안제품은 해커와 내부 비인가자들로부터 자료를 원천적으로 보호할 수 있는 보안성이 뛰어난 제품으로서 관공서 및 금융기관에 큰 호응을 얻고 있을 뿐만 아니라 수출지향적으로 설계사상을 구축, 구현하였으므로 내수 뿐 만아니라 수출에도 큰 성과를 올릴 것이다.

동 상

Cloud-Secu (서버암호화보안제품)

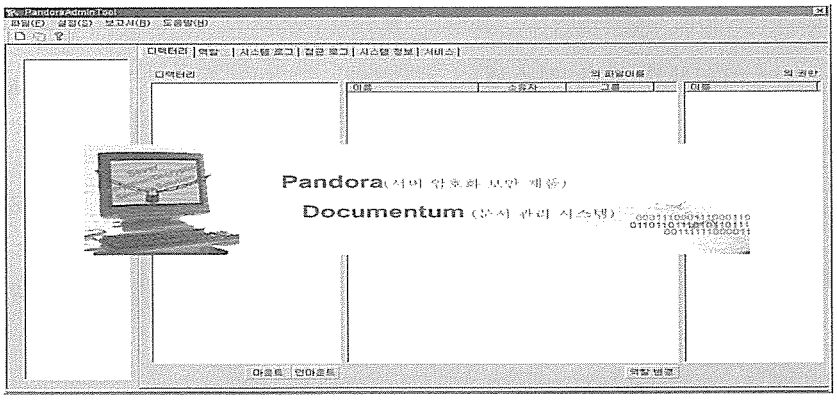
1. 작품명 : Cloud-Secu (서버 암호화 보안솔루션)

2. 제작자 :

대표자 : (주)전유시스템
개발참여자 : 안선일, 성준이, 김성기, 김정수 외 4명
주소 : 서울시 서초구 서초동 1355-8 중알로얄빌딩 1407호
전화 : 02) 3486-4340
팩스 : 02) 3486-4342
email : master@jyou.co.kr

3. S/W 요약설명

Cloud-Secu는 암/복호화를 지원하는 보안 운영체제로써, 시스템에서 기본으로 제공되는 접근 제어에 더하여 운영체제 수준에서



보다 세분화한 강제적인 역할 통제 기능을 제공한다. 이를 통해 시스템을 안전하게 보호하고 자료의 불법적인 유출을 차단하고, 원천적으로 해킹을 방어할 수 있다. 또한 암호화 파일 시스템을 지원하여 파일 시스템 이하 수준에서 디스크에 대한 물리적인 접근을 통한 자료 유출을 차단한다. 그리고 GUI 기반의 관리 도구를 통해 여러 서버를 한곳에서 관리하도록 하여 관리의 편의성을 도모하였다.

3.1 개발 배경

유닉스(UNIX) 운영체제는 '70년대에 개발되어 현재 대부분 정보시스템의 운영체제로 사용되고 있으나, 인터넷을 비롯한 분산 통신망 환경의 급속한 확산에 따라 많은 보안 취약점이 노출되고 있다. 이러한 보안 취약점을 개선하려는 노력은 미국을 비롯한 선진 외국에서는 이미 정부 차원의 보안 평가 기관 설립 및 보안 평가 기준 제정과 더불어 업계에서는 물론 정부차원에도 안전한 운영체제를 개발하고 있는 실정이다. 이에 국내에서도 정보시스템의 시스템 취약점을 운영체제 커널 수준에서 강화된 정보보호 기술을 적용함으로써 수준 높은 안전한 운영체제를 개발하여 정보통신망에서의 정보시스템의 보안 기능을 강화하여할 필요성이 대두되고 있다.

과거의 네트워크 기반 보안 시스템들은 크게 침입 차단 시스템과 침입 탐지 시스템으로 나뉜다. 각 보안 시스템들이 갖는 단점들은 다음과 같다.

1) 침입 차단 시스템

- 시스템이 아닌 네트워크 트래픽만을 보호하고, 내부 네트워크에 존재하는 각 서버 자체를 보호하지 않는다.
- 검사하는 IP 주소 및 포트 번호와 같은 정보는 정확하지 않을 수 있다.
- 사이트 및 관리자의 요구사항에 맞게 유연하게 설정되어야 한다.

2) 침입 탐지 시스템 (IDS)

- 알려진 공격만 탐지하는 수동형 탐지 시스템
- 관리의 오버헤드가 큰 편
- 감사 기록의 보호가 어렵다.

3) 응용프로그램(Application) 수준의 보안 시스템 한계

- 전체적인 시스템 감시가 어렵다.

정보화가 발전될수록 해킹, 바이러스 및 내부자 정보 유출 등의 위협은 점차 자동화, 지능화 대중화, 분산화 되어 탐지하고 예방하기가 어려워 가는 경향이 있다. 이러한 해킹의 지능화에 따라 기존의 운영체제로써는 해결하기 어려운 보안 문제들이 존재하므로 이러한 부분을 보완하기 위한 방법이 필요하다.

3.2 시스템 개요

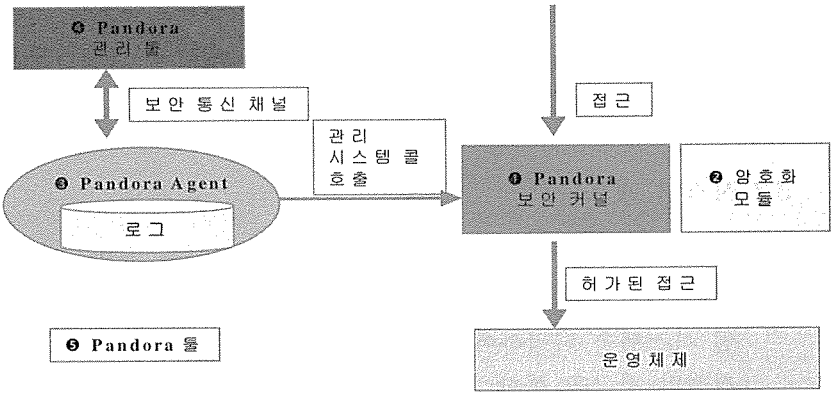
Cloud-Secu는 암호화 파일 시스템을 지원하는 보안 운영체제로써, 강제적인 역할 통제 기능을 원척적으로 해킹을 차단하고, 암호화 파일 시스템을 지원하여 파일 시스템 이하 수준에서 디스크에 대한 물리적인 접근을 통한 자료 유출을 차단하는 보안 솔루션이다.

3.3 시스템 특징

- 여러 서버를 한 곳에서 GUI 기반의 관리 도구를 통해 관리할 수 있어 관리의 효율성을 높임
- 암호화 파일 시스템 제공하여 파일 시스템 이하 수준에서 디스크에 대한 물리적인 접근을 통한 자료 유출을 차단
- 역할 기반의 강제적 접근 제어를 통해 해킹 시도를 원천적으로 차단
- 보안 정책의 효율적인 상속을 통한 유연한 보안 정책 설정
- Setuid/Setgid 제어를 통한 해킹 시도 차단
- 중요 프로세스 종료 보호
- 사용자 자신의 암호만을 변경할 수 있도록 암호 변경 제어 기능 제공

- 보안 정책의 테스트를 위한 테스트 모드 지원
- 무분별한 root 권한사용 제어
- 로그 관리 및 침입 탐지 기능
- 시스템 정보 제공
- 재부팅에도 보안기능 유지
- 역할 초기화 기능 제공

3.4 제품 구성



1) 보안 커널
   - 해당되는 시스템 콜 등을 후킹하면서 시스템에 대한 접근 통제
   - 비인가자 접근에 대한 감사 기록
   - 역할에 기반 한 시스템 접근 통제

2) 암호화 파일 시스템
   - 디렉터리 단위의 암호화
   - 파일 시스템 하위의 디스크 불법 접근을 방지

3) Agent
   - 보안 커널과 관리 툴 사이의 통신을 담당

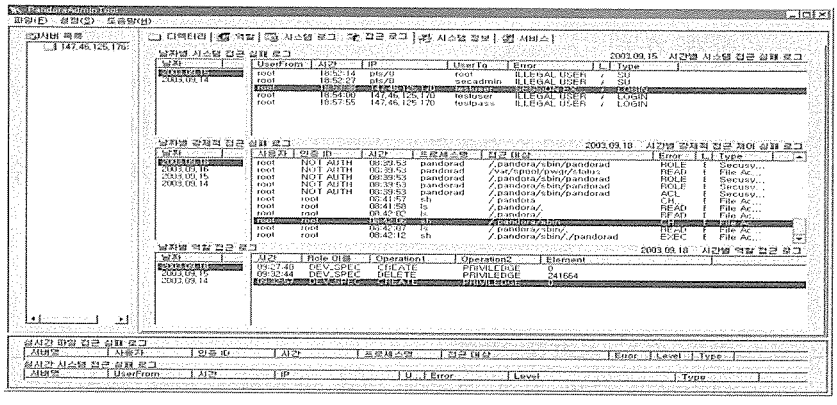
4) 관리 툴

- 보안 커널 정책 설정 및 암호화 파일 시스템 관리를 위한 GUI 툴

5) 툴

- root 권한의 분산을 위한 툴 (su, passwd, userdel)
- 시스템 관리자가 실행하는 경우라도 암호를 요청

3.5 프로그램구성 및 주요기능



Cloud-Secu관리도구

· 역할 및 접근 제어 설정을 통한 보안 정책의 설정
· GUI 기반의 관리 도구로써 여러 서버를 동시에 관리
· SMS 수준의 시스템 상세 정보 제공
· Cloud-Secu Agent 프로그램과 비밀 채널을 유지
· 보안 정책 위반시 경고음 및 핸드폰 메시지 전송

Cloud-Secu Agent 프로그램

· Cloud-Secu 관리 도구로부터의 보안 정책 변경에 따른 메시지를 보안 커널에 전달
· Cloud-Secu 보안 커널로부터 발생한 로그를 영구적으로 관리하고,

Cloud-Secu 관리 도구에 로그를 필요에 따라 전송
- 암복호화에 따른 디렉터리별 키와 위치 정보의 관리
- 보안 정책인 역할 정보를 영구적으로 관리
- 필요한 경우 시스템 정보를 추출하여 Cloud-Secu 관리 도구에 전달
- 사용자 자신의 암호만을 변경할 수 있도록 암호 변경 제어 기능 제공

Cloud-Secu 툴
- SU, PASSWD 프로그램의 실행에 시스템 관리자(root)도 암호 입력 요구
- USERDEL프로그램을 통해 보안 관리자(secadmin)만 사용자 삭제 가능
- PAM 모듈을 통한 인증 정보의 전달 및
- PAM 모듈을 이용하여 IP, 서비스, 사용자별 필터링 지원
- Cloud-Secu 유틸리티는 변경되지 않도록 접근 제어가 필수적임

암호화 모듈
- 동적 커널 모듈로 동작
- 디스크 수준의 직접 접근에 대해 암호화를 통한 사용자 중요 데이터의 보호
- 암호화는 사용자에게 투명하게 이루어지므로 사용자는 사용하는 파일이 암호화되었는지의 여부를 알 수 없음
- 디렉터리 별 암호화 지원
- 비교적 빠른 성능을 보이는 SEED, blowfish 암호화 알고리즘 지원
- 키는 Cloud-Secu Agent에 의해 영구적으로 관리

보안 커널 모듈
- 역할 기반의 강제적 접근 제어를 통해 해킹 시도를 원천적으로 차단
- 보안 정책의 효율적인 상속을 통한 유연한 보안 정책 설정

· Setuid/Setgid 제어를 통한 해킹 시도 차단
· 중요 프로세스 종료 보호
· 보안 정책의 테스트를 위한 테스트 모드 지원
· 무분별한 root 권한사용 제어
· 로그 관리 및 침입 탐지 기능
· 재부팅에도 보안기능 유지

4. 개발단계별 기간 및 투입인원수

개발단계	개발시간	인원	비고
시스템 설계	02. 6 ~ 02.11	4	구축목표 설정, 구축내용 구상, 동종서비스분석, 프로세스 설계
프로그래밍	02.10 ~ 03. 8	7	접근/관리영역 구축, 시스템 디자인, 기능 구축
통합 테스트	03. 6 ~ 03.10	4	단위모듈 테스트 개발시 계속 진행, 모듈 통합테스트
매뉴얼제작	03. 7 ~ 03.10	5	사용자 설명서, 설치 지침서, 자켓디자인, CD디자인

5. 사용 또는 개발언어, TOOL

Cloud-Secu 관리 도구 부분 : Microsoft Visual Studio 6.0
Cloud-Secu 서버 보안 부분 : Ansi C

6. 사용시스템

사용OS	HP-UX 11.0/11i
CPU	Daul CPU 이상
메모리	256M이상
HDD	1GB 이상