멀티 유저 윈도우 환경에서의 실시간 데이터 접근 모니터링 시스템 설계 및 구현

박영철*, 박진섭*, 김형선**, 송영기***
*대전대학교 컴퓨터공학과
**한국전자통신연구원 인터넷컴퓨팅연구부
***천안외국어대학교 컴퓨터벤처과

Design and Implementation of Real-time File Access Monitoring System on NT Server

Young-Chul Park*, Jin-Sub Park*, Hyoung-sun Kim*, Young-Kee Song**
*Dept. of Computer Engineering, Daejeon University
**Dept. Internet Computing, ETRI
***Dept. of Computer Venture, Cheonan College of Foreign Studies

요 약

최근 대부분의 기업 정보 범죄가 기업 내부자 소행으로 일어난다. 허가되지 않은 사용자의 불법적인 사용 및 도용은 기업 내부의 정보유출, 파괴등 기업에 막대한 피해를 가져온다. 이런 환경에서 공용으로 사용되는 기업 정보에 대한 사용자별 파일 또는 디렉토리 접근에 대한 실시간적인 관리가 이루어져야 한다.

본 논문에서는 멀티 유저 윈도우서버의 디렉토리 및 파일에 접근하는 사용자를 실시간적으로 모니터링하고, 사용자 권한에 위배되는 행동을 모니터링하는 시스템을 설계 및 구현한다.

1. 서론

정보 산업의 급속한 발전으로 컴퓨터 시스템의 사용이 급격히 증가하고 있다. 또한 인터넷의 확장에 따라 네트워크를 통한 정보의 교류가 많아지게 되었고 정보의 교류에 상업적 또는 기술적으로 중요한 데이터를 네트워크를 통하여 전송 또는 수신하게 되었다. 그러나 사용자들이나 기업은 인터넷을 통한 정보 처리의 편리성을 누리게 된 반면 컴퓨터 시스템은 정보보호 상의 다양한 문제에 직면하게 되었다. 특히 인터넷이 정보유통 수단으로 광범위하게 이용되면서 정보유출로 인해 개인은 물론 기업이나 국가 차원의 손실로 이어질 수 있는 가능성이 높아지고 있다.

많은 사람들은 정보유출의 원인을 해킹이나 바이러스 등 외부에 의한 침입으로 생각하지만 실제로는 내부자에 의한 것이 훨씬 많다. 경찰청 집계에 따르면 내부자에 의한 정보유출 및 해킹 등의 범죄건수는 2000년 278건에서 2001년 7595건으로 급증했으며 2002년에는 약 1만5000건에 이를 것으로 추산되는 등 해마다 급증하는 추세다.

기업의 주요 정보가 문서가 아닌 디지털 파일 형태로 기록되면서 내부자가 이를 악용하는 범죄사례가 늘고 있으며 피해금액도 큰 폭으로 증가하고 있다. 특히 금융권이나 대기업 연구소 등 핵심 정보가 있는 곳에서 내부자에 의한 정보유출이 일어날 경우 이는 엄청난 사회적 파장을 일으키며 국가 경쟁력 약화로까지 이어질 수 있다. 따라서 내부보안에 관한 대책이 필요하다.

그동안 해킹 및 바이러스 등 외부침입에 대한 방지 시스템 마련에 집중했던 국내 보안산업의 패러다임이 내부자에 의한 정보유출을 막는 방향으로 확대되고 있다. 이는 갈수록 내부자에 의한 정보유출의 피해가 늘어남에 따라 보다 적극적인 보안수단의 필요성이 대두되었기 때문이다.

내부 보안 시스템의 하나로 다중 사용자가 사용하는 서버 컴퓨터에서의 사용자별 디렉토리 및 파일에 대한 접근 모니터링이 필요하다.

접근 모니터링의 목적은 컴퓨팅 자원, 통신 자원 및

정보자원 등에 대하여 허가되지 않은 접근을 감시하는 것이다. 허가되지 않은 접근이란 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 커맨드의 발행을 포함하고 있다. 즉, 접근 모니터링은 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 된다.

기존의 접근 모니터링 시스템들은 거의 Unix나 Linux 머신에서 실행되고 있는 실정이다. 반면 윈도우 서버인 NT나 2000의 경우 극히 희박한 실정이다. 윈도우 서버상의 불법적인 자원 사용 및 도용은 시스템의 중요한 파일을 손상시키거나 삭제하고 중요 정보를 유출시킬 수 있는 문제점을 야기시킨다.

이에 본 논문에서는 윈도우 환경에서의 불법적인 내부 사용자에 대한 파일 및 디렉토리 접근을 실시간적으로 모니터링하는 시스템 제안한다.

본 논문의 구성은 다음과 같다. 먼저, 2장에서는 접근 모니터링의 개념과 기존 Unix 상에서의 접근 모니터링 로그를 살펴보고 최근 접근 제어 모니터링 기술의 동향을 분석해 본다. 그리고 3장에서는 제안된 파일 및 디렉토리 접근 모니터링 시스템의 설계 및 구현을 보인다. 마지막으로 4장의 결론에서는 향후의 연구과제를 제시한다.

2. 관련연구

2.1 접근 제어 모니터링 기술 분석 및 동향

(1) 모니터링 기술 분석

(가) 접근 모니터링 개요

정보시스템에서는 보유하고 있는 정보 및 자원의 불법 유출을 방지하고 사용 원칙에 위배되는 불법 행위의 추적을 위한 감사 능력이 제공되어야 하며 나아가 시스템 관리 및 운영자의 책임을 명확히 하고 사용자의 행위를 명확히 구분지을 수 있는 모니터링 메커니즘이 요구된다.

모니터링은 언제, 누가, 어떤 자원을, 어떻게 이용하는가 하는 자료를 기초로 하여 다음과 같은 용도로 이용될 수 있다.

- 백업, 통계유지 등 시스템 사용 현황 파악 및 시스템 증설 기초 자료로 이용
- 사용료 청구 등 회계측면의 기초 자료로 이용
- 시스템 자원 사용에 대한 추적자료로 이용

(나) 유닉스 로그 파일 분석

초기 유닉스 버전에서는 누가 로그인 했고, 로그아웃 했으며 로그인에 성공한 후 무슨 작업을 했는지 기록하는 것이 전부였다. 최근 유닉스 버전에서는 그와 같은 단순한 기록 이외에 시스템 최고 권한을 가지고 있는 수퍼 유저의 권한을 도용하고자 하는 시도, 전자 우편, 파일 전송, 사용자 행위감시, 기타 시스템 서비스 내역 등 다양한 정보를 로그 파일에 기록하고 있다.

로그 파일의 종류 및 기본적인 기능은 다음 표1과 같다.

<표 1. 유닉스 로그파일 종류 및 기능>

파일명	기능
acc 또는 pacct	사용자별로 시행되는 모든 명령어 기록
lastlog	각 사용자의 가장 최근 로그인 시간을 기록
loginlog	잘못된 로그인 시도를 기록
messages	부트 메시지등 시스템의 콘솔에서 출력된 결과를 기록하고 syslog에 의하여 생성된 메시지도 기록
sulog	su 명령 사용 내역 기록
utmp	현재 로그인한 각 사용자의 기록
wtmp	사용자의 로그인, 로그아웃 시간과 시스템의 종료 시간, 시작 시간드을 기록

(2) 접근제어 모니터링 기술 동향

윈도우 시스템의 커널이 공개되지 않아 상대적으로 불법적인 접근 분석을 위한 도구 개발이 윈도우에서는 어려운 실정이다. 리눅스나 유닉스의 경우 커널이 공개되고 사용자들이 프로그램을 공유함으로써 해킹 프로그램뿐만 아니라 이에 대한 대응 도구와 가능한 보안상의 문제에 대한 사전 대응책 개발 역시 많은 사용자들에 의하여 활발하게 진행되고 있다. 이로 인하여 윈도우 보안에 대한 전문적인 지식과 기술을 갖춘 소수의 해커들이 음성적으로 개발하는 해킹 기법 및 도구에 의하여 다수의 사용자들이 피해를 입고 때로는 피해 사실조차 모르는경우도 있으며, 새로운 바이러스 등에 의하여 많은 사용자들이 피해를 입고 사회적인 문제가 된 후에야 이에 대한 피해 등의 대응

책이 개발 보급되는 악순환이 계속되고 있는 실정이다.

윈도우 NT/2000 서버 환경에서의 불법적인 접근 상황을 시스템 차원에서 종합적으로 분석할 수 있는 적절한 도구가 거의 없는 실정이며, 이러한 도구 개발에 대한 국내에서의 노력이 저조한 편이다.

3. 접근 모니터링 시스템

3.1 시스템 분석

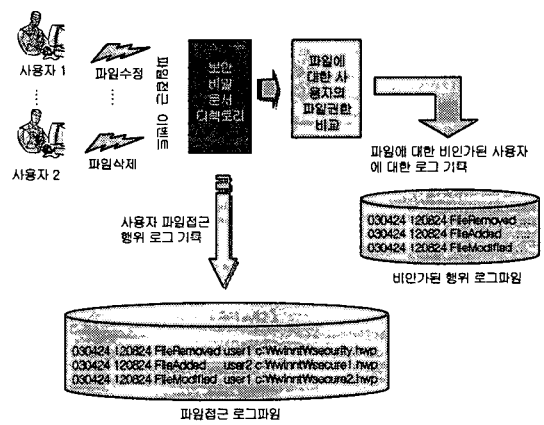
본 절에서는 윈도우 2000 환경에서 파일 및 디렉토리 접근에 대한 모니터링 방법에 대하여 기술한다.

파일 모니터링은 파일의 크기나 생성 시간, 변경 시간, 수정, 삭제, 추가에 대해서 상태를 확인한다. 특정 시스템 파일에 대해서 모니터링 기록을 남기고, 그 접근이 올바른 사용자에 의한 접근인지를 비교, 비인가된 접근에 대하여 별도의 로그파일로 기록한다.

또한 파일 모니터링은 여러 사용자로부터의 접근을 통해 파일의 변조 및 삭제등을 확인할 수 있으므로 파일의 무결성을 조사한다.

3.2 시스템 설계

본 절에서는 앞절의 접근 모니터링 방법에 기초하여 실시간 접근 모니터링 시스템 개발을 위한 기본 모델에 대하여 기술한다.



<그림 1. 윈도우 파일 접근 모니터링 시스템 구성도>

그림1은 윈도우 접근 모니터링 시스템의 구성도이다. 파일 접근 모니터링은 사용자의 특정 시스템 파일 접근에 대해 로그를 저장하고 또한 그 접근 행위가 비인가된 사용자에 의한 접근인지를 특정 룰에 적용하여 권한 위반 시 별도의 로그 파일로 저장을 하게 된다.

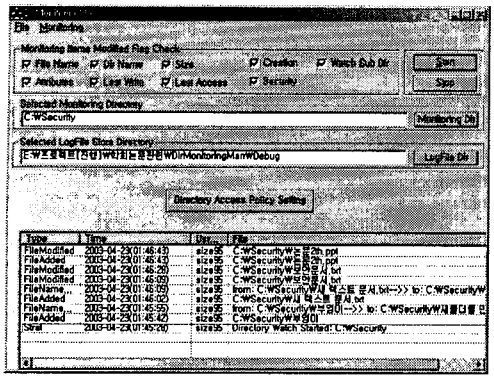
3.3 시스템 구현

본 절에서는 앞절의 윈도우 파일 접근 모니터링 방법 및 시스템 설계에 따라 실시간 파일 접근 모니터링 시스템의 구현에 대하여 기술한다.

본 시스템은 Windows 2000 서버 환경에서 C++, MFC를 이용하여 구현하였다. 사용자에 대한 권한 정책 및 파일 모니터링 로그와 비인가자에 대한 불법적인 행위 로그들은 텍스트 파일로 저장을 하였다.

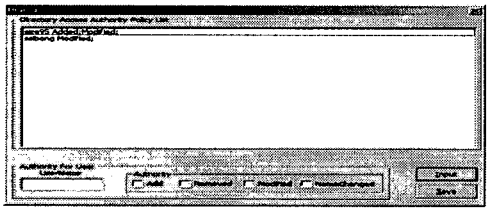
실시간 파일 접근 모니터링 시스템의 단계별 처리를 나타내면 아래와 같다.

① 모니터링 대상 디렉토리 및 모니터링 로그 저장 디렉토리를 선택한다.
② 모니터링에 적용될(검사하고자하는) 파일 속성 항목들의 값을 체크한다.
  - 파일이름변경검사, 폴더이름변경검사,
  - 파일사이즈검사, 최근엑세스시간검사,
  - 최근수정한시간검사, 보안속성검사,
  - 서브디렉토리까지검사여부 체크
③ 모니터링 대상 디렉토리에 대한 윈도우 사용자별 파일 접근(화일 생성, 삭제, 수정등) 권한을 설정한다.
④ 파일 모니터링을 시작, 실시간으로 모니터링을 한다.
⑤ 특정 디렉토리 파일에 대한 접근이 있을 경우 접근시간, 접근행위, 접근사용자, 접근화일에 대한 로그를 저장 및 화면에 디스플레이 한다.
⑥ 특정 디렉토리 파일에 대한 접근자를 기입력한 사용자별 파일 접근 정책과 비교, 만약 정책에 위반된 불법적인 접근이라면 별도의 로그화일에 로그을 기록한다.

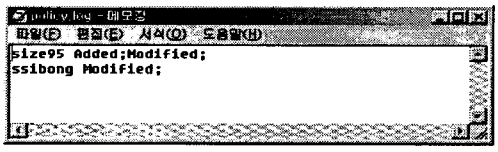


<그림 2. 실시간 파일 모니터링 실행 화면>

그림2는 실시간 파일 모니터링이 실행되는 화면으로 "C:₩Security"라는 폴더에 사용자의 파일에 대한 접근 행위를 모니터링하는 화면이다.
그림3과 그림4는 사용자별 파일 접근 권한을 설정하는 화면과 저장 파일을 나타낸다. 이 파일은 파일 접근 권한 정책 비교에 사용된다.

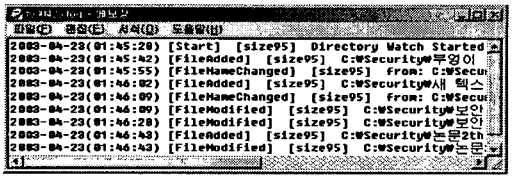


<그림 3. 사용자별 파일 접근 권한 설정 화면>

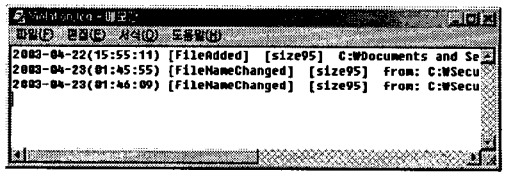


<그림 4. 사용자별 파일 접근 권한 파일>

그림5와 그림6은 실시간 파일 접근 모니터링을 한 결과를 저장한 로그화일이다.



<그림 5. 실시간 파일 접근 모니터링 로그 파일>



<그림 6. 파일접근 권한정책에 위반된 접근 로그 파일>

그림5는 파일에 대한 사용자 접근이 있을 때마다 로그가 생성되며, 그림6은 파일접근 권한에 위배된 행위를 할 때 생성된다.

4. 결론

본 논문에서는 다중 사용자가 공용하는 윈도우 서버 환경에서 서버의 디렉토리나 파일에 접근하는 사용자를 모니터링 하고, 비밀문서 접근 즉, 파일의 수정, 삭제 등에 대한 행위를 실시간적으로 모니터링 하는 시스템을 구현하였다. 이 시스템은 사용자별 파일 접근행위 기록 및 사용자별 권한 위반 행위 기록과 비밀문서에 대한 파일 무결성을 제공한다.
또한 구현한 시스템은 조직의 합법적인 내부 사용자에 대한 파일의 접근 및 행위내용을 감독함으로써 책임추적성(Accountablity)을 제공하는데 목적이 있다.
향후 연구계획으로는 모니터링한 결과에 대한 적절한 대응 방안이 있다.

[참고문헌]

[1] 박정진, "NT서버 실시간 이벤트 감시 시스템의 설계 및 구현", 석사학위논문, 대전대학교, 2003.
[2] Richard, Barber. "The Evolution of Intrusion Detection systems - The Next Step", Computer&SEcurity, 2001.
[3] Chirillo, John, "HACK ATTACKS REVEALED" , WILEY, 2001.
[4] "로그파일 위·변조 방지 기술", http://www.kisa.or.kr/technology/sub3/logfile.html
[5] "접근통제 기술 개요", http://www.kisa.or.kr/technology/sub3/AC_9901.html
[6] http://www.certcc.or.kr
[7] http://www.ahnlab.co.kr