보안운영체제의 보안 로그 관리에 관한 연구

정창성*, 박태규**, 조인구*, 임연호*
*티에스온넷㈜ 정보보호연구소, **한서대학교
e-mail:csjung@tsonnet.co.kr

A Study on Management of Security Logs of Secure OS

Chang-Sung Jung*, Tae-Kyou Park**, In-Gu Jo*, Yeon-Ho Im*
*Research Center, TSonNet Co.,Ltd., **Hanseo University

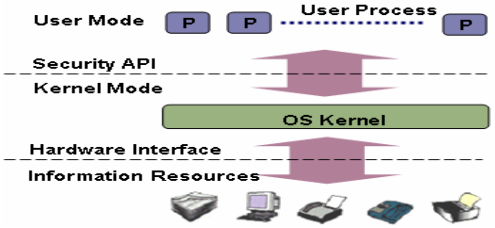
요 약

대부분의 기관들은 악의적인 행위들을 포착하거나 시스템과 데이터를 보호하고 사고에 대응하기 위한 시도들을 지원하기 위해 몇 가지 형태의 네트워크 기반 보안솔루션을 사용하고 있다. 하지만 기존 네트워크 레벨 보안의 한계로 인하여 시스템 상에서 일어나는 행위를 제어하기 위한 차세대 보안솔루션으로 보안운영체제를 도입하고 있다. 최근에는 전자금융거래법 등의 세칙에 의해 정보처리 시스템 내의 정보의 유출, 변조 및 파괴 등을 보호하는 것은 물론 세부 작업 내역의 로깅에 대한 요구가 지속적으로 증가하고 있다. 이에 본 논문에서는 보안레이블에 의한 시스템 보안 강화 기술을 소개하고 강제적 접근 제어 결과에 의해 생성되는 보안 로그에 대한 구체적인 관리 전략을 제시한다.

1. 서론

오늘날 급속히 보급되어 사용되고 있는 컴퓨터 시스템에 대한 보안 문제점으로 인하여 많은 형태의 공격자 침입 및 자료 유출, 무단 변조 등의 사고가 증가하고 있으며 이에 대응하기 위한 보안의 필요성 또한 더욱 증가하고 있다. 국가의 중요 정보통신 기반구조를 보호하기 위한 기술은 정보통신 기반구조 방어기술 및 공격기술로 분류할 수 있으며, 방어기술의 핵심 중의 하나는 정보시스템을 보호하기 위한 보안 운영체제 기술이다[1]. 국가 정보통신 기반구조는 정보 통신망 및 정보 시스템으로 구성되어 있으므로 정보통신 기반구조의 구성 요소를 보호하기 위해서는 근본적인 보안 기술을 소유해야 한다.

이미 1970 년대부터 미국이나 유럽 등의 선진국에서는 중요 정보 및 비밀 정보 처리를 위한 컴퓨터 시스템의 필요성을 인식하여, 신뢰성을 평가할 수 있는 기준을 제정하는 한편, 보안운영체제를 연구하여 안전하고 신뢰성 있는 컴퓨터 시스템 개발에 박차를 가하기에 이르렀으며, 1980 년대 이후부터는 운영체제의 커널 수준에 안전한 운영체제를 탑재한 컴퓨터 시스템이 보급되기에 이르렀다. 미국의 경우, 신뢰성 컴퓨터 평가 기준(TCSEC : Trusted Computer System Evaluation Criteria)[2]에 기반한 컴퓨터 시스템에서는 안전한 운영체제의 구현 대부분을 보안 커널(Security Kernel)로 구현하고 있으며, 높은 보안 수준으로 평가받은 컴퓨터 시스템에 대해서는 해외로 수출을 금지하고 있다. 다음 그림은 보안운영체제 상에서 보안 커널이 탑재되는 위치를 보이고 있다.

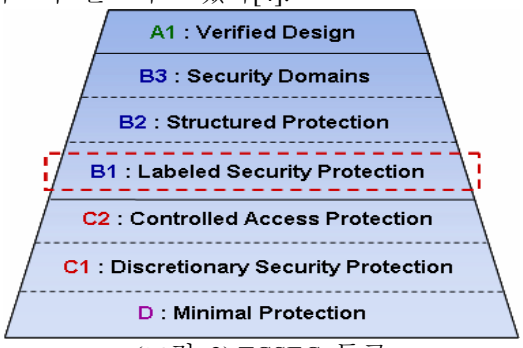


(그림 1) 보안 커널

세계 표준화 기구에서도 1980 년대 중반부터 전 세계의 네트워크가 확장되고, 정보의 유통이 활발해짐에 따라 발생되는 많은 역기능적인 보안의 문제점을 최소화시키기 위하여 보안성 컴퓨터에 대한 표준화에 노력을 기울인 결과로 1998 년 ISO/IEC/JTC1 에서 CC (Common Criteria) Version 2 기준을 내놓은 실정이다[3]. 국제공통 평가기준인 CC 는 접근통제, 무결성, 감사추적, 신분확인, 키 관리 등의 정보보호 전 분야에 대한 포괄적인 보안요구 사항뿐만 아니라, 요즈음 새로이

등장하고 있는 보안 엔지니어링 개념을 도입한 보증 요구사항도 포함하고 있다.

TCSEC 에서는 다음 그림과 같이 7 가지 등급으로 분류하여 각 기관별 특성에 맞는 시스템을 도입 및 운영하도록 권고하고 있다[4].



(그림 2) TCSEC 등급

이러한 보안운영체제에서는 운영체제의 보안을 강화하기 위해서 사용자의 접근을 차단하며, 자원에 대한 사용을 제어할 수 있는 다중등급보안(MLS : Multi Level Security) 모델을 제시하고 있다. 이 모델에서는 특정 권한이 있는 사용자에게만 특정 데이터 또는 자원이 제공되는 것을 보장하기 위해 접근 제어를 구현하고 있다[5]. 보안운영체제는 주체와 객체에 보안레이블을 부여하고 다중등급보안 정책을 적용하여 강제적 접근제어를 시행하게 된다. 이러한 강제적 접근제어는 TCSEC B1 급 이상의 컴퓨터에서 반드시 요구되는 중요한 기술이다.

보안운영체제를 포함하여 다양한 보안 솔루션에서 발생하는 보안 로그는 보안 로그 관리에 대한 필요성을 낳게 되었다. 로그 관리는 컴퓨터의 보안 기록이 일정한 시간 동안 안전하고 체계적으로 보관되고 있다는 것을 증명하기 위해 필수적이다. 정기적인 로그 분석은 보안 사건이나 정책의 위반, 부정한 행위 그리고 운영상의 문제점 등을 식별해 내는데 효과적이다. 1996 년도 “건강보험 통산제와 기록보존의무에 관한 결의(HIPAA)”, 2002 년도 “연방 정보보안 관리 결의(FISMA) ” , “ Sarbanes-Oxley 결의(SOX) ” , “ Gramm-Leach-Bliley 결의(GLBA)", "지불카드산업에 대한 데이터 보안기준(PCI DSS)" 등과 같이 미국 정부들이 규정하는 법률과 규칙들의 요구수준에 부응하기 위하여 특정 로그들을 보관하고 분석할 수 있어야 한다[6]. 일본에서는 이러한 정보보호관련 통제 법안을 2008 년부터 본격적으로 적용할 예정이며 국내에서도 2007 년부터 전자금융거래법 제정안의 시행으로 금융권과 공공시장의 정보보호에 대한 책임, 의무가 강화됨에 따라 보안 로그 분석 수요가 계속적으로 확산될 것으로 예상된다. 이와 같이 보안 로그는 내부적인 조사를 지원하고 기반을 확립하여 운영상의 흐름과 장기적인 문제점들을 구별해 냄으로써 포렌직 분석을 실시하는데 있어서 매우 유용하다.

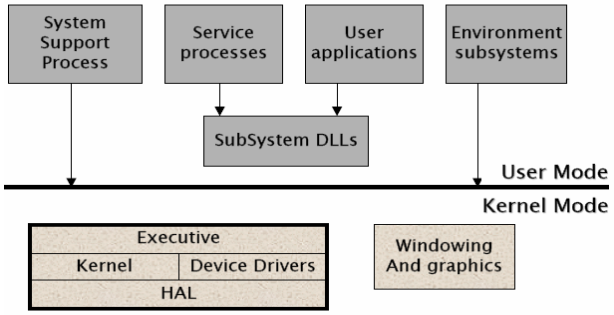
그리하여 본 논문에서는 효율적으로 접근을 제어하기에 적합한 수정된 BLP(Bell & LaPadula) 모델을 적용하여 윈도우 커널에 다중등급보안 강제적 접근제어(MAC : Mandatory Access Control) 시스템을 구현하여 시스템 자원에 대한 사용자의 접근을 제어하고, 중요 파일에 보안레이블을 설정하여 접근을 제어하고 보안 로그를 생성하여 시스템의 피해를 최소화하기 위한 모델을 제시하고 구현하였다. 추가적으로 다중등급보안 시스템이 구현된 윈도우 시스템을 실시간으로 감사 추적할 수 있도록 감사 기능을 구현하였다.

본 논문은 2 장에서는 윈도우 운영체제 상에서 보안운영체제의 보안 커널을 구현하기 위한 파일시스템 필터 드라이버 구현 기술을 중심으로 기술하고, 3 장에서는 구현된 강제적 접근제어 시스템에서 생성되는 로그를 포함하여 시스템 내의 모든 보안 로그를 관리하기 위한 방법에 대해 기술한다.

2. 강제적 접근 제어 시스템의 구현

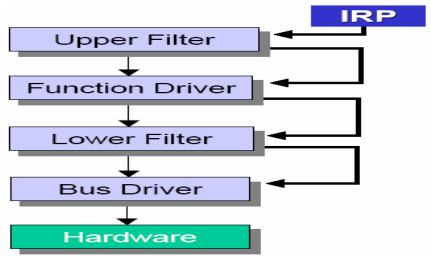
윈도우 운영체제 상에서 수정된 BLP 모델을 구현하기 위해서는 커널 모드에서 동작하는 파일시스템 필터 드라이버(FSFD : File System Filter Driver)를 작성하여야 한다[7].

윈도우 드라이버 모델(WDM : Windows Driver Model)의 계층상 평션 드라이버는 디바이스의 주된 기능 및 기초 I/O 연산을 관리한다[8]. 파일시스템에서의 평션 드라이버인 파일시스템 드라이버는 운영체제 내의 파일을 관리하기 위한 시스템 드라이버이다. 즉, 파일 읽기, 쓰기, 변경 등 파일과 디렉터리에 관련된 모든 동작을 수행한다. 파일시스템 드라이버는 드라이버 스택의 최상위층에 위치하며 Cache Manager 와 Virtual Memory Manager, I/O Manager 등과 연동관계에 있다. 다음 그림은 윈도우 시스템의 구조를 보이고 있다.



(그림 3) 윈도우 NT 구조

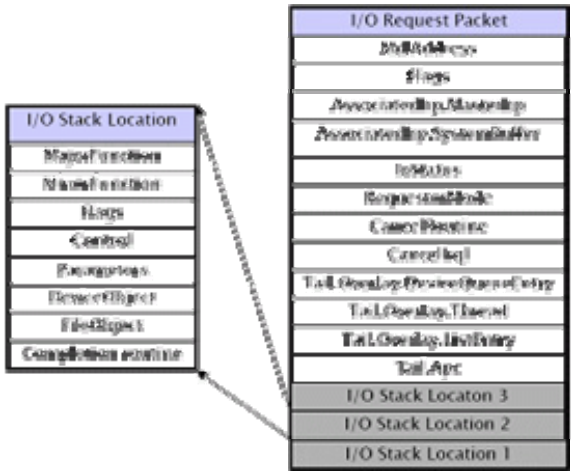
다음 그림 4 에서와 같이 평션 드라이버의 상위 혹은 하위에 위치하여 표준적인 행동을 변경하는 드라이버를 필터 드라이버라고 한다. 실제 디바이스에 값을 추가하거나 상태를 수정하는 선택적인 드라이버라고 말할 수 있다. 파일시스템 상에서의 파일시스템 필터 드라이버는 특정 드라이버와의 입출력을 감시하거나 지원되지 않는 기능들을 추가할 목적으로 작성된 드라이버이다[8,9]. 바이러스 체크를 위한 드라이버나 파일 암복호화 기능을 지원하는 드라이버 등은 파일시스템 필터 드라이버의 한 예라고 할 수 있다. 파일시스템 필터 드라이버는 일반적인 장치 관리자 보다는 윈도우 운영체제의 파일시스템과 밀접한 관련이 있다.



(그림 4) 윈도우 드라이버 계층 구조

실질적으로 다른 WDM 드라이버를 구현할 때와 마찬가지로 필터 드라이버를 구현할 때도 드라이버가 처리할 것으로 예상되는 IRP(Io Request Packet)의 타입들을 제외한 IRP 의 모든 타입을 위해 디스패치 루틴을 등록해야 한다. IRP 는 운영체제가 커널 모드 드라이버와 통신하기 위해 사용하는 구조체이다. 커널 모드 드라이버가 IRP 를 생성할 때면 해당 IRP 와 조합된 IO_STACK_LOCATION 구조체가 생성된다. 이 구조체는 IRP 를 처리할 각각의 드라이버를 위한 스택 공간과 IRP 를 위한 타입 코드와 매개 변수 정보 등을 포함하고 있다[8,9].

다음 그림에서 MajorFunction 은 IRP 와 관련된 주된 함수 코드이다. 이는 드라이버 객체의 MajorFunction 테이블 안의 디스패치 함수 포인터 중의 하나와 일치하며 IRP_MJ_CREATE 등과 같은 값을 갖는다. 이 코드는 특정한 드라이버를 위한 I/O 스택 공간에 있다. IRP 는 IRP_MJ_CREATE 와 같이 IRP 를 시작할 수 있고 드라이버의 스택 하위로 진행되면서 그 밖의 무엇인가로 변형된다고 할 수 있다.



(그림 5) IRP 와 IO_STACK_LOCATION

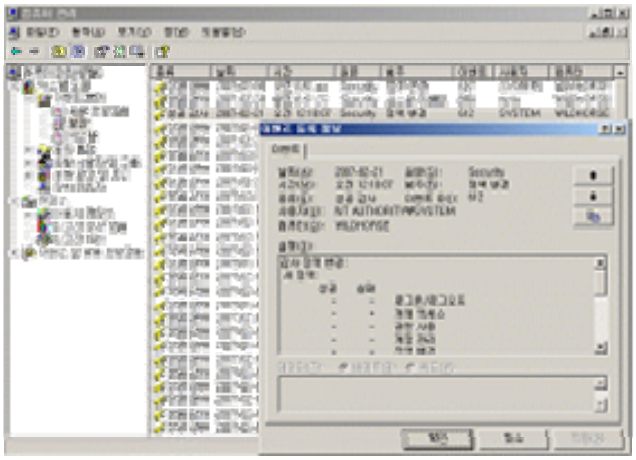
강제적 접근제어 및 실행, 변조 제어는 본 논문에서 구현한 파일시스템 필터 드라이버의 핵심이다. 이를 위해 데이터를 파일시스템에 전송하기 전 필터링하여 필요한 작업을 수행하기 위한 선처리 루틴과 파일시스템에서 처리한 IRP 결과를 응용단에 리턴하는 시점을 필터링하여 필요한 작업을 수행하는 후처리 루틴으로 구분하여 처리한다.

선처리 과정에서 다루는 IRP 는 IRP_MJ_CREATE 와 IRP_MJ_SET_INFORMATION 이다. 응용단에서 특정 객체를 접근하기 위한 IRP 를 생성하면 주체 및 객체의 보안레이블을 확인하여 접근 권한을 체크하여 접근 제어를 실시하고 보안 로그를 생성된다. 후처리에서는 IRP_MJ_CREATE 요청의 IRP 를 대상으로 객체 생성시 주체의 보안 레이블을 상속하여 객체의 보안 레이블을 생성한다.

3. 구체적인 보안 로그의 관리 전략

로그 데이터에는 보안, 성능, 오류, 경고 및 운영 정보 등의 중요 정보가 기록되어 있다. 이러한 컴퓨터 로그들은 안티바이러스 소프트웨어나 방화벽 혹은 침입 탐지 시스템과 같은 보안 소프트웨어, 서버, 워크스테이션 그리고 네트워킹 장비의 구동시스템, 그리고 수 많은 응용프로그램들은 물론 본 논문에서 구현한 다중등급보안 시스템으로부터 생성된다.

기존 윈도우 운영체제의 감사 추적은 정적으로 기록된 사건 로그 파일을 이용하여 그림 6 과 같이 별도의 이벤트 뷰어와 같은 감사 추적 프로그램을 통해서 가능하였다[10]. 이 경우 시스템 관리자 등에 의한 실시간 추적이 불가능할 뿐만 아니라 운영체제 내부에서 감지되는 다양한 사건 정보의 획득이 어렵다. 본 논문에서는 높은 수준의 보안성을 제공하는 다중등급보안 시스템을 구현하는 것은 물론이고 그에 적합한 감사 추적 시스템을 설계하여 완벽한 보안 시스템을 구현하였다. 즉, 다중등급보안 윈도우는 주체의 객체에 대한 일체의 접근을 통제하는 참조 모니터를 통해 내부 또는 외부 침입 및 자료 유출을 운영체제 커널 모드에서 접근을 제어하고 추가적으로 로그를 저장하기 위한 데이터베이스를 구축하여 실시간으로 추적할 수 있도록 하였다.



(그림 6) 윈도우 이벤트 로그

본 논문에서 구현한 강제적 접근제어에 의해 발생하는 보안 로그를 포함하여 시스템 내의 모든 로그들을 관리하기 위한 방법을 제시한다. 로그는 본디 문제들을 해결하기 위해 이용되어 왔지만 최근에는 시스템이나 네트워크의 효율을 최적화하거나, 사용자들의 행동을 기록하거나, 악의적인 행위들을 조사하기 위해 유용한 데이터를 제공하기 위해 사용되고 있다. 주기적으로 로그를 검토하고 분석하는 것은 보안사건이나 정책의 위반, 부정한 행위와 운영상의 문제점들이 발생한 직후에 이들을 식별해 내고 해결하는데 유용한 정보를 제공한다는 점에서 유익하다. 로그는 또

한 기관의 내부적인 조사를 지원하고 토대를 확립하며 운영상의 흐름과 장기적인 문제점들을 구별해 냄으로써, 감사를 실시하거나 포렌직 분석을 실시하는데 매우 유용하게 이용될 수 있다.

보안 로그 관리 및 분석은 일관성이 없는 로그의 항목과 포맷 그리고 발생 시간 기록과 로그 소스들의 다양성과 발생빈도 등의 문제점 때문에 초기의 로그 생성과 관련하여 잠재적인 문제점이 있다. 로그에 대한 분석을 용이하게 하기 위해 다른 항목과 포맷으로 된 로그들을 하나의 표준 포맷과 고정된 데이터 필드로 변환시키는 작업을 수행해야 한다. 또한 모든 로그 발생 서버에 대한 시간을 일정하게 동기화하여 관리할 필요성도 있다. 사건 분석에 대한 오해 소지와 각 시스템에서 발생하는 사건간의 시간 간격의 계산 오류를 방지하기 위해 윈도우 운영체제는 시스템 시간을 인터넷상의 시간 서버와 동기화 시켜주는 Windows Time 서비스를 제공하고 있다[10].

로그를 관리하는데 있어서 유의할 점은 생성된 로그의 기밀성, 무결성 그리고 유효성이 부주의로 혹은 의도적으로 파손될 수 있다는 것이다. 로그 관리는 로그의 유용성을 보장하는 것과 함께, 로그의 기밀성과 무결성을 파손의 위험으로부터 보호하는 것도 포함한다. 그렇기 때문에 보안 로그 자체에 대한 보안에도 관심을 기울여야 한다. 로그 파일에 대한 접근을 제한해야 하며 각 로그 항목을 생성하는 프로세스도 안전하게 보호해야 한다. 각 시스템에서 중앙화된 로그 관리 서버로 로그 데이터를 전송할 때에는 암호화 등의 보안 메커니즘을 적용해야 한다. 본 논문에서는 로그 파일이 저장되어 있는 디렉터리에 보안레이블을 부여하여 권한이 없는 사용자의 로그 파일에 대한 접근을 원천적으로 차단하였다.

공격에 대한 근원지를 찾아낼 수 있다면 공격으로 인한 자산의 손실에 대해서 공격자에게 법적 책임을 묻기 위해 로그를 증거로 제출할 수 있을 것이다. 이렇듯 보안관리를 위해서는 시스템에서 발생할 수 있는 취약점 점검 및 제거와 같은 예방활동도 중요하지만 만일의 사고에 대비하여 로그를 관리하고 주기적으로 분석하는 작업 또한 중요한 것임을 알 수 있다.

4. 결론

본 논문에서는 강제적 접근제어 정책을 적용하여 다중등급보안 윈도우 시스템을 구현하기 위해 참조모니터 기능을 수행하는 보안 커널을 설계하고 구현하였다. 강제적 접근제어에 의해 생성되는 보안 로그는 현재 윈도우 운영체제 수준의 정보보다 구체적이고 사건의 원인 규명적인 정보를 획득한 다음 데이터베이스화하여 관리하였다. 그 결과 시스템 침입이나 자료의 유출 및 변경 등을 실시간으로 감시할 수 있다는 측면에서 보안 기능이 강화되었다. 추가적으로 향후 포렌직 분석 등을 고려하여 보안 로그를 효율적으로 관리할 수 있는 방안을 제시하였다.

기존 BLP 모델을 시스템에 적용하기에 부적절한 부분이 있어 이를 수정한 BLP 모델을 정의하고 구현하였다. 수정된 BLP 모델을 적용한 강제적 접근제어는 사용자의 차별적인 보안등급을 통해 정보를 보호 관리할 수 있다. 즉, 보안등급이 부여되지 않은 사용자 또는 보안등급이 맞지 않는 사용자가 임의적으로 보안등급을 갖는 파일, 디렉터리, 레지스트리에 대한 읽기, 쓰기, 실행 등의 접근을 커널 모드에서 원천적으로 차단할 수 있다. 즉, 공격용 프로그램 등을 이용하여 시스템 관리자의 권한을 획득하더라도 보안등급을 획득할 수 없기 때문에 파일을 불법적으로 변조하는 것을 방지하는 것과 같이 원천적으로 시스템 보안을 가능하게 하며 이를 이용하여 상위 레벨 즉, 어플리케이션에서 보안 기능을 추가로 이용하기 쉽게 할 수 있다는 장점을 제공한다.

이와 같이 구현된 시스템은 커널에서 동작하기 때문에 운영체제의 하위 계층인 커널에서 정보보안의 주요 결정이 이루어진다. 그 결과 정보가 존재하는 기억장치의 가장 근접한 곳에서 접근제어가 이루어지므로 시스템의 오버헤드를 줄일 수 있어 정보보안에 따른 성능저하를 최소화할 수 있다.

본 논문에서는 객체에 보안레이블을 부여하기 위해 윈도우 NTFS 파일시스템에서 제공하는 확장 파일 속성 영역을 사용하였는데 이 필드는 구조적으로 한계가 있기 때문에 보안등급 및 보호범주를 설정하는데 있어서 범위가 한정적이거나 다양하게 보안레이블을 사용하는데 있어서 제한된다. 또한, 다른 프로그램에서 같은 필드를 사용하는 경우가 발생할 수 있으며, 차후 파일시스템 변경 등의 원인으로 인하여 확장 파일 속성을 사용하는데 예기치 않은 문제가 발생할 수 있다. 이러한 문제점을 근본적으로 해결하기 위해서는 운영체제 차원의 지원이 필수적이다. 즉, 공통된 표준을 마련하고 이를 기반으로 안정적이면서도 시스템 성능에 최소한의 영향을 미치도록 설계된 강제적 접근 제어 솔루션을 만들어야 한다.

참고문헌

[1]Bell. D. and Lapadula, "Secure Computer System : Mathematical Foundations and Model", MITRE Report MTR 2547, v2 Nov. 1973.

[2]DoD, “Trusted Computer System Evaluation Criteria”, DoD 5200.28.STD, 1985.

[3]ISO/IEC JTC1/SC 27, Information Technology-Security Techniques-Security Information Objects, N2315, 1999.

[4]http://www.radium.ncsc.mil/tpep/epl/

[5]NIST, Minimum Security Requirements for Multi-user Operating Systems, 1993.

[6]http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

[7]Rajeev Nagar, “Windows NT File System Internals” O'Reilly. 1997.

[8]Walter Oney, "Programming the Windows Driver Model", Microsoft Press, Sep. 1999.

[9]Dabak, Phadke and Borate, "Undocumented Windows NT", M&T Books, 1999.

[10]http://technet.microsoft.com