다중등급보안정책(MLS)에서 개선된 참조모니터

이승민, 이영구, 이상훈, 전문석
숭실대학교 컴퓨터학과
e-mail:cowaboonga@hotmail.com

Enhanced Reference Monitor on MLS(Multi Level Security) Policy

Seung-Min Lee, Young-Gu Lee, Sang-Hun Lee,
Moon-Seog Jun
Dept of Computer Science, Soong-sil University

요 약

정보보호를 위해 네트워크 수준에서의 침입탐지 시스템이나 방화벽 시스템을 사용한다. 그러나 외부에서의 공격을 네트워크 수준에서 미처 대비하지 못하였을 경우에는 각 호스트들은 무방비 상태이므로 공격받을 경우 침형적인 피해를 입을 수 있다. 이러한 피해를 막기 위해서는 운영체제단에서의 대비가 필요하다. 이에 본 논문에서는 보안 운영체제 연구에 대한 동향을 살펴보고, MLS(Multi Level Security)정책을 사용하는 보안 운영체제에서 보안등급이 서로 다른 주체와 객체의 긴급접근이 이루어져야 할 때, 기존 MLS의 참조모니터(Reference Monitor)를 개선시켜 접근을 해결하는 방안을 제시했다.

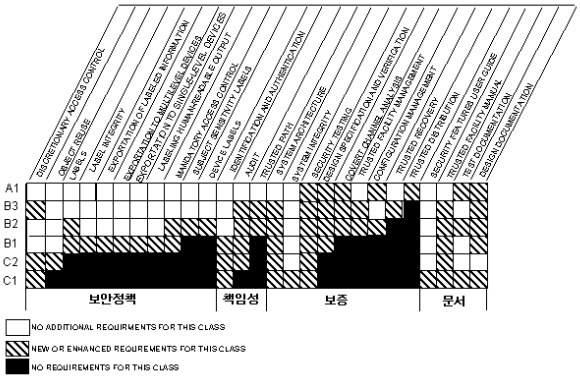
1. 서론

전 세계의 네트워크를 통한 해킹기법이 점차 다양화 되고, 지능화됨에 따라 오로지 네트워크 수준에서의 해킹 차단은 새로운 해킹수법에 의해 하루아침에 무너지고 있는 실정이다. 국가적으로 중요하고 기밀문서나 정보를 관리하는데 있어서 네트워크 수준의 해킹 차단만 믿는 다는 것은 집안의 보안 안전장치 없이 울타리에만 신경 쓰는 것과 마찬가지이다. 이런 중요한 정보들이 네트워크를 통해 전 세계로 유통된다면 개인이나, 단체, 기업의 입장에서는 막대한 손해의 결과로 돌아올 것이다. 이를 방지하기 위하여 네트워크수준에서 뿐만 아니라 내부의 각각의 운영체제에 보안 운영체제를 적용하여, 외부 울타리공격방어에는 실패 했더라도 내부에서 다시 한 번 보안을 강화하여 최종공격을 막아낼 수 있는 기능이 필요하게 되었고, 현재 이런 기능을 가지고 있는 많은 보안 OS 제품들이 출시되고 상용화 되었다. 이 논문에서는 긴급업무 발생시, MLS정책에서 보안등급이 다른 주체와 객체간의 접근을 허용할 수 있도록 모바일을 통한 임의 접근 허가 방법을 제안하였다. 이 방법은 참조모니터(Reference Monitor)에 긴급 접근 모듈을 삽입하는 것이다. 본 논문의 구성은 2.2절과 2.3절에서 커널 수준에서 구현된 강제적 접근통제(MAC : Mandatory Access Control) 모델인 BLP(Bell & LaPadula) 분석하고, 2.4절에서는 이 모델을 적용한 다중등급보안(MLS)에 대해 개략적으로 기술을 하였다. 3절에서는 MLS정책상의 제약사항을 다루었고, 4절에서는 제약사항을 해결할 방안을 제시하였다. 5절에서는 결론과 향후 연구과제로 본 논문을 마무리 지었다.

2. 보안 OS 관련 연구

컴퓨터 보안 기술 분야는 접근제어와 비밀성을 다룬다. 미국의 국방부, NIST, MITRE 안전한 컴퓨터 시스템의 계속적인 연구로 TCSEC(Trusted Computer System Evaluation Criteria)초안이 제정되고 국방부 표준으로 채택되었다[1]. TCSEC을 7가지 등급(D, C1, C2, B1, B2, B3, A1)으로 분류하고 각 기관별 특성에 맞는 컴퓨터 시스템을 도입하도록 하고 있다. TCSEC은 보안정책(Security Policy), 책

임성(Accountability), 보증(Assurance) 및 지속적인 보호(Contiguous Protection)등의 기본적인 컴퓨터 보안을 요구한다. 안전한 컴퓨터가 갖추어야하는 보안정책과 신분확인, 감사 추적 등의 책임성, 보증 및 문서부분으로 나누어서 그림 1과 같이 각 등급별 요구 사항을 명시하고 있다.



(그림 1) TCSEC 등급별 보안요구사항

2.1 다중등급 보안의 개요

MLS는 주체와 객체간의 상호작용을 지원하는 BLP 모델의 일종이다. 보안정책 데이터베이스를 사용해서 사용자(주체)와 해당 MLS 범위를 결정할 수 있다. Source와 Target 범위간의 관계를 결정함으로써 접근이 결정 된다.

2.2 BLP 모델

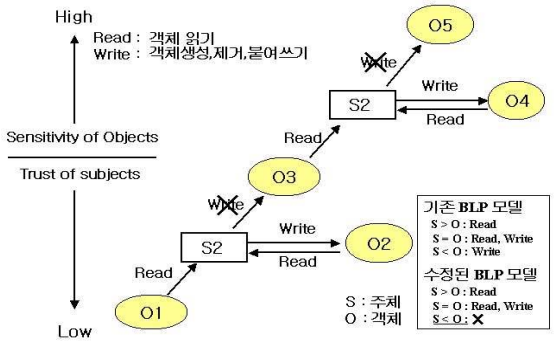
접근제어의 방법으로 DAC(Discretional Access Control)과 MAC(Mandatory Access Control)이 있다. 리눅스에서는 일반적으로 임의적 접근제어(DAC)를 사용하고 있다[2]. DAC은 ID에 근거하여 객체에 대한 접근을 제한하는 방법이다. 접근 제어는 개체의 소유자에 의하여 임의적으로 이루어진다. 따라서 접근 허가를 가지고 있다면 다른 주체에게 자신의 권한을 넘겨 줄 수도 있다.

MAC 정책은 객체에 포함된 정보의 비밀성과 주체가 갖는 권한에 대한 접근을 제한한다. 많은 MAC 기법들은 다중등급보안정책에 근간을 두고 있다. 그래서 다중등급보안과 MAC을 분리하여 생각할 수 없고 컴퓨터에 저장된 정보의 보호를 위해 사용하는 방법 중 하나가 MAC를 이용하고 이것의 최초의 수학적 모델이 BLP 모델 이다[3]. 사용자 임의로 접근 제한을 변경하지 못하도록 제한함으로써 Root 권한 탈취 시 권한 남용의 피해를 줄일 수 있다. BLP 모델에서 수정된 BLP 모델은 (그림 2)와 같다.

BLP 모델의 정책

주체 S는 객체 O를 오직 C(S) >= C(O) 일 경우에만 읽을 수 있다. (1) 주체 S는 객체 O를 오직 C(S) =< C(O) 일 경우에만 쓸 수 있다. (2) C(S):Clearance(Subject) C(O):Clearance(Object)

원래 BLP의 모델은 (2)에서와 같이 C(S) <= C(O) 일 경우에도 쓰기 연산을 허용했으나, 수정된 BLP



(그림 2) 수정된 BLP 접근제어 모델

에서는 낮은 등급의 주체가 더 높은 등급의 객체를 붙여 쓰기, 삭제가 가능하다는 것은 보안상으로 문제가 발생되기 때문에 쓰기 연산을 제한했다.
따라서 다음과 같이 수정이 되었다.

수정된 BLP 모델 정책

주체 S는 객체 O를 오직 C(S)=C(O)일 경우에만 쓸 수 있다. (3)

주체 S는 객체 O를 등급이 같은 경우에만 read/write가 가능하고, 객체보다 등급이 높은 경우에는 낮은 등급의 객체를 read만 가능하다. BLP 모델의 성질을 이용하여 정보의 불법적인 흐름을 차단하게 되었다.

2.3 MAC

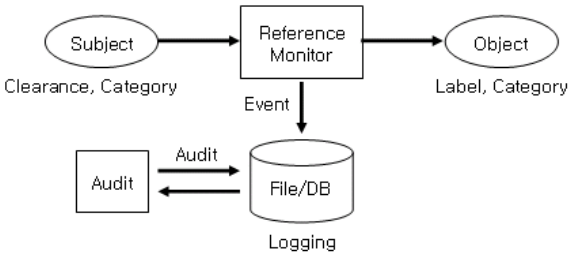
BLP의 모델의 성질을 적용하기 위하여 강제적 접근 제어(MAC)를 사용하는데, 한 상용화된 제품에서는 각 파일마다 보안 레이블을 적용한다. 리눅스의 Ext2 파일 시스템내의 디스크의 i-node 구조에 보안 등급과 카테고리를 삽입하여 각 파일 마다 보안 등급과 카테고리를 갖게 되며, Root 권한일지라도 보안 등급과 카테고리가 보안정책에 따라 아무 파일에나 접근 권한이 부여 되지 않는다.

2.4 MLS

MLS는 1960년대 후반 미국의 국방성에서 시작되었다. 컴퓨터의 발전으로 종이 형태로 보관되던 정보는 컴퓨터 옮겨지게 되었고, 종이가 갖고 있던 보안등급도 컴퓨터로 옮기게 되었다. MLS에서 사용하는 정책은 군사 보안정책에서 유래되었고, 보안정책은 문서에 대한 보안등급과 문서에 접근하고자 하는 사람의 보안등급을 비교해 주는 것이었다. 현재의 MLS는 주체의 보안등급이 객체의 보안등급과 같거나 클 경우에 접근이 허가 되며, 주체의 카테고리는 객체의 카테고리를 포함해야 접근이 허가된다.

3. MLS정책상의 제약사항 도출

기존의 상용화 된 제품의 경우 MLS 정책에서 Reference Monitor의 기능은 권한이 없는 사용자가 불법적인 접근 또는 악의적인 목적으로 시도되는 해킹을 Reference Monitor가 판단하여 차단시킨다. (그림 3)과 같이 보안등급, 보호범주와 객체의 레이블, 보호범주를 비교하여 강제적 접근 제어를 하게 된다. BLP모델을 기초하여 주체 S는 객체 O를 오직 C(S)=C(O)일 경우에만 쓸 수 있다.

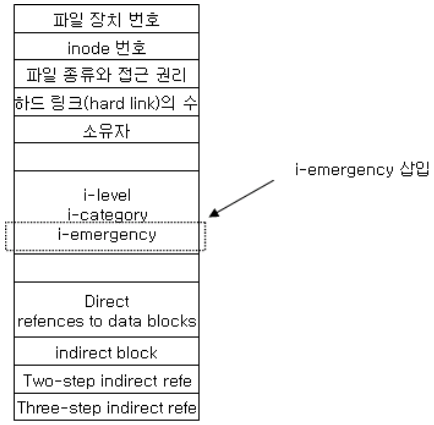


(그림 3) Reference Monitor 구성도

BLP모델은 MLS을 위한 가장 기본적인 규칙이라 할 수 있다. 그러나 보안상에 있어 위와 같은 강제적 접근제어(MAC)를 사용하는 것은 가장 큰 장점이면서 단점으로 작용될 수도 있다. 회사 내에서의 업무상의 경우, 긴급한 상황에서 동료의 부재로 인해 불가피하게 동료의 작업 중인 파일(객체)에 접근해야 할 경우 MLS 정책에 따라 보안등급이 다르기 때문에 위배되어 접근을 할 수 없다. 접근을 시도하기 위해서 작업자는 부재중인 동료와 연락을 시도해야할 것이고, 부재중인 동료의 허락 하에 보안관리자가 객체의 보안등급과 보호범주 변경할 것이다. 그때서야 파일에 접근이 가능 할 것이다. 만약 보안관리자도 부재중이라면 이 긴급 상황을 처리하기 위해 많은 시간이 소비 될 것이다. 또한 객체의 보안등급과 보호범주를 변경하게 되면 뜻하지 않은 정보의 노출이 우려될 수 있고 회사는 큰 손해를 입을 수 있다.

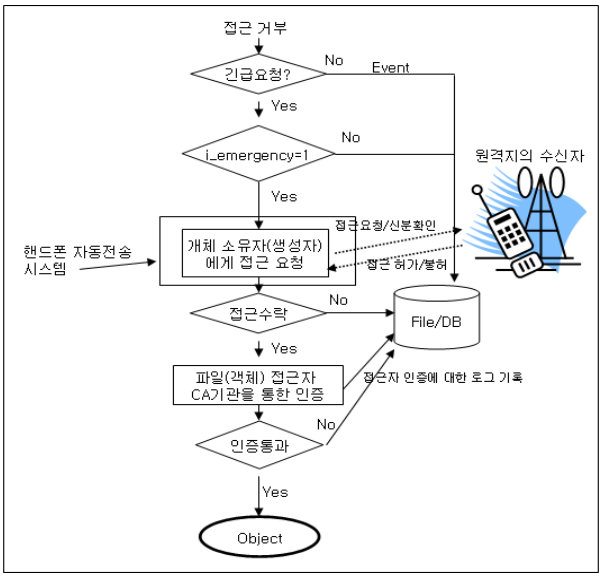
4. MLS 제약사항 해결 방안

주체에 대한 보안 레이블 구현을 위해 프로세스마다 존재하는 Process Control Block인 task_struct의 마지막 부분에 보안 레이블을 추가하였고, 객체의 보안 레이블은 리눅스 파일 시스템의 모든 폴더, 파일마다 하나씩 i-node를 가지고 있으므로, Ext2 파일 시스템 내에 예약되어 있는 i-node 구조를 사용하고 있다[4]. (그림 4)는 i-node 구조를 나타내고 있다. 여기에 앞으로 쓰여 질 필드로 i_emergency를 더 추가한다.



(그림 4) 수정한 i-node 구조

i_emergency 필드는 보안등급이 다른 주체와 객체 간의 긴급접근이 요구되는 상황에서 MLS 정책에 위배되더라도 객체 소유자(생성자)에게 접근 요청하기 위해 사용될 필드이다.



(그림 5) 긴급기능을 추가한 Reference Monitor

객체에 접근이 실패하게 되면 기존의 MLS Reference Monitor는 데이터 베이스에 로그를 남기는 것으로 그친다. 하지만 앞에서 다루었던 회사에서의 긴급접근 상황시 문제를 해결하기 위해서 (그림 5)에서와 같이 Reference Monitor에 모듈을 추가하였다. 이 모듈은 객체에 대한 접근이 거부되면 긴급요청의 재접근 시도를 묻게 된다. 재접근에 응하면, i_emergency값을 확인해서 이 객체(파일)이 긴급접근이 가능한지 불허한지를 판단하게 된다.

- i_emergency=1 (긴급접근 가능)
- i_emergency=0 (긴급접근 불가능)

i_emergency 필드는 객체(파일) 생성자(소유자)가 상황에 따라 1로 하거나 0으로 한다. 곧 휴가를 떠날 생성자(소유자)는 대리인의 작업을 위해 1로 설정할 것이다. 그래서 이 객체가 긴급접근이 가능한 객체라면 객체(파일) 소유자에게 핸드폰을 통한 자동 메시지를 전달하게 된다. 예를 들면 “이승민님의 lsm.txt라는 파일에 엘리스가 접근하기를 원합니다. 수락하시겠습니까? 수락은 1번 불가는 2번을 눌러주십시오.” 만약 1번을 눌렀을 경우 “이승민님의 주민번호 13자리와 우물정자를 눌러주십시오.” 라고 메세지가 전송된다. 만약 lsm.txt 파일에 앨리스의 접근이 허가 되었을 때 이 모듈에서는 다시 앨리스의 인증과정을 거치게 된다. CA기관을 통한 앨리스의 인증과정이 진행되고 무조건 데이터 베이스에 앨리스 인증 성공에 대한 로그가 남게 된다. 이것은 휴가 중이던 객체 생성자가 돌아와서 파일 접근 흔적을 확인하기 위함이다. 인증이 통과되면 비록 주체와 객체간의 보안등급이 다르지만 Reference Monitor에서 강제적으로 객체에 대한 접근이 가능하게 만든다. 그리고 인증을 실패하게 되더라도 실패에 대한 로그가 남게 된다. 이로써 긴급접근 상황시에 MLS 정책에 준하여 접근이 불가능 한 것을 i_emergency 필드를 추가하여 접근이 가능토록 해결 방법을 제시하였다. 또 파일 소유자가 먼 곳에 출타 중이어도 핸드폰만 있다면 보안관리자를 거치지 않고 직접 파일접근에 대한 허가를 빠르게 요청할 수 있고 승낙할 수 있다.

5. 결론 및 향후 연구과제

방화벽이나 IDS 같은 보안제품이나 응용 프로그램으로 보안성을 확보하기에는 한계가 있다. 그래서 보안운영체제를 사용하고 Network방어에 실패했을 경우 Host방어를 보안 운영체제가 담당하게 되는 것이다. 본 논문은 여기서 그치는 것이 아니라, 좀 더 개선된 MLS의 Reference Monitor를 제안하였다. 상용화된 제품 중, MLS 정책을 사용하는 제품의 Reference Monitor에 긴급접근 기능의 모듈을 추가함으로 견고한 규칙으로 인해 발생된 문제점들을 유연성 있게 해결하고자 하였다. 이를 통하여 보안성을 유지하면서 동시에 MLS 정책을 깨뜨리지 않는 방법을 제안하였다. 이 방법으로 보안관리자의 간섭 없이 서로 다른 보안등급간의 빠른 임시적(임의적) 접근을 가능하게 할 수 있다.

앞부분의 4장에서 허가 및 인증 과정을 거친 후 엘리스가 강제적으로 객체에 접근시키는 방법은 향후 연구과제로 남기겠다. MLS의 규칙이 여전히 적용되고 있기 때문에 Reference Monitor안에서의 동작 중에 주체(Subject), 위의 예에서 즉, 엘리스의 보안등급을 잠시 동안 객체와 같게 만들고 파일 접근 후에는 원래의 등급으로 전환하는 방법을 연구할 것이다.

톱니바퀴처럼 빠르게 맞물려 돌아가고 있는 현대 산업에 있어서 제때의 한수가, 다시 말해서 제때의 올바른 동작이 나비효과를 나타 낼 수도 있다는 것을 유념해야할 것이다.

참고문헌

[1] ISO/IEC 15408 Common Criteria, common-critera.org 1999. 8.

[2] D. D. Downs et al., "Issues in Discretionary Access Control," Proc. of IEEE Symposium on Security and Privacy, pp.208-218, 1985

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

[4] R. Magnus et al, LINUX KERNEL INTERNALS, 1999

[5] Dod, Trusted Computer System Evaluation Criteia, Dod 5200.28.STD, 1985

[6] 박태규, 이형수, “컴퓨터/네트워크 시스템 보안 표준화 동향분석”, 제 2회 정보 보호와 암호에 관한 워크샵, 1990. 9.

[7] 손형길, 박태규, 이금석 다중등급 보안 리눅스 구현 및 시험 평가, 2003. 4.

[8] Security Enhanced Linux, http://www.nsa.gov/selinux/.

[9] Immunix, http://immunix.org/.