

MLS(MultiLevel Secure) 연구 개발 동향

최창민*, 김상훈**, 정정수*

*동명정보대학교 컴퓨터공학과

**동명정보대학교 정보기술원

A Study On The Development MLS

*ChangMin Choi, **Sanghoon Kim, *ChungSoo Chung

*Dept. of Computer Science, TongMyung University of Information Technology.

**TongMyung Institute of Information Technology

요약

컴퓨터 시스템이 다수의 사용자에게 다수의 응용을 제공하는 특성을 갖게 되면서 데이터 보안 문제에 대한 관심이 높아지게 되었다. 시스템 관리자나 소프트웨어 개발자들은 권한이 있는 사용자들에게만 특정 데이터 또는 자원을 제공하기 위해 서로 다른 종류의 접근제어(Access Control) 구현에 대한 문제가 대두 되었다. 본 논문에서는 특정 사용자에게 데이터 또는 자원을 제공하기 위한 접근제어 방법인 MLS(MultiLevel Secure)의 정의와 구조를 알아보며 MLS의 연구 개발 동향에 대하여 알아본다.

1. 서론

은행, 병원 등의 고객, 내부직원 및 해커로부터의 위협에 따른 금융, 의료 시스템에 대한 보안상의 취약점은 다른 어떤 정보처리 시스템에서 보다도 심각한 결과를 초래할 수 있는 위험 요소를 가진다..

정보시스템에서의 보안 사고는 개인 고객의 피해 차원을 넘어서 사회 전체적인 혼란의 결과를 초래 할 수 있음을 국내외에서 발생되고 있는 신용카드 사고 등의 예를 봐서도 쉽게 알 수 있다.

기업은 기업활동 과정에서 발생하는 다양한 형태의 기업정보를 컴퓨터로 관리하고 있지만 기업의 규모가 커지고 업무과정에서 정보에 관련된 사람들이 많아져 정보에 대한 보안상의 관리가 어려움을 겪게 되어, 업무에 대한 효율성을 떨어트리지 않으면서도 효과적으로 중요정보를 보호할 수 있는 방법을 필요

로 하게 되었다. 이러한 문제점은 특정 사용자에게만 특정 데이터 혹은 특정 자원을 제공하기 위해 서로 다른 접근제어가 필요하게 되었다.[9]

이러한 문제점을 해결하기 위하여, 특정 사용자 층에게 서로 다른 권한을 부여하는 MLS가 제시되었다.

여기서 접근이란 컴퓨터 내의 자원에 대해 어떤 작업을 할 수 있는 능력을 말한다. 접근제어는 그런 능력을 가능하게 하거나 제한 할 수 있는 수단이다. 컴퓨터에 기초한 접근제어는 어떤 사용자(혹은 프로세스)가 시스템의 특정한 자원을 사용 할 수 있는지에 대해 기술하며 어떤 유형의 접근 형태가 허용되는지에 대해서도 기술한다.[1]

본 논문에서는 계층적 접근제어인 MLS의 개발동향에 대하여 알아보며, 2장에서는 MLS 및 BCMLS (Brief-Consistent Multilevel Secure)에 대하여 정의하며, 3장에서는 MLS의 구조를 살펴본다. 4장에서는 MLS

의 관련연구들을 알아보며, 끝으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 MLS의 정의

MLS 모델은 안정성을 위협하지 않으면서도 동일한 데이터에 대한 서로 다른 사용자의 동시 접근을 허락하기 위한 접근 제어 기술의 하나로, 각 사용자는 자신에게 할당된 보안 정책에 맞추어 데이터에 접근할 수 있다. MLS 모델을 이용한 정보 시스템의 미래를 주제로 열린 Conference에서는 MLS 모델이 가져야 하는 특징에 대해 다음과 같이 정의하고 있다. [2]

첫째, 정보시스템 내에 저장된 각각의 데이터에 대해 서로 다른 관점에서의 접근을 허락할 수 있는 능력을 가져야 한다.

둘째, 시스템의 각 사용자는 자신에게 할당된 서로 다른 허가권 (Clearance)과 권한(Authorization)을 가지고 동일한 시스템 내에 포함된 정보를 처리할 수 있어야 한다.

셋째, 자신에게 허락되지 않은 정보나 사용 권한이 없는 데이터에 대한 접근이 금지되어야 하며, 그러한 데이터가 존재한다는 사실조차 알려져선 안 된다.

MLS 모델의 특징은 시스템 구성 요소의 분류에 근거를 두고, 그에 따른 접근 계층을 분류한다는 점이다. 객체의 접근 계층은 하나의 접근 계층 또는 계층 목록을 가질 수 있는 접근 부호로 표시되며, 각각의 사용자는 하나의 접근 계층을 할당 받는다.

MLS 모델에서 각각의 접근 계층은 전체적으로 또는 부분적으로 정렬된 형태의 격자를 형성함으로써 서로 다른 우선 순위를 가지는 계층 관계를 구성하게 된다.

2.2 MLS 관계형 모델

Bell-Lapadula의 원칙에 기반하여 얻어진 성과로 MLS 관계형 모델(Multilevel Secure Relational Model)을

들 수 있다. MLS 관계형 모델은 관계형 데이터베이스의 투플이나 필드와 같은 요소들의 관계에 의하여 각기 요소들이 포함한 데이터의 등급을 지정하고 접근할 수 있는 방식을 결정한다. 관계형 데이터베이스에서 가장 단순한 형태인 각 사용자 별로 접근할 수 있는 접근 계층을 분리하여, 특정한 사용자는 오직 자신이 존재하고 있는 등급과 일치하거나 또는 자신의 등급 하부에 있는 데이터에만 접근할 수 있도록 조작되는 MLS 모델중의 하나이다. 이러한 개체는 자신의 등급으로 접근할 수 있는 데이터만을 갱신하고, 삭제하고, 삽입할 수 있다. 이러한 각 투플에 대한 가시성이 기반한 MLS 모델을 MLS 관계형 모델이라 한다. [3]

2.3 BCMLS

MLS 모델을 각 사용자가 지니고 있는 정보에 대한 신뢰성 일치하도록 확장한 모델을 BCMLS 모델이라고 한다. BCMLS 모델을 이용하면 모든 정보에 대한 설명이 각 사용자의 접근 계층에 따라 다르게 처리됨으로써, 정보가 지니고 있는 이러한 모호성이 제거될 수 있다. BCMLS 모델은 낮은 접근 수준에 위치한 정보를 사용자의 접근 권한에 따른 적절한 해석을 가능하도록 하는 포괄적인 수단을 제공한다. BCMLS 모델에서 높은 수준의 접근 권한을 가진 각 사용자는 자신이 인식하는 정보가 더 낮은 접근 권한을 갖는 사용자에게는 다르게 해석될 수 있다는 가능성을 인식할 수 있으므로, 자신보다 낮은 계층에 위치한 정보에 대한 다양한 해석이 가능하다. 높은 계층의 사용자는 자신보다 낮은 계층에 위치한 정보를 <표1>과 같이 4가지 방법으로 해석할 수 있다.

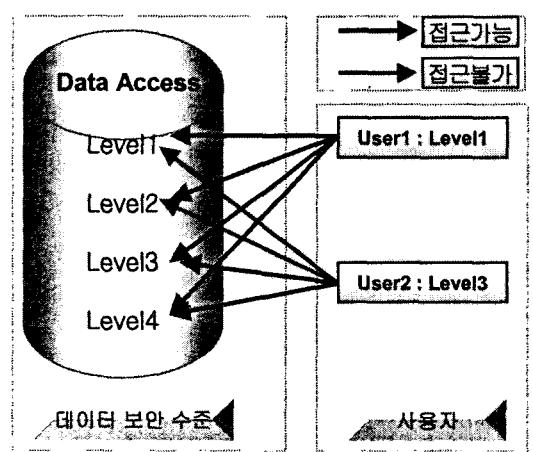
<표1> BCML 모델의 4가지 해석방법

구 분	내 용
진실/완벽	하위 수준의 정보는 정확하고 완전한 정보이다. 즉, 자신의 접근 수준에서 보게 되는 정보와 정확히 일치한다.
부분적 거짓	하위 수준의 정보는 자신의 접근 계층에서 인식하게 되는 정보와 부분적으로 상이하다.

완전한 거짓	하위 계층에서 인식하게 되는 정보는 자신의 수준에서 보게 되는 정보와는 완전히 틀리다.
해석 불능	하위 수준에서 인식한 정보가 자신의 접근 수준으로는 아직 해석 불가능하다.

3. MLS의 구조

하위 계층의 데이터 즉, 사용자의 등급보다 낮은 등급에 있는 데이터로의 접근 허용 이를 숨은 채널 (Covert Channel) 이라 칭한다 은 MLS 관계형 모델에서 반드시 구현되어야 할 것 중의 하나이다. 예를 들어서, 특정 사용자의 등급에 기반하여 각 데이터의 등급으로 부호화된 투플에 접근하는 형태라고 한다면, 특정 사용자는 자신이 볼 수 있는 데이터가 자신의 등급보다 높은 등급에는 접근할 수 있어서는 안되며, 자신의 등급보다 낮은 등급에 있는 데이터만을 읽을 수 있어야 한다. 사용자의 등급을 기준으로 읽을 수 있는 데이터의 흐름이 반드시 등급 아래쪽의 데이터만을 읽을 수 있는 형태라야 하며, 아래쪽에 있는 데이터와 통신할 수 있어야 한다. (그림1)은 MLS의 구조를 보여준다.



(그림1) MLS의 구조

그러므로, 각 투플에 대한 가시성은 사용자의 등

급 아래에 있는 데이터에 대해서만 허용되어야 하며 어떠한 상위 등급의 데이터도 접근한 사용자에게 보여지는 것을 방지할 수 있어야 한다. 이러한 가시성의 채널 조정이 MLS 관계형 모델의 기반이 된다.

4. 관련연구

4.1 RBAC(Role Based Access Control)

MLS의 정책의 응용분야는 다중등급 보안 커널을 이용한 RBAC을 구현한 것이다.[7] 이 방법은 다중 등급 보안 커널에서는 모든 주체(프로세스)와 객체(정규파일, 디렉토리, 특수 장치 파일)레이블을 부여하며, 새로운 프로세스의 생성(fork)에 따른 레이블의 상속화, 수정된 BLP(Bell & LaPadula) 모델에 따른 강제적 접근제어, 보안등급 파일에 대한 커널 모드의 암호화/복호화, 데이터 베이스를 이용한 실시간 감사 추적 시스템[8] 뿐만 아니라 스마트 카드를 이용한 사용자 인증, 출력된 문서에 대한 보안 표시 정보의 강제적 출력, 다중등급 보안 기능의 추가에 따른 추가적 보안 응용 프로그램 인터페이스(Security API)들을 제공한다.[4]

4.2 MISSI(Multilevel Information System Security Initiative) 분석

오늘날과 같이 각 국가기관별 전용의 전산망을 구축 운영하고 있는 상황에서 각 전산망의 효율적인 운영을 위하여 분리된 개개의 전산망을 통합적인 하나의 전산망으로 구축 운영하려는 시도가 미국을 중심으로 하여 이루어지고 있다. 이 경우, 통합된 전산망에 서로 다른 등급의 정보가 저장, 처리 및 송·수신될 수 있으므로 이를 효과적으로 통제하고, 선택적으로 분배할 수 있는 기능은 필수적이라 하겠다. 이것은 국방분야뿐 만 아니라 지적사회(intelligence community)의 주요 요구사항이며, 이와 같이 서로 다른 다중의 보안등급을 가진 정보를 처리할 수 있도록 하는 것이 MLS이며 MISSI는 위와 같은 요구사항 및 현재 구축중인 미 국방부 초고속망(DII, Defense Information Infrastructure)을 위한 보안 해결책을 제공하고자 NSA(National Security Agency)가 주도가 되어 구축하고 있는 프로젝트의 명칭이다. 현재

미국은 MISSI의 사용자 요구사항을 병합하고 계속하여 그 기능을 향상시키고 있다.[5]

4.3 다중상속에 대한 보안속성 확장 사용

다중상속에 따른 새로운 보안속성은 중복 메소드 상속에 따른 문제점을 제시 및 정의 하였으며, 일반적인 상속 관계에서 다중 상속이 추가되었을 때의 클래스의 보안등급을 정해주는 속성을 정의했다. 이러한 다중상속에 따른 보안속성의 제안은 기존에 정의된 상속속성과 함께 객체지향 데이터베이스를 위한 보안 모델을 제시할 때 유용하게 활용될 것이다.[6]

4.4 객체의 안전한 보안등급의 하강을 위한 접근 제 메커니즘

MLS 정책기반의 안전한 운영체제에서 발생할 수 있는 보안등급의 변화에 관련된 요구사항 중 특히 시스템의 환경에 의해 주체의 보안등급이 하강 되었을 때 해당 주체가 생성했던 객체들 중 비밀성이 저해되지 않는 범위 내에서 객체의 보안등급의 안전한 하강과 관련된 보안 요구사항을 해결할 수 있는 접근통제 메커니즘을 제안하였다.[7]

4.5 다중등급 영향 행위 기반 접근 통제

여기서 제안하는 접근통제 기법인 ML-RBBAC은 MAC와 RBBAC을 정책간의 충돌 없이 동시에 지원하는 안전한 운영체제를 설계하도록 하며, 다음과 같은 장점을 제공한다.

첫째, 유연한 보안 서비스를 가능하게 한다. 이는 MAC의 엄격한 정보 흐름 통제를 완화함으로써 얻어진다. 보안 관리자가 명시할 경우, MAC의 규칙을 우회 할 수 있다. 그러나, 이 경우에도 RBBAC의 규칙에 어긋나는 접근 행위는 허용되지 않으므로, 안전한 접근을 보장 할 수 있다.

둘째, RBBAC을 도입함으로써, 보안 관리의 부담을 감소시킨다. 또한, 계층적 구조로 설계된 시스템에서의 자원 계층 확장성을 제공하는 RBBAC의 장점을 통해 시스템 자원 관리를 효율적으로 할 수 있게 된다.

그리고 현재 제안된 접근통제 기법은 현재 광주과학

기술원에서 개발된 강제 접근통제 기반 안전한 운영체제인 CSRL 시스템에 적용 중이다.[8]

5. 결론

시스템 관리자나 소프트웨어 개발자들이 권한이 있는 사용자들에게만 특정 데이터 또는 자원을 제공하기 위해 제시되었던 문제점은 계층간의 접근허용 레벨을 둘으로써 문제를 해결 할 수 있었다.

앞으로 이러한 MLS를 다양한 영역에 적용할 수 있도록 지침이나 보완에 대한 상세 연구가 필요하다.

[참고문헌]

- [1] David D. Clack and David R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," Proceedings of the 1987 IEEE Symposium on Security and Privacy, pp. 184-194, 1987
- [2] D. Richard Kuhn "Role Based Access Control on MLS Systems without Kernel Changes", Proceeding of the Third ACM workshop on Role Base Access Control ACM, 1998
- [3] Ken Smith, "Entity Modeling in the MLS Relational Model", Marianne Winslett Department of Computer Science University of Illinois, 1992
- [4] 김현정, 박태규, "다중등급 보안커널 구현과 보안 API", 한국정보보호학회 종합학술 발표회 논문집, 제 10권, 1호, 2000
- [5] 이철원, 국가기간전산망을 위한 MISSI 분석, KISA
- [6] 조기천, 신문선, 김은희, 류근호, 김명은, "객체지향 데이터베이스에서 다중상속에 대한 보안속성 확장", 정보과학회, 2001
- [7] 박춘구, 신욱, 강정민, 이동의, "MLS에서 객체의 안전한 보안등급의 하강을 위한 접근통제메커니즘에 관한 연구", 정보과학회, 2001
- [8] 신욱, 박춘구, 강정민, 이동익, 정승욱, "안전한 운영체제를 위한 다중 등급 역할 행위 기반 접근통제", 정보처리학회 제8권, 제2호, 2001
- [9] 김현정, "MLS 커널을 이용한 RBAC의 설계 및 구현", 한서대학교, 2002