LDAP을 이용한 네트워크 기반의 다중레벨보안 시스템의 구현

이병주*, 이승형*, 홍순좌**, 박중길**

*광운대학교 전자공학부, **국가보안기술연구소

Implementation of A Network-based Multi-Level Security System using LDAP

B.J. Lee*, S.H. Rhee**, S.J. Hong**, J.G. Park**

*Department of Electronics Engineering, Kwangwoon Univ.,

**National Security Research Institute

요 약

다중레벨보안은 하나의 시스템 내에 여러 보안등급의 데이터와 사용자를 수용하여 효율성을 높이기 위한 것이다. 본 논문에서는 네트워크를 통해서 여러 보안등급의 데이터가 저장된 디렉토리 서버에 다중레벨의 사용자들의 접근을 통제하기위한 방안을 제시하고 구현한다. 보안과 무결성 모두를 보장해주기 위해서 보안 모델과 무결성 모델을 결합한 새로운 형태의 모델을 정의한다. 이 모델을 OpenLDAP의 ACL(Access Control List)을 사용하여 구현하고 사용자의 등급에 따른 시스템의 접근통제를 가능하게 한다.

I. 서론

다중레벨보안(Multi-Level Security)은 하나의 정보 시스템 내에 여러 보안등급의 데이터가 동시에 저장되고 처리되며, 사용자들 역시 서로 다른 보안등급 및 권한을 가지며 부여된 등급 및 권한을 벗어나는 정보는 접근을 차단시키는 능력을 의미한다. 이러한 기능에 의하여, 한 가지 보안 등급만을 갖는 경우에 발생하는 불필요한 접근 차단 및 암호화로 인한 시스템의 비효율성을 극복할 수 있다. 또한, 여러 보안등급의 사용자들을 위하여 별도의 단말기를 설치할 필요 없이, 단일 인터페이스를 갖는 하나의 단말기, 즉 다중레벨보안 시스템을 통하여 여러 보안등급에서의 시스템 접근을 가능하게 할 수 있다.

다중레벨보안 시스템에 대한 표준화는 미국 국방성(DoD)에 의해 진행되어 왔다. 1985년 미국의 국가표준위원회와 마이터(Mitre Corporation)가 주축이 되어 DoD5200.28-STD 표준을 제정했는데, 이 표준의 목적은 전자문서의 형태로 저장된 비밀정보가 종이문서의 형태로 저장된 경우와 같은 정도의 통제 및 보호가 가능하도록 하는데 있다.[1] 이러한 보호를 가능하게 해주는 시스템을 TCB (Trusted Computer Base)라 한다. 이 TCB는 DoD5200.28-STD의 보안 요구사항을 만족시켜 주는 하드웨어, 펌웨어 혹은 소프트웨어들로 구성된다. 이러한 시스템은 현재 십여 개의 제품에 대하여 평가 및 인증이 이루어진 상태이다. 예를 들어 다중레벨 보안을 지원하는 시스템의 경우에는 Wang Government Service Inc.의 XTS-300을 비롯한 몇 개 제품만이 인증을 획득하였다.

다중레벨보안 시스템을 효율적으로 구축하기 위한 다중레벨보안 모델은 1973년 Bell과 LaPadula에 의해 처음 제시되었다. 이들에 의해 제안된 BLP(Bell and LaPadula) 모델은 이후에 다중레벨보안 시스템을 구축하는데 자주 적용되었다. 이 모델은 사용자와 데이터 사이에 레벨을 비교하여 보안을 보장하는 모델이다.[9] 또 하나의 모델은 Biba 모델로서, 이 모델 역시 사용자와 데이터의 레벨을 비교하여 무결성을 보장하는 모델이다. 본 논문의 목적은 레벨 간 보안과 무결성을 모두 보장하는 BLP 모델과 Biba 모델이 결합된 형태의 모델의 시스템을 구현하는 것이다.

2장에서 기존에 BLP모델과 Biba 모델 그리고 두 모델의 결합된 형태의 모델에 대해서 설명한다. 3장에서는 OpenLDAP과 ACL에 관해서 설명한다. 4장에서는 새로운 시스템의 구현하는 과정과 새로운 시스템의 결과를 검증한다.

II. Information Flow의 control

1. BLP(Bell and LaPadula) 모델

군이나 정부에서 쓰이는 정보는 대부분 그 정

보의 내용에 따라 각각 분류되어 주의 깊게 취급되어야 한다. 이러한 배경을 바탕으로 1973년 BLP 모델이 제안되었다. BLP 모델은 subject와 object의 액세스 클래스(access class) 사이의 지배 관계를 바탕으로, 이 두 요소간의 read 접근과 write 접근에 관해 기술한다. 모든 subject는 자신과 같은 레벨의 object에 read 접근과 write 접근을 할 수 있다. subject는 read 접근의 경우 자신보다 낮은 레벨의 있는 모든 object를 read 할 수 있고, write의 경우는 자신의 레벨보다 높은 레벨의 object에만 write를 할 수 있다. 따라서 이 두 가지 원칙으로부터 BLP 모델의 특징을 정리하면 다음과 같다.

- No Read Up (NRU)
- No Write Down (NWD)

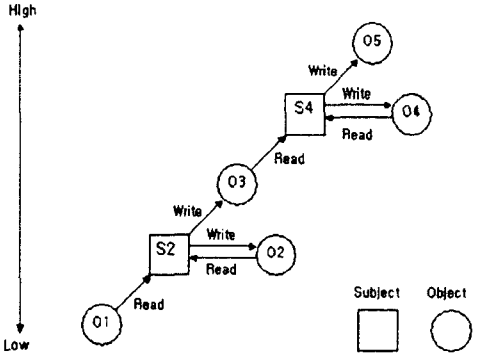

그림1: BLP모델의 보안 보장

이러한 특징을 지닌 BLP 모델을 보안 정보의 흐름관점에서 설명하면 그림1과 같다. 위 그림을 통해서 알 수 있듯이, subject는 object가 이 subject와 같은 등급의 액세스 클래스를 가질 때 object를 읽고 쓸 수 있다. 그러나 다른 레벨에 있는 subject와 object의 관계는 NRU와 NWD의 원칙에 따른다.

2. Biba 모델

Biba 무결성 모델은 read 접근과 write 접근을 제한함으로써 허가 없이 정보를 수정하는 것을 막음으로써 정보의 무결성을 보장한다. 이를 위해서 Biba 모델은 앞에서 언급한 BLP 모델과는 반대되는 두 가지 규칙, 즉, No Write Up(NWU)과 No Read Down(NRD)을 바탕으로 하고 있는데, 이 때문에 이것을 BLP Upside-Down이라고도 한다.

- No Write Up (NWU)
- No Read Down (NRD)

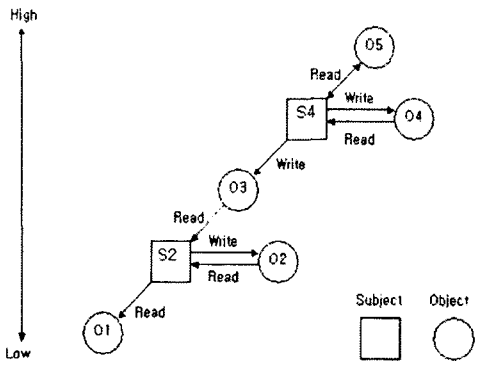

그림2: Biba 모델의 무결성 보장

그림2에서 보듯이 subject와 object가 같은 레벨에 무결성 레벨을 갖고 있을 때만 read와 write를 할 수 있다. 다른 무결성 클래스에 있는 subject와 object의 관계는 NWU와 NRD의 규칙을 따른다.

3. BLP모델과 Biba모델의 결합

이 절에서는 위에서 설명한 BLP모델의 장점인 보안과 Biba모델의 무결성이라는 장점을 결합하여 새로운 모델을 정의한다. 이 결합 모델에서 subject와 object는 액세스 클래스와 무결성 클래스를 동시에 갖는다. 즉 S를 시스템에 있는 모든 subject s의 집합이라고 하면 각각의 subject s는 C(s)라는 액세스 클래스와 I(s)라는 무결성 클래스를 갖는다. 마찬가지로 O를 시스템에 있는 모든 object의 집합이라고 하면 각각의 object o에는 C(o)라는 액세스 클래스와 I(o)라는 무결성 클래스가 존재한다. 이 결합 모델에서는 각각의 subject와 object가 두 가지의 클래스의 조합으로 read 접근과 write 접근을 갖게 된다. 이 결합 모델의 액세스 클래스는 BLP모델에서처럼은 Top Secret, Secret, Confidential로 분류되고, 무결성 클래스는 Secret Administrator, Administrator, User로 분류된다. Read 접근은 C(o)와 C(s)사이에는 No Read Up을 적용하고 I(o)와 I(s)사이에서는 No Read Down이 적용된다. Write 접근에서는 C(o)와 C(s)사이에서는 No Write Down이 적용되고, I(o)와 I(s)사이에서는 No Write Down이 적용된다. 예를 들면 C(o)는 Secret의 레벨을 갖고, I(o)는 Administrator의 레벨을 갖는 object를 read 할 수 있는 subject는 C(s)는 Secret 이상, I(s)는 Administrator 이하의 레벨을 갖는 subject들이다. 그리고 write할 수 있는 subject는 C(s)는 Secret이하의 레벨을 갖고, I(s)는 Administrator이상의 레벨을 갖는 subject들이다. 이와 같이 BLP모델과 Biba모델을 결합하면, 보안과 무결성을 동시에 보장해주는 모델을 구현 할 수 있다. 이를 도식화하면 다음 그림과 같다.

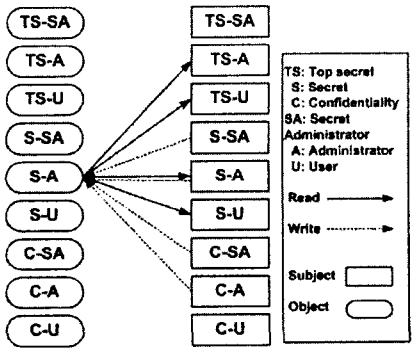

그림3: 결합 모델의 예.

이 중에 TS-U 클래스를 system-high라 한다. 이유는 이 클래스에 속하는 subject는 모든 object에 대해서 read 접근을 가지고 있기 때문이다. 그리고 이 클래스에 속하는 object의 경우에는 모든 subject가 write 접근을 가지고 이 object에 write를 할 수 있다. 반대로 C-SA 클래스는 system-low라 한다. TS-U와는 반대로 이 클래스에 속하는 object는 모든 subject가 읽을 수 있고, 여기에 속하는 subject는 모든 class의 object에 write를 할 수 있다.

III. OpenLDAP에 의한 Access Control

1. OpenLDAP

OpenLDAP 은 LDAP(Lightweight Directory Access Protocol)의 전신이라고 할 수 있는 Umich(미시간 대학) LDAP 3.3을 기반으로 새롭게 만든 LDAP 프로젝트의 산물이다. 오픈소스정책을 따르면서도 상용 LDAP서버 못지않은 응용프로그램들과 서버 기능을 제공하겠다는 목적 아래 웹상의 많은 개발자들이 자원해서 개발되었다. OpenLDAP은 그 자체에 저장 구조를 갖추고 있지 않으며 다양한 저장 구조를 붙여 사용할 수 있다. 버클리DB, GDBM, NDBM, 쉘 패스워드, SQL 등의 데이터베이스를 백앤드(back-end)로 지원한다. OpenLDAP의 엔트리 데이터는 읽고 작성 가능한 텍스트 형식으로 보여주는 LDIF(LDAP Data Interchange Format)이다. OpenLDAP은 이런 LDIF 데이터를 디렉토리 구조에 읽고, 쓰기위한 디렉토리 시스템이다.

2. Access Control List

ACL이란 파일 시스템에서 파일과 디렉토리에 소유자의 권한을 설정해주는 것과 같이 각각의 엔트리에 액세스 권한을 설정하는 역할을 수행한다. 또한 ACL 설정으로 LDAP 내부 각각의 entry, attribute 액세스에 대해 권한을 설정할 수 있으며 액세스 가능한 호스트에 대한 설정을 할 수 있다. 따라서 LDAP 관리자는 반드시 데이터의 중요도에 따라 ACL을 설정해야 하며 이러한 설정이 올바르게 적용되고 있는지 확인해 주어야 한다. 일반적으로 다음과 같은 형식으로 설정을 한다.[10]

access to <권한제한을 설정할 것>

by <누구에게> <액세스 권한>

IV. 시스템 구현

1. 시스템 구성

시스템을 구성하기 위해서는 OpenLDAP이 설치된 LDAP server와 LDAP server에 접속할 수 있는 client가 필요하다. LDAP server와 client는 LINUX 2.4.13기반의 PC이다. 여기에 OpenLDAP 2.0.11을 설치한다. OpenLDAP client는 server에 bind해서 디렉토리에 add와 search를 수행한다. 기본적인 구성은 다음과 같다.

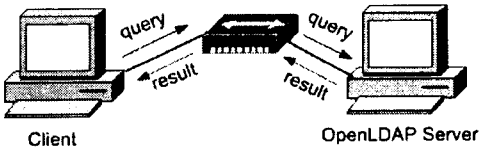

그림 4: 시스템 구성.

위에서 보는 것처럼 OpenLDAP Server는 client의 query에 대해서 절절한 응답을 해주어야 한다. 그러기 위해서는 OpenLDAP에 적절한 설정을 해주어야 한다. 설정 파일의 설정부분은 크게 schema파일의 include부분, Access Control List부분, rootdn과 root password를 설정하는 부분으로 나뉜다.

2. 스키마 파일 작성

Schema는 OpenLDAP에서 사용되는 attribute와 object class를 정의해 놓은 부분이다. LDAP에 다중레벨보안을 구현하기 위해서는 새로운 object class를 정의해 주어야 한다. [4]

3. Access Control List 설정

기본적인 디렉토리는 다음과 같이 구성한다.

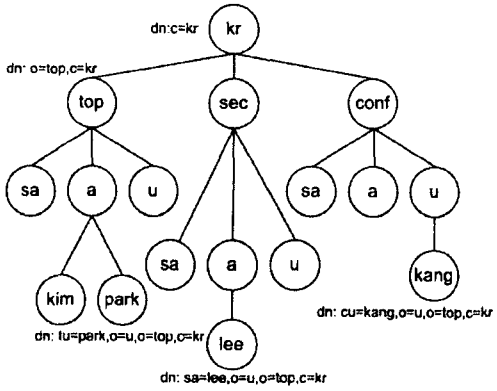

그림5: DIT(Directory Information Tree)의 구성.

위와 같은 DIT에서 각각의 entry들은 고유한 dn(distinguished name)를 갖는다. 위와 같은 DIT에 ACL를 적용시키려면 루트로부터 상위 3번째 단계에 있는 entry 이하에 ACL을 적용시켜야 한다. S-A class에 ACL을 적용하는 부분의 예를 보면 다음과 같다.

access to dn=".+,o=a,o=sec,c=kr"

by dn=".+, o=a,o=conf,c=kr" write

access to dn=".+,o=a,o=sec,c=kr" 은 dn이 o=a, o=sec,c=kr이하에 있는 모든 entry에 대해서 ACL을 적용하겠다는 의미이다. 그리고 by dn=".+, o=a,o=conf,c=kr" write는 dn이 o=a,o=top,c=kr이하에 있는 모든 entry에 대해서 write access를 주겠다는 의미이다.

4. 결과 확인

결과 확인은 Client의 사용자가 LDAP 서버에 자신의 Distinguished name과 패스워드를 제시하고 bind 한다. 디렉토리에 데이터를 add하는 query를 보내고 그에 따른 결과를 확인하면서 ACL 적용 여부를 확인하고, 보안과 무결성 모두 보장되는지 확인한다.

V. 결론

본 논문의 목적은 네트워크를 통해 시스템에 접속하는 사용자의 등급을 여러 개의 레벨로 두어서 레벨에 따른 각기 다른 권한을 갖는 시스템의 구현에 있다. 보안과 무결성을 보장하기 위해 BLP 모델과 Biba모델의 결합으로 새로운 모델을 정의하고 그 모델을 OpenLDAP의 디렉토리 시스템에 구현함으로서 결과를 확인한다. 현재 OpenLDAP과 인증서버의 연동을 통해 search를 제어하는 기능을 테스트 중에 있다.

참고문헌

[1] "Department of Defense Trusted Computer System Evaluation Criteria," *DoD*, Aug. 1983.

[2] V Hassler, "X.500 and LDAP Security: A Comparative Overview," *IEEE,* Dec. 1999.

[3] K. Kampman and C Kampman, *All About Network Directories.* Wiley Computer Publishing, pp. 1-82. 2000.

[4] Ian Clatworthry, "OpenLDAP 2.0 Administrator's Guide," *OpenLDAP Foundation*, Sep 2000.

[5] "Secure Computer System: Unified Exposition and Multics interpretation," *MITRE* MTR-2997 Rev.1, Mar.1976.

[6] "The Directory: Overview of Concepts, Models and Service," *CCiTT Recommendation* X.500, 1988.

[7] M. Wahl, A. Coulbeck, T. Howes, and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions," RFC 2252, Dec.1997.

[8] K. Knorr, "Dynamic Access Control through Petri New Workflows," *Proceedings of the 16th Annual Computer Security Applications Conference*, pp. 159-167, Dec 2000.

[9] J. Davis, D. Jacobson, S. Bridges and K. Wright "An Implementation of MLS on a Network of Workstations Using X.500/509," *,IEEE Conference*, 1997.

[10] http://database.sarang.net