망관리 객체의 컨텍스트 기반 강제적 접근통제 모델

오이면, 최은복
전주대학교 정보기술공학부

Context Based Mandatory Access Control Model of Network Managed Objects

Yi-Myun Oh, Eun-Bok Choi
School of Information Technology and Engineering, Jeon-ju University

요 약

안정적이고 효율적인 네트워크 환경을 제공하기 위해서는 네트워크상에 존재하는 각종 자원들을 감시, 제어하는 네트워크 관리가 필수적이며 이러한 네트워크 관리 객체를 저장·관리하는 관리정보베이스에 대한 보안이 필수적이다. 본 논문에서는 안전한 관리정보베이스의 보장을 위하여 시스템 상태정보, 연산모드, 관리객체와 접근권한으로 구성되는 컨텍스트를 기반으로 한 강제적 접근통제 정책을 네트워크 관리 모델에 적용하므로서 관리정보의 무결성을 보장한다.

1. 서 론

현대의 네트워크를 이용한 정보 이용기술은 규모나 성능면에서 하루가 다르게 변화하고 있으며 급속한 성장을 이루고 있다. 이러한 급속한 정보기술을 이용한 다양한 서비스들이 개발되므로서 서비스를 이용하는 업체나 사용자들의 업무환경에 많은 변화를 불러오고 있다. 한편 다양해진 네트워크 서비스와 이를 이용하는 사용자들의 증가는 정보를 제공하는 업체에서의 과금문제, 자료 전송에따른 교통량 증가, 네트워크 자체 결함, 외부로부터의 불법적인 침입 등의 여러 문제점을 야기시켰다[1].

이러한 네트워크를 기반한 정보기술의 사용이 보편화되고 이에따른 통신기술이 급속히 발전함에도 불구하고 다양한 정보의 효과적 이용과 안전한 정보관리 측면의 정책이 미비하다고 할 수 있다. 또한, 급속한 망의 성장에 따라 기존의 중앙집중적인 관리 시스템은 관리자의 시스템의 복잡도 및 관리 트래픽의 증가로 인해 관리상의 많은 문제점을 노출하고 있다. 그러므로 안정적이고 효율적인 네트워크 환경을 제공하기 위해서는 네트워크상에 존재하는 각종 자원들을 감시, 제어하는 네트워크 관리가 필수적이며 이러한 네트워크 관리 객체의를 저장관리하는 관리정보베이스(MIB)에 대한 보안 필수적이다[11].

본 논문에서는 안정적이고 효율적인 네트워크 환경을 제공하기 위하여 상업적인 환경에 적합한 강제적접근통제모델중 하나인 Biba 정책을 네트워크 관리 모델에 적용하므로서 관리정보의 무결성을 보장한다. 관리객체에 대한 연산을 수행하기 위한 관리 정책은 시스템 상태정보와 연산모드 그리고 용도(purpose)와 제약조건(condition)의 속성을 갖는 관리객체와 접근권한으로 구성되는 컨텍스트에 기반하여 구성된다.

2. 관련연구

강제적 접근통제정책은 시스템 관리자에 의해 보안등급이 결정되는 정책으로 관리주체에 부여되는 등급을 인가등급(Clearance level)이라 하며 관리객체에 부여되는 등급을 보안등급(Classification level)이라 한다. 강제적 접근통제 정책을 이용한 대표적인 모델로는 정보의 무결성을 강조하는 Biba 모델이 있다[2].

2.1 Biba 모델

BLP 모델은 권한을 갖지 않는 사용자에게 정보가 흡

러가는 것을 예방하는 비밀성에 기반을 둔 모델이다. 이 모델은 정보의 비밀성은 보장하지만 등급이 낮은 관리 주체가 등급이 높은 관리객체의 정보를 변경할 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 Biba 모델이 제안되었다. 이 모델에서도 관리주체와 관리객체의 보안등급에 의해 정책이 수행되는데 특히 보안등급을 무결성 등급이라 한다. 이 무결성 등급은 크게 두가지로 분류한다. 하나는Crucial(C), Very Important (VI), Important(I)로 구분되는 무결성등급이고 다른 하나는 범주의 집합이다. 무결성 등급은 C>VI>I의 관계를 형성하며 범주의 집합은 BLP모델과 마찬가지로 비계층 구조 관계를 갖는다.

2.2 네트워크 관리

네트워크 관리는 컴퓨터에서 사용되는 자원들을 제어하고 모니터링하는 전반적인 활동을 말한다. 여기서 자원은 컴퓨터 통신과 연결에 사용되는 요소들과 이에 이용되는 응용프로그램들이 해당된다. 주로 LAN이 분산컴퓨팅 환경을 대별하는데 LAN 환경에서 관리는 대등한(Peer to peer) 망관리이며 이를 때론 분산망관리라 한다. 여기서 관리주체는 중앙관리주체가 아닌 서로 대등한 역할을 수행하는 관리주체라 볼 수 있다[12].

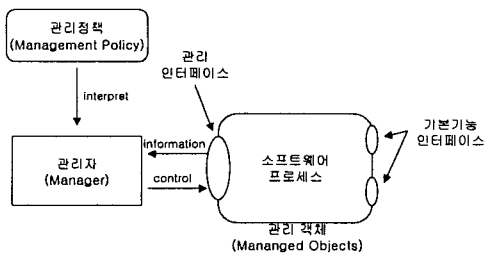

그림 1. 네트워크 관리

1) 네트워크 관리 구성요소

▨ 관리주체(Managing Subjects)

관리자 또는 관리주체는 구성관리(configuration Management) 기능에 대한 전반적인 활동에 대한 책임을 가지고 있으며 구성관리에 해당하는 데이터를 수집하기위해 각 관리객체를 관리하고 있는 대리자에게 명령어와 연산을 보낸다.

▨ 관리객체(Managed Objects)

관리객체는 관리시스템에 의해 제어되는 하드웨어나 소프트웨어 컴포넌트로 정의할 수 있다. 관리객체는 정보를 송수신하기 위한 하나의 관리인터페이스와 관리객체간의 정보를 처리하기위해 연산을 송수신하는 기본기능 인터페이스로 구성된다. 관리인터페이스에는 시스템의 시작, 정지 등과 같은 제어명령어와 상태정보의 요청 그리고 관리객체에 의해 생성되는 모니터링 정보와 같은 처리연산을 포함한다[11].

관리주체는 관리정보를 개념적이고 논리적이고 실질적인 관리 정보 베이스인 MIB(Management Information Base)에 저장하는데 이러한 관리객체 클래스에는 관리객체에서 수행될 속성값을 수정하거나 질의하는 등의 연산이 포함된다.

▨ 관리 영역

매우 규모가 큰 분산 시스템의 경우 수많은 관리객체들이 존재하는데 이러한 관리객체들에 대한 관리정책을 개별적으로 관리하는게 불가능하다. 그러므로 관리객체들을 그룹으로 묶어 영역으로 관리하는 관리영역의 개념이 필요하다. 관리 영역은 분산 망관리 기능에서 중요한 개념으로 시스템 관리 목적을 위해 관리객체들을 집합한 개념으로 관리의 책임성과 권한성을 동반한다. 관리영역은 유일한 이름을 가져야하며 영역내에서 관리되어질 관리객체를 포함하고 관리영역에 있는 하나의 관리객체는 다른 관리영역에 속할 수 있다.

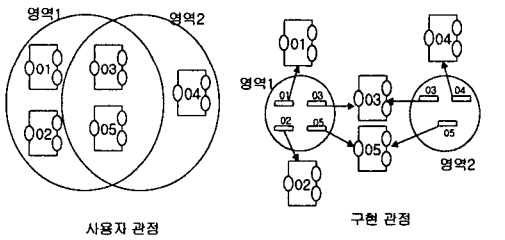

그림2. 관리영역의 사용자/구현 관점

3. 컨텍스트 기반 강제적 접근통제 모델

안정적이고 효율적인 네트워크 환경을 제공하기 위해서는 네트워크상에 존재하는 각종 자원들을 감시, 제어하는 네트워크 관리가 필수적이며 이러한 네트워크 관리 객체를 저장·관리하는 관리정보베이스에 대한 보안이 필수적이다.

본 논문에서는 안전한 관리정보베이스의 보장을 위하여 시스템 상태정보, 연산모드, 관리객체와 접근권한으로 구성되는 컨텍스트을 기반으로 한 강제적 접근통제 정책을 네트워크 관리 모델에 적용하므로서 관리정보의 무결성을 보장한다.

3.1 시스템 상태와 연산모드

시스템 상태는 다음과 같이 3가지 구성요소인 b, M, f

를 갖는다.

◇ b : 3가지 튜플(관리주체, 관리객체, 접근권한)인 (Manager Subject(MS), Managed Object(MO), Permission)로 구성

◇ M : 관리주체와 관리객체에 접근할 수 있는가 [M(MS, MO)], 관리주체가 또 다른 관리주체를 호출할 수 있는가[M(MSi, MSj)]를 나타내는 접근행렬

◇ f : 관리주체와 관리객체에 연관되어있는 등급함수로 f : MS ∪ MO → L로 구성

관리주체가 관리객체에 대해 수행할 수 있는 연산모드에는 다음과 같다. 관리정보 모델에는 관리연산을 크게 전반적인 관리객체에 적용되는 연산과 속성값에 적용되는 연산으로 구분하고 있다[12]. 전반적인 관리객체에 적용되는 연산에는 관리객체의 인스턴스를 생성하고 삭제하는 create, delete 연산과 개별적인 관리객체의 요구조건을 정의하는 action 연산이 있다. 그리고 속성값에 적용되는 연산에는 속성값을 읽는 get 연산, 속성값을 쓰는 replace 연산, 그리고 관리객체 정의시 명기되어있는 값으로 재정의하여 쓰는 replace with default 연산 등이 있다. 또한 특별한 속성 타입을 정의하기 위한 것으로 동일한 데이터 타입의 멤버들의 비순서 집합을 추가, 삭제하는 addMember와 removeMember 등이 있다.

관리객체와 접근권한은 용도(purpose)와 제약조건(condition)의 속성을 갖는 컨텍스트로 구성되며, 제약조건은 논리함수로 표현되며 표현식의 오퍼랜드는 관리주체, 관리객체, 접근권한, 목적의 속성으로 구성되며 이들 표현식의 오퍼레이터로는 관계연산자와 논리연산자로 표현된다.

각 사용자에게는 2가지 보안등급이 있는데, 하나는 사용자가 생성될 때 부여되는 보안등급인 FS이고 다른 하나는 현재 사용자가 수행중인 보안등급인 FC이다. 보안등급은 사용자가 수행중인 동안에는 여러 가지 보안등급을 가질 수는 있지만 생성시 부여되는 보안등급이 현재 수행중인 보안등급을 지배해야 하는 조건을 만족하여야 한다. 이것은 보안등급을 지배하는 시스템은 언제라도 로그인할 수 있음을 의미한다.

3.2 컨텍스트 정보

컨텍스트 정보에는 용도요소와 제약조건의 속성을 갖는다. 용도(purpose) 요소는 세가지 종류가 있다. 하나는 개인용 자료 용도 요소(personal data purpose element)로서, 관리주체와 정보소유주인 개인에게 정보의 이용 권한이 있는 요소로 고객의 동의가 필요하다. 또 하나는 공개용 용도 요소(public purpose element)로 관리주체나 개인 뿐만 아니라 일반적인 등급의 소유자에게 정보가 공개되는 공개용 요소이다.

마지막으로 비공개용 용도 요소(private purpose element)는 정보의 소유주인 개인에게만 정보가 제공된다. 만약, 고객이 비공개용 자료목적 요소로 정보 사용에 동의하였다면, 그 정보는 상위 무결성 등급을 갖는 관리주체라 하더라도 정보 소유주인 해당 고객 이외에는 정보가 제공되지 않는다.

관리주체가 관리객체에 대한 연산을 수행할 때 연산별로 선행되어야 할 제약조건은 다음과 같다.

▨ Create, Delete, addMember, removeMember 연산 ∈ M[MS, MO]

⇒ FS(MS) ≥ FC(MS)

▨ Get 연산 ∈ M[MS, MO]

⇒ FS(MS) ≥ FC(MS) AND FC(MS) ≤ FC(MO)

▨ replace, replace with default 연산 ∈ M[MS, MO]

⇒ FS(MS) ≥ FC(MS) AND FC(MS) ≥ FC(MO)

그림3에서는 BNF 표기법에 의해 관리연산을 정의하였으며 그림4에서 Get 연산을 예로 들어 표현하여 보았다. 그리고 그림5에서 본 모델의 구성요소를 표현하였다.

```
Operation ::= <L_Exp> <L_Op> <L_Exp>
<L_Exp> ::= <R_Exp> <R_Op> <R_Exp> |
True | False
<R_Exp> ::= <Sec_Cat> '(' <Sec_Level> ':'
Target ')'
<Sec_Cat> ::= 'FS'|'FC'
<Sec_Level> ::= 'C'|'VI'|'I'
<Target> ::= 'MS'|'MO'
```

그림 3. 관리연산의 BNF 표기법 정의

```
Get ::= <L_Exp1> AND <L_Exp2>
<L_Exp1> ::= <R_Exp1> >= <R_Exp2>
<L_Exp2> ::= <R_Exp3> <= <R_Exp4>
<R_Exp1> ::= FS(VI:MS)
<R_Exp2> ::= FC(I:MS)
<R_Exp3> ::= FC(VI:MS)
<R_Exp4> ::= FC(I:MO)
```

그림 4. Get 연산 정의의 예

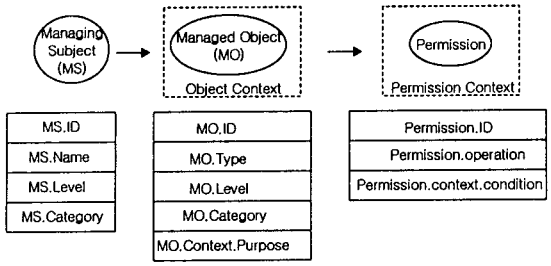

그림 5. 컨텍스트 기반 MAC 모델의 구성요소

4. 결 론

네트워크를 기반한 정보기술의 사용이 보편화되고 이에따른 통신기술이 급속히 발전함에도 불구하고 다양한 정보의 효과적 이용과 안전한 정보관리 측면의 정책이 미비하다고 할 수 있다. 또한, 급속한 망의 성장에 따라 기존의 중앙집중적인 관리 시스템은 관리자의 시스템의 복잡도 및 관리 트래픽의 증가로 인해 관리상의 많은 문제점을 노출하고 있다. 그러므로 안정적이고 효율적인 네트워크 환경을 제공하기 위해서는 네트워크상에 존재하는 각종 자원들을 감시, 제어하는 네트워크 관리가 필수적이며 이러한 네트워크 관리 객체의를 저장관리하는 관리정보베이스(MIB)에 대한 보안이 필수적이다.

이러한 환경을 제공하기 위해서는 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 부적절하게 접근하는 것을 방지하며, 정당한 권한을 갖는 사용자의 정보처리 서비스를 시스템에서 거부되지 않도록 보호하기 위한 적절한 접근통제 정책이 요구되어진다.

본 논문에서는 안정적이고 효율적인 네트워크 환경을 제공하기 위하여 상업적인 환경에 적합한 Biba 정책을 네트워크 관리 모델에 적용하므로서 관리정보의 무결성을 보장한다. 관리객체에 대한 연산을 수행하기 위한 관리 정책은 시스템 상태정보와 연산모드 그리고 용도(purpose)와 제약조건(condition)의 속성을 갖는 관리객체와 접근권한으로 구성되는 컨텍스트에 기반하여 구성된다.

[참고문헌]

[1] Charles P.Pfleeger, Security in Computing, Prentice Hall

[2] Silvana Castano, DATABASE SECURITY, ADDISON-WESLEY

[3] Ravi S. Sandhu and Pierangela Samarati, "Access Control : Principles and Practice",IEEE Communications Magazine, 9, 1994.

[4] Ravi S. Sandhu, "Lattice-Based Access Control Models", IEEE COMPUTER, 11, 1993.

[5] Martin Rscheisen and Terry Winograd, "A Communication Agreement for Access/Action Control", IEEE Symposium on Security and Privacy, 5, 1996.

[6] Ravi Sandhu, "Access Control : The Neglected Frontier", Proc. First Australasian Conferenceon Information Security and Privacy, 6. 1996.

[7] Warwick Ford, Computer Communications Security, Prentice Hall

[8] D. G. Cholewka, R. H. Botha, and J. H. P. Eloff. " A Context Sensitive Acess Control Model and Prototype Implementation", In Proceedings of the IFIP TC11 15th Interanational Conference on Information Secuirty, 2000

[9] Marc Wilikens, Simone Feriti, Marcelo Masera, "A Context-RelatedAuthorization and Access Control Method Based on RBAC", ACM SACMAT'02, 2002.

[10] Network Management Systems Essentials, Divakara K. Udupa

[11] Morris Sloman, "Network and Distributed Systems Management", 1994

[12] Morris Sloman, Network and Distributed Systems Management, Addison-Wesley, 1994