컨텍스트 기반 강제적 접근통제 모델

오이면, 최은복
전주대학교 정보기술공학부
e-mail:ebchoi@jj.ac.kr

Context-Based Mandatory Access Control Model

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

요 약

정보통신기술의 급속한 발전과 웹을 통한 기업모델의 다양화로 인해 개인정보를 통한 새로운 경영기법의 발전은 향상되었던 반면 개인정보의 오용과 남용은 인터넷 발전의 가장 큰 저해 요소 중 하나로 대두되게 되었다. 그러므로 방대한 정보를 부당한 사용자로부터 보호하면서 개인의 프라이버시를 보장하기 위해서는 적절한 접근통제 정책이 요구되어진다. 본 논문에서는 Biba 모델의 엄격한 무결성 정책에 대한 접근모드, 시스템 상태정보 그리고 주체의 생성과 실행에 따른 제약조건을 기술하였다. 또한, 객체의 용도(purpose)와 접근권한의 제약조건으로 구성되는 컨텍스트를 엄격한 무결성 정책에 적용하므로서 주체에 의한 객체정보의 임의적 연산을 방지하므로서 객체 정보를 보호할 수 있다.

1. 서 론

개방형 분산 환경에서 정보 보호에 대한 중요성은 매우 중요하다. 특히 정보 통신망에서 운영되는 정보를 저장 관리하는 시스템에서 보안의 필요성은 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 부적절하게 접근하는 것을 방지하며, 정당한 권한을 갖는 사용자의 정보처리 서비스를 시스템에서 거부되지 않도록 보호하기 위한 것이다.

정보 보호에는 다음과 같은 세 가지 특성을 갖는다. 첫째, 권한을 가지고 있지 않은 사용자에게 중요한 내용이 흘러가는 것을 방지하는 정보의 비밀성과 둘째, 불법적인 사용자로부터 내용이 변경되는 것을 방지하는 정보의 무결성, 그리고 정당한 사용자가 정보를 이용할 수 있도록 하는 정보의 가용성을 들 수 있다[1]. 이중에서 가용성은 데이터나 자원에 접근하고자 하는 서비스 모두에게 적용되는 보안 목표로서, 첫째, 시의 적절한 응답(timely response), 정당한 할당(fair allocation), 고장 허용 한계(fault tolerance), 동시성 제어, 데드락 관리, 배타적 접근에 관한 정책이 제공되어야한다. 이러한 가용성을 보장하기 위해서는 객체가 사용 가능한 형태로 존재하고 서비스 욕구에 맞는 용량을 가지고 있어야 하며, 정해진 대기시간에 서비스가 제공되어야 한다.

접근통제시스템은 접근이 불허되는 주체에 대한 규칙만을 점검하는 개방형 시스템과 접근이 허가되는 주체에 대한 규칙을 지정한 시스템인 폐쇄형 시스템으로 나뉜다. 개방형은 시스템은 정보의 가용성 측면에서 융통성과 정보의 공유 측면에서 많은 특징을 갖는데 반해 정보의 안전성에서는 다소 폐쇄형보다는 미흡하다고 볼 수 있다[3].

본 논문에서는 Biba 모델의 엄격한 무결성 정책에 대한 접근모드, 시스템 상태정보 그리고 주체의 생성과 실행에 따른 제약조건을 기술하였다. 또한, 객체의 용도(purpose)와 접근권한의 제약조건으로 구성되는 컨텍스트를 엄격한 무결성 정책에 적용하므로서 주체에 의한 객체정보의 임의적 연산(observe,

invoke, modify)을 방지하므로서 객체 정보를 보호할 수 있다.

2. 관련연구

강제적 접근통제정책은 시스템 관리자에 의해 보안등급이 결정되는 정책으로, 사용자이거나 프로그램의 한 에이전트인 주체가 객체에 대한 권한을 자율적으로 수행하는 자율적 접근통제와는 다른 정책이다. 특히, 강제적 접근통제 정책에서는 주체에 부여되는 등급을 인가등급(Clearance level)이라 하며 객체에 부여되는 등급을 보안등급(Classification level)이라 한다. 강제적 접근통제 정책을 이용한 대표적인 모델로는 비밀성을 중요시하는 BLP 모델과 정보의 무결성을 강조하는 Biba 모델이 있다[2].

2.1 BLP 모델

BLP model은 강제적인 정책에 기반을 둔 데이터보호를 위한 참조 모델이다. 각 등급은 두 가지 구성요소에 의해 정의되어지는데, 하나는 보안등급이고 다른 하나는 범주의 집합이다. 보안등급은 TS, S, C, U의 4가지 요소로 구성되고 이들은 TS > S > C > U의 관계를 갖는다. 범주의 집합은 요소들의 비계층 구조를 가지는 부분집합으로 정보가 포함되는 조직의 환경에 의해 명명되어진다. 보안등급은 지배관계를 형성하는 부분 순서 집합의 격자구조를 형성한다. 만약, C1≥C2이고 S1⊇S2의 관련성을 가지면 보안등급 L1(C1,S1)은 보안등급 L2(C2,S2)를 지배한다. 만약 보안등급 L1과 L2가 L1≥L2의 관계도 아니며 L1≤L2 관계도 갖지 않으면 이 두 가지 보안등급은 서로 비교불가능하다고 한다[3].

2.2 Biba 모델

BLP 모델은 권한을 갖지 않는 사용자에게 정보가 흘러가는 것을 예방하는 비밀성에 기반을 둔 모델이다. 이 모델은 정보의 비밀성은 보장하지만 등급이 낮은 주체가 등급이 높은 객체의 정보를 변경할 수가 있어 정보의 무결성을 보장하지는 못한다. 이러한 단점을 보완하기 위해 Biba 모델이 제안되었다. 이 모델에서도 주체와 객체의 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.

만약, C1≥C2 이고 S1⊇S2의 관계를 가지면 무결성 등급 L1=(C1,C2)는 L2=(C2,S2)를 지배한다. 무결성 등급이 L1≥L2 나 L2≥L1 의 관계가 모두 아니면 이 두 등급은 비교불가능하다고 한다. 사용자를대신하여 수행하는 프로세스나 접근이 수행되는 객체에게 무결성 등급이 부여된다. Biba 모델은 하나의 보안정책을 사용하지 않고 정보의 무결성을 보장하기 위해 해당 보안 환경에 맞는 보안정책을 사용한다[2].

3. 컨텍스트기반접근통제모델

정보통신기술의 급속한 발전으로 인해 웹을 통한 기업모델의 개발에 따른 기업모델의 다양화로 인해 개인정보를 통한 DB의 집적, 고객관계관리와 같은 새로운 경영기법의 발전을 이끌었던 반면 개인정보의 오용과 남용은 인터넷 발전의 가장 큰 저해 요소 중 하나로 대두되게 되었다. 그러므로 방대한 정보를 부당한 사용자로부터 보호하면서 개인의 프라이버시를 보장하기 위해서는 적절한 접근통제 정책이 요구되어진다.

주체와 객체의 보안등급에 의해 정보의 접근권한을 부여하는 강제적 접근통제모델은 상위등급에 의해 하위등급의 객체 정보가 소유주의 의사와는 무관하게 이용 및 변경될 수 있는 우려가 있어 사생활을 보호할 수 있는 개인정보 보호 대책이 부가된다면 더욱더 정보의 무결성을 강화할 수 있을 것이다.

자연어로 명시된 고수준의 프라이버시 정책과 요구조건은 기술적으로 구현되기 전에 적법한 접근통제 규칙에 의해 정형화가 되어야 한다.

본 논문에서는 Biba 모델의 엄격한 무결성 정책에 대한 시스템 상태정보, 연산 그리고 주체의 생성과 실행에 따른 제약조건을 기술하였다. 또한, 객체의 용도(purpose)와 접근권한의 제약조건으로 구성되는 컨텍스트를 엄격한 무결성 정책에 적용하므로서 주체에 의한 객체정보의 임의적 연산을 방지하므로서 객체 정보를 보호할 수 있다.

3.1 시스템 상태와 연산모드

시스템 상태는 다음과 같이 3가지 구성요소인 b, M, f를 갖는다.

◇ b : 3가지 튜플(주체, 객체, 접근권한)인 (Subject, Object, Permission)로 구성

◇ M : 주체와 객체에 접근할 수 있는가[M(S, O)], 주체가 또 다른 주체를 호출할 수 있는가[M(Si,Sj)]를 나타내는 접근행렬
◇ f : 주체와 객체에 연관되어있는 등급함수로 f : S ∪ O → L로 구성
주체가 객체에 대해 수행할 수 있는 연산에는 다음과 같다.
◇ Modify : 객체에 정보를 쓰는 연산으로 다른 모델에서는 write 모드와 유사하다.
◇ Observe : 객체의 정보를 읽는 연산으로 다른 모델에서는 read 모드와 유사하다.
◇ Execute : 객체(프로그램)의 정보를 실행하는 연산이다.
◇ Invoke : 앞의 모드들은 객체에 적용되는 모드이지만 Invoke 모드는 주체에 적용되는 모드로서 다른 주체와 호출을 하기 위한 연산이다.

객체와 접근권한은 용도(purpose)와 제약조건(condition)의 속성을 갖는 컨텍스트로 구성되며, 제약조건은 논리함수로 표현되며 표현식의 오퍼랜드는 주체, 객체, 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, 관리자와 정보소유주인 개인에게 정보의 이용 권한이 있는 요소로 고객의 동의가 필요하다. 또 하나는 공개용 용도 요소(public purpose element)로 관리자나 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 개인용 자료목적 요소로 정보 사용에 동의하였다면, 그 정보는 상위 무결성 등급을 갖는 주체라 하더라도 정보 소유주인 해당 고객 이외에는 정보가 제공되지 않는다.

제약조건은 Observe, Modify, Invoke 연산별로 나뉜다. 첫째, Observe 연산에 관련된 제약조건은, 주체가 수행중인 무결성등급[fc(S)]은 주체가 생성시 부여된 무결성등급[fs(S)]보다 반드시 적거나 같아야 하며, 주체의 수행중인 무결성 등급이 객체의 수행중인 무결성 등급에 지배된다면 주체는 객체에 Observe 오퍼레이션을 수행할 수 있다.

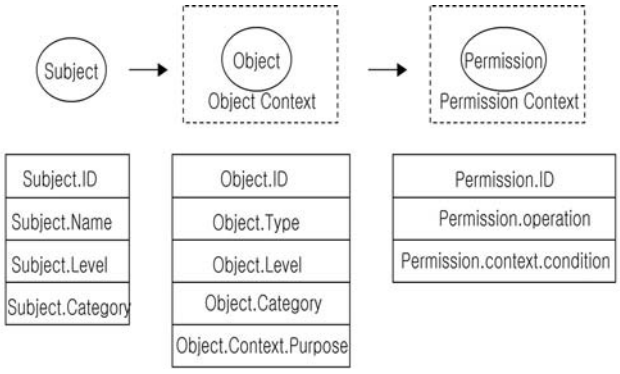
· Observe ∈ M[S, O] ⇒
fs(S) ≥ fc(S) AND fc(S) ≤ fc(O)

둘째, Modify 연산에 관련된 제약조건은, 주체가 수행중인 무결성등급[fc(S)]은 주체가 생성시 부여된 무결성등급[fs(S)]보다 반드시 적거나 같아야 하며, 주체의 수행중인 무결성 등급이 객체의수행중인 무결성 등급을 지배한다면 주체는 객체에 Modify 오퍼레이션을 수행할 수 있다.

· Modify ∈M[S, O] ⇒
fs(S) ≥ fc(S) AND fc(S) ≥ fc(O)

셋째, Invoke 오퍼레이션을 요청할 주체의 무결성 등급이 요청될주체의 무결성 등급을 지배한다면 Invoke 오퍼레이션을 수행할 수 있다.

· Invoke ∈ M[S1, S2] ⇒
fs(S1) ≥ fc(S1) AND fs(S2) ≥ fc(S2)
AND fc(S1) ≥ fc(S2)



<그림 1> 컨텍스트기반 MAC 모델 구성요소

4. 결 론

개방형 분산 환경에서 정보 보호에 대한 중요성은 매우 중요하다. 특히 정보 통신망에서 운영되는 정보를 저장 관리하는 컴퓨터 시스템에서 보안의 필요성은 컴퓨터에서 처리되는 정보를 권한이 없는 사용자가 판독하거나 또는 부적절하게 기록하는 것을 방지하며 그리고 정당한 권한을 갖는 사용자의 정보처리 서비스를 컴퓨터에서 거부되지 않도록 보호하기 위한 것이다.

정보통신기술의 급속한 발전으로 인해 웹을 통한 기업모델의 개발에 따른 기업모델의 다양화로 인해 개인정보를 통한 DB의 집적, 고객관계관리와 같은 새로운 경영기법의 발전을 이끌었던 반면 개인정보의 오용과 남용은 인터넷 발전의 가장 큰 저해 요소 중 하나로 대두되게 되었다. 그러므로 방대한 정보를 부당한 사용자로부터 보호하면서 개인의 프라이버시를 보장하기 위해서는 적절한 접근통제 정책이 요구되어진다.

주체와 객체의 보안등급에 의해 정보의 접근권한을 부여하는 강제적 접근통제모델은 상위등급에 의해 하위등급의 객체 정보가 소유주의 의사와는 무관하게 이용 및 변경될 수 있는 우려가 있어 사생활을 보호할 수 있는 개인정보 보호 대책이 부가된다면 더욱더 정보의 무결성을 강화할 수 있을 것이다.

본 논문에서는 Biba 모델의 엄격한 무결성 정책에 대한 접근모드, 시스템 상태정보 그리고 주체의 생성과 실행에 따른 제약조건을 기술하였다. 또한, 객체의 용도(purpose)와 접근권한의 제약조건으로 구성되는 컨텍스트를 엄격한 무결성 정책에 적용하므로서 주체에 의한 객체정보의 임의적 연산(observe, invoke, modify)을 방지하므로서 객체 정보를 보호할 수 있다.

추후 연구방향으로는 주체에 대한 컨텍스트와 객체 및 접근권한 컨텍스트를 강화하고자 한다. 또한, 용도요소를 확장하여 용도 계층(purpose hierarchy)을 생성하여 이들간의 관련성을 기술하고자 한다.

[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.