通信情報保護學會誌
第7卷 第1號, 1997. 3

OSI 보안 프레임워크에서 접근 제어 시스템

The Access Control Systems on OSI Security Framework

조 인 준*, 김 동 규**

요 약

OSI 통신망 보안의 전체적인 보안 프레임워크는 ITU-T X.810, 인증(Authentication) 프레임워크는 ITU-T X.811 그리고 접근 제어(Access Control) 프레임워크는 ITU-T X.812에서 각각 기술하고 있다. 이들은 OSI 참조 모델을 기반으로 한 보안 시스템 설계의 기본 골격을 제공한다.

본 고에서는 통신망 보호를 위한 기밀성(Secrecy), 무결성(Integrity), 가용성(Availability) 보안 서비스들 중에서 기밀성 보장에 해당하는 접근 제어(Access Control) 프레임워크를 ITU-T Rec. X.812(1995.7)를 기반으로 분석 하였다.

I. 서 론

정보 통신망을 이용한, 정보의 자동화는, 자동화 이전의 정보 보안체계를 통신망 내로 구현해야 하였다. 그러나 대부분의 정보 통신 망 하드웨어 및 소프트웨어 설계 과정에 이 체계를 적용하지 않아 외부의 침입자에 의한 정보의 노출 및 파괴가 심각한 사회현상으로 대두되고 있다.[2)3)] 이러한 현상은 최근 들어 컴퓨팅 환경이 네트워크를 통한 분산 환경으로 급속히 전환됨에 따라 이에 대한 보안대책이 절박한 실정에 있다.

본 논문에서는 정보 통신망 보안 서비스 중 기밀성 보장을 위한 접근 제어 기술을 분석한 내용이다. 접근 제어의 목적은 정보 통신망 내의 적법한 사용자가 수행할 수 있는 연산(Operations) 또는 행위(Actions)를 제한하여 정보의 기밀성(Secrecy)보장에 있다.

본문의 내용은 2장에 접근 제어와 보안 서비스간의 관계를 정리하였다. 3장에는 X.812에서 정의한 접근 제어 개요를 설명 하였고, 4장에는 접근 제어 정책의 일반적인 개념을 설명 하였다. 5장에는 접근 제어 정보와 접근 제어 모듈을 중심으로 접근 제어 시스템 동작 방법을 설명 하였다. 마지막으로 6장에서는 접근 제어 메카니즘을 X.812를 기반으로 설명 하였다.

II. 접근 제어와 보안 서비스 관계

접근 제어는 정보 통신망 내의 다른 보안 서비스와 상호 공존 또는 의존한다. 접근 제어는 시스템 내의 객체(Object)를 대상으로 이루어지는 사용자의 접근 시도를 관리하는 참

* 배재대 컴퓨터 공학과 교수
** 아주대 컴퓨터 공학과 교수

조 모니터(Reference Monitor)에 의해 구현될 수 있다[1)2)3)]. 참조 모니터는 어떤 연산을 시도한 주체(Subject)가 그 연산을 실행할 자격이 있는지 결정하기 위해서 접근 제어 정보 DB(Authorization Database)를 참조한다. 이 데이터 베이스 내에 보관된 접근 제어 정보는 보안 관리자에 의해 운영 및 유지된다. 관리자는 그 조직의 보안 정책 규정에 따라 접근 권리(Right)를 정한다. 사용자는 제한된 범위(예: 개인적인 파일에 접근 허용 권 조정 등.) 내에서 접근 인가 데이터 베이스를 조정할 수 있다. 무결성(Integrity) 보장은 구성 요소 사이에 입출력 되는 데이터의 불법적 변경 방지를 말한다. 기밀성(Confidentiality)은 정보 내용에 암호 기술을 적용, 불법적인 정보 내용 노출에 대한 대비책이다. 감사(Audit)는 시스템 내에서 일어나는 접근 행위 정보를 보관하고 감시한다. 이들의 상호관계를 논리적으로 정리하면 그림1) 과 같다.

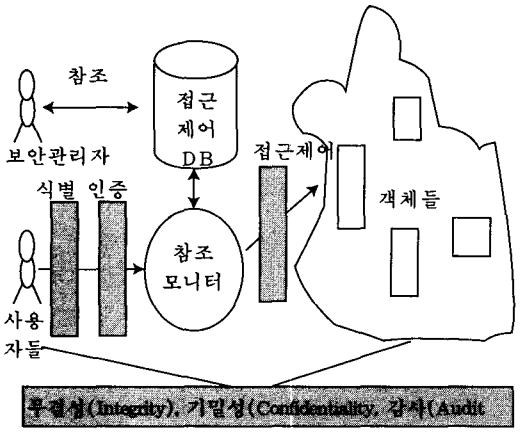


그림 1) 접근 제어와 보안 서비스 관계

접근 제어는 식별 및 인증과 분명하게 구별된다. 사용자의 식별을 올바르게 한다는 것은 인증 서비스의 책임이다. 접근 제어의 실행은 성공적인 식별 및 인증을 전제로 이루어진다.

또한 접근 제어가 안전한 시스템(Secure System)의 완벽한 해법은 아니다. 여기에는 위에서 설명한 무결성, 기밀성, 감사 등과 같은 보안 서비스가 이루어져야 한다. 특히 감사 제어에서는 모든 사용자 행위와 요구 사항을 기록할 것을 요구한다. 이는 보안 시스템에서 취약 지점을 발견해 내는데 유용하게 사용된다.

III. X.812 접근 제어의 개요

1. 개요

접근 제어 시스템은 크게 제어의 실체(대상)와 이에 행해지는 접근 제어 행위로 나눌 수 있다. 실 시스템에서 제어 실체는 여러 가지 유형이 있다. 실 시스템 자체와 같은 물리적 실체, OSI 계층, 파일, 조직, 기관과 같은 논리적 실체 그리고 사람 등을 들 수 있다. 접근 행위 또한 여러 가지 유형이 있다. 이는 접근 제어를 관리 측면에서 행위와 운용(Operation) 측면에서 행위로 대별 된다. 전자의 행위로는 접근 제어 정책 표현을 설정하는 행위, ACI(Access Control Information)표현을 설정하는 행위, 접근을 시도하는 주체(Initiator 또는 Subject), 접근을 받는 객체(Target 또는 Object) 그리고 접근-요구(Access Request) 등의 요소에 ACI를 할당하는 행위, 상기 요소에 ACI를 결합 시키는 행위, ACI를 수정하는 행위, ADI(Access Decision Information)를 제거하는 행위 등이다. 후자의 행위로는 ADF (Access Decision Function)에 가용한 ADI를 만드는 행위와 접근 제어 기능을 실행하는 행위 (AEF(Access Enforcement Function)) 등이다.

이들 행위는 실 시스템에서 하나의 식별 가능한 행위로 그룹화 될 수 있고, 이들 행위 사이에 실행의 우선 순위가 있을 수 있고, 이들 사이에 실행이 겹칠 수 있고, 또한 몇몇 행위

는 반복적으로 실행될 수 있다. 이러한 행위를 접근 제어 기능 실행 측면에서 분석하면 다음과 같다.

2. 접근 제어 기능 실행

그림2)는 접근 제어 시스템의 기본적인 구성 요소와 기능간의 관계를 나타내고 있다. 이들 기능은 다양한 방법으로 구현 된다. 구현 방법에 따라 접근 제어 기능과 ACI 분배 방법도 다양하다. 그리고 동일 또는 서로 다른 보안 영역에서 접근 제어 기능간의 통신도 다양한 유형으로 이루어 진다.

그림 2)에서 기본적인 접근 제어 실체는 주체와 객체이고, 접근 제어 기능은 접근 요구를 받아 이를 실행하는 AEF와 접근 제어를 결정하는 ADF이다. 주체란 객체에 접근을 시도한 사람이거나, 직접 객체에 접근하는 컴퓨터와 같은 실체를 말한다. 실 시스템에서 주체는 주체(사람)의 행위에 따라 컴퓨터란 실체가 접근-요구(Access Request)를 하게 된다.

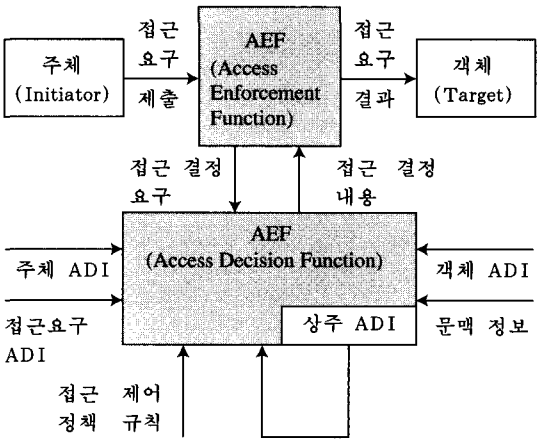


그림 2) X.812 기본 접근 제어 개념도

객체란, 주체가 접근을 시도하거나 접근 하는 컴퓨터란 실체 또는 통신 실체가 된다. 예를 들면, OSI 계층 요소, 파일, 실 시스템 등이다. 접근-요구(Access Request)란, 시도된 접근 행위를 나타내는 오퍼레이션과 오퍼랜드를 말한다.

접근 제어 실행 기능(AEF)이란, ADF를 호출하여 주체에 허용된 객체에만 접근이 가능토록 하는 기능을 말한다. ADF는 주체가 객체에게 특정 접근을 요구할 때, 접근 결정을 하여 이를 AEF에게 넘겨준다.

접근 결정 기능(ADF)이란 AEF가 요구한 접근 요구에 대해 접근 결정을 하는 기능을 말한다. ADF는 AEF의 접근-요구와 더불어 다음과 같은 접근 제어 결정 정보(ADI)를 제공 받는다. 주체에 결합된 ACI로부터 유도된 주체-ADI, 객체에 결합된 ACI로부터 유도된 객체-ADI, 접근-요구에 결합된 ACI로부터 유도된 접근-요구-ADI, ADF의 보안 영역 관리자로부터의 보안 정책 규칙, ADI나 보안 정책 해석에 필요한 문맥 정보 그리고 이전 접근 제어 결정으로부터 상주한 ADI등을 입력으로 받는다. 여기에서 문맥 정보란 주체의 위치, 접근 시간 또는 사용할 특정 통신 경로 정보 등을 말한다.

ADF는 상기와 같은 입력 정보를 기반으로 객체에 접근 유무를 결정한다. 이 결정 결과가 AEF에게 운반된다.

여러 가지 상황이 주체가 객체에 접근하고자 할 경우 관련된다. 전형적인 예는 주체의 응용이 상대 객체의 응용 프로세스에 연결을 오픈(Open) 하고, 동일한 ADI(상주 ADI)를 사용하여 여러 접근들을 실행할 경우이다. 이러한 연결에서 일어나는 순차적인 접근-요구에 추가적인 ADI가 필요할 수도 있다. 또 다른 상황은 보안 정책에서 주체들 사이에서 관련된 접근-요구들을 가질 것을 요구하는 경우이다. 이때, 객체들이 주체의 접근 제어를 제한한다. 이 경우 ADF가 특정 접근-요구에 접근 결정

을 행하기 위해서 다중 주체와 객체를 포함한 이전의 결정으로부터 상주한 ADI를 사용한다.

한 접근-요구를 AEF가 허용한다면, 한 객체를 대상으로 주체가 단일 접근 행위를 한다. 주체와 객체 사이에 몇몇 접근-요구는 다른 접근-요구에 순수하게 독립적이지만, 질의·응답 응용과 같은 형태에서는 두 실체가 관련된 접근·요구의 집합에 관여 될 수 있다. 이 경우, 주체와 객체의 직무가 필요에 따라 동시 또는 선택적으로 접근 실체에 의해 추정되고, 접근 제어 기능은 분리된 AEF, ADF, 접근 제어 정책에 따라 각 접근-요구를 실행한다.

3. 기타 접근 제어 행위

첫째, 접근 제어 정책 표현 행위이다. 접근 제어 정책은 광범위한 원칙들을 가지고 있다. 예를 들면 "자격을 가진 관리자만이 고용자의 급여 정보를 다룰 수 있다"는 원칙이다. 이러한 원칙을 규칙화 시키는 것은 보안 프레임워크 영역에 포함되지 않지만, 접근 제어 행위가 이루어지기 전에 필수적으로 선행되어야 한다. 이의 자세한 내용은 2장에서 설명한다.

둘째, ACI표현 행위이다. 이는 실 시스템 내의 자료 구조로 ACI를 표현하는 방법과 시스템간에 교환되는 ACI 구문(Syntax) 정의를 말한다. 여러 가지 가능한 표현들이 보안 프레임워크에서 논의 되어 진다. ACI표현은 지정된 접근 제어 정책을 지원할 수 있어야 한다. 몇몇 ACI표현이 실 시스템 내 또는 실 시스템 간에 사용될 수 있도록 적합해야 한다. 서로 다른 ACI 표현이 특정 요소들 사이에 서로 다른 목적을 위해 사용될 수 있다.

선택된 ACI 표현은 보안 영역 내의 요소들(주체, 객체 등)에 특정 ACI값 할당을 위한 가늠자 역할을 한다. ACI표현의 한 측면은 보안 영역 내의 요소에 할당할 수 있는 ACI값의 유형과 범위를 결정한다. 접근 제어 관리 목적 또는 실체간의 ACI교환과 같은 접근 제어 기능 목적을 위해서, 실 시스템 간에 교환되는 ACI 표현을 OSI표준에서 추천하고 있다. 교환되는 ACI 보호 문제는 다음 장에서 설명한다.

OSI 참조 모델에서 접근 제어는 연결 설립 혹은 데이터 전송 단계 설립 과정에서 이루어진다. 따라서 이는 네트워크 층(3층), 전송층(4층), 응용 층(7층)에서 이루어진다. OSI응용 층에서 ACI표현은 (속성 유형, 속성 값)쌍으로 정의된다.

셋째, 주체 또는 객체에 ACI를 할당(Allocation)하는 행위이다. 이는 한 요소에 할당된 ACI의 속성 유형과 값은 SAD(또는 이의 대리자) 또는 자원의 소유자가 결정한다. 이를 결정하는 실체는 보안 영역의 정책에 따라 ACI할당을 지정 및 수정할 수 있다. 한 실체가 할당한 ACI를 다른 실체가 그 ACI에 결합시킨 ACI로 제한을 할 수 있다. 또한 요소들에 ACI 할당은 새로운 요소가 보안 영역에 추가 될 때 마다 이루어진다. 여기에서 주체나 객체에게 "접근 권리(Access right)"를 허용하는 관리적 행위를 인가 행위(Authorization)라고 한다. 이 의미는 주체나 객체에 ACI 할당 행위를 말한다.

ACI는 단일 실체, 또는 실체들간의 관계에 관한 정보가 될 수 있다. 한 주체에 할당된 ACI는 순수하게 그 주체에 관한 것이 될 수 있고, 또는 그 주체와 특정 객체들, 또는 그 주체와 가능한 문맥들 사이의 관계를 표시한 정보가 될 수 있다. 따라서 주체에 할당된 ACI는 주체 ACI, 또는 객체 ACI, 또는 문맥 정보를 포함할 수 있다. 이는 객체에 할당된 ACI도 동리한 원리이다.

실 오퍼레이션에서 ACI는 해당 요소에 결합되어야 한다. 이는 ADF가 실체에 결합된 ACI로부터 유도된 ADI를 신용하기 위한 행위이다. 따라서 해당 요소에 ACI할당이 결합-ACI

구성의 선행 요구 사항 이지만, 한 요소에 할당된 ACI만이 실 개방 시스템에 나타난다.

넷째, 주체, 객체, 접근-요구에 ACI를 결합(Binding)시키는 행위이다. 상기와 같은 요소 각각에 ACI-결합은 요소와 이에 결합된 ACI 사이에 안전한 연결 링크 생성을 의미한다. 결합 행위는 ACI가 진정으로 특정 요소에 할당되었다는 사실과 결합 행위가 이루어진 후 그 결합에 어떤 수정도 일어나지 않았다는 사실을 접근 제어 기능과 다른 요소에게 보장하는 행위이다.

결합 행위는 무결성 보안 서비스를 통해서 이루어진다. 결합 메카니즘은 요소와 ACI의 위치, 그리고 봉인 및 서명 방법에 따라 다양하다. 요소들에 ACI-결합 행위시 무결성은 주체 및 객체 시스템 내, 그리고 ACI 교환시에 보장될 필요가 있다. 시스템 내 및 시스템간에 다양한 요소의 ACI 표현이 가능하기 때문에 서로 다른 결합 메카니즘들이 동일한 ACI에 대해서 사용된다.

요소들에 ACI-결합은 새로운 요소가 보안 영역에 추가될 때마다 이루어지는 행위이다. 보안 정책에 따라, SDA, SDA 대리자, 또는 자원의 소유자가 ACI-결합을 추가 및 삭제할 수 있다. 특히, SDA는 보안 정책 및 속성 변경을 위해서 요소의 결합-ACI를 수정 할 수 있다.

결합된 ACI에는 결합 유효 기간 표시가 있다. 이는 후에 이를 폐지해야 하는 ACI 수를 최소화 하기 위한 것이다. 각 요소와 실체에 ACI-결합 시기(결합 메카니즘 호출 시기)는 요소의 유형에 좌우 된다. 주체는 접근 실행 시점 까지 SDA 또는 그 대리자로부터 ACI-결합이 이루어져야 한다. 객체는 주체가 접근이 가능하게 될 때까지 SDA나 그 대리자로부터 ACI-결합이 이루어져야 한다. 사용자 또는 다른 응용의 행위에 의해 생성된 객체는 생성 시간 또는 생성 후에 결합-ACI를 가져야 한다.

접근-요구에서는 사용자 또는 응용의 행위에 따라 사용자 또는 응용, SDA, 또는 그 대리자가 ACI를 결합 시킨다. 접근-요구의 결합-ACI는 사용자 또는 응용에 결합된 ACI내의 제약 조건에 따라 좌우된다. 접근·요구가 새로 만들어진 객체(예, 시스템간에 파일 전송시)를 대상으로 할 때, 객체의 ACI가 접근-요구에 결합된 ACI에 지정되거나, 이로부터 유도될 수 있다.

다섯째, ADF에게 가용한 ADI를 만드는 행위이다. 이는 접근 제어 정책과 사용 중인 결합 메카니즘에 따라, 주체 또는 객체에 결합된 ACI의 일부(Subset), 즉 ADI를 접근 제어 결정 목적을 위해 ADF에게 제공한다. 한 요소에 결합된 ACI는 한 실체가 다른 실체의 행위에 따라 동작할 때, 다른 요소에 임시로 결합될 수 있다. 이러한 기능을 실행하기 위해서 다양한 ADI가 ADF에 주어진다.

세 가지 가능성이 주체, 객체, 또는 접근-요구 ADI에 있을 수 있다. 첫째, ACI 값 할당(Allocation) 후, ADI를 ADF 구성 요소에 미리 제공할 경우, 둘째, 접근 제어 과정에 ADF에 도달한 결합-ACI로부터 ADI를 유도할 경우, 셋째, 디렉토리 서비스 대리자와 같은 다른 실체로부터 얻은 결합-ACI로부터 ADI를 유도할 경우이다. 일반적으로 주체 또는 객체가 결합-ACI를 얻거나, ADF가 필요에 따라 결합-ACI를 얻는다.

ADF가 결합-ACI를 얻은 후, 이를 통한 ADI 유도 방법은 규정하지 않는다. 주체 결합-ACI는 필수적으로 주체에 의해 유도될 필요가 없다. 이는 객체 및 접근-요구 결합-ACI도 마찬가지다.

여섯째, ACI의 수정 행위이다. 이는 SDA가 보안 속성 변경 필요에 따라 요소에 할당된 ACI 또는 결합-ACI를 수정하는 행위를 말한다.

일곱째, ADI의 폐지 행위이다. 이는 ACI가

폐지된 후, 그 ACI에서 유도된 ADI 사용은 인가되지 않은 접근 결과를 가져올 수 있다. 따라서 ADI 폐지 후 ACI로부터 유도된 ADI 사용을 금지시키거나, 접근 자체를 거부해야 한다. ACI가 폐지될 때, 이전에 ACI로부터 유도된 ADI를 사용하는 접근은 접근 제어 정책에서 종료를 요구할 필요가 있다.

4. ACI 전진(Forwarding)

분산 시스템에서 접근 행위는 한 실체에서 다른 실체로 이루어진다. 모든 실체가 주체와 객체 두 역할 모두로 가정할 수 없지만, 주체와 객체는 실체에 의해 가정된 직무를 말한다. 어떤 실체는 한 실체에 상대적으로 주체의 역할을 하고 반면에 객체 스스로가 다른 실체서 상대적으로 주체 직무를 한다. 이를 연쇄된(Chained) 접근이라 한다. 이를 그림 2)에서 나타내고 있다.

이에 대한 기본 개념들은 매우 다양하다. 이들은 연쇄 접근 허용을 나타내는 정책에 의해 요구된 ACI들의 조합, 그리고 그 ACI 가 적정 구성 요소에 어떻게 가용하게 만들어 지냐에 따라 다르게 나타난다.

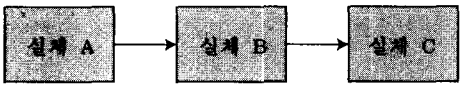


그림 3) ACI 전진

어떤 정책에서 B는 A가 접근을 실행하기 위해서 이미 B에 결합시킨 ACI 이외는 필요하지 않을 수 있다. 또 다른 정책에서는 B가 접근에 관련된 A로부터 얻은 ACI만을 사용한 경우도 있다. 일반적인 경우는 A와 B에 결합된 ACI를 사용한다.다음과 같은 예가 이러한 변형 규정을 정립하는대 사용될 수 있다. 첫째, 가장 단순한 경우로 A가 B의 ACI로 A의 접근-요구 실행이 충분 조건 일 경우, 접근을 B에게 요구한 경우이다. 둘째, A가 접근-요구를 위해서 접근-요구 구성요소가 허락할 수 있는 ACI 모두 또는 일부를 제공한 경우이다. 이때 A는 접근-요구와 함께 B에게 ACI를 전달함으로써 ACI를 제공한다. 또한 A가 접근을 실행하기 위해서 B를 요구하기 전에 C로부터 미리 접근 인가를 요구한 경우이다. 이때, A는 A가 만든 토큰을 통해서 C에게 ACI를 제공한다. 이 토큰은 요구된 접근과 함께 A가 B에게 보내지고 C가 이를 인식한다. 그림3)은 여러 개의 중간 실체를 일반화한 것이다.

5. 접근 제어 구성요소의 분산

접근 제어의 기본 기능인 AEF나 ADF가 한 개 이상의 접근 제어 구성 요소(AEC(AEF Component),ADC(ADF Component))에서 실행될 수 있다. 접근 제어 기능이 접근 제어 정책에 따라 이들 구성 요소 사이에 분산될 수 있다. 기본적인 접근 제어 기능은 구성 요소의 위치, 그들 사이의 통신, 가능한 기능의 분산 등에 독립적이다. 이때 고려 사항은 AEC와 ADC의 수와 위치, 그리고 주체, AEC, ADC, 객체간의 상호작용이다. AEC와 ADC의 물리적 구성 방법은 여러 가지 있다. 일반적인 구성 요소들의 분산은 그림 4)와 같다. 그림에서처럼 AEC가 종단 시스템 내·외에 존재할 수 있다. 이들의 장단점은 접근 제어 정책, 구현 안전성 등에 따라 다르다. ADC도 비슷하게 존재할 수 있다.

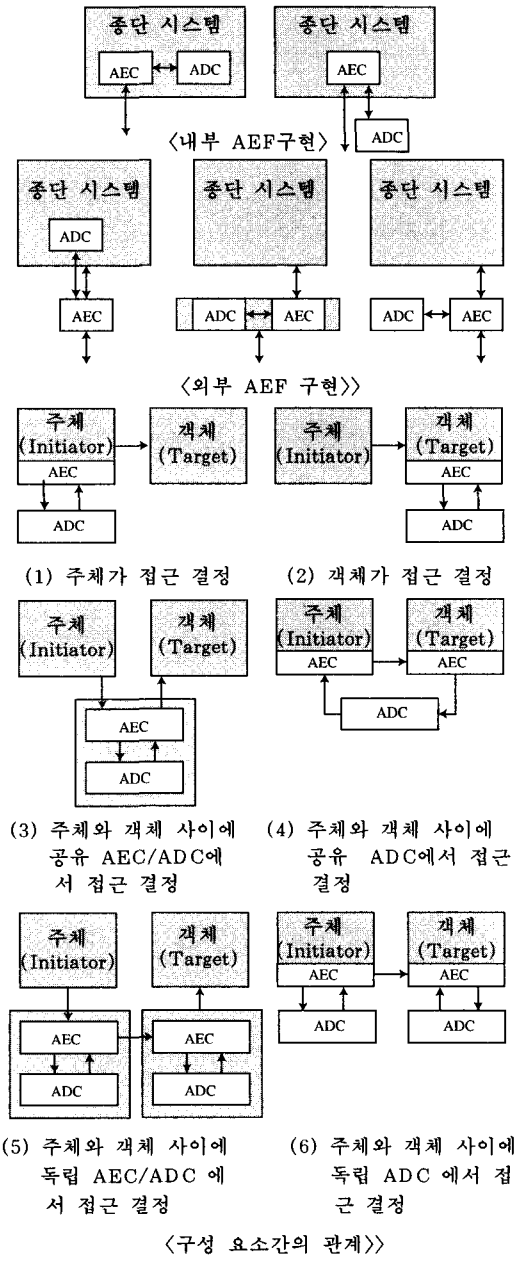


그림 4) 접근 구성 요소의 분산

그림의 각 구성 요소의 관계에서 AEC가 주체 AEC를 통해서만 객체에 동작할 수 있도록 각 주체와 객체 사이에 놓인다[(1), (3), (6)]. 한 ADC가 AEC구성 요소와 밀접하게 결합될 수 있고[(3),(5)] 그렇지 않을 수 있다[(1),(2),(4),(6)]. ADC가 한 개 이상의 AEC에 제공될 수도 있다. 이 반대도 성립이 된다. AEF와 ADF를 밀접하게 결합시킨 배치는 통신 지연을 줄여 효율적이고, AEF와 ADF사이 통신 보안을 피하는 장점이 있다. 여러 개의 AEF에 제공된 ADF는 ACI 분배를 줄여주는 장점이 있고, 용이하게 감사와 같은 부가적인 보안 기능 구현에 장점이 있다.

이들 구성 요소의 위치를 정할 때 다음 사항이 고려된다. 첫째, SDA가 들어오는 접근 제어 요구를 객체에서 충분히 만족하도록 배치한다. 이때 객체의 AEC에 들어오는 접근 제어 정책을 구현 하고, 객체가 그 객체에 맞지 않은 정책일 경우 요구를 받아들이지 못하게 한다. 이는 주체가 보낸 접근-요구가 객체 AEF에 도달을 의미하고, ADF에 구현된 접근 제어 정책을 만족하는지를 객체 AEF가 검증한다는 의미이다. 둘째, SDA가 주체 AEF에 의해 나가는 접근 제어가 필요할 경우, 주체에 접근 제어 정책 구현 함으로써 객체가 허용하지 않는 접근을 방지 하도록 한 것이다. 이 경우 주체는 자신의 보안 영역의 접근 제어 정책에 부합되지 않은 접근을 실행할 수 없다. 셋째, AEF가 주체와 객체 사이에 존재할 경우, SDA가 주체와 객체 사이에서 접근을 정제하는 경우이다. 양자간에 위치한 AEF에는 들어오고 나가는 접근 제어 정책 둘 다를 구현할 수 있다. 이러한 접근 제어 정책은 주체와 객체의 보안 영역 접근 제어 정책에 독립적이다.

6. 다중 보안 영역간에 접근 제어 구성

요소의 분산 한 보안 영역의 자원이 다른 보안 영역으로부터 접근되도록 관계 규정을 보안 영역간에 규정할 수 있다. 보안 영역 중 일부가 ACI 접근 제어에 관여될 수도 있다. 이들의 보안 영역은 다음처럼 나눌 수 있다.

ACI를 주체에 결합시키는 보안 영역, 주체가 상주하는 보안 영역, ACI를 접근-요구에 결합시키는 보안 영역, 객체에 ACI를 결합 시키는 보안 영역, 객체가 상주하는 보안 영역, 접근 제어 결정이 이루어지는 보안 영역들, 접근 제어 결정이 구현된 보안 영역 등이다. 접근 제어 결정은 동일 SDA에서 AEF와 ADF가 행했던 것과 비슷하게 이루어진다. 하지만 SDA들, 보안 영역 관계들 그리고 영역들간의 통신들이 추가되어 복잡하게 된다.

영역간에 통신은 ACI의 새로운 결합 또는 ACI의 수정에 관여한 SAD 또는 이의 대리자들간에 인식, 시도된 접근에서 ACI 및 접근 제어 정책 표현의 번역과 검증 그리고 요구에 대한 응답 요청, 요구에 응답과 접근 요청 등에 관여한다.

7. 접근 제어 위협자

ACI와 접근 제어 기능들은 여러 실 시스템과 보안 영역들간에 분산됨을 앞 절에서 보였다. ACI가 안전하지 못한 통신 설비를 통해서 교환될 수 있고, 다른 SDA가 관여한 요소들에 의해 다루어질 수 있다. 다른 SDA들이 관여 될 때, 이들간에 보안 관계 정립이 필요하다. 이들에서 고려될 수 있는 위협자는 다음과 같다.

실체에 의해 적정한 AEF 또는 ADF로 가장(Masquerade), 어떤 AEF를 무사 통과, 접근 제어에 관련된 통신 또는 ACI의 채취(Interception), 재현, 수정 등의 위협, 의도하지 않은 주체, 객체, 또는 접근 요구가 ACI 오용, 잘못된 ADF가 ACI 오용, 규정된 제약 조건을 벗어난 ACI오용 등이다. 이러한 위협자에 보호 수단 제공은 4장에서 설명한다.

IV. 접근 제어 정책

1. 개요

접근 제어 정책은 보안 영역에서 정의한 보안 요구 사항이다. 이들이 ADF에 제공될 때, 접근 제어 규칙들의 집합으로 표현된다. 접근 제어 정책에서 2가지 중요한 측면은, 정책 표현 방법과 관리 방법이다. 일반적으로 관리적 측면에서 접근 제어 정책(Administratively-imposed access control policy)은 보안 레이블(Security Label)을 사용하여 표현 및 구현되고, 사용자 선택 접근 제어 정책(User-selected access control policy)은 주체나 객체의 신분을 기반으로 표현 및 구현된다. 접근 제어 정책의 표현 및 관리 기법은 논리적으로 독립적이다.

2. 접근 제어 정책의 표현 법

접근 제어 정책의 표현에 따른 분류는 규칙 기반(Rule-based) 정책과 신분 기반(Identity-based) 정책으로 나눈다(ISO 7498-2). 이는 DoD의 강제 접근제어(MAC(Mandatory Access Control)) 정책과 임의 접근 제어(DAC(Discretionary Access Control)) 정책에 대응한다. 이와 더불어 현대의 상용 환경에서는 상기의 두 정책을 병용한 직무 기반 접근 제어(Role-based Access Control) 정책이 확산되고 있다.

규칙 기반 접근 제어(MAC과 동일) 정책은 보안 관리자가 주체와 객체에 보안 레이블 형태로 제어 규칙을 할당한다. 시스템은 이 규칙에 의해서만 접근 제어가 수행되도록 한 정책이다. 이에는 주체가 "1급 비밀" "2급 비밀"과 같은 보안 등급(Clearance) 레이블을 소유하고, 객체도 이와 비슷한 보안 레이블(Classification)

을 소유하여 이들을 비교하여 접근을 제어하는 다중 보안 등급(Multi-level) 정책과 객체의 집합을 하나의 구획(영역) 이름으로 정의하고, 주체에 그 구획 내 객체 접근용 보안 레이블(Clearance)을 할당, 이들을 비교하여 접근 제어를 하는 구획-기반(Com- partment/Category-Based) 정책이 있다. 규칙 기반 접근 제어의 예는 그림5)와 같다. 이는 다중 등급 정책 예이다. 여기에서 보안 등급은 TS(Top Secret), S(Secret), C(Confid- ential), U(Unclassified) 등급 체계이다. 이들간의 관계는 TS>S>C>U이다. 주체에 의한 객체의 접근은 다음과 같은 두 가지 규칙에 의해 행해진다.

- o 아래로 읽기(Read down) : 주체의 보안 등급이 읽게 될 객체의 보안등급 보다 높아야 한다.
- o 위로 쓰기(Write up) : 주체의 보안등급이 쓰게 될 객체의 보안등급 보다 높아야 한다.

상기의 원칙을 만족하면, 상위 등급 객체(더 기밀한 객체)가 하위 등급의 객체로 정보가 흐르는 것을 막을 수 있다. 이러한 시스템에서 동일 보안등급의 정보는 단지 그 등급 이상으로만 흐르게 된다.

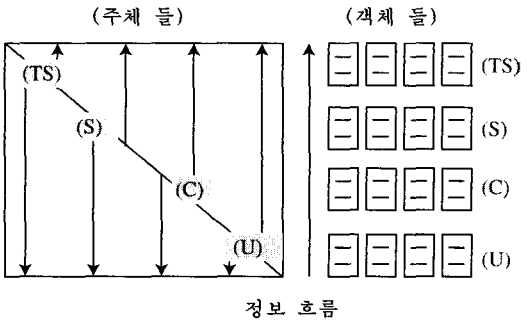


그림5) 규칙 기반 정책 예

신분 기반 접근 제어(DAC과 동일)정책은 각 요소의 신분 또는 ACI를 기반으로 개인 및 그룹 등에 접근 허용 유무를 결정한다. 이는 자원의 소유자 혹은 제어자가 임의적으로 허용된 접근을 바꿀 수 있다는 점에서 임의적이다. 이 정책은 각 객체를 중심으로 개개의 주체에 인가된 접근 오퍼레이션 리스트를 표기, 접근을 제어하는 개인-기반(Individual-Based) 정책과 한 객체에 대해 동일 접근 오퍼레이션을 가진 주체들을 그룹화 하여 그룹 이름으로 객체에 접근을 제어하는 그룹-기반(Group-Based)정책으로 분류할 수 있다.

직무-기반 정책은 사용자에게 상용 조직에서 사용하는 직무(인사 담당자, 회계 담당자, 지점장, 고객, 감사 등등)를 할당하고, 객체에 각 직무에 허용된 접근을 정의하여 양자를 비교, 접근 제어 결정을 한다. 여기에서 직무는 주체 그룹에 해당하고(신분-기반 정책), 직무 이외의 접근을 강제적으로 금지(규칙-기반 정책) 한다.

상기의 세 정책간의 관계는 그림 6)같이 해석할 수 있다.

그림에서 규칙 기반 정책의 주체 보안 레이블(Clearance)은 신분 기반 정책에서 주체의 ACI와 근본적으로 같을 수 있다.

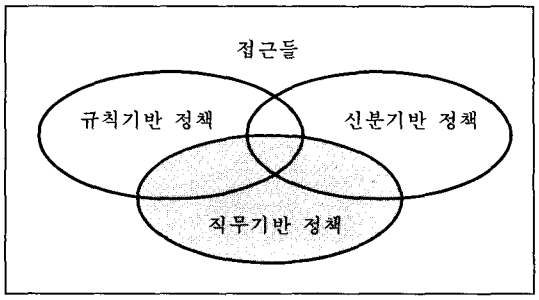


그림6) 규칙/신분/직무 기반 정책 관계

따라서, 규칙 기반 정책에 관련된 보안 레이블(Clearance)이 특정 주체의 ACI로 생각될 수 있다. 만약 규칙 기반 정책에서 사용자가

비계층 보안 레이블(Clearance)을 갖게 되면 이는 신분 기반 정책의 사용자 신분과 같고, 객체의 보안 레이블(Classification)은 신분 기반 정책의 ACL 엔트리와 같게 된다. 이러한 접근 요구는 위 그림에서 교집합 부분이다.

주체 그룹 또는 지정된 주체의 직무를 기반으로 한 접근 제어 정책은 신분 기반 접근 제어 정책의 특정 유형이다(X.812). 즉 X.812는 직무-기반 접근 제어 정책을 신분 기반 정책의 부분 집합으로 정의하고 있다. 여기에서 그룹이란, 특정 접근 제어 정책에서 동일한 구성원으로 정의한 주체의 집합을 말한다.

그룹은 객체ACI에 개개의 주체 신분 없이 그리고 각 주체에 동일한 ACI를 할당 하지 않고, 그룹(주체 집합)으로 특정 객체에 접근이 가능하다. 그룹 구성은 관리의 주체인 SDA가 행한다. 이에는 그룹의 생성 및 수정을 포함한다.

직무란, 사용자가 한 조직에서 행하는 정해진 기능을 말한다. 주어진 직무는 사용자 개인 또는 여러 사람에게 적용된다.

그룹과 직무는 주체의 신분, 그룹, 직무에 따라 계층적으로 결합 할 수 있다.

보안 레이블은 규칙 기반 접근 제어 정책의 기반을 이룬다. 주체와 객체에 서로 다른 보안 레이블이 결합되고, 접근 결정은 이를 비교하여 이루어진다. 이 정책은 지정된 보안 레이블을 가진 주체와 객체 사이에 일어나는 접근 규칙들로 표현된다.

보안 레이블로 접근 제어 정책의 표현은 무결성 및 기밀성 서비스를 제공할 때, 특히 유용하다.

3. 접근 제어 정책 관리

접근 제어 정책 관리는 고정(Fixed) 정책, 관리 중심(Administratively-imposed) 정책, 사용자 선택(User-selected) 정책으로 나눌 수 있다. 고정 정책은 변경이 불가능한 정책이고, 관리 중심 정책은 인가자만이 변경이 가능한 정책이고(MAC관리), 사용자 선택 정책은 상기 두 정책이 항상 강제적으로 적용되는 정책인 반면에 이는 주체 또는 객체가 접근-요구할 경우 사용자가 임의적으로 변경 가능한 정책이다(DAC관리). 그리고 이는 주체 또는 객체, 또는 그 주체 또는 객체의 자원을 포함한 접근-요구에 대해서만 적용되는 정책이다.

4. 접근 범주(Granularity)와 봉쇄

보안 정책에 다양한 등급의 접근 범주를 정의할 수 있다. 접근 범주를 대상으로 나누어지는 각 등급은 자신의 논리적인 정책을 가질 수 있고, 서로 다른 AEF와 ADF 요소를 사용할 수 있다. 예를 들어 접근 제어가 데이터베이스 서버 자체를 접근 범주로 하여 이루어질 수 있다. 이는 주체의 요구가 서버를 범주로 하여 접근을 부정하거나, 서버 내의 객체에 접근을 허용하는 것이다. 또 다른 방법으로 접근 범주가 개개의 파일, 파일 내의 레코드, 레코드 내의 항목을 단위로 제어 될 수 있다.

봉쇄는 객체 집단 중 어느 하나의 객체에 접근이 허용될 때만 그 객체 집단에 접근을 허용하는 접근 정책을 지정하여 이루어진다. 또한 이는 주체들의 대 그룹 내의 부 그룹에 적용될 수 있다. 가끔 봉쇄의 개념이 데이터베이스 내에서 파일 또는 파일 내에서 데이터 항목과 같은 다른 주체에 관련 된 주체에 적용되어진다. 다른 요소 내의 요소인 경우, 내부 요소에 접근을 시도하기 전에 그 요소를 통과하기 위한 접근 권리를 주체에게 주는 것이 필요하다. 보안 정책의 설계자가 세밀하게 이를 고려하지 않으면, 결과적으로 한 정책에서 부인된 접근이 의도하지 않은 사람에 의해 허용될 수 있다.

5. 상속 규칙

기존의 요소를 복사, 변경, 결합 또는 재구성하여 새로운 요소가 만들어진다. 새로운 요소의 ACI는 생성자의 ACI 또는 복사, 수정, 결합된 요소의 ACI 요소에 영향을 받을 수 있다. 상속의 규칙에 이러한 종속성들을 지정한다. 상속의 규칙은 ACI의 생성 및 수정 또는 보안 영역의 구성요소를 기반으로 한 요소에 ACI의 간접 적용 등을 결정하는 접근 제어 정책의 한 분야이다. 상속 규칙은 복사, 수정, 결합된 요소에 상속을 허용할 수도 있고 그렇지 않을 수도 있다. 한 요소가 다른 요소에 포함될 때, 자신의 ACI 일부 또는 전부가 상속 규칙에 따라, 포함된 요소의 ACI에 상속될 수 있다. 이러한 상속 규칙은 수 많은 요소에 적용된 통일 접근 제어 정책 관리를 단순화 시킨다.

6. 접근 제어 정책 규칙간의 우선권

접근 제어 규칙들이 적용될 때 이들간에 충돌이 있을 수 있다. 우선권 규칙에서 접근 제어 정책 규칙이 적용되는 순서를 지정한다. 예를 들면, 접근 제어 정책의 규칙 A와 규칙 B가 요구된 접근에 대해 서로 다른 접근 결정을 ADF가 한다면, 우선권 규칙에서 이 적용 순서를 결정한다. 이러한 규칙은 주체가 그룹 구성원 또는 특별한 직무로 동작할 때, 주체 ACI 사용에 적용될 수 있다. 우선 규칙은 가정된 직무나, 그룹의 ACI에 묶여진 주체 소유 ACI를 허용하고, 충돌 ACI가 어떻게 묶여지는지를 결정 해야 한다. 또한 우선 규칙은 그룹 또는 직무 ACI가 특정 접근-요구에만 적용된다는 것도 명시 해야 한다.

7. 디폴트(Default) 접근 제어 정책 규칙

이는 주체가 지정 객체에게 명확하게 접근 허용 및 부인을 지정하지 않았을 경우 사용한다. 예를 들면, 이 규칙으로 접근에 관련된 ADI에 적용된 다른 접근 제어 정책 규칙이 명확하게 부인을 하지 않으면, 객체에 접근을 허용하도록 정의할 수 있다.

8. 상호 동작 보안 영역간의 정책 사상

보안 영역간에 접근-요구에 접근 제어를 제공할 때, 접근-요구에 결합된 ACI를 변환하거나 사상할 필요가 있다. 이는 동일 ACI가 서로 다른 보안 정책으로 해석될 수 있고, ACI에 대해 보안 영역에 따라 서로 다른 표현을 가질 수 있다. 보안 영역간에 사상 되는 정보는 다음과 같다.

개인, 그룹 또는 직무의 식별자(예, 보안 영역 X에서 개인JSmith는 보안 영역 Y에서 개인 XJSmith로 인식 된다.)

직무와 속성(예, 사설 망에서 보안 관리자가 공용 망에서 가입자 보안 관리자로 인식된다.) 직무 또는 그룹에게 개개의 식별자(예, 사설 망의 모든 개인은 공용 망의 가입자 개인의 역할에 사상 될 수 있다.)

V. 접근 제어의 동작

1. 접근 제어 정보와 접근 제어 모듈

접근 제어 시스템에서 제어 정보와 제어 모듈간의 관계를 그림6)에서 설명하고 있다.

2. ACI (Access Control Information)

ACI는 접근 제어 서비스 실현을 위한 보안 정보이다. ACI는 주체, 객체, 접근-요구, 오퍼

레이션, 오퍼랜드, 문맥 정보 형태로 나눌 수 있다. ACI는 접근 제어 기능을 위해 실 시스템 사이에 교환 될 수 있다. 교환이 일어날 때, 각 객체는 추상 구문(Abstract Syntax)을 서로가 인지해야 한다. 이는 접근 제어 스킴 설명에 기초가 된다. 즉 선택된 보안 정책에 따라, 어떤 ACI가 요구되는 지를 정의할 필요가 있다.

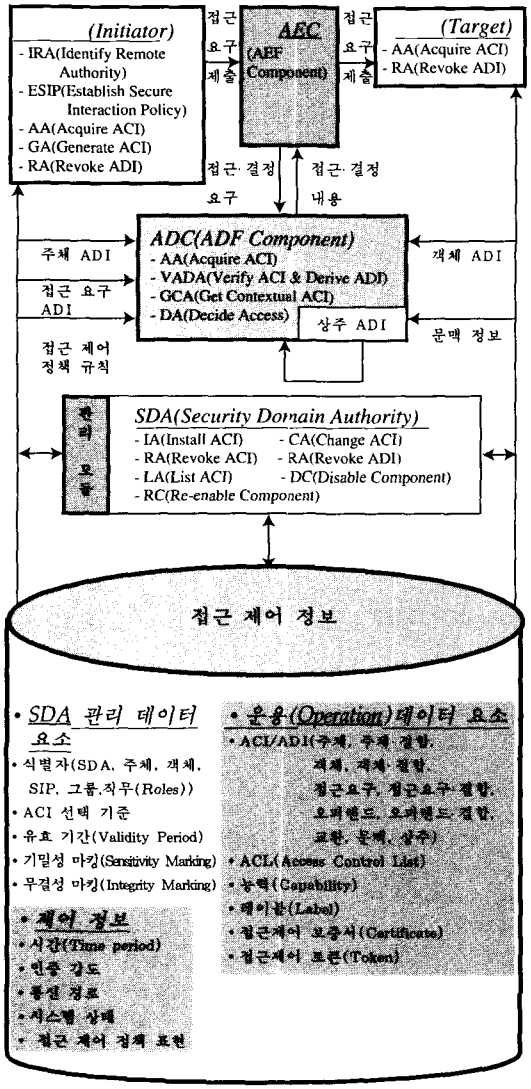


그림 6) 접근 제어 정보 및 기능 모듈 구성도

1) 주체 ACI :

주체 ID	그룹 ID	직무 ID	기밀성 마킹	무결성 마킹	기타

상기에서 주체 ACI내용 예를 보였다. 주체의 접근 제어 신분, 주체의 계층 그룹의 식별자, 주체의 기능 그룹의 식별자, 주체의 직무 식별자, 기밀성 마킹(Sensitivity Marking), 무결성 마킹 등이다. 주체의 접근 제어 신분은 인증, 감사, 사용료 부과 신분과 같을 필요는 없다. 이는 보안 영역 내에서 유일해야 한다.

2) 객체 ACI :

객체 ID	기밀성 마킹	무결성 마킹	Container ID	기타

상기에서 객체 ACI내용 예를 보였다. 객체 접근 제어 신분, 기밀 마킹, 무결성 마킹, 객체를 포함하는 용기(Container)의 식별자 등이다.

3) 접근-요구 ACI :

Operation Class (예, 읽기, 쓰기)	보안 등급	데이터 유형	기타

상기에서 접근-요구 ACI 내용 예를 보였다. 읽기, 쓰기 등과 같은 오퍼레이션들의 허용군, 오퍼레이션의 무결성 등급,오퍼레이션의 데이터 유형 등이다.

4) 오퍼랜드 ACI :

기밀성 마킹	무결성 마킹	기타

5) 문맥 정보 :

유효 기간	접근 경로	주체 위치	시스템 상태	인증 강도	기타

상기에서 문맥 정보 내용 예를 보였다. 접근 허용 유효 기간, 접근 허용 경로(Route), 특정 위치의 시스템에만 접근을 허용하는 시스템 위치 정보, 시스템이 특정 상태일 경우만 접근을 허용하는 시스템 상태 정보, 인증의 강도에 따라 접근을 허용하는 인증 강도 정보 등이다.

6) 주체-결합 ACI :

주체 ACI	객체 접근 제어 신분	객체에 허용된 접근법	주체 위치	기타

이는 주체 ACI, 객체 ACI, 선택된 문맥정보를 가질 수 있다. 이들의 형태는 보안 레이블, 능력, 접근 제어 보증서 형태로 나타난다. 이들에 포함된 정보의 예를 상기에서 보였다. 주체 ACI, 객체 접근 제어 신분과 객체에 허용된 접근들(능력 리스트), 주체 위치 정보 등이다.

7) 객체-결합 ACI :

주체 ID, 객체 접근들	계층 그룹 ID및 객체 접근 들	기능 그룹 ID및 객체 접근 들	직무 ID 및 객체 접근 들	인가된 권한 및 접근들

이는 주체와 객체의 ACI 그리고 문맥정보를 가질 수 있다. 이의 표현 형태는 ACL과 보안 레이블 형태로 다음 장에서 논의한다. 이에 포함될 수 있는 정보와 형태는 상기와 같다. 이의 예는 개개의 주체 접근 제어 신분들과 이들에게 객체 접근이 허용 및 부인되는 접근 정보, 계층 그룹 구성원 접근 제어 신분들과 이들에게 객체 접근이 허용 및 부인되는 접근 정보, 기능 그룹 구성원 접근 제어 신분들과 이들에게 객체 접근이 허용 및 부인되는 접근 정보, 직무 접근 제어 신분들과 이들에게 객체 접근이 허용 및 부인되는 접근 정보, 이들에게 허용된 권한들과 접근 정보 등이다.

8) 접근-요구-결합 ACI :

접근 허용 주체/객체 쌍	접근 허용 객체들	접근 허용 주체들	기타

이는 주체 ACI, 객체 ACI, 문맥 정보를 포함할 수 있다. 이의 예로 접근이 허용될 주체와 객체 쌍, 주체들, 객체들 등이다.

3. ACI의 보호

보안 메카니즘은 보안 서비스를 위해 실체들간에, 또는 보안 당국(Security Authority)과 실체간에 보안 정보(보안 정책 규칙, 인증 정보, 접근 제어 정보, 보안 레이블, 보안 보증서 및 보안 토큰 등)를 교환한다. 이들 정보는 암호 기술에 따라 다양한 방법으로 보호된다. ACI 보호는 ACI 보증서와 토큰을 사용하여 보호 된다.

1) 접근제어 보증서(Access control certificate)

접근 제어 보증서는 접근 제어 당국이 발행한 접근 제어 관련 데이터 집합이다. 이는 접근 제어 기능 수행 시, 접근 제어 당국에서 실체까지 ACI 운반용 보안 정보 단위이다. 실 시스템간에 교환되는 ACI는 여러 위협자로부터 보호되어야 한다. ACI를 발행한 당국은 ACI로부터 유도된 ADI를 사용하는 ADF에 의해 검증 되어야 한다. 이러한 검증 수단은 ACI발의 당국자가 서명 또는 봉인 된 보안 보

증서로 ACI를 꾸러미화 한다. 이 꾸러미를 접근 제어 보증서라 한다. 접근 제어 보증서는 다양한 형태의 정보를 가질 수 있다. 이들을 주체, 객체, 접근-요구로 나누어 보면 다음과 같다.

주체 ACI	보증서 검증수단	사용료 부과-ID	감사 실체-ID	보증서 사용 가능 횟수(주체)

<<주체 접근 제어 보증서 정보 내용>>

상기에서 주체에 지정된 정보를 보였다. 이는 주체 ACI, 다른 주체가 이 ACI 사용 금지를 위해, 접근 제어 보증서 결합을 검증하는 수단, 접근에 사용료 청구용 식별자, 회계 또는 감사 목적을 위한 객체의 식별자, 특정 주체가 접근 제어 보증서를 사용할 수 있는 횟수 등으로 구성된다.

객체 ACI	다른 객체에 사용 금지를 위한 보증서 검증 방법	보증서 사용 가능 횟수(주체)

<<객체 접근 제어 보증서 정보 내용>>

상기에서 객체에 지정된 정보를 보였다.

이는 객체 ACI, 다른 객체가 이 ACI사용 금지를 위해, 접근 제어 보증서 결합을 검증하는 수단, 특정 주체가 접근 제어 보증서를 사용할 수 있는 횟수 등이다.

접근 요구 ACI	보증서 검증수단(1)	보증서 검증수단(2)	보증서 사용 가능 횟수(주체)

<<접근 요구의 접근 제어 보증서 정보 내용>>

상기에서 접근-요구에 지정된 정보를 보였다. 이는 접근-요구 ACI, 이 ACI가 다른 접근-요구에 사용됨을 방지하기 위해, 접근-요구에 보증서의 결합을 검증하는 수단(1)과 접근-요구의 전진(Forwarding)시 한 개 이상의 접근-요구에 보증서 결합을 검증하는 수단(2), 특정 객체가 접근 제어 보증서를 사용할 수 있는 횟수 등이다.

2) 접근 제어 토큰(Access Control Token)

ACI 보호의 또 다른 일반적인 수단은 보안 토큰에 ACI를 포함 시키는 것이다. 보안 토큰은 접근 제어 당국이 봉인 또는 서명 하는 보안 보증서 생성과는 다르게 주체가 토큰을 만들고, 이를 보호하기 위한 암호 서비스를 한다. 접근 제어의 경우에, 보안 토큰은 접근-요구-결합 ACI와 특히 관계가 많다. 접근 제어 보증서는 여러 접근-요구에 사용을 위해서 보안 영역 내의 당국자가 생성한다. 하지만, 주체가 특정 접근-요구에 접근 제어 보증서를 결합 시키기 위해 보안 토큰을 만들 수 있다. 보안 토큰은 여러 가지 유형의 정보를 가진다. 이는 ITU-T Rec. X.800/ ISO/IEC 10181-1에 설명되어 있다.

4. 접근 제어 모듈

그림6)에서 접근 제어 모듈의 전체적인 구성을 보였다. 실 시스템에서 접근 제어는 여러 가지 접근 제어 모듈에 의해 이루어진다. 이 모듈은 특정 메카니즘에 독립적이다. 접근 제어 모듈은 크게 관리 모듈과 운용 모듈로 나눈다. 관리 접근 제어 모듈은 요소에 ACI결합, ACI의 수정 및 제거 행위를 지원한다. 그리고 운영 접근 제어 모듈은 ADF에 가용한 ADI를 만들고, 접근 제어 기능 실행을 지원한다. 서로 다른 실 시스템 또는 보안 영역에서 각각 다른 ACI표현을 사용할 때, 추가적인 접근 제어 모듈이 그들 사이에 ACI표현 사상을 지원해야 한다.

1) 관리 관련 접근 제어 모듈

접근 제어 정책 및 ACI의 표현의 설정 그리고 요소에 ACI의 할당은 여기에서 다루지 않는다. 여기에서는 ACI의 변경 및 제거, 접근 제어 구성 요소 사용의 가부 결정 모듈 및 한 요소의 ACI를 검색 지원 모듈 들이다. 이들을 정리 하면 다음과 같다.

ACI 설치 모듈로 요소에 초기 ACI를 결합 기능을 한다. 예를 들면, 주체가 사용할 능력, 주체 및 객체가 사용할 보안 레이블, 객체를 위한 ACLs의 결합들이다.

ACI 변경 모듈이다. 이는 요소에 결합된 ACI에 삭제와 추가와 같은 수정을 행하는 모듈이다. ACI제거 모듈은 ACI가 그 요소에 관계 하지 않도록 그 요소에 결합된 ACI사용을 제거한다. 이는 ACI에 관련된 어떤 ADI를 제거하는 ACI변경과는 다르다.

ACI 검색 모듈이다. 이는 주어진 요소에 결합된 지정된 ACI를 나열한다.

접근 제어 구성요소 사용 금지 모듈이다. 이는 접근 제어 기능 구성요소 사용을 금지한다. AEF 구성 요소 경우, 이 설비가 AEF를 통한 모든 접근을 금지 한다.

사용 금지 해제 모듈이다. 이는 접근 제어 기능 구성 요소가 재 가동하게 한다.

2) 운영 관련 접근 제어 모듈

접근 제어 프레임워크에서 5개의 모듈로 설명하고 있다. 이는 접근 제어 수행에 있어서 모든 단계를 요구하지 않지만 다음과 같은 절차에 따라 시행 된다.

첫째, ITSA(Identify Trusted Security Authorities) 모듈의 실행이다. 이는 최초에 접근을 요구한 주체가 요구 행위에 포함된 요소에 대해 SDAs를 결정한다. 이 모듈의 실행 결과는 접근-요구 행위에 사용할 안전한 상호 동작 정책(Secure interaction policy) 설정이다.

둘째, AGA(Acquire & Generate ACI) 모듈 실행이다. 이는 요소들에게 ACI를 결합 작업을 한다.

셋째, VBADA(Verify Bound ACI and Derive ACI) 모듈 실행이다. 이는 ADF에 ADI를 가용하게 만드는 기능을 한다.

넷째, GCI(Get Contextual Information) 모듈 실행이다. 이는 안전한 상호 작용 정책에 따라 문맥 정보를 얻는 기능을 한다.

다섯째, DA(Decide Access) 모듈 실행이다. 이는 접근 제어 결정을 행하는 기능을 한다.

이러한 기본 모듈에 다음과 같은 모듈들이 보안 정책에 따른 기밀성과 무결성을 보장하기 위해서 ACI 보호 모듈로 사용된다.

첫째, AIBA(Acquire initiator-bound ACI) 모듈이다. 이는 접근-요구 전에, 주체-결합 ACI가 포함된 접근 제어 보증서 또는 접근 제어 토큰을 얻는 기능을 한다. 이는 주체나 ADF가 호출한다. 호출시 필요한 입력은 인증된 주체 신분(ISO/IEC 10181-2, X.811에 정의된 검증 설비로부터 얻어진다), 주체-결합 ACI 선택 기준, 유효 기간, 객체 또는 객체 그룹의 신분, 안전한 상호작용 정책 등이다. 모듈의 출력은 이 설비 수행의 실패 유무를 나타내는 상태 정보, 주체-결합 ACI이거나, 주체-결합 ACI를 포함한 접근 제어 보증서 또는 접근 제어 토큰이다.

둘째, ATBA(Acquire Target-Bound ACI) 모듈이다. 이는 객체-결합 ACI를 생성한다. 이는 ADF가 호출한다. 호출시 가능한 입력은 객체 신분, 객체-결합 ACI 선택 기준, 유효 기간, 안전한 상호작용 정책 등이다. 가능한 출력은 이 설비 수행의 실패 유무를 나타내는 상태 정보, 객체-결합 ACI이다.

셋째, AARBA(Acquire access request-bound

ACI) 모듈이다. 이는 접근 제어 결정을 위해서 접근-요구에 주체-결합 ACI, 접근-요구 ACI, 오퍼랜드-결합 ACI등을 결합시키는 기능을 한다. 이는 주체가 호출한다. 호출시 가능한 입력은 주체-결합 ACI(또는 주체-결합 ACI 또는 상주 ADI를 포함한 접근 제어 보증서), 오퍼랜드-결합 ACI, 객체 신분, 오퍼레이션과 오퍼랜드, 유효 기간, 안전한 상호작용 정책 등이다. 이 모듈의 출력은 이 모듈 수행 실패 유무를 나타내는 상태 정보, 접근-요구-결합 ACI, 접근 제어 토큰, 접근 제어 보증서(주체에게 SDA가 생성), 상주 ADI 등이다.

넷째, VBADA(Verify Bound ACI and Derive ADI) 모듈이다. 이는 결합된 ACI 타당성을 검증하고 이로부터 ADI 유도 기능을 한다. ADI가 ADF에 미리 저장되어 있는 경우, 미리 저장된 ADI를 검색하여 대체 기능도 한다. ADF가 이 모듈을 호출한다. 호출시 가능한 주체, 객체, 접근-요구 또는 오퍼랜드 각각에 결합된 ACI, 접근 제어 토큰, 접근 제어 보증서, 오퍼레이션 및 오퍼랜드, 유효기간, 안전한 상호작용 정책 등이다. 가능한 출력은 이 모듈 실행의 성공 유무를 나타내는 상태 정보, 오퍼레이션 및 오퍼랜드, 각각 요소(주체, 객체, 접근-요구 또는 오퍼랜드)의 ADI등이다.

다섯째, GCI(Get Contextual Information) 모듈이다. 이는 접근 제어 결정에 필요한 문맥 정보를 얻는 기능을 한다. 이는 ADF 또는 주체가 호출한다. 호출시 가능한 입력은 오퍼레이션 및 오퍼랜드, 요구된 문맥 정보, 안전한 상호작용 정책 등이다. 가능한 출력은 이 설비 수행의 실패 유무를 나타내는 상태 정보, 문맥 정보이다.

여섯째, DA(Decide access) 모듈이다. 이 모듈은 접근 허용 유무를 결정하는 기능을 한다. 이는 ADF가 호출한다. 호출시 가능한 입력은 오퍼레이션과 오퍼랜드, 주체 ADI, 오퍼랜드 ADI, 객체 ADI, 문맥 정보, 상주 ADI, 안전한 상호 작용 정책 정보 등이다. 이 모듈의 출력은 접근 제어 결정 내용, 결정 내용의 유효 기간, 인가된 접근-요구의 순서, 상주ADI등이다.

VI. 접근 제어 메카니즘

1. 접근 제어 메카니즘의 분류

접근 제어 메카니즘은 접근 제어 스킴(Access Control Scheme)과 그 스킴의 ADF에 ADI 제공을 지원하는 메카니즘으로 구성된다. 이 장에서는 접근 제어 스킴을 분류하고, 접근 결정을 지원하기 위한 접근 제어 모듈을 중심으로 일반적인 메카니즘을 설명한다. 이들은 여러 측면에서 장·단점과 함께 통일된 프레임워크에 적용된다. 전형적인 접근 제어 스킴은 다음과 같이 분류된다.

첫째, 능력(Capability) 스킴이다. 이는 주체-결합 ACI가 (객체 신분, 오퍼레이션들) 쌍를 갖고, 객체-결합 ACI가 객체 신분을 가지고 접근 제어가 이루어지는 스킴이다.

둘째, 레이블 기반(Label-based) 스킴이다. 이는 주체-결합 ACI가 보안 등급(Clearance)이란 보안 레이블을 갖고, 객체-결합 ACI가 보안 등급 분류표(Classfication)를 가지고 이들을 비교하여 접근제어가 이루어지는 스킴이다.

셋째, 접근 제어 리스트(Access Control List) 스킴이다. 이는 주체-결합 ACI가 주체 신분, 객체-결합 ACI가 (주체 신분, 오퍼레이션들)쌍을 가지고 접근 제어가 이루어지는 스킴이다.

넷째, 문맥 기반 접근 제어 스킴(Context-based access scheme)이다 이는 규칙에 관련된 문맥 정보(V장 참조)가 다른 접근 제어 스킴들에 결합 된다. 이러한 문맥 정보를 활용하여 상기의 기본 접근 메카니즘을 보완하여 접근

제어가 이루어지도록 한 스킴이다. 문맥 정보는 주체-결합 ACI, 접근-요구-결합 ACI, 또는 객체-결합 ACI 등의 일부가 될 수 있거나, 다른 ACI와는 독립적으로 ADF에 이 정보가 활용될 수 있다.

2. ACL 스킴

이 스킴 예는 그림 7)과 같다.

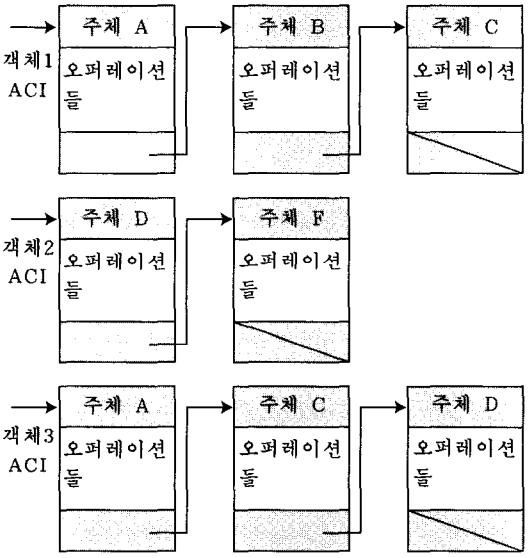


그림 7) ACL 스킴 예

1) 기본 특징

첫째, 접근 제어가 객체-결합 ACI에 (주체 이름, 오퍼레이션 이름)쌍 리스트, 주체-결합 ACI는 개인/그룹/직무 식별자 표기로 이루어진다. 둘째, 접근 제어 범주가 매우 작았을 때, 그리고 주체 또는 발신 그룹 수가 적을 경우, 객체나 객체 그룹의 접근을 폐지할 경우, 접근 제어 관리가 주체 단위 중심 보다는 객체 단위 중심 관리 등일 때 편리하다. 셋째, 주체 또는 주체 그룹이 빈번하게 변경될 경우는 불편하고, 객체 측의 변화에는 편리하다.

2) ACI

주체-결합 ACI는 개인, 그룹 또는 직무의 식별자로 이루어지고, 객체-결합 ACI는 엔트리의 집합으로 이루어지고, 각 엔트리는 2개의 항목으로 이루어진다. 첫번째 항목은 주체 이름으로 오퍼레이션 적용시 주체 식별 기능을 한다. 이는 직무 또는 그룹 구성원과 같은 더 일반적인 주체 ACI로 표현될 수도 있다. 두 번째 항목은 오퍼레이션 이름으로 첫번째 항목의 주체에게 적용될 오퍼레이션 이름 또는 오퍼레이션 그룹 이름이 표기된다.

3) 지원 메카니즘

DA(Decide Access) 접근 제어 모듈에서 요구한 ADI를 유도하기 위해, 2개의 메카니즘이 주체-결합 ACI를 얻는대 사용된다. 첫째는 인증 정보를 사용한 것이다. 이는 접근 제어가 개인의 신분을 기반으로 이루어진다면, 이 신분이 인증에서 검증된다. 만약 접근 제어가 그룹 또는 직무를 기반으로 이루어진다면, 인증된 신분은 타당한 그룹이나, 직무를 얻기 위해서 사용된 AIBA(Acquire Initiator-Bound ACI) 모듈의 매개변수가 된다. 두 번째 메카니즘은 접근 제어 보증서 또는 토큰을 사용하는 경우로 주체가 AIBA접근 제어 모듈을 사용하여 접근 제어 보증서 및 토큰을 얻는다. 이 보증서 및 토큰은 주체가 GARBA(Generate Access Request-Bound ACI) 접근 제어 모듈을 사용하여 접근-요구(Access Request)에 결합된다. 마지막으로 ADF가 VBADA(Verify Bound ACI & Derive ADI) 접근 제어 모듈을 사용하여 검증한다. 접근 제어 보증서 내의 보증 기관의 수용 허용 유무 및 접근 제어 토큰 내의 주체는 VBADA접근 제어 모듈을 통해서 결정 된다.

주체 ADI(개인, 그룹 또는 직무의 식별자), 접근-요구 및 객체 ADI(접근-요구 이름)는 ADF 접근 제어 모듈의 매개 변수가 된다. 적당한 사상 알고리즘을 사용해서, 주체 ADI와 접근-요구로부터 얻은 오퍼레이션을 ACL의 각 엔트리(주체, 오퍼레이션들)와 비교한다. 접근 제어 결정은 이러한 비교를 통해서 일치 여부로 이루어진다.

2. 능력(Capability) 스킴

능력 스킴의 예를 그림 8)에서 보여 주고 있다.

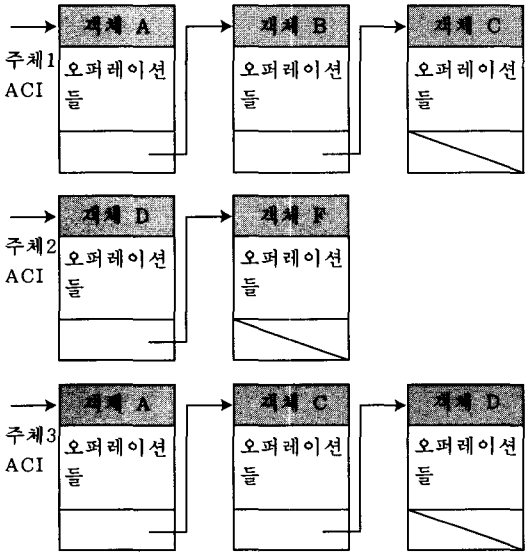


그림 8) 능력 스킴 예

1) 기본 특징

이는 주체 결합-ACI에 (객체 이름, 오퍼레이션) 쌍 리스트(능력)를 갖고, 객체 결합-ACI에 객체 이름을 가지고 접근 제어가 이루어진다. 이는 객체 수가 적을 때 편리하고, 주체 SDA가 주체의 접근 권리 제거 관리를 할 경우 편리하다. 하지만, 주체에게 허용된 능력들 각각이 식별 되지 않으면, 객체에서 객체의 접근 제거는 불편하다. 따라서 이는 접근 제어 관리가 주체에 의해 이루어질 때 편리하다. 또한 능력은 적은 객체를 접근하는 많은 사용자 또는 그룹일 경우와 객체와 사용자가 다른 보안 영역일 경우 편리하다. 접근 제어를 위해서 암호를 사용한 경우는 능력을 사용하는 경우 비슷한 측면이 있다. 암호의 기본 특징은 접근 제어가 주체와 객체간에 공용하는 ACI를 기반으로 한다. 또한 접근 제어는 전송에서처럼 주체와 객체간에 유지되는 ACI의 기밀성에 좌우된다. 이러한 기밀성을 유지 또한 어려울 수 있다. 암호의 변경 역시 여러 주체가 동일한 암호를 사용한다면 어렵다.

2) ACI

주체 ACI는 능력들의 집합으로 이루어진다. 능력은 객체 또는 객체 집합 이름과 그 객체에 허용된 오퍼레이션 리스트로 정의된다. 능력은 SDA관리자에 의해 봉인 되거나, 서명 된 접근 제어 보증서로 운반될 수 있다. 주체-결합 ACI는 엔트리 집합이다. 각 엔트리는 SDA에서 인가한 신분과 이에 허용된 오퍼레이션들로 구성된다.

3) 지원 메카니즘

주체는 AIA 접근 제어 모듈을 사용하여 접근 제어 보증서 또는 토큰을 얻는다. 그리고 이는 GARBA(Generate Access Request-Bound ACI)를 사용하여, 주체의 접근-요구에 결합된다. 마지막으로 VADA를 사용하여 ADF가 검증한다. 주체 ADI(능력 내용들), 오퍼레이션 이름, 객체 ADI는 DA의 매개변수가 된다. 객체 ADI가 능력 내의 객체 이름들 중 하나와

일치 하는지를 검사하고, 오퍼레이션이 능력 내의 오퍼레이션 중 하나와 일치 하는지를 검사한다. 이 두 가지 검사가 성공할 경우 접근은 허용된다. DA는 다음 사항에 대해서 접근을 거절한다. 첫째, 표현된 능력이 정당한 능력으로 인식 되지 않거나, 객체에 대한 접근이 SDA가 인정하지 않는 오퍼레이션을 가질 경우, 마지막으로 접근-요구로부터 유도된 오퍼레이션이 능력 내 오퍼레이션과 일치 하지 않을 경우이다.

4. 레이블(Label) 기반 스킴

보안 레이블 스킴의 예는 그림 9)와 같다.

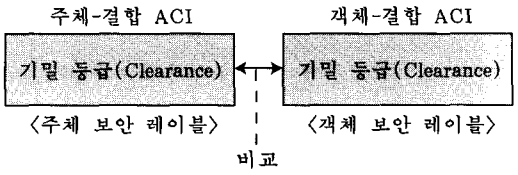


그림 9) 보안 레이블 스킴

1) 기본 특징

이 스킴은 주체가 접근 요구를 할 경우 주체의 기밀 등급(Clearance)을 객체에게 알리기 위해서 모든 접근 요구에 보안 레이블을 붙여서 요구한다. 또한 모든 객체는 자신의 기밀 등급(Classification)을 알리기 위해 보안 레이블을 가지고 있다. 접근이 요구될 경우 주체와 객체의 보안 레이블을 비교하여 접근을 결정한다.

이는 주체가 여러 객체를 접근 하는 경우가 빈번할 때 그리고 접근 범주가 임의적일 때 편리하다. 그리고 이는 주어진 보안 정책(예, 기밀성 또는 무결성)에서 정보의 흐름을 제어하는대 유용하다. 보안 레이블은 또한 보안 영역간에 접근 제어 제공에도 편리하다. 마지막으로 허용된 오퍼레이션이 주체 또는 객체-결합 ACI에 명확하게 포함되지 않고, 보안 정책의 일부로 정의될 수 있다. 주지할 사항은 레이블이 단순한 구조일 필요는 없다.

2) ACI

주체 및 객체-결합 ACI 각각은 보안 레이블이다. 이의 표현은 보통 이들을 비교하기 쉽게 표기되지만 꼭 동일한 표현일 필요는 없다. 보안 정보 표현의 번역은 ITU-T Rec X.810에 설명되어 있다. 또한 접근-요구의 오퍼랜드에도 보안 레이블을 결합 시킨다. 레이블 된 오퍼랜드는 레이블 된 데이터의 특별한 경우이다. 레이블 된 데이터는 2가지 보안 속성이 지켜져야 한다. 이는 데이터에 레이블 결합 시 무결성 보장과, 주체가 레이블 된 데이터 생성 권리를 가져야 한다.

주어진 정책에 따라 보안 레이블화는 한 보안 영역 내, 또는 보안 영역간 데이터에 일반적인 접근 제어 제공에 사용된다. 레이블 된 데이터의 예는 문서, 전문, 비 연결 데이터 단위, 전송 중인 파일이 될 수 있다.

3) 지원 메카니즘

DA가 사용할 주체 및 객체-결합 ACI를 얻는 방법에는 4가지 메카니즘이 있다. 첫째, 접근 제어 보증서 또는 토큰을 사용하는 방법이다. 둘째, ADF가 인증된 주체의 신분을 얻은 다음, 주체의 기밀 등급(Clearance)을 얻기 위해서 이를 사용하는 방법이다. 셋째, 레이블 된 채널을 사용하는 방법이다. 이는 주체의 기밀 등급 또는 데이터의 레이블이 접근-요구를 운반하는 체널-레이블에 포함 될 수 있다. 특정 채널에 레이블을 결합 시킬 때의 무결성은 무결성 서비스 사용을 통해서 보장 된다. 채널

에 레이블이 정당하게 할당 되었다는 보장은 이를 검증하는 통신 서비스 제공자를 신뢰함으로써 이루어 진다. 비슷하게 이러한 보장은 객체 측에서 채널이 설정되기 전에 채널 사용 자격이 있는지를 검사하여 이루어질 수도 있다. 넷째, 레이블 된 데이터를 사용하는 방법이다. 주체의 기밀 등급 레이블이 접근-요구의 오퍼랜드 레이블에 포함될 수 있다. 데이터에 레이블 결합의 무결성은 근본적으로 채널의 무결성 또는 SDA가 만든 데이터 및 보안 레이블에 서명 또는 무결성 검사 코드 사용을 통해서 제공된다.

보안 레이블이 객체를 보호하기 위해서 객체 ACI로 사용될 수 있다. 이는 접근 규칙이 주어진 주체와 객체의 보안 레이블에 허용된 접근 오퍼레이션들을 정의하여 이루어진다. 만약, 보안 정책에서 보안 레이블 내의 ACI를 객체 ACI로 사용하도록 규정되면, 그 객체를 중심으로 데이터 흐름 제어할 수 있다. 결국 객체 내외로 잘못 흐르는 데이터를 동일 보안 정책을 적용하여 보안 영역에서 분석할 수 있다.

또한, 객체가 다른 객체들 내에 생성될 수 있다. 이의 예는 OSI N 엔터티, 디렉토리 서비스 엔트리, 파일 저장소의 파일, 데이터베이스 엔트리 등이다.

4) 객체처럼 레이블 된 채널

채널 생성자(SDA)가 채널에 보안 레이블을 할당한다. 할당된 채널을 사용할 경우, DA모듈에 주체-ACI와 채널에 할당된 보안 레이블이 동시에 입력된다. 이때, 채널이 객체처럼 다루어진다. 즉, 채널 내로 운반된 데이터 레이블은 채널의 레이블과 일치 해야 한다. 채널에 할당된 레이블은 또한 채널의 루트(Route) 제어에 사용될 수 있다. OSI에서 N 계층 엔터티와 릴레이 시스템은 N-1계층 연결과 비연결 데이터 단위를 접근 한다. 따라서 N 계층 엔터티는 N-1계층 엔터티 연결과 비연결 데이터 단위에 대한 접근 규칙을 만족해야 한다. 레이블된 채널의 예는 결합(Association), OSI N계층 연결, 프로세스간 채널 등이다.

5. 문맥 기반 스킴(Context based scheme)

1) 기본 특징

ADF가 보안 정책 또는 ADI를 해석하기 위해서 문맥 정보(5장 참조)를 요구한다. 이 스킴의 접근 제어는 주체 및 객체-결합 ACI로 이루어지거나, ADF로부터 얻어진 정보와는 독립적으로 이루어 진다. 이는 모든 주체에 적용한 규칙을 시행하는대 편리하다.

2) ACI

이는 문맥 제어 리스트와 문맥 정보로 구성된다. 전자는 엔트리의 집합으로 구성된다. 각 엔트리는 오퍼레이션의 적용 조건(예, 시간, 경로, 위치)을 진(True),위(False)로 표기한 문맥 한정자(Context qualifier) 항목과 이에 인가된 오퍼레이션을 표기한 오퍼레이션 한정자(Operation qualifier) 항목으로 구성된다. 후자는 접근-요구가 이루어질 때, 문맥으로부터 얻어진다. 문맥은 ADF가 접근-요구를 받았을 당시 환경에 좌우된다. 문맥 정보는 계층 서비스 인터페이스에서 또는 지역 관리 인터페이스 등에서 얻어진다.

3) 지원 메카니즘

ADF는 GCI(Get Contextual Information) 모듈로 문맥 정보를 얻는다. DA 모듈에 얻어

진 문맥 정보와 접근-요구가 입력 된다. DA 모듈은 이로부터 요구된 오퍼레이션을 유도한다. 그리고나서 접근 허용 유무를 결정하기 위해서 각각의 문맥 한정자와 오퍼레이션 한정자를 비교한다.

VII. 결언

정보 통신망을 대상으로 상용화 되어 유통되고 있는 대부분의 보안 시스템은 인증 서비스 중심 보안 체계를 갖추고 있다. 따라서 인증 이후에 파생될 수 있는 위협에 대한 안전 대책이 취약한 실정이다. 최근 들어 상용화를 목표로 개발되고 있는 보안 제품은 인증 및 접근 제어 서비스를 종합적으로 지원하도록 하고 있다. 본 고에서 분석한 X.812 접근 제어 프레임워크는 접근 제어 시스템 설계의 골격을 제공한다. 특히 정보 통신망의 다양성 때문에 하나의 접근 제어 스킴으로 표준 안을 권고하지 않고, 여러 스킴들을 수용하는 측면에서 표준 안이 정립되어 가고 있는 추세이다. 따라서 접근 제어 시스템은 매우 복잡한 형태를 띄고 있다. 이러한 환경에서 종합적인 보안 시스템을 개발할 경우 보다 심도 있게 접근 제어 기술이 고려되어야 할 것이다.

참 고 문 헌

[1] Warwick Ford, Computer Communications Security, Prentice-Hall, 1994, pp149-174

[2] Charles P, Pfleeger, Security in Computing, Prentice-Hall, 1989, pp212-221

[3] Morrie Gasser, Building a secure computer systems, Van Nostrand Reinhold Company, 1988,pp55-66

[4] Silvana Castano, Data Base Security, Addison-Wesley,1955,pp39-1375. Ravi S. Sandhu, Access Control : Principles and Practice ,IEEE Communications Magazine,1944, pp40-48

[6] ITU-T SG/7 & Working parties, Final text for recommendation X.812 Information Technology-Open systems interconnection Security framework for open systems : Access control framework, Geneva,26 June-7 July 1995.

[7] ITU-T Recommendation X.810, Information Technology-Open systems interconnection-Security framework for open systems : Overview, 95.11.

[8] ITU-T Recommendation X.811, Information Technology-Open systems interconnection-Security framework for open systems : Authentication framework, 95.04.

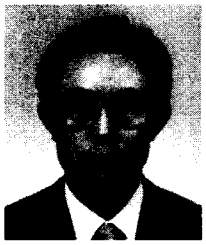
[9] 홍기웅,이철원, 컴퓨터 보안 모델의 분석 및 비교에 관한 연구, 전자통신 동향 분석, 1990.10. pp71-89

□ 著者紹介

조 인 준

1982년 2월 전남대학교 전자계산학과 졸업(석사)
1985년 2월 전남대학교 전자계산학과 대학원 졸업(석사)
1995년 2월 현재 아주대학교 컴퓨터 공학과(박사과정중)
1990년 12월 정보처리 기술사(전산 조직 응용)
1983년 9월 ~ 1994년 2월 한국전자통신 연구소(선임연구원)
1994년 3월 현재 배제대학교 컴퓨터 공학과(교수)

※ 주관심분야 : 전산 조직응용 및 정보 통신 Security



김 동 규

서울대학교 공과대학 졸업(학사)
서울대학교 자연과학대학원 졸업(석사)
미국 Kansas 주립대 대학원 졸업(Ph.D. 전산학 박사, 정보통신 전공)
미국 Kansas 주립대 전산학과 교수
1979. 3 - 현재 아주대학교 컴퓨터공학과 교수
저서 : 데이타 통신시스템, 회중당, 1986년
저서 : 컴퓨터 통신 네트워크, 상조사, 1988년
한국통신학회 상임이사, 한국통신정보보호학회 부회장

※ 주관심분야 : 컴퓨터 네트워크, 정보통신 프로토콜 엔지니어링,
정보통신 Security, 분산처리 시스템