通信情報保護學會誌
第4券 第1號, 1994. 3

분산 시스템을 위한 정형화된 보안 모델 분석

The Analysis of Formalized Security Models for Distributed Systems

서 재 현*, 김 태 연**, 노 봉 남***

요 약

분산 시스템 환경에서 정보 보안의 필요성이 크게 부각되고 있으며 응용영역에 있어서 보안 모델들의 정형화가 요구되고 있다. 본 논문에서는 분산 시스템 환경의 보안요구 사항을 파악하고 모델링을 위해서 접근 제어, 정보 흐름 제어, 무결성, 인증 프로토콜에 관한 정형화된 모델들을 기술하고 이를 비교 분석하였다.

1. 서 론

각 조직체에서는 컴퓨터에 저장된 정보의 중요성을 인식하여 왔고, 컴퓨터에 대한 우연한 혹은 고의적인 사용자 행위에 대한 취약성 역시 중요한 요소로서 인식하고 있다. 특히 다중 사용자 또는 네트워크의 발전으로 정보 보안의 필요성이 크게 부각되고 있다. 정보 보안의 주요한 관심 분야는 비밀성, 무결성, 가용성에 있다. 비밀성(secrecy)은 정보의 누출을 방지하고, 무결성(integrity)은 불법적인 정보의 변경을 금지하며, 가용성(availability)은 정보의 접근 거절과 관련된다.[1] 정부 기관이나 국방 조직의 보안정책은 불법적인 정보 유출을 막는 비밀성에 중점을 두고 있으나, 자료 처리를 주로 다루는 조직의 상업적 보안 정책은 비밀성보다는 불법적인 자료의 변경을 방지하는 것을 최우선 정책으로 하고 있다. 각 조직체의 일반적인 정보 보안 정책은 정보의 접근 권한을 허용하거나 허용할 수 없는 사용자의 행위를 정의하는 것이다. 보안 구조의 가장 중요한 구성 요소인 보안 정책은 조직체들이 중요한 정보를 분배, 보호하거나 관리하는 방법을 규정하는 법칙과 규칙들의 집합이다.

가장 널리 사용되고 있는 접근 제어 정책은 임의적 접근 제어와 강제적 접근 제어 방법을 이용한다. 임의적 접근 제어는 특정한 주체가 임의의 객체에 대한 접근을 제한하는 방법이며, 강제적 접근 제어 방법은 객체에 대한 보안 등급과 그 객체를 접근하는 주체의 인가등급을 기반으로 객체에 대한 주체의 접근을 제한하는 방법이다. 접근 제어 보안 정책은 임의적 접근 제어와 강제적 접근 제어 방법을 각각 독립적으로 사용하거나 두 방법을 혼합하여 사용할 수 있다. 대표적인 접근 제어 모델은 BLP 모델로 임의적 접근 제어와 강제적 접근 제어를 모두 사용하여 주체가 객체에 대한 접근을 제한하는 모델이다. 그러나 접근 제어는 객체에 접근을 제어하는 것으로 객체 내에 포함된 정보에 대한 규제는 고려하지 않는다.

* 정회원, 전남대학교 대학원 전산통계학과 박사과정
** 정회원, 광주예술전문대학 컴퓨터 그래픽 디자인학과 전임강사
*** 종신회원, 전남대학교 전산학과 부교수

정보 흐름 제어 정책은 객체 사이의 정보 전달을 제어하는 방법이다. 흐름 제어를 위한 대표적 모델인 격자 모델은 정보 흐름 정책과 정보 흐름에 적합한 채널에 대해서 기술하고 있다[2]. 또다른 유형의 보안 모델은 불법적 정보 유출보다는 불법적인 정보의 변경을 보호하기 위한 무결성 보안 모델이다. 무결성 보안 정책은 사용자의 고의적인 장난이나 실수에 의한 자료의 변경을 방지하는 것이 주 목적으로 대표적인 모델은 Biba 모델, Clark과 Wilson 모델 등이 있다. 마지막으로 인증 프로토콜 모델은 분산 시스템에서 송신자와 수신자에 동등한 권한을 부여하고 특정사건의 시간순서가 세션계층에 영향을 주지 않토록하는 모델이다.

본 논문에서는 분산 시스템 환경에서 보안 요구사항들을 파악하고 모델링을 위해, 널리 연구되어지고 있는 정형화된 모델들, 즉 접근제어 모델인 BLP 모델, 수취-부여 모델, 정보흐름 제어모델인 격자 모델, 무결성 모델인 Biba 모델과 Clark과 Wilson 모델, 인증 모델로 Sidhu 모델과 Varadharajan 모델을 분석하였다. 2장에서는 여러가지 보안 정책을 설명하였고, 3장에서는 보안 정책에 따르는 보안 모델을 기술하였으며, 4장에서는 보안 모델들을 비교 분석하였다. 마지막으로 5장에서는 결론 및 추후 연구 방향을 논하였다.

2. 보안 정책

접근 제어 정책은 컴퓨터에 저장된 정보를 사용자의 접근 여부와 수행 능력을 제어하는 것이다.[1] 보안 정책의 주요한 요소인 접근 제어를 위해 필요한 접근 제어 방법으로 임의적 접근 제어(discretionary access control)와 강제적 접근 제어(mandatory access control)가 있다. 임의적 접근 제어는 특정한 주체가 임의의 객체에 대한 접근을 제한하는 방법이다. 객체에 대한 주체의 접근 권리는 접근 행렬에 의해 표현되는데 행은 주체를 열은 객체를 나타낸다.

이들의 근본적인 문제점은 객체를 다른 객체로 복사하는데 대한 제약 조건을 제공하지 못한다는 것이다. 예를 들면, 갑, 을, 병이 사용자들일때, 갑이 갖는 *A*라는 화일을 을은 읽게하고 병은 읽지 못하게 하려고 한다. 그래서 갑은 을에게만 화일 *A*를 읽을 권리를 부여했다. 그러나 을은 새로운 화일 *AB*를 만들어 화일 *A*의 내용을 *AB*에 복사하여 갑의 의도를 전복시킬 수 있다. 그러면 이제 을이 *AB*화일의 소유자가 되고 병에게 *AB*화일을 읽을 권리를 부여한다면, 결국 병은 본래의 의도와는 달리 화일 *A*를 읽을 수 있게 된다. 이러한 제어는 어떤 객체에 대한 접근 허가를 가진 주체가 그 허가를 다른 주체에 넘겨 줄 수 있다는 의미에서 임의적이다. 또 다른 문제점은 트로이목마에 취약하여 임의적 접근 제어만으로는 정보 흐름을 제어하기에 부적절하다.

강제적 접근 제어는 객체에 대한 보안 등급과 그 객체를 접근하는 주체의 인가 등급을 기반으로 객체에 대한 접근을 제한하는 방법이다. 임의적 접근 제어와는 달리 강제적 접근 제어는 새로운 객체가 생성될 때 특정한 보안 등급 부여 메카니즘에 의하여 객체에 보안 등급이 부여되어야 한다. 강제적 제어 정책은 모든 주체와 객체에 대하여 일관성이 있다. 즉 한 주체가 어느 한 객체를 접근하지 못하면 이때에 그 주체는 그 객체와 동일한 보안등급을 갖는 모든 객체에 접근이 허락되지 않는다. 접근 제어 정책에서는 임의적 접근 제어와 강제적 접근 제어 방법을 각각 사용하거나 두 방법을 혼합하여 사용한다. 대표적인 접근 제어 모델은 BLP모델로 임의적 접근 제어와 강제적 접근제어를 모두 사용하여 주체가 객체에 대한 접근을 제한하는 모델이다. 접근제어를 이용하는 모델에는 High-water Mark모델, BLP모델, UCLA 자료 구조 모델 등이 있다.[8]

접근 제어는 주체의 객체에 대한 접근을 제한하는 것으로 주체가 객체 내에 포함된 정보에 대해서 제한하지는 않는다. 정보 유출에 관련되는 많은 문제는 잘못된 접근 제어 때문이 아니고 정보 흐름에 대한 정책의 부족으로부터 발생하게 된다.

정보를 포함하는 객체와는 무관하게 흐름 제어는 정보의 배포(dissemination)의 권한에 관련되어지며 정보가 흐를 수 있는 정당한 채널(channel)을 기술한다. 즉, 정보흐름 정책은 하나의 보안 클래스에서 다른 보안 클래스로의 정보 흐름과 관계가 있다. 여기서 보안 클래스는 보안등급과 범주를 포함하는 용어이다. 정보 흐름은 객체에 대한 보안 클래스를 할당하여서 제어될 수 있는데 객체 X에서 객체 Y로의 정보 흐름이 있을 때는 X의 보안 클래스로부터 Y의 보안 클래스로 정보 흐름을 수반한다. 정보 흐름 제어는 객체들 사이에 정보를 전달하는 실제적인 동작에 촛점을 맞추고 있다.[1,4]

세번째 정책은 불법적 정보 유출보다는 불법적인 정보의 변경을 방지하기 위한 무결성 보안 정책이다. 무결성 보안 정책은 사용자의 고의적인 장난이나 실수에 의한 자료의 변경을 방지하는 것이 주 목적으로 대표적인 모델은 Biba, Lipner, Clark과 Wilson 모델 등이 있다. Biba 모델의 정책은 주체는 자신의 무결성 등급보다 크거나 같은 객체를 읽을 수 있고, 무결성 등급보다 같거나 낮은 객체에 대한 변경을 허용한다. 이와 같은 Biba 모델의 기본 개념은 낮은 무결성 정보로부터 높은 무결성 정보의 오염을 방지하여 정보의 불법 변경을 허락하지 않는다.

Biba 모델과 BLP 모델을 혼합한 새로운 모델로서, Lipner는 비밀성과 무결성을 보장하는 또 다른 모델을 제안하였다.[7] Lipner는 전통적인 자료 처리 응용에 적용할 수 있도록 세개의 무결성 등급과 두개의 비밀성 등급으로 구성된 복합적인 격자 구조를 만들었다. 이러한 무결성 등급과 비밀성 등급을 기반으로 비밀성과 무결성을 동시에 유지시키는 보안 모델이다. Clark과 Wilson 모델의 보안 정책은 사용자의 고의적인 장난이나 실수에 의한 자료의 변경을 방지하기 위해 잘 정의된 트랜잭션(well-formed transaction)과 사용자들 사이의 임무의 분리(separation of duty)의 기법을 사용한다.[7,10]

네번째 정책인 인증은 사용자 인증, 메세지인증, 개체인증, 프로토콜인증이 있으며 인증 프로토콜 모델은 Sidhu 모델, Varadharajan 모델 등이 있다. 프로토콜은 방향성 그래프로 표현된 모든 입력을 받아들여야 하는 완결성, 프로토콜이 다음 단계로 전송이 불가능하거나 시스템 상태가 무한 상태에 빠지지 않는 교착상태 회피, 시스템 상태들 사이에 반복 루틴이 형성되지 않는 기아상태(livelock)예방, 프로토콜이 초기상태에서 시작하여 최종 상태로 끝나야 하는 종결성, 각 채널을 통해 전송되는 메세지의 최대수는 항상 채널용량을 초과하지 않는 제한성, 정상적인 조건하에서 실행될 수 없는 상호작용이 제약조건을 만족해야 한다.

3. 보안 모델

3.1 접근 제어 모델

정형화된 접근제어 모델은 자료나 정보에 사용자의 접근을 제어하는 모델이며 이 모델에서 사용되는 두가지 구성요소는 능동적인 주체(사용자나 프로그램)와 수동적인 객체(화일이나 프로그램)로 구성된다. 보안 정책은 하나의 특별한 주체가 임의의 객체에 접근에 관한 규칙들의 집합이다. 본 절에서는 가장 대표적인 접근제어 모델인 BLP 모델과 수취 - 부여 모델을 살펴본다.

3.1.1. BLP 모델

Bell과 LaPadula에 의해 개발되어 정부 기관이나 국방조직에서 가장 널리 사용되어지는 BLP 모델의 보안 정책은 불법적인 정보 유출을 보호하는데 있다.[1,2,3,4] BLP 모델은 주체와 객체에 각각 보안 등급을 부여하여 허가되지 않는 사용자로부터 객체에 대한 접근을 금지한다. 이 모델은 임의적 접근 제어와 강제적 접근 제어의 두단계 과정을 통하여 접근을 제어한다.

정형화된 BLP 모델은 보안 정책을 기반으로 능동적인 주체 집합S(사용자나 프로그램)에 의해

수동적인 객체 집합 0(화일이나 프로그램)의 접근 제어 방법이다. 객체에 대한 주체의 접근을 접근 모드에 의해 표현된다. 접근 모드는 다음과 같다. e(읽기 금지, 변경 금지), r(읽기 가능, 변경 금지), a(읽기 금지, 변경 가능), w(읽기 가능, 변경 가능)등이 있다.

BLP모델에서, 시스템 상태 V는 $V=(b,M,f)$로 표현된다. b는 현재의 접근 집합으로 주체, 객체와 접근 모드의 부분 집합으로 표현되고, M은 접근 허가 행렬을 나타내며 f는 주체나 객체에 보안등급을 부여하는 함수이다. R은 시스템 상태 V의 요소들을 변화 시키는 요구들의 집합이며, 상태 변환 함수 $T:R\times V\rightarrow V$는 하나의 상태에서 또다른 상태로 시스템을 변화 시키는 함수이다. BLP 모델은 유한상태 기계로 시스템 상태를 변화시키는 요구 R에 따라 변환 함수 T에 의해 하나의 상태에서 다음 상태로 전환된다. X,Y,Z가 T에서 R,D,V로 각각 대응하는 함수의 집합이고 W가 $R\times D\times V\times V$의 부분 집합일때 시스템의 상태 변이 관계는 다음과 같이 정의된다.

▨ 정 의 상태변이

시스템(R,D,W,Z_0)은 $(X,Y,Z)\in(R,D,W,Z_0)$가 되는 X Y Z의 부분 집합이다.

iff

$\leftrightarrow$ 각 $t\in T$에 대하여 $(X_t,Y_t,Z_t,Z_{t-1})\in W$

BLP모델의 보안 특성은 다음과 같이 두가지 규칙들로 정의된다.

(1) 단순 성질(simple property)

주체가 객체를 읽기 위해서는 주체의 보안등급이 객체의 보안등급을 지배해야 한다. 즉 모든 $(S,O,x)\in b$에 대하여 $L(S)\leq L(O)$이어야 한다.

(2) *-성질(star property)

주체가 객체를 쓰기 위해서는 객체의 보안등급이 주체의 보안등급을 지배해야 한다. 즉 모든$(S,O,x)\in b$에 대하여 $L(S)\geq L(O)$이어야 한다.

BLP모델은 접근 제어를 위해 두 단계의 과정을 거친다. 첫단계는 임의적 보안 성질 즉, 접근 허가 행렬에 저장되어 있는 주체와 객체에 대한 접근 모드와 요청된 접근모드가 일치하는가를 적용하는 단계이다. 접근 허가 행렬은 사용자에 의해 내용이 변경될 수 있다. 두번째 단계는 사용자에 의해 제어권이 없는 강제적 접근 제어로 주체와 객체에 부여된 보안 등급에 단순성질과 *-성질을 적용하는 단계이다. 이와같이 BLP모델은 임의적 접근 제어와 강제적 접근 제어가 모두 사용된다.

이 모델의 기본적인 보안은 현재 상태에서 다음 상태로의 변경이 보안 위반의 원인이 되지 않을때 보안이 보장될 수 있다. 만약 시스템의 상태가 변경되어질때 임의적 보안성질, 단순성질과 *-성질이 모두 만족되어 진다면 시스템은 보안이 유지되어진다. 이 모델은 하나의 상태로부터 다른 상태로의 보안 유지는 전체 시스템 보안을 보장한다는 것이 귀납적 해결 방법으로 제시되었다.

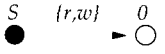
이 모델은 최초의 수학적인 모델로 가장 널리 사용되어 왔으나, 사용자의 인가 등급 융통성에 문제점이 있다. 예를 들면 객체의 보안 등급보다 인가 등급이 높은 주체가 그 객체를 읽을 수 있으나 쓸 수 없다. 그러나 주체가 자신의 인가등급을 객체의 보안 등급으로 낮추어 다시 쓰기 연산을 수행해야 한다. 또한 강제적 접근 제어는 트로이 목마 문제를 완전히 해결하지는 못했다. 인가 등급이 높은 주체가 시스템 내의 기억장치를 확보했을때 인가 등급이 낮은 주체의 가용 기억 용량을 알아보므로써 인가 등급이 높은 주체의 사용 공간을 알아볼 수 있다. 즉, 인가등급이 낮은 주체는 아주 큰 용량을 시스템에 요구하여 이러한 요구를 시스템의 승인 여부에 따라 인가 등급이 낮은 주체는 사용 가능한 기억공간을 알아 낼 수 있다. 이러한 종류에 간접적인 통신 방법인 비밀(covert) 채널의 문제점이 남아 있다.

3.1.2 수취-부여(Take-Grant) 모델

BLP모델은 임의적 접근 제어와 강제적 접근 제어를 복합적으로 사용하지만 강제적 접근 제어 중점을 두고 있다. 임의적 접근 제어를 위해 접근

제어 행렬이 사용되어진다. 접근 제어 행렬은 많은 기억 장치가 필요하지만 실제적으로는 적은 부분만이 사용되어진다. 이러한 접근 권한의 부여가 행렬에 의해서 부여되므로 행렬의 다음 상태들을 예측하기가 어렵다. 이러한 문제점을 극복하기 위해 수취-부여 모델이 제안되었다.[2,11]

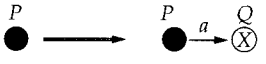
이 모델에서는 접근제어 행렬이 보호(Protection) 그래프에 의해 표현되어진다. 보호 그래프는 주체와 객체가 정점으로 표현되며 접근 권리는 간선에 레이블(lebel)로 표현한다. 즉 ●는 주체, ○는 객체, ⊗는 주체/객체를 표현한다. 그래서 만약 주체 S가 객체 O에 대하여 접근 권리 {r,w}를 갖는다면 다음과 같이 표현된다.



보호 그래프는 새로운 노드에 특권(priviledge)들을 생성하거나 또는 다른 노드들에 특권을 전달하거나 존재하는 특권을 감소시키는 주체의 행위에 의해 변경되어 질 수 있다. 이러한 행위는 수취-부여 모델에서 생성(Create), 제거(Remove), 수취(Take)와 부여(Grant)등의 규칙들로 정형화 되어진다.

(1) 생성

이 규칙은 그래프 G에 있는 주체 P가 새로운 노드 Q를 생성하는 것으로써, a로 레이블 된 간선이 추가되어 새로운 그래프 G'가 생성된다. 이 규칙은 아래 그림으로 표현된다.



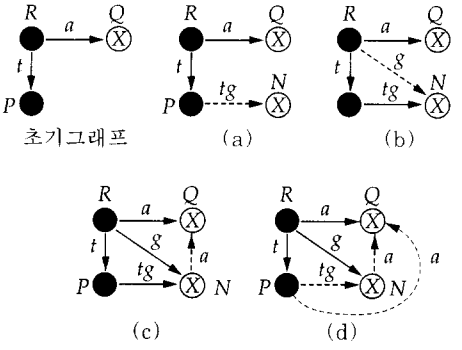
(2) 제거

이 규칙은 정점 P에서 다른 정점 Q에 대하여 갖는 특권들을 축소시킨다. 결과적으로 권리가 모두 없어지면 간선 자체가 제거된다. 이 규칙은 아래 그림으로 표현된다.

(3) 수취

이 규칙은 정점들 사이에 특권들의 부분집합이 이행적인 성질을 만족하도록 정의된 규칙이다. 주체 P에서 Q로의 간선에 a로 레이블하여 새로운 그래프를 생성한다. 아래 그림에 이 규칙을 표현하였다.

지금까지 정의된 규칙들을 정점 P,Q,R,N과 특권 a,t,g를 사용하여 주체 P가 Q에 대한 접근 권리 a를 얻는 과정을 도식화 하면 다음과 같다.



(a) Create ($P \rightarrow N$: 특권 tg)
(b) take ($R \Rightarrow P \rightarrow$: 부분특권 g)
(C) grant ($R \Rightarrow N \rightarrow$: 특권 a)
(d) take ($P \rightarrow N \Rightarrow$: 특권 a)

(4) 부여

이 규칙은 정점들 사이의 권리를 위임시키는 규칙이다. 주체 P로부터 R로의 간선에 Grant 특권 g로 레이블되어 있고 P에서 Q로의 간선에 a로 레이블되어 있을때 Grant 규칙은 R에서 Q로의 간선에 a레이블을 추가해서 새로운 그래프를 생성한다. 이 규칙은 다음 그림으로 표현된다.

수취/부여 특권은 모델내에서 주체와 객체에

부여되지만 생성/제거 특권은 주체에만 부여된다. 그러므로 보호 그래프가 반드시 주체를 포함해야 하는 조건은 실제 응용에 있어서 너무 제한적이다.

3.2 정보흐름 모델

정보흐름 제어는 서로 다른 보안 등급 사이의 정보 흐름을 제한하는 것으로 더 낮은 보안 등급의 정보가 같은 보안 등급이나 더 높은 보안 등급을 갖을 경우에만 정보흐름이 발생하도록 제한한다. 정보흐름 제어 모델로 격자 모델을 기술하였다.

3.2.1 격자 모델

흐름 제어를 위한 격자 모델(Lattice model)은 Denning에 의해 제안된 모델로 BLP모델을 확장한 모델이다.[1,2] 격자 모델에서는 정보 흐름 정책과 정보 흐름에 적합한 채널이 기술되었다. 정보 흐름 시스템은 격자 구조 정보 흐름 정책과 상태 그리고 상태 변이에 의해 모델화되는 추상적인 상태변이 기계 모델이다. 보안 클래스는 보안 등급과 범주의 순서쌍으로 기술될 수 있는데 보안 클래스 사이에는 순서화되지만 모든 주체와 객체에 대해서는 순서화되지 않고 부분 순서화 된다.

Denning은 정보 흐름 모델 FM을 다음과 같이 정의하였다.

$FM = \langle N, P, ⓐ, \rightarrow \rangle$.

. $N = \{a, b, \ldots\}$: 정보를 포함하는 객체들의 집합으로 객체들은 화일, 프로그램, 변수와 사용자 등을 나타낸다.

. $P = \{p, q, \ldots\}$: 정보 흐름에 책임이 있는 프로세스의 집합이며, $SC = \{A, B, \ldots\}$은 보안 클래스의 집합이다.

. ⓐ은 보안 클래스를 결합시키는 결합 연산자이다.

. $\rightarrow$ 은 정보 흐름 관계이다.

정보 흐름 정책은 구성원소 $\langle SC, \rightarrow \rangle$의 격자 구조에 의해 정의된다. SC는 보안 등급과 범주가 유한하며 순서쌍 $\langle SC, \rightarrow \rangle$는 부분 순서화된 집합이다. 순서쌍 $\langle SC, \rightarrow \rangle$에 있어서 $\rightarrow$는 재귀성, 이행성, 비대칭성을 만족해야 한다.

즉, $A, B, C \in SC$

$A \rightarrow A$(재귀성),

$A \rightarrow B$ and $B \rightarrow C$

$\Rightarrow A \rightarrow C$ (이행성),

$A \rightarrow B$ and $B \rightarrow A$

$\Rightarrow A = B$ (비대칭성)이다.

모든 $A \in SC$에 대하여 $A \rightarrow A$인 재귀성 관계는 같은 클래스에 정보 흐름이 발생할 수 있다는 것이다. 만약 $A \rightarrow B$이고 $B \rightarrow C$이면 $A \rightarrow C$인 경우는 이행적인 경우로, A에서 B를 통하여 C에 정보 흐름이 간접적으로 발생한다고 가정하면 A에서 C로 직접적인 정보 흐름을 허용한다. 비대칭성은 $A \rightarrow B$이고 $B \rightarrow A$이면 $A = B$를 의미한다. 즉 재귀성, 이행성이 만족되면 비대칭성의 요구는 단지 불필요한 보안 클래스를 제거하는 것이다.

Denning은 공리들을 통해 정보 흐름 정책이 유한한 격자 구조를 형성할 수 있음을 보였다. Denning이 정의한 공리는 다음과 같다.

(1) 보안 클래스 SC는 유한 집합이다.

(2) 흐름이 발생할 수 있는 관계 $\rightarrow$ 는 SC에 대하여 부분 순서화 된다.

(3) SC는 하한을 갖는다.

(4) 연산자는 최소 상한 연산자로 정의된다.

연산자 $\rightarrow$는 두 보안 클래스 사이에 정보 흐름이 허용된다는 것을 의미한다. 보안 클래스 A, B에 대하여 관계 $A \rightarrow B$는 클래스 B의 정보보다 A의 정보가 낮거나 같다는 것이다. 정보는 클래스 내부나 윗쪽으로 정보 흐름이 발생하지만 아래쪽이나 관련이 없는 클래스사이에는 정보 흐름을 허용하지 않는다. 연산자는 두개의 보안 클래스로부터 정보를 합성하여 얻어진 정보에 새로운 등급을 부여하는 상한 연산자이다. 예를 들어 A ⓐ $B = C$는 A와 B의 보안클래스의 정보를 포함하는 객체는 보안클래스 C로 등급이 부여되어야 한다.

하나의 보안등급이 다른 보안등급의 지배 관계

를 갖는 순서화된 클래스 *TC*, *S*, *C*, *U*의 격자 구조가 그림 1(a)에 나타내었다. 이 경우는 두개의 보안 클래스의 정보가 결합될때 두 클래스 중에서 더 높은 클래스의 등급이 채택된다. 그림 1(b)는 부분 순서화된 격자 구조이며 보안 클래스들은 { *A*, *B*,*C* }의 멱집합으로 표현된다. 봉급 정보가 {*A*}이고 의료 정보가 {*B*}라고 할때 공집합은 봉급 정보와 의료 정보가 아닌 공공 정보를 갖을 수 있다. 봉급정보 {*A*}와 의료정보 {*B*}가 새로운 객체에 결합될때, 이들 범주 {*A*}와 {*B*}는 지배관계가 없는 부분 순서화된 정보이므로 새로운 보안 클래스는 $A \cup B = \{A,B\}$로 부여된다.

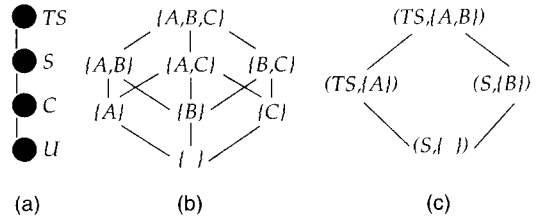


그림 1 정보 흐름 격자 구조

격자 구조의 보안 클래스는 그림 1(c)와 같이 두 구성요소인 보안 등급과 범주를 포함할 수 있다. 여기에서 하나의 보안 클래스 각각의 구성요소가 다른 보안 클래스에 대응하는 각각의 구성요소를 지배한다면 하나의 보안 클래스는 다른 보안 클래스를 지배한다고 한다. 예를 들면 〈 *TS*, {*A*} 〉가 〈 *S*, {*A*} 〉를 지배하지만 〈 *S*, {*B*} 〉와는 지배관계를 비교할 수 없다.

이 모델은 BLP모델의 주체의 인가 등급보다 낮은 객체를 읽고 인가 등급보다 높은 객체에 기록하는 정책을 자연스럽게 따르고 있다. 예를 들면 보안 클래스 (*S*, {*B*})를 갖는 객체는 (*S*, { })를 갖는 객체를 읽을 수 있지만 높은 보안 클래스 (*TS*, {*A*,*B*})를 갖는 객체는 읽을 수 없다. 또한 보안 클래스 (*TS*, {*A*})와 (*S*, {*B*}) 사이에는 정보 흐름이 발생하지 않는다.

이 정책에서 정보 흐름은 부분 집합들의 관계에서 확인되고 지배 관계는 상위 집합들과 관련지어지며, 서로 지배 관계가 없어 비교할 수 없는 객체 사이에는 정보 흐름이 발생할 수 없고, 보안 클래스의 결합은 보안 클래스들의 합집합으로 새로운 보안 클래스가 부여된다.

3.3 무결성 모델

정형화된 보안 모델의 또다른 중요한 목적은 고의적인 장난이나 실수로부터 정보의 무결성을 보장하는 것이다. 대표적인 무결성 모델인 Biba모델과 Clark과 Wilson모델을 기술하였다.

3.3.1 Biba 모델

BLP 모델은 불법적인 정보유출을 막는 모델이며 정보의 불법적인 변경에는 무관하다. Biba 모델은 BLP 모델과 유사하게 주체 또는 객체의 무결성이나 신뢰도에 따라 등급을 부여하여 자료의 무결성을 유지하기 위한 모델을 제한했다.[11,4,7] Biba 모델에 있어서 기본 개념은 낮은 무결성 정보가 높은 무결성 정보에 흘러가지 못하도록 하는 모델로 하나의 무결성 등급이 다른 무결성 등급을 지배하는 경우에만 정보 흐름이 발생할 수 있도록 하고 있다.

BLP 모델의 강제적 제어 정책이 Biba 모델에서는 다음과 같이 변경되었다.

(1) 단순 무결성 성질(Simple integrity property)
만약 $W(S) \geq W(0)$이면 주체 S는 객체 0를 읽을 수 있다.

(2) 무결성 *-성질(Integrity *- property)
만약 $W(S) \leq W(0)$이면 주체 S는 객체 0에 기록할 수 있다. 여기서 *W*는 주체나 객체에 무결성 등급을 부여하는 함수이다.

BLP 모델과 Biba 모델의 근본적인 차이는 없다. 즉 두 모델은 보안 클래스 사이의 정보 흐름에 관여하며 정보의 흐름은 한쪽 방향으로만 발생한

다. 단지 Biba 모델은 강제적 제어 정책에 의해 정보 흐름이 높은 보안 클래스에서 낮은 보안 클래스로 발생한다. Biba 모델은 강제적 제어 정책에 의해 주체는 낮거나 같은 무결성 등급을 갖는 객체에 기록하도록 하여 더 신뢰성이 없는 객체로부터 높은 무결성을 갖는 객체의 오염을 방지한다.

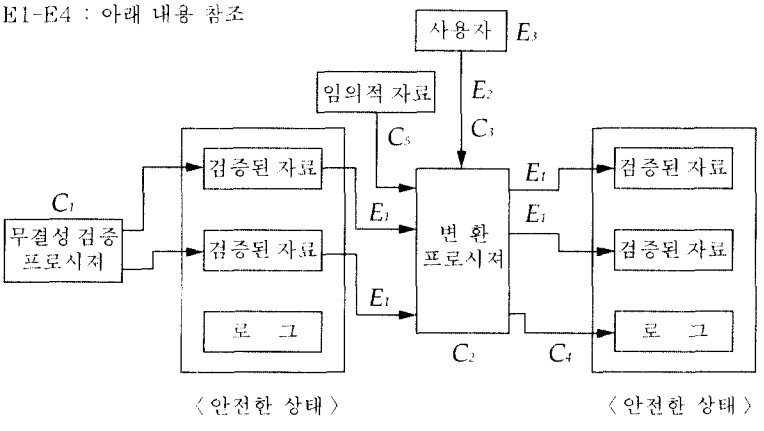
3.3.2 Clark과 Wilson 모델

정보 보안의 관심사는 불법적인 정보유출을 막는 비밀성에 촛점을 맞추어 왔으나 상업적인 보안 모델의 중요한 관심사는 고의적인 장난이나 실수로 인한 불법적인 정보의 변경을 방지하여 무결성을 보장하는 것이다. 이러한 무결성을 보장하기 위한 Clark과 Wilson 모델에서는 시스템 내의 자료는 두 가지로 분류된다.[12,10] 첫째는 이 모델의 규칙에 적용되어야 하는 자료인 검증된 자료(constrainted Data Item)이고, 둘째는 무결성이 유지되지 않고 임의적으로 조작되는 임의적 자료(unconstrainted Data Item)이다. 또 다른 개념은 무결성 정책이 무결성 검증 프로시져와 변환 프로시져로 구분한다. 무결성 검증 프로시져의 목적은 시스템내의 모든 검증된 자료들이 프로시져가 수행되는 동안에 무결성이 유지되는 즉 안전한(secure) 상태임을 확인하는 것이고, 변환 프로시져(transformation Procedures or TPs)는 잘 정의된 트랜잭션이다. 잘 정의된 트랜잭션은 무결성을 유지하기 위해 사용자가 임의적인 트랜잭션에 의해 자료를 조작하지 않고 그 자료와 관련된 프로그램에 의해서만 자료를 변경시킬 수 있도록 하는 것이다.

즉, 변환 프로시져의 목적은 검증된 자료들을 안전한 상태에서 또 다른 안전한 상태로 변경시킬 수 있도록 하는 것이다. 무결성 규칙들이 적용되는 모든 자료들은 트랜잭션들에 의해 임의적으로 변경되어질 수 없고 변환 프로시져에 의해서만 변경되어져야 안전한 상태가 유지되어질 수 있다. 이 모델은 BLP 모델과 유사하게 무결성 검증 프로시져에 의해 시스템의 초기 상태가 안전함이 확인되고 변환 프로시져에 의해서만 다음 상태로 변경을 허용한다면 시스템은 안전한 상태가 보장 된다는 것을 귀납적 방법으로 증명한다.

무결성을 보증하기 위한 두가지 과정이 있다.

첫째는, 무결성 검증 프로시져들과 변환 프로시져들이 시스템에 무결성을 보장하는지를 결정하는 증명 과정으로 이는 응용과정에 책임이 있는 보안 관리자, 시스템 소유자와 시스템 관리자에 의해 행해진다. 둘째는, 강화규칙으로 특정응용에 독립적이며, 시스템에 의해 행해져야 하는 기능들이다. 이러한 두과정은 〈그림 2〉와 같다.



〈 그림 2 〉 Clark과 Wilson 모델

모델의 증명(Certification) 규칙은 다음과 같다.

C_1: 무결성 검증 프로시져가 수행되는 동안에 모든 검증 자료들이 안전한 상태에 있다는 것을 보장해야 한다.

C_2: 변환 프로시져들이 검증 자료들을 안전한 상태에서 다른 안전한 상태로 변경 시키는 것이 입증되어야 한다. 보안 관리자는 각 변환 프로시져와 변환 프로시져가 수행하는 검증 자료들과의 관계를 (TPi(CDTa, CDTb...)) 형태로 기술해야 한다.

C_3: E_2내의 관계 리스트가 임무의 분리 요구사항들을 만족하는지 입증되어야 한다.

C_4: 변환 프로시져들이 수행하는 모든것이 로그에 추가되는지 입증되어야 한다.

C_5: 비검증 자료에서 검증 자료로의 변환은 변환 프로시져에 의해서만 수행한다는 것이 입증되어야 한다.

강화(enforcement)규칙들은 다음과 같다.

E_1: 시스템은 C_2규칙에서 기술된 관련 리스트를 유지하고 리스트내의 규정에 따라 검증 자료가 하나의 변환 프로시져에 의해서만 수행되도록 보장해야 한다.

E_2: 시스템은 사용자, 변환 프로시져와 자료 객체의 관련 리스트를 관리하고 리스트 내의 구성요소의 하나가 수행될 수 있다는 것을 보장해야 한다.

E_3: 시스템은 변환 프로시져를 수행하는 사용자의 신원을 인증해야 한다.

E_4: 보안 관리자만이 관련 리스트를 변경시킬 수 있어야 한다.

Clark과 Wilson 모델은 무결성 보장을 위해 정형화된 수학적 표기법은 제공하지 않았지만, 객체의 변경은 무결성 보장을 위해 인가된 사용자와 신뢰성있는 프로그램을 통해 수행할 수 있도록 한다. 이 모델은 자료의 변환이 변환 프로시져에 의해서만 수행되도록 하였다.

3.4 인증 프로토콜의 모델

인증 프로토콜은 분산 환경에서 두개 이상의 개체들 사이에 인증을 하는 절차로서 인증을 다음과 같이 크게 네가지 분야로 나눌수 있다.[13]

(1) 사용자 인증(User Authentication)

시스템을 사용하는 사용자가 정당한 사용자인가를 인증하는 절차이다. 사용자는 일반적 시스템 사용자뿐만 아니라 사용 데이타베이스 내에서 유지되고 있는 고객들도 포함된다. 사용자 인증을 함으로써 자원을 사용하기 편리하고 데이타를 보호할 수 있는 잇점을 얻을 수 있다.

(2) 개체 또는 노드인증
(Peer or Node Authentication)

개방형 시스템 환경에서 여러 노드가 존재할 경우에 사용자가 사용하는 노드들이 올바른 개체인가를 인증하는 절차이다. 노드의 식별은 이름이나 네트워크 주소에 의해서 이루어진다. 노드인증에는 다음과 같은 몇가지 요구조건들이 있다.

첫째, 목적지노드에 접근권한이 위임되기 전에 목적지노드의 신원증명이 타당해야 한다.

둘째, 지정된 노드가 특정 시스템 서비스를 제공할 수 있는 권한을 가지고 있어야 한다.

셋째, 요청하는 사용자와 보호된 자원 사이의 위임체인에 관한 중간매체로서 작용하는 노드에 대한 접근제어 정책을 지원해야 한다.

넷째, 동등노드 참조 모니터에 대한 권한을 갖기 위해서는 접근등급과 정책 영역 관계가 결정되어야 한다.

(3) 메세지 인증(Message Authentication)

사용자간에 통신할때 주고 받는 메세지가 정당한 사용자가 사용한 메세지인가를 인증하는 절차이다.

(4) 프로세스 인증

프로세스 인증은 사용자인증과 유사하지만 프로세스는 동등프로세스를 인증하기위해 다른 자원 성분을 사용하지 않고 암호화 기능을 수행할 수 있으며 패스워드에 관련된 크기와 기억공간에 제한을 받지 않는 인증 데이타 항목을 유지하고 있다. 프로토콜의 모델은 일반적으로 송신자와 수신자에 대해 동등한 권한을 주지만 특정 사건의 시간 순서가 세션설정에 영향을 미치지 않는다.

3.4.1 Sidhu 모델[2]

인증 프로토콜은 첫째, 송신자와 수신자 사이에 인증이 대칭적으로 이루어지고, 둘째, 특정 사건의 시간 순서에 관한 가정은 고려하지 않는다. 비대칭을 통한 인증은 많은 비용이 든다. 이러한 오버헤드를 줄이기 위해서는 인증이 대칭적으로 이루어지도록 하는 것이 효율적이다. 두번째 성질은 프로세스간에 동기화를 고려하지 않는 가정이다. 이러한 동기화 문제를 해결하기 위해서는 두 엔티티사이에 이루어져야 하는 모든 사건의 시간 순서를 프로토콜에 지정하는 방법이 필요하다.

예를 들면 시간 순서를 고려한 Kerberos는 티켓 제공서버(ticket-granting server)개념을 사용하고 있으며 DES방법과 Needham-schroeder 공동키 분배 프로토콜에 기반을 두고 있다. 엔티티는 그들의 패스워드로부터 유도되는 비밀키에 의해 인증되어진다. 이 키는 인증서버와 함께 공유되어지며 인증서버는 하나의 로그인 세션(login session)을 통해 생성된 티켓을 부여하게 된다. 그리고 KAS는 인증을 요구하는 개체가 네트워크 서비스에 접근하기 위해 티켓 제공서버로부터 다른 티켓을 획득하도록 하여준다. 티켓은 티켓 제공서버로부터 생성된 암호화된 세션키와 타임 스템프, 유효시간(lifetime), 사용자의 식별자로 구성된다.[14]

메세지 1. $A \rightarrow KAS$: A, TGS, T_1

메세지 2. $KAS \rightarrow A$: $\{K_{A,\ TGS}\}K_{KAS,\ TGS}$, $\{\mathrm{Ticket}_{A,\ TGS}\}K_{KAS,\ TGS}$

메세지 3. $A \rightarrow TGS$: $\{A, T_3, W_A\}K_{A,\ TGS}$, B $\{\mathrm{Ticket}_{A,\ TGS}\}K_{KAS,\ TGS}$

메세지 4. $TGS \rightarrow A$: $\{K_{A,\ B}\}KA_{,\ TGS}'$, $\{\mathrm{Ticket}_{A,B}\}K_{B,\ KAS}$

메세지 5. $A \rightarrow B$: $\{A, T_5, W_A\}K_{A,\ B}'$, $\{\mathrm{Ticket}_{A,B}\}K_{B,\ KAS}$

메세지 6. $B \rightarrow A$: $\{T5+1\}K_{A,B}$

여기에서 A와 B는 사용자 A와 B의 id, TGS는 TGS의 id, $K_{A,\ TGS}$는 사용자 A와 TGS사이의 공통 세션키, $K_{A,\ KAS}$는 사용자 A와 KAS사이의 공통키, $K_{KAS,\ TGS}$사이의 공통키, $\{M\}K$는 키 K로 공통키 방식을 암호화된 메세지 M, $\mathrm{Ticket}_{A,\ TGS}$는 $\{K_{A,TGS}, A, {}_{TGS}, T_2, W_A, L\}$, $\mathrm{Ticket}_{A,B}$는 $\{K_{A,B}, A, T_A, L\}$, L은 티켓의 유효시간, W_A는 워크스테이션 A의 주소, T_1, T_2, T_3, T_4, T_5는 타임스템프를 나타낸다.

그리고 프로토콜은 방향성 그래프로 표현된 모든 입력을 받아들여야 하는 완결성, 프로토콜이 다음 단계로 전송이 불가능하거나 시스템 상태가 무한 상태에 빠지지 않는 교착상태 회피, 시스템 상태들 사이에 반복 루틴이 형성되지 않는 기아상태(livelock)예방, 프로토콜이 초기상태에서 시작하여 최종상태로 끝나야하는 종결성, 각 채널을 통해 전송되는 메세지의 최대수는 항상 채널 용량을 초과하지 않는 제한성, 정상적인 조건하에서 실행될 수 없는 상호작용의 제약조건을 만족해야 한다.

3.4.2 Varadharajan 모델

정형적인 분석을 위해 사용된 인증 프로토콜은 어느 특정 알고리즘과 독립적으로 사용되고, ISO/TC97/SC20/WG1과 Needham-Schroder 프로토콜에 기술된 동등 개체 인증 메카니즘과 유사하다[2]. 두 개체사이에 안전한 통신을 위하여 필요한 통신키를 분배하는데 중요한 역할을 하는 키분배 센터(KDC)인 권한 대행자의 존재를 가정한다.

프로토콜은 통신 프로세스들의 집합으로 구성되고, 프로세스내의 각 개체는 하나의 프로세스가 유지된다. 프로토콜의 각 개체는 유한 상태 기계로 표현할 수 있다. 이러한 상태기계에서 메세지 입력과 출력은 상태들 사이에 방향성 그래프로 표시한다. 그리고 상태 전이는 전송 메세지와 수신 메세지 사건에 의해서 이루어진다.

프로토콜의 실행은 상태 순서로 간주될 수 있는데, Sidhu 모델과는 달리 시간 논리가 상태 순서를 추론하는데 유용하게 이용된다. 시간 논리는 시간에 관련이 없는 성질을 추론하는 서술논리(predicate logic)에 시간에 관련된 연산자를 첨가한 논리이다. Varadharajan에 의해서 확인된 성질에서도 완결성, 교착상태 회피, 기아상태 방지, 종결성, 제한성을 만족한다.

4. 보안 모델 비교 분석

지금까지 일반적인 보안정책과 보안모델들을 기술하였다. 이장에서는 접근제어 모델, 정보 흐름 모델, 무결성 모델, 인증 프로토콜 모델들에 대한 강제적 접근 제어와 임의적 접근 제어의 이용 여부와 각 모델에 적용되는 객체들을 보호하기 위한 방법 및 정보 흐름의 특징 등을 비교 분석하였다. 또한 분산 환경에 적용을 위해 정형화된 보안 모델을 분석하였다.

4.1 보안 모델 분석

접근 제어 모델, 정보 흐름 모델, 무결성 모델, 인증 프로토콜의 보안 특징의 분석 결과는 다음과 같다.

BLP 모델은 접근 제어 방법을 이용한 모델로 강제적 접근 제어의 특성인 단순성질과 *-성질은 높은 비밀 등급의 정보가 낮은 비밀 등급의 객체로 정보가 유출되지 못하게 하므로써 흐름 제어에 대한 보호를 하고 있다. BLP 모델의 임의적 접근 제어에서 사용하는 접근 제어 행렬은 기억 장소의 낭비 및 접근 권한이 추가됨에 따라 예측의 어려움이 있다. 수취-부여 모델에서는 접근 제어 행렬을 보호 그래프를 사용하여 주체와 주체/객체 사이의 접근 권리를 표현하였다. 이 모델은 임의적 접근 제어 방법이 사용되고 있다. 그러나 수취-부여 모델에서는 수취/부여 특권이 주체와 객체에 부여되지만 생성/제거 특권은 주체에만 부여된다. 그러므로 보호 그래프가 반드시 주체를 포함해야 하는 조건은 실제 응용에 있어서 너무 제한적이다.

접근 제어는 객체에 접근을 제어하는 것으로써 객체 내에 포함된 정보에 대한 규제는 고려하지 않는다. 정보 흐름 제어 정책은 객체 사이의 정보 전달을 제어하는 방법이다. 흐름 제어를 위한 대표적 모델인 격자 모델은 정보 흐름 정책과 정보 흐름에 적합한 채널을 기술한다. 격자 모델에서는 임의적 접근 제어는 사용하지 않으며 강제적 접근 제어만 사용되고 있다. Biba 모델에서는 낮은 무결성 정보가 높은 무결성 정보로 흘러가는 것을 방지하기 위한 모델로 강제적 접근 제어 방법을 사용하여 하나의 무결성 등급이 다른 무결성 등급을 지배하는 경우에만 정보흐름이 발생할 수 있도록 하고 있다.

Clark과 Wilson 모델은 시스템내의 자료가 안전한 상태를 유지하기 위해서는 임의의 트랜잭션에 의해 자료의 변환이 수행되지 않고 변환 프로

구 분	종 류	주체/객체 제어	정보 흐름	강제/임의 정책
접근 제어	BLP	접근권리, 보안등급	지배관계	강제/임의
	수취-부여 모델	접근권리	보호 그래프	임의
정보 흐름	격자모델	보안등급 + 객체 관련성	채널 설정	강제
무 결 성	Biba모델	무결성 등급	지배관계	강제
	Clark과 Wilson모델	프로시저 사용권한	변환 프로시저	
인증 프로토콜	Sidhu	사건의 만족	프로토콜	
	Varadharajan			

시져에 지료가 변경되는 무결성 모델이다. 일반적인 강제적 접근 제어와 임의적 접근 제어 방법은 사용하지 않았고 이것들을 변환 프로시져와 변환 프로시져의 사용 권한으로 접근 제어를 하였다.

인증 프로토콜 모델에서 프로토콜은 방향성 그래프로 표현된 모든 입력을 받아들여야 하는 완결성, 프로토콜이 다음 단계로 전송이 불가능하거나 시스템 상태가 무한 상태에 빠지지 않는 교착상태 회피, 시스템 상태들 사이에 반복 루틴이 형성되지 않는 기아상태(Livelock)예방, 프로토콜이 초기상태에서 시작하여 최종 상태로 끝나야하는 종결성, 각 채널을 통해 전송되는 메세지의 최대수는 항상 채널 용량을 초과하지 않는 제한성, 정상적인 조건하에서 실행될 수 없는 상호작용의 제약조건을 만족해야 한다.

4.2 분산 환경을 위한 보안 모델

분산 시스템은 자료의 분산된 성격, 자원의 높은 정도의 개방성 그리고 사용자들의 자원 공유를 요구하는 특징이 있다. 이러한 분산 시스템 자원의 분산된 특성 때문에 BLP모델은 하나의 시스템 내의 정보의 흐름 정책을 검증할 수 있지만 다른 시스템으로부터의 정보의 흐름에 관한 정책을 강화할 수 없다. 정보 흐름 모델은 서로 다른 보안 클래스를 갖는 두 사용자간의 정보의 흐름에 관계가 있다. 또한 사용자가 분산시스템 자원이나 사용자를 대신해 수행되는 프로세스에 대한 접근 권한 정책을 강화할 수 없다.

수취-부여 모델에서는 접근 제어 행렬을 보호 그래프를 사용하여 주체와 주체/객체 사이의 접근 권리를 표현하였다. 이 모델은 임의적 접근 제어 방법이 사용되고 있다. 그러나 수취-부여 모델에서는 수취-부여 특권이 주체와 객체에 부여되지만 생성/제거 특권은 주체에만 부여된다. 그러므로 보호 그래프가 반드시 주체를 포함해야 하는 조건은 실제 응용에 있어서 너무 제한적이다. 수취-부여 모델을 분산 시스템에 적용하기 위해서는 주체가 접근권한의 부분집합을 양도할 수 없도록 하는 연구가 필요하다.

Clark과 Wilson모델은 분산시스템에서는 유용하지 않다. 왜냐하면 변환 프로시져가 분산 시스템의 모든 정보에 관여 한다고 가정할 수 없기 때문이다. 변환 프로시져가 총체적인 검증 자료에 관한 정보를 갖을 수 없고 지역적 보안 정책내에 정의되고 사용가능한 정보에 의해 처리되어지기 때문에 하나의 변환 프로시져에 의해 생성된 안전한 결과가 다른 프로시져에 의해서는 안전하지 않을 수 있다.

5. 결 론

본 논문에서는 분산 시스템 환경에서의 보안요구 사항을 파악하고 모델링을 위하여, 정형화된 보안모델들에 대한 특성들을 알아보고 이를 분석하였으며, 보안모델들간의 관계를 비교 분석하였다.

보안 모델들의 분석결과 정형화된 보안 모델들의 공통적인 특징은 어떤 주체가 개체에 접근할 수 있는가, 또는 어떤 일을 수행할 수 있는가에 관련되었다. 또한 대부분의 정형화된 모델들은 시스템의 초기상태가 안전하고 특정 보안 정책에 의해 다음 상태로 안전하게 변환되는 상태변이 기계를 이용하여 시스템이 안전한가를 검증하고 있다.

정형화된 모델을 분산시스템 적용하기 위해 분석된 결과는 다음과 같다.

1. 일반적인 정형화된 모델에서 수행하는 연산들은 순차적으로 수행하는 단일 시스템에 관련되며 분산시스템의 구조를 반영하지 않고 있다.

2. 정형화된 모델들은 주체가 객체에 접근 및 수행에 관한 특별한 보안 서비스들만의 구현에 관여하며 분산환경의 다양한 보안 서비스를 제공하지 못하고 있다.

3. 정형화된 보안 모델들은 특정 연산과 제약조건으로 특별한 운영환경을 위해 정의되었으며 분산환경을 고려하지 않는다.

4. 강제적 정책을 이용하는 각 모델에 있어서 주체와 객체에 보안등급을 부여하는 문제가 어렵다.

5. 인증 정책에 필요한 오버헤드가 발생할 수 있으며 권한이 있는 사용자가 서비스를 받을 수 없는 경우가 발생할 수 있다.

이와 같이 대부분의 정형화된 모델들은 특별한 보안 서비스와 그들의 구현을 검증하기 위해 설계되었다. 분산 시스템을 위한 보안 모델은 분산 시스템 구조와 분산시스템에 적합한 보안 서비스들의 확장에 관한 새로운 연구가 필요하다.

참 고 문 헌

[1] William Caelli, Dennis Longley, Michael Shain, INFORMATION SECURITY HANDBOOK, Macmillan Publishers Ltd, 1991, pp 707 - 754.

[2] Sead Muftic, Ahmed Patel, Peter Sanders, Rafael Colon, Jan Heijnsdijk, Unto Pulklinen, SECURITY ARCHTECTURE FOR OPEN DESTRIBUTED SYSTEMS, John Wiley & Sons Ltd, 1993, pp 97 - 146.

[3] Frank L. Mayer, "An Interpretation of a Refined Bell-La Padula Model For the TMach Kernel," Fourth Aerospace Computer Security Applications Conference, December, 1988, pp 368 - 378.

[4] Ravi Sandhu, "Lattice-Based Access Control Models," IEEE COMPUTER, November, 1993, pp 9-19.

[5] F. Rabitti, et al., "A Model of Authorization for Next Generation Database System," ACM Trans. on Database Systms, Vol. 16, No 1, March, 1991. pp 88 - 131.

[6] John McLean, "The Specification and Modeling of Computer Security," IEEE Computer, January, 1990, pp9-16.

[7] G. F. G. O'Shea, "Operationg System Integrity," Computer & Security, Oct., 1991, pp 443-465.

[8] WEN-PAI LU, MALUR K. SUNDARESHAN, "A Model for Multilevel Security in Computer Networks," IEEE TRANSA-CTIONS ON SOFTWARE ENGINEERING, Vol.16, No.6, June, 1990, pp 647 - 659.

[9] M. D. Abrams, E. G. Amoroso, L. J. Lapadula, T. F. Lunt and J. G. Williams, "Report of an integrity research study group," Computers & Security, Dec. 1993, pp 679 - 689.

[10] D. D. Clark, D. R. Wilson, "A Cpmparison of Commercial and Military Computer Security Policies," IEEE Symp. on Security and Privacy, IEEE, New York, 1987, pp 184 - 194.

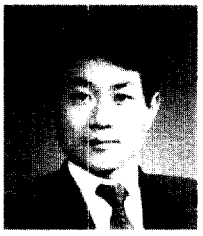
[11] Dacier Marc, "A PETRI NET REPRESENTATION OF THE TAKE-GRANT MODEL," proceedings The Computer Security Foundations Workshop VI, 1993, pp 99 -108.

[12] Leonard J. Lapadula, James G. Williams, "Toward a Universal Integrity Model," proceedings The Computer Security Foundations Workshop IV, 1991, pp 216 - 218.

[13] John Linn, "Practical Authectication for Distributed Computing," IEEE Computer Socitey Symposium on Reaearch in Security and Privacy, May, 1990, pp 31 - 40.

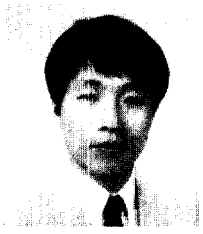
[14] D. Gollmann, T. Beth, F. Damm, "Authentication services in distributed systems," Computers & Security, Dec, 1993, pp 753 - 764.

□ 著者紹介



서 재 현

1985년 전남대학교 계산통계학과 미학사
1988년 중앙대학교 대학원 전자계산학과 미학석사
1988년 - 현재 송원전문대학 전자계산학과 전임강사
1993년 - 현재 전남대학교 대학원 전산통계학과 박사과정
관심분야 : 객체지향 시스템, 분산처리 시스템, 정보 보안 등



김 태 연

1986년 전남대학교 계산통계학과 미학사
1988년 전남대학교 대학원 계산통계학과 미학석사
1993년 - 현재 전남대학교 대학원 전산통계학과 박사과정
1993년 현재 광주예술전문대학 컴퓨터그래픽 디자인학과 전임강사
관심분야 : 분산처리 시스템, 통신 보안, 컴퓨터 그래픽스 등

노 봉 남

1978년 전남대학교 수학교육학과 미학사
1982년 한국과학기술원 전산학과 미학석사
1994년 전북대학교 대학원 전산통계학과 미학박사
1983년 - 현재 전남대학교 전산학과 부교수
관심분야 : 객체지향 시스템, 통신망 관리, 정보 보안, 컴퓨터와 정보사회 등