# BLP 모델과 Biba 모델 결합을 통해서 기밀성과 무결성을 보장하는 보안 모델

° 김 민정, 박석
서강대학교 전자계산학과 데이타베이스 연구실

# A security model considering secrecy and integrity using the combination of BLP model and Biba model

° Kim Min-jeong, Park Seog
Dept. of Computer Science, Sogang University

## 요 약

정보 보안의 세 가지 목적은 기밀성, 무결성, 유용성이다. 모든 정보 시스템에서 정보 보안에 관한 필요성이 대두되면서 기밀성뿐만 아니라 무결성도 보장하는 보안 모델이 필요하다. BLP와 Biba는 각각 기밀성과 무결성을 보장하는 보안 모델로서 BLP 모델이 무결성을 고려하지 않기 때문에, Biba 모델은 기밀성을 고려하지 않기때문에 접근할 수 있는 정보에 한계가 있다.

본 논문에서는 여러 정보 시스템중에서 주로 군사 정보 시스템으로 구현된 BLP와 Biba 모델을 이용해서 기밀성과 무결성을 만족하는 보안 모델을 제시한다. BLP 모델과 Biba 모델을 결합함으로써 BLP 모델을 통해 기밀성을, Biba 모델을 통해 무결성을 보장한다

## 1. 개 요

다중사용자 컴퓨터 시스템의 출현으로 시스템 설계자와 사용자들은 정보 보안에 대한 필요성을 더욱 심각하게 인지하게 되었다. 정보 보안이라 하면 아래와 같이 개별적이고 서로 관계가 있는 세 가지 목적을 갖는다[1]. 첫 째는 기밀성(confidentiality or secrecy)으로서 정보의 유출과 관련이 있는 것이고 두 번째 무결성 무결성(integrity)으로서 정보의 수정과 관련이 있다 그리고 마지막으로 유용성(availability)은 정보로의 접근 거부와 관련이 있다.

정보 시스템이 위에서 언급한 정보 보안의 목적을 만족하기 위해서는 보안 시스템에서 가정한 보안 정책과 이에 맞은 보안 모델이 있어야 한다[1)]

현대 사회에서는 정보량이 많고 종류도 다양해짐에 따라 군사 보안 시스템이 다루는 정보에도 여러 종류가 있다. 특히, 기밀성과 무결성을 동시에 고려해서 정보로의 접근을 제어해야만 하는 정보가 있다. 군사 및 군사 관련 분야에서 기밀성과 무결성 보안 모델로 BLP와 Biba가 있으나, 이러한 기존의 모델들은 정보의 기밀성과 무결성을 함께 고려하지 못한다. 따라서, 두 개념을 동시에 고려하는 보안 모델이 필요하다. 본 논문에서는 기존의 보안 모델들을 이용해서 이러한 보안 모델을 제시했다. 기밀성뿐만 아니라 무결성도 보장하는 전혀 새로운 보안 모델을 제시하는 방법도 있으나 그것은 새로이 제시하고자 하는 보안 모델의 요구 사항중 일부분을 만족하는 기존의 보안 모델을 사장시킨다는 극복하기 어려운 단점이 있다. 그러므로, 본 논문에서는 기존의 보안 모델, 특히 BLP와 Biba 모델의 결합을 통해서 기밀성과 무결성을 동시에 고려하는 보안 모델

1) 본 논문 아하에서 기밀성 보장을 위한 보안 정책과 이에 맞는 보안 모델을 기밀성 보안 정책, 기밀성 보안 모델이라 하고, 무결성에 대해서도 무결성 보장을 위한 보안 정책과 이에 맞는 보안 모델을 무결성 보안 정책, 무결성 보안 모델이라 한다.

을 제시했다.

## 2. 기존의 보안 모델

기존의 보안 모델들을 응용 분야, 접근 제어 기법등을 통해서 분류하면 표 1과 같다. 보안 모델 집합 - I 에는 주로 군사 및 군사 관련 분야에서 시스템으로 구현된 BLP와 Biba 모델등이 있고 보안 모델 집합-II에는 주로 상업 분야에서 이용되는 Clark-Wilson 모델[2,8], 역할 기반 접근 제어 모델[4], 의무 분리를 위한 모델[3]등이 있다. 보안 모델 집합- I 은 보안 등급을, 보안 모델 집합-II는 역할을 근거로 정보로의 접근을 제어한다.

| | 보안 모델 집합- I | 보안 모델 집합-II |
|---|---|---|
| 응용 분야 | 군사 및 군사 관련 분야 | 상업 분야 |
| 접근 제어 기법 | 강제적 접근 제어 기법 | 임의적 접근 제어 기법 |
| 접근 제어 | 래티스를 기반으로 정보의 흐름 제어 | 역할을 기반으로 정보로의 접근 제어 |
| 보안 모델 | BLP 모델, Biba 모델 | Clark-Wison 모델, 역할 기반 접근 제어 모델, 의무 분리를 위한 모델 |

【표 1】 기존 보안 모델의 분류

앞에서도 언급한 바와 같이 본 논문에서는 주로 군사 정보 시스템으로 구현될 보안 모델을 제시하고자 한다. 따라서 보안 모델 집합-II보다는 보안 모델 집합- I 을 이용한다.

### 2.1 BLP(Bell-La Padula) 모델

BLP 모델은 정보 보안의 세 가지 목적중에서 기밀성을 보장한다. 이 모델을 구현한 보안 시스템은 객체, 주체 그리고 객체와 주체에 지정되는 기밀성 등급으로 구성되어 있다. 주체와 객체에 지정된 기밀성 등급에 근거하여 객체로의 접근을 제어한다. 기밀성 등급을 구성하는 계층적 등급은 전체 순서화 되어 있고 범주 집합은 부분 순서화되어 있다.

**기밀성 등급의 종류**

Top Secret (TS) > Secret (S) > Confidentiality (C) > Unclassified (U)

기밀성 등급 SL(Secrecy Level) = (C, S)

단, C는 계층적 등급으로 2급 비밀, 3급 비밀, 대외비, 평문등으로 구성되고 S는 범주 집합으로 인사, 작전, 군수, 정보등으로 구성된다.

이러한 기밀성 등급들은 지배(dominace) 관계에 따라 부분 순서화 되어 래티스를 구성한다. 기밀성 보장을 위해서 주체는 아래에 있는 보안 정책을 만족할 경우에만 객체로의 접근이 가능하다. 아래에서 SL(S), SL(O)는 각각 주체와 객체의 기밀성 등급이다.

**BLP 모델의 보안 정책**

1) 주체 S는 다음의 조건을 만족할 때에만 객체 O에 대한 판독 연산이 가능하다.

조건 : $SL(S) \geq SL(O)$.

2) 주체 S는 다음의 조건을 만족할 때에만 객체 O에 대한 갱신 연산이 가능하다.
조건 : SL(S) ≤ SL(O).

### 2.2 Biba 모델

Biba 모델은 정보 보안의 세 가지 목적중에서 무결성을 보장한다. 이 모델도 모델을 구현한 보안 시스템은 객체, 주체 그리고 객체와 주체에 지정되는 무결성 등급으로 구성되어 있다. 주체와 객체에 지정된 무결성 등급을 근거로 하여 객체로의 접근을 제어한다. 무결성 등급을 구성하는 계층적 등급은 전체 순서화 되어 있고 범주 집합은 부분 순서화되어 있다.

**무결성 등급의 종류**

Crucial (C) > Very Important (VI) > Important (I)

무결성 등급 IL(Integrity Level) = (C, S)

단, C는 계층적 등급으로 무결성에 차이가 있는 정보로 구성되고 S는 범주 집합으로 인사, 작전, 군수, 정보등으로 구성된다.

이러한 무결성 등급들은 지배 관계에 따라 부분 순서화 되어 래티스를 구성한다. 무결성 보장을 위해서 주체는 아래에 있는 보안 정책을 만족할 경우에만 객체로의 접근이 가능하다. 아래에서 IL(S), IL(O)는 각각 주체와 객체의 무결성 등급이다.

**Biba 모델의 보안 정책**

1) 주체 S는 다음의 조건을 만족할 때에만 객체 O에 대한 판독 연산이 가능하다.
조건 : IL(S) ≤ IL(O).
2) 주체 S는 다음의 조건을 만족할 때에만 객체 O에 대한 갱신 연산이 가능하다.
조건 : IL(S) ≤ IL(O).

### 2.3 문제 제기

기존의 보안 모델, BLP와 Biba는 군사와 군사 관련 분야에서 각각 기밀성과 무결성을 보장하는 대표적인 보안 모델이다.. 그러나, BLP 모델은 무결성을 거의 고려하지 않는다. 이로 이해 기밀성이 있는 데이타를 다루는 것에 한계가 있고 Biba도 이와 유사한 문제점이 있다. 이러한 한계는 BLP 모델이나 Biba 모델이 실지로 응용될 수 있는 분야에 많은 제한을 가져온다.

## 3. BLP 모델과 Biba 모델의 결합 : BB 모델

본 논문에서는 BLP와 Biba 모델을 결합하는 여러 방법중에서 보안 등급을 기밀성 등급과 무결성 등급으로 구성하는 방법을 이용하여 한다[1,8]. 기밀성 등급은 BLP 모델에서의 보안 정책에 적용하고 무결성 등급은 Biba 모델에서의 보안 정책에 적용한다. 즉, 두 모델에서의 보안 정책을 모두 포함하는 단일 보안 정책을 사용함으로써 기밀성과 무결성을 모두 고려한다.

### 3.1 BB 모델

BB 모델은 BLP와 Biba 모델을 결합하여 기밀성과 무결성을 함께 고려하는 보안 모델이다. 이 모델을 구현하는 시스템은 BLP나 Biba 모델을 구현한 시스템과 전체 구성도가 동일하다. 즉,

객체와 주체 그리고 객체와 주체에 지정되는 보안 등급으로 구성되어 있다.

BB 모델에서의 보안 등급[2]도 두 개의 구성 요소로 이루어진다. 보안 등급은 L = (C, S)와 같이 정의된다. 이 때, C는 계층적 등급이고 S는 범주 집합으로 인사, 군수, 정보등으로 구성된다. 계층적 등급의 명칭은 구성 요소인 두 개의 계층적 등급을 언더바로 연결했다. 언더바 앞이 기밀성 등급, 뒤가 무결성 등급에서의 계층적 등급이다. BB 모델에서 계층적 등급은 표 2와 같다.

| | | |
|---|---|---|
| TS_C(Top Secret_Crucial) | TS_VI(Top Secret_VeryImportant) | TS_I(TopSecret_Imporant) |
| S_C(Secret_Crucial) | S_VI(Secret_Very Important) | S_I(Secret_Important) |
| C_C(Confidential_Crucial) | C_VI(Confidential_Very Important) | C_I(Confidential_Important) |
| U_C(Unclassified_Crucial) | U_VI(Unclassified_Very Important) | U_I(Unclassified_Important) |

【표 2】 BB 모델에서의 계층적 등급

BLP나 Biba 모델에서는 모든 보안 등급[3]이 전체 순서화 된다. 그러나, BB 모델에서는 기밀성 정도또는 무결성의 정도로 보안 등급을 순서화 할 수 없는 경우가 있다. 다시 말해서, 보안 등급을 구성하는 기밀성 등급과 무결성 등급이 다를 경우에는 두 보안 등급의 지배관계를 기밀성 측면에서도 무결성 측면에서도 하나로 결정할 수가 없는 경우가 있다. 따라서, BLP와 Biba 모델과 같이 전체 순서화된 래티스를 기반으로 정보의 흐름을 제어하는 것이 불가능하다.

본 논문에서는 그림 1과 같이 BB 모델에서의 보안 등급을 원소로 하는 행렬을 기반으로 정보의 흐름을 제어한다. 아래의 행렬을 보안 등급 행렬이라고 칭한다. 보안 등급 행렬에서 위로 갈수록 보안 등급의 기밀성 등급이 높고 우에서 좌로 갈수록 무결성 등급이 높아진다.

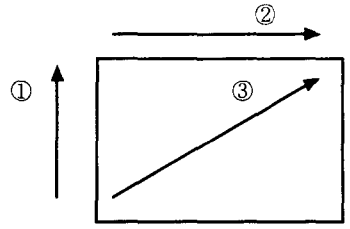
| | 1열 | 2열 | 3열 |
|---|---|---|---|
| 1행 | TS_C | TS_VI | TS_I |
| 2행 | S_C | S_VI | S_I |
| 3행 | C_C | C_VI | C_I |
| 4행 | U_C | U_VI | U_I |

【그림 1】 보안 등급 행렬

【기호 1】 Li = (Ri, Ci)는 보안 등급 Li의 행렬 상의 위치를 (행, 열)의 형태로 나타낸 것이다. Ri는 Li의 행 번호이고 Ci는 Li의 열 번호이다. (i = 1,2,3 ...)

그림 2에서 사각형이 보안 등급 행렬이라면 보안 등급 행렬상에서는 그림 2와 같은 세 가지 방향의 정보 흐름이 존재한다.

2) 기밀성 보안 모델에서의 보안 등급은 기밀성 등급, 무결성 보안 모델에서의 보안 등급은 무결 성 등급이라 한다. 본 논문 3.3절부터 보안 등급이라 하면 BB 모델에서의 보안 등급을 뜻한다.
3) 원래 보안 등급은 계층적 등급과 범주 집합으로 구성된다. 그러나, 본 논문 이하에서는 범주 집합은 생략하고 계층적 등급을 보안 등급이라고 칭한다.




【그림 2】 보안 등급 행렬에서 정보의 흐름

1) 방향 1 : 행렬의 아래에서 위로

임의의 두 보안 등급, L1과 L2의 열 번호가 동일하고 행 번호가 같거나 다를 때에는 정보가 아래에서 위로 흐른다[4]. 예를 들어서, TS_I, S_I, C_I, U_I는 보안 등급 행렬에서 3열을 이루는 보안 등급들로서 무결성 등급은 I로 동일하고 기밀성 등급에만 차이가 있으므로 기밀성만을 고려하여 정보의 흐름을 제어한다. 따라서, 보안 등급 행렬에서 3열을 구성하는 보안 등급들중 임의의 두 보안 등급사이에서 정보는, BLP 모델의 보안 정책에 따라서 기밀성 등급이 낮은 아래에서 기밀성 등급이 높은 위로 흐른다.

2) 방향 2 : 행렬의 좌에서 우로

임의의 두 보안 등급, L1과 L2의 행 번호가 동일하고 열 번호가 같거나 다를 때에는 정보가 좌에서 우로 흐른다[5]. 예를 들어서, TS_C, TS_VI, TS_I는 보안 등급 행렬에서 1행을 이루는 보안 등급들로서 기밀성 등급은 TS로 동일하고 무결성 등급에만 차이가 있으므로 무결성 등급만을 고려하여 정보의 흐름을 제어한다. 따라서, 보안 등급 행렬에서 1행을 구성하는 보안 등급들중 임의의 두 보안 등급사이에서 정보는, Biba모델의 보안 정책에 따라서 무결성 등급이 높은 좌에서 무결성 등급이 낮은 우로 흐른다.

3) 방향 3 : 행렬의 아래,좌에서 위,우로

임의의 두 보안 등급, L1과 L2이 있다고 하자. 두 보안 등급의 행 번호와 열 번호의 관계는 $R1 < R2$ 이고 $C1 > C2$ 이다. 즉, 보안 등급 행렬상에서 L1이 L2와 비교해서 오른쪽,위에 있을 경우에는 정보가 아래, 왼쪽에서 위, 오른쪽으로 흐른다.[6] 예를 들어서, 보안 등급 행렬에서 L1, L2와 같은 두 개의 보안 등급은 TS_VI와 S_C이다. 기밀성 입장에서는 L1이 더 높은 등급을 소유하고 무결성 입장에서는 L2가 더 높은 등급을 소유한다. 따라서, BLP 모델에 근거하여 정보는 L2(아래,왼쪽)에서 L1(위,오른쪽)으로, Biba 모델에 근거해도 L2(아래,왼쪽)에서 L1(위, 오른쪽)으로 흐른다. 그러므로, 보안 등급 행렬에서 아래,왼쪽에 있는 보안 등급과 위,오른쪽에 있는 두 보안 등급사이에서 정보는 아래,왼쪽에서 위,오른쪽으로 흐른다. 만일 기밀성입장에서 고려한 정보의 흐름과 무결성 입장에서 고려한 정보의 흐름이 다르면 두 보안 등급 사이에는 어떠한 정보의

4) L1의 행 번호가 L2의 그것보다 작다면 즉, L1의 기밀성등급이 L2의 그것보다 높을 경우 S1과 S2의 관계는 $S1 \supseteq S2$ 이다. S1, S2는 L1와 L2의 범주 집합이다. 만일, L1의 행 번호가 L2의 그것보다 작지만, 범주 집합의 관계가 $S1 \supseteq S2$가 아니라면 L1과 L2사이에서 어떠한 정보의 흐름도 있을 수 없다.

5) L1의 열 번호가 L2의 그것보다 작다면 즉, L1의 무결성등급이 L2의 그것보다 높을 경우에 S1과 S2의 관계는 $S1 \supseteq S2$ 이다.S1과 S2는 L1와 L2의 범주 집합이다.만일, L1의 열 번호가 L2의 그것보다 작지만, 범주 집합의 관계가 $S1 \supseteq S2$가 아니라면 L1과 L2사이에서 어떠한 정보의 흐름도 있을 수 없다.

6) L1의 범주 집합과 L2의 범주 집합은 동일하다. L1과 L2의 범주 집합을 S1, S2라 하면, L1의 기밀성 등급이 L2의 그것보다 높기 때문에 $S1 \supseteq S2$이고 L1의 무결성 등급이 L2의 그것보다 낮기 때문에 $S1 \subseteq S2$이다. $S1 \supseteq S2$ 와 $S1 \subseteq S1$ 을 동시에 만족하는 포함계는 $S1 = S2$이므로 두 범주 집합은 동일하다.

흐름도 있을 수 없다.

이와 같이 세 가지 방향으로 정보의 흐름이 존재한다. 이러한 방향은 BLP 와 Biba 모델에서의 정보의 흐름을 모두 고려함으로써 BB 모델이 기밀성과 무결성 모두를 보장하게 한다.

기밀성과 무결성 보장을 위해서, 보안 등급을 소유한 주체는 아래에 있는 보안 정책을 만족할 경우에만 객체로의 접근이 가능하다. 임의의 두 보안 등급 L1(S)와 L2(O)는 각각 주체와 객체의 보안 등급이다.

**BB 모델의 보안 정책**

**보안 정책 1.**

주체 S는 다음의 조건중 하나를 만족할 시에만 객체 O에 대한 판독 연산을 수행할 수 있다.

조건 1) $(R1 \leq R2) \wedge (C2 = C1)$

L1과 L2가 보안 등급 행렬상에서 동일 열상에 위치해 있으면서 주체의 보안 등급, L1이 객체의 보안등급, L2와 같거나 L2보다 위에 있다. 따라서, 그림 2에서 방향 ①에 의해서 주체가 객체를 판독할 수 있다.

조건 2) $(R1 = R2) \wedge (C2 \leq C1)$

L1과 L2가 보안 등급 행렬상에서 동일 행상에 위치해 있으면서 주체의 보안 등급, L1이 객체의 보안등급, L2와 같거나 L2보다 오른쪽에 있다. 따라서, 그림 2에서 방향 ②에 의해서 주체가 객체를 판독할 수 있다.

조건 3) $(R1 < R2) \wedge (C1 > C2)$

L1과 L2가 보안 등급 행렬상에서 L1이 L2보다 오른쪽,위에 있다. 따라서,그림 2에서 방향 ③에 의해서 주체가 객체를 판독할 수 있다.

**보안 정책 2.**

주체 S는 다음의 조건중 하나를 만족할 시에만 객체 O에 대한 갱신연산이 가능하다. 아래에 있는 조건 4,5,6도 보안 정책 1과 유사한 방식으로 설명될 수 있다.

조건 4) $(R1 \geq R2) \wedge (C2 = C1)$

조건 5) $(R1 = R2) \wedge (C1 \leq C2)$

조건 6) $(R1 > R2) \wedge (C1 < C2)$

조건 1)과 조건 4)에서, C1과 C2가 동일한 경우에는 주체와 객체는 동일한 무결성 등급과 다른 기밀성 등급을 소유한다. 이러한 경우는 BLP 모델을 근거로 판독, 갱신 연산을 수행한다. 조건 3)와 조건 5)에서, R1과 R2가 동일한 경우에는 주체와 객체의 기밀성 등급이 동일하고 무결성 등급이 다르기 때문에 Biba 모델을 근거로 판독, 갱신 연산을 수행한다. 조건 3)과 조건 6)에서, R1과 R2가 동일하지 않고 C1과 C2가 동일하지 않은 경우에는 기밀성 입장에서 가능한 연산과 무결성 입장에서 가능한 연산의 교집합이 되는 연산을 수행한다.

이와 같이 BB 모델은 위의 보안 정책을 시행함으로써 정보 보안의 세 가지 목적중 기밀성과 무결성을 동시에 보장하게 된다.

### 3.2 BB 모델 보안 정책의 정확성 증명

BB 모델은 BLP 모델을 통해서 기밀성을, Biba 모델을 통해서 무결성을 보장한다. 따라서, BB 모델 보안 정책의 정확성을 증명하려면 아래에 있는 두 개의 정리를 증명해야 한다. (Li(S), Lj(O) 는 정보의 흐름이 존재하는 주체와 객체의 보안 등급이다.)

【기호 2】 Li = SLi_ILi 는 보안 등급 Li가 기밀성 등급, SLi와 무결성 등급, ILi로 구성되어 있음을 나타낸다. (i = 1,2,3 ...)

【정리 1】 BB 모델의 보안 정책은 보안 등급, Li와 Lj를 구성하는 기밀성 등급, SLi와 SLj만을 고려하여 판독과 갱신 연산을 수행할 시에 하향 판독, 상향 갱신 연산만을 수행한다.

【증명】

BB 모델의 보안 정책 1에서 조건 1, 조건 2, 조건 3을 만족하는 경우에만 주체가 객체에 대해 판독 연산을 수행할 수 있다. 조건 1에서 주체의 보안 등급, Li는 객체의 보안 등급, Lj보다 보안 등급 행렬에서 위에 위치해야만 판독 연산을 수행할 수 있다. 조건 2에서 SLi와 SLj는 동일하므로 주체가 객체에 대해 어떠한 연산을 수행해도 기밀성에는 영향을 미치지 않는다. 조건 3에서 Li은 Lj보다 보안 등급 행렬에서 위에 위치해야만 판독 연산을 수행할 수 있다.

∴ SLi가 SLj보다 높을 경우에만 판독 연산이 가능하다.

BB 모델의 보안 정책 2에서 조건 4, 조건 5, 조건 6을 만족하는 경우에만 주체가 객체에 대해 갱신 연산을 수행할 수 있다. 조건 4에서 주체의 보안 등급, Li는 객체의 보안 등급, Lj보다 보안 등급 행렬에서 아래에 위치해야만 갱신 연산을 수행할 수 있다. 조건 5에서 SLi와 SLj는 동일하므로 주체가 객체에 대해 어떠한 연산을 수행해도 기밀성에는 영향을 미치지 않는다. 조건 6에서 Li은 Lj보다 보안 등급 행렬에서 아래에 위치해야만 갱신 연산을 수행할 수 있다.

∴ SLi가 SLj보다 낮을 경우에만 갱신 연산이 가능하다.

【정리 2】 BB 모델의 보안 정책은 보안 등급, Li와 Lj를 구성하는 무결성 등급, ILi와 ILj만을 고려하여 판독과 갱신 연산을 수행할 시에 상향 판독, 하향 갱신 연산만을 수행한다.

【증명】

BB 모델의 보안 정책 1에서 조건 1, 조건 2, 조건 3을 만족하는 경우에만 주체가 객체에 대해 판독 연산을 수행할 수 있다. 조건 1에서 주체와 객체의 무결성 등급, ILi와 ILj는 동일하므로 주체가 객체에 대해 어떠한 연산을 수행해도 무결성에는 영향을 미치지 않는다.조건 2에서 Li는 Lj보다 보안 등급 행렬에서 오른쪽에 위치해야만 판독 연산을 수행할 수 있다. 조건 3에서 Li은 Lj보다 보안 등급 행렬에서 오른쪽에 위치해야만 판독 연산을 수행할 수 있다. 즉, ILi가 ILj보다 낮을 경우에만 판독 연산을 수행할 수 있다.

∴ ILi가 ILj보다 낮을 경우에만 판독 연산이 가능하다.

BB 모델의 보안 정책 2에서 조건 4, 조건 5, 조건 6을 만족하는 경우에만 주체가 객체에 대해 갱신 연산을 수행할 수 있다. 조건 4에서 주체와 객체의 무결성 등급, ILi와 ILj는 동일하므로 주체가 객체에 대해 어떠한 연산을 수행해도 무결성에는 영향을 미치지 않는다. 조건 5에서 Li는 Lj보다 보안 등급 행렬에서 왼쪽에 있어야만 갱신 연산을 수행할 수 있다. 조건 6에서 Li는 Lj보다 보안 등급 행렬에서 왼쪽에 있어야만 갱신 연산을 수행할 수 있다.

∴ ILi가 ILj보다 높을 경우에만 갱신 연산이 가능하다.

그러므로, BB 모델은 기밀성 입장에서 하향 판독, 상향 갱신만을 무결성 입장에서 상향 판독, 하향 갱신만을 수행한다. 즉, BB 모델은 기밀성과 무결성을 모두 만족한다.

## 4. 기존 모델과의 비교

기밀성만을 보장하는 모델, BLP 와 무결성만을 보장하는 Biba 모델은 접근할 수 있는 정보가 제한적이고 이로 인해 실지로 BLP나 Biba 모델이 시스템으로 구현되어 사용되는 응용 분야도 제한적이다. BB 모델은 먼저 보안 모델이 접근할 수 있는 정보의 범위를 기존의 것들보다 훨씬 넓히고 나아가서 보안 모델이 실질적으로 사용되는 응용 분야도 넓힌다.

### 4.1 BLP 모델

| TS_C | TS_VI | TS_I |
|---|---|---|
| S_C | S_VI | S_I |
| C_C | C_VI | C_I |
| U_C | U_VI | U_I |

【그림 3】 BLP 모델(Biba)을 구현한 시스템의 주체와 객체에 지정되는 보안 등급

BLP 모델은 군사 정보 시스템에서 기밀성이 있는 정보를 다루는 대표적인 보안모델이다.그러나, 기밀성이 있는 모든 정보를 다루는 것에는 한계가 있다.

BLP 모델을 구현한 보안 시스템, SYS는 그림 3에서 하나의 열을 구성하는 보안 등급만 주체와 객체에 지정할 수 있다. 예를 들어서, SYS가 소유하는 보안 등급으로 이루어진 리스트, L이 있다고 하자. L을 (TS_C,S_C,C_C,U_C)라 하면 SYS는 TS_C, S_C, C_C, U_C만을 주체와 객체에 지정한다. 실지로 BLP 모델의 보안 정책은 L이 유지하는 보안 등급이외의 다른 보안 등급을 소유한 객체를 다룰 수 없다. 예를 들어서, SYS에서 TS_C를 보안 등급으로 소유하는 주체, S가 보안 등급이 C_VI인 객체, O로의 접근 시도한다고 하자. 주체는 S는 BLP 모델의 보안 정책에 따라서 O를 판독할 것이다. 그러나, O를 판독하면 S는 정확하지 못한 값을 판독해서 S와 동일한 보안 등급을 지닌 객체, O1을 갱신함으로써 O1의 무결성을 파괴할 수 있다. 이러한, BLP 모델이 처리할 수 있는 기밀성 정보에는 한계가 있다. 그러나, BB 모델을 구현한 시스템을 구성하는 주체와 객체에게는 그림 3에 있는 모든 보안 등급이 지정될 수 있다. 그림 3에서 색칠한 하나의 열은 BLP가 다룰 수 있는 보안 등급이 BB 모델이 다룰 수 있는 보안 등급의 1/3에 불과함을 보이고 있다.

### 4.2 Biba 모델

Biba 모델도 무결성 보장을 위한 모델임에도 불구하고 무결성이 있는 모든 정보를 다루는 것에는 한계가 있다. Biba 모델을 구현한 보안 시스템, SYS는 그림 3에서 하나의 행을 구성하는 보안 등급만을 주체와 객체에 지정한다. 예를 들어서, 시스템, SYS가 소유하는 보안 등급으로 이루어진 리스트, L이 있다고 하자. L을 (TS_C,TS_VI,TS_I)라 하면 SYS는 TS_C, TS_VI, TS_I만을 주체와 객체 지정한다. 실지로 Biba 모델의 보안 정책은 L이 유지하는 보안 등급이외의 다른 보안 등급을 소유한 객체를 다룰 수 없다. 예를 들어서, SYS에서 TS_C를 보안 등급으로 소유하는

주체, S가 보안 등급이 S_VI인 객체, O로의 접근 시도한다고 하자. 주체는 S는 Biba의 보안 정책에 따라서 O를 갱신할 수 있다. 그러나, 이러한 갱신 연산은 기밀성 입장에서 S가 하향 갱신 연산을 수행하는 것이 되므로 기밀성이 있는 정보가 유출될 수 있다. 즉, Biba 모델에서의 보안 정책은 기밀성 등급을 전혀 고려하지 않으므로 그림 3에서 하나의 행에 해당하는 보안 등급만을 다룰 수밖에 없다. 그러나, BB 모델을 구현한 시스템을 구성하는 주체와 객체에게는 그림 3에 있는 모든 보안 등급이 지정될 수 있다. 그림 3에서 색칠한 하나의 행은 Biba가 다룰 수 있는 보안 등급이 BB 모델이 다룰 수 있는 보안 등급의 1/3에 불과함을 보이고 있다.

이와 같이 BB 모델은 기존의 보안 모델과 비교하여 제어할 수 있는 정보의 법위가 넓다. 이로 인해 실제로 사용되는 응용 분야도 기존의 보안 모델보다는 훨씬 넓힐 수 있다.

## 5. 결론 및 이후 연구 방향

시간이 흐를수록 늘어나는 정보의 홍수속에서 기밀성과 함께 무결성이 요구되어지는 정보가 생겨 났다. 본 논문에서는 응용 분야를 군사 및 군사 관련된 분야로 놓고 기밀성과 무결성을 동시에 고려하는 보안 모델을 제시했다. 기존의 보안 모델, BLP와 Biba는 각각 기밀성과 무결성을 보장한다. 그러나, BLP 모델은 무결성을 거의 고려하지 않기때문에 기밀성이 있는 데이타를 다루는 것에 한계가 있고 Biba도 이와 유사한 문제점이 있다. 하지만, 두 개념을 동시에 고려하는 BB 모델은 두 모델의 결합을 통해서 BLP모델을 통해서 기밀성을, Biba 모델을 통해서 무결성을 고려한다. 이렇게 함으로써 기존의 보안 모델에서 처리 불가능인 정보의 처리가 가능해졌다. 기존의 보안 모델을 결합하는 방법을 사용함으로써 이미 구현되어 있는 시스템의 일부는 현 그대로 사용할 수 있게 하였다.

## 참고 문헌

[1] Ravi S. Sandhu, "Lattice-Based Access Control Models", IEEE, Computer, Volume 26, Number 11, November 1993.

[2] David D. Clark and David R. Wilson, "A Comparison of Commercial and Military Computer Security Policies", Proc. 1987 Symposium on Security and Privacy, April 1987.

[3] Ravi Sandhu, "TRANSACTION CONTROL EXPRESSIONS FOR SEPARATION OF DUTIES", Fourth Computer Security Application Conference, 1988.

[4] Ravi S. Sandhu and Edward J. Coyne, "Role-Based Access Control Models", IEEE, Computer, Volume 29, Number 2, February, 1996.

[5] Phil Terry and Simon Wiseman, "A 'New' Security Policy Model", IEEE Symposium on Security and Privacy, 1989.

[6] Ravi S. Sandhu, "On Five Definitions of Data Integrity", Database Security, Ⅶ, 1994.

[7] Silvana Castano, Maria Grazia Fuggini, Giancario Martella, Pierangela Samarati, DATABASE SECURITY, ACM press.

[8] Edward G. Amoroso, FUNDAMENTALS OF COMPUTER SECURITY TECHNOLOGY, PTR Prentice Hall.

[9] Ravi Sandhu, "MANDATORY CONTROLS FOR DATABASE INTEGRITY", Proc.of the WG 11.3 Workshop on Database Security, 1989.

[10] Lee, T.M.P., "Using Mandatory Integrity to Enforce 'Commercial' Security", Proc. 1988 IEEE Symposium on Security and Privacy Okland CA., April,1988.