김일성종합대학학보
정보과학

주체109(2020)년
제66권 제4호

자료기지관리체계에서 행표식보안을 리용한 강제접근조종의 한가지 방법

최 성 란

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《우리의 과학연구사업은 자립적민족경제의 위력을 충분히 발휘하도록 하는데 이바지하는 과학연구사업으로 되여야 하며 과학연구성과들은 현실에 제때에 도입되여야 합니다.》

자료기지보안을 위해서는 기밀성(confidentiality), 완전성(Integrity), 유용성(Availability)의 요구를 만족시켜야 한다.[1] 이를 위하여 접근조종기술을 리용한다.

자료기지관리체계에서의 접근조종방법에는 자유접근조종(Discretionary Access Control)과 강제접근조종(Mandatory Access Control), 역할에 기초한 접근조종(Role Based Access Control)이 있다.[2]

자유접근조종은 사용자준위의 접근조종으로서 자원의 소유자가 접근권한을 임의로 변경시킬수 있으며 접근조종행렬모형에 기초하고있으므로 잠복통로를 통한 정보의 루설을 막지 못하여 보안에서 기밀성이 파괴되는 약점이 있다.

한편 강제접근조종은 체계준위의 접근조종으로서 자원의 소유자가 허가권을 임의로 변경시킬수 없다. 또한 주동체에는 허가등급을 할당하고 객체에는 보안등급을 할당한데 기초하여 정보흐름을 정확히 조종하므로 잠복통로를 통한 정보의 루설을 막을수 있다.

그리고 역할에 기초한 접근조종은 자유 및 강제접근조종의 결합으로 리용되고있다.

론문에서는 자유접근조종이 구현되여있는 MySQL자료기지관리체계에서 강제접근조종을 구현하기 위한 한가지 보안방책을 제안하였다.

1. 제안된 행표식보안방책

강제접근조종에서는 객체와 사용자에게 각각 보안등급과 허가등급을 매기고 등급들사이의 부분순서관계에 의하여 접근조종을 진행한다.

이로부터 론문에서는 표의 1개 행을 객체로 설정하고 강제접근조종을 실현함으로써 행준위로 접근조종을 진행한다.

사용자가 표에서 자료를 읽거나 쓸 때 자료기지관리체계는 먼저 자유접근조종에 의하여 그 표에 대한 접근권한이 있는가를 검사한 다음 강제접근조종에 의하여 접근하려고 하는 행에 대한 접근권한을 검사한다. 따라서 행에는 자료외에 표식이 붙으며 표에는 표식마당이 첨가된다. 이것을 행표식이라고 부르며 이에 기초한 보안을 행표식보안(row label security)이라고 부른다.

이제 행표식보안방책(Row Label Security Policy)을 정의하자.

행표식보안방책은 구성요소들과 보안프로화일, 보안표식, 보호되는 표(또는 보안방책이 적용되는 표)들로 이루어진다.

매 구성요소들은 준위, 구분, 모임이라고 부르는 요소들로 이루어진다.

한편 사용자는 보안프로화일을 할당받게 되며 보호되는 표의 매 행들은 보안표식으로 표식되는데 이것은 준위, 구분, 모임의 요소값쌍으로 되여있다.

행표식보안은 USERS, PROFILES, LABELS, OBJECTS를 비롯한 10개의 기초요소와 11개의 관계들로 이루어진다.

제안한 행표식보안방책의 구조는 그림과 같다.

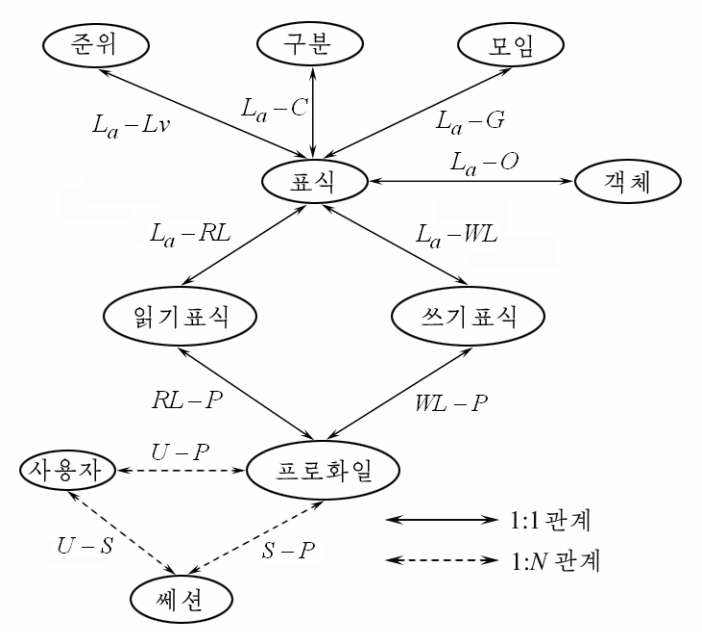

그림. 행표식보안방책의 구조

2. 행표식보안방책의 모형화

1) 구성요소

구성요소는 준위, 구분, 모임으로 표현되는데 이것을 정식화하면 다음과 같다.

① 준위(Levels)

준위는 보안방책에서 보안등급이나 허가등급을 의미한다.

$$Lv=\{lv_i \mid i=\overline{1,\ n}\} \tag{1}$$

여기서 $i<j$이면 $lv_i<lv_j$이고 lv_i는 자료와 주동체(프로화일)의 순위이다. 그리고 n은 보안방책에서 리용되는 준위의 총 개수이다.

② 구분(Compartments)

구분은 정보를 구분하는 역할을 수행한다.

$$C=\{c_i \mid i=\overline{1,\ m}\} \tag{2}$$

여기서 $i\neq j$이면 $c_i\neq c_j$이고 c_i는 접근이 발생할 때 배타적인 포함관계를 요구하는 자료의 종류이다. 그리고 m은 보안방책에서 리용되는 구분의 총 개수이다.

③ 모임(Groups)

$$G=\{g_i,\ gp_i \mid i=\overline{1,\ k},\ \ gp_1=\phi\ \} \tag{3}$$

여기서 $gp_i \in \{(g_p) \mid p = \overline{1,\ k}\}$ 이고 $i \neq j$ 이면 $g_i \neq g_j$ 이다. 그리고 g_i 는 하나의 모임을 나타내고 gp_i 는 g_i 의 부모를 나타낸다. k 는 보안방책에서 리용되는 모임의 총 개수이다.

모임은 자료의 계층구조를 표현한다.

2) 표식

$$La = \{la_i \mid i = \overline{1,\ n}\} \tag{4}$$

여기서 $la_i = (lv_k^i,\ C$의 부분모임, $g_t^i)$ 이다.

이때 표식들사이 반순서관계는 다음과 같다.

$$la_i \le la_j \Leftrightarrow lv_i \le lv_j,\ c_i \le c_j,\ g_i \le g_j \tag{5}$$

$$la_i \ge la_j \Leftrightarrow lv_i \ge lv_j,\ c_i \ge c_j,\ g_i \ge g_j \tag{6}$$

3) 프로화일과 사용자

① 프로화일을 정의하면 다음과 같다.

$$P = \{p_i \mid i = \overline{1,\ n}\} \tag{7}$$

여기서 $p_i = (p\_name,\ RL_{\text{def}},\ RL_{\max},\ RL_{\min},\ WL_{\text{def}},\ WL_{\max},\ WL_{\min},\ RO_{\text{def}})$ 이며 p_name 은 프로화일의 이름, RL_{def} 는 표준읽기표식, $RL_{\max}$ 는 최대읽기표식값, $RL_{\min}$ 은 최소읽기표식값, WL_{def} 는 표준쓰기표식, $WL_{\max}$ 는 최대쓰기표식값, $WL_{\min}$ 은 최소쓰기표식값, RO_{def} 는 표준행표식이다.

이 프로화일요소값들은 다음의 조건을 만족시킨다.

$$RL_{\max} \ge RL_{\min}$$
$$RL_{\max} \ge RL_{\text{def}} \ge RL_{\min}$$
$$WL_{\max} \ge WL_{\min}$$
$$WL_{\max} \ge WL_{\text{def}} \ge WL_{\min}$$
$$WL_{\max} \ge RO_{\text{def}} \ge WL_{\min}$$

② 사용자는 다음과 같이 정의한다.

$$U = \{u_i \mid i = \overline{1,\ n}\} \tag{8}$$

여기서 $u_i = (name,\ host,\ p\_name)$ 이다.

4) 표와 기록

① 행표식보안방책이 적용된 표의 구조도식은 다음과 같다.

$$S = (REL_{\text{name}},\ F_{\text{inf}}) \tag{9}$$

여기서 REL_{name} 은 행표식보안방책이 적용된 표의 이름이다. 그리고 F_{inf} 는

$$S = \{REL_{\text{name}},\ F_{\text{inf}}\} = \{(fn_i,\ fd_i,\ F_{rla},\ \text{int}) \mid i = \overline{1,\ N}\}$$

으로서 fn_i 는 i 번째 마당의 이름, fd_i 는 i 번째 마당의 정의역, F_{rla} 는 표식마당이다.

② 행표식보안방책이 적용된 표의 실체(기록들의 모임)는 다음과 같이 정의한다.

$$SI = \{r_i \mid r_i = (f_{v_1}^i,\ f_{v_2}^i,\ \cdots,\ f_{v_N}^i,\ f_{rlb}^i)\},\ f_{v_k}^i \in fd_k,\ fd_k \in S,\ i = \overline{1,\ M},\ k = \overline{1,\ N} \tag{10}$$

여기서 r_i 는 i 번째 기록(행), $f_{v_k}^i$ 는 i 번째 기록의 k 번째 마당의 값, f_{rlb}^i 는 i 번째 기록의 표식마당값, M 은 기록모임의 원소수(농도)이다.

기록모임에서 매 기록은 구조도식에서 정의된데 따라 동일한 개수의 마당으로 구성

된다.

5) 보안방책

보안방책은 다음과 같이 정의한다.

$$Po = (U,\ P,\ La,\ C,\ O) \tag{11}$$

우와 같은 모형화에 기초하여 자료의 읽기와 쓰기는 다음과 같이 진행한다.

우선 자료의 읽기는 다음의 식들을 만족하는 경우에 허가된다.

어떤 사용자의 프로화일표식 p_i: $WL_{\min}$을 la_i라고 할 때

$$la_i = (l_{k1}^i,\ c_{p1}^i,\ g_{t1}^i)$$

이고 접근하려는 j번째 기록의 표식마당값을

$$f_{rla}^j == la_j = (l_{k2}^j,\ c_{p2}^j,\ g_{t2}^j)$$

이라고 하자. 이때

① $l_{k1}^i \geq l_{k2}^i$

② $c_{p1}^i = \phi$이면 $c_{p2}^j = \phi$이고 그렇지 않으면 $c_{p1}^i = c_{p2}^j$ 혹은 $c_{p2}^j = \phi$이다.

③ $g_{t1}^i \supseteq g_{t2}^j$

를 만족하면 사용자는 기록을 읽을수 있다.

다음 자료의 쓰기는 다음의 식들을 만족하는 경우에 허가된다.

어떤 사용자의 프로화일 p_i: $WL_{\max}$를 la_i라고 할 때

$$la_i = (l_{k1}^i,\ c_{p1}^i,\ g_{t1}^i)$$

이고 쓰기하려는 j번째 기록의 표식마당값을

$$f_{rla}^j == la_j = (l_{k2}^j,\ c_{p2}^j,\ g_{t2}^j)$$

이라고 하자. 이때

① $l_{k1}^i \leq l_{k2}^i$

② $c_{p1}^i = \phi$이면 $c_{p2}^j = \phi$이고 그렇지 않으면 $c_{p1}^i = c_{p2}^j$ 혹은 $c_{p2}^j = \phi$이다.

③ $g_{t1}^i \subseteq g_{t2}^j$

를 만족하면 사용자는 기록을 추가하거나 변경시킬수 있다.

맺 는 말

행표식보안방책을 MySQL자료기지에 추가하여 강제접근조종을 구현하기 위한 한가지 방법을 제기함으로써 MySQL자료기지에서 권한없는 불순한 사용자가 권한있는 사용자의 비밀자료를 절취할수 있는 보안취약성을 완전히 극복하고 자료기지의 보안을 담보할수 있게 하였다.

참 고 문 헌

[1] Akshay Patil et al.; International Journal of Engineering Research and Applications, 2, 3, 2248, 2012.

[2] Bertino Elisa et al.; IEEE Transactions on Dependable and Secure Computing, 2, 1, 369, 2005.

주체109(2020)년 8월 5일 원고접수

A Method of Access Control Using Row Label Security in DBMS

Choe Song Ran

In this paper we suggested a security policy in MySQL that contained discretionary access control to implement mandatory access control and enabled it to assure the security of database.

Keywords: mandatory access control, privilege, row label security policy