Доступ к файлам как частный случай доступа к разделяемым ресурсам

Многоуровневая (мандатная) модель доступа

Многоуровневая модель доступа

Объекты многоуровневой модели имеют различные уровни доступа, а субъекты – степени доступа. Владельцы объектов лишены возможности управлять доступом к ним по своему усмотрению. Членам какой-либо группы не разрешается предоставлять свои права членам групп более низких уровней иерархии доступа.

Особенности многоуровневой модели доступа:

1. Данные могут передаваться субъектом самому себе.
2. Данные могут передаваться от субъекта A к субъекту C, если они могут передаваться от субъекта A к субъекту B и от B к C.

Особенности многоуровневой модели доступа:

3. Если X не больше У и У не больше X, то X=У.

Эти правила представляют свойства рефлективности, транзитивности и асимметричности.

Многоуровневая модель доступа

Многоуровневая модель доступа в современных системах защиты реализуется через мандатный контроль или мандатную политику.

Многоуровневая модель доступа

Монитор обращения - подсистема мандатного контроля, удовлетворяющая некоторым требованиям.


Объект: O
обладает
Функцией: c(O)
Субъект
имеет
Метку: S
содержит
Класс доступа: c(S)
Мандатный контроль сравнивает метки
C(S) > C(O)
Да
Нет
Субъект S может произвести чтение объекта O
Субъект S может произвести запись в объект O
Конец

Свойства многоуровневой модели доступа

- Многоуровневая модель доступа устойчива к атакам троянским конем;
- Такая модель создана, в основном, для сохранения секретности информации;
- Вопросы целостности при помощи этой политики не решаются или решаются как побочный результат защиты секретности.

Модель Белла – Лападулы

Модель состоит из следующих элементов:

- S – множество субъектов (пользователи системы и программы);
- O – множество объектов системы (все системные файлы);

Модель Белла – Лападулы

- G – множество прав доступа {*read (r), write(w), execute (e), append (a)*};
- B - список текущего доступа;
- Z - список запросов;
- L – уровни секретности.

Модель Белла – Лападулы

Каждому субъекту s принадлежащему S, сопоставляются два уровня защиты:

- базовый $L_s(S_i)$ принадлежащий множеству L, задаваемый в начале работы и остающийся неизменным;
- текущий $L_t(S_i)$ принадлежащий множеству L, зависящий от уровней защиты тех объектов, к которым субъект S_i имеет доступ в настоящий момент времени.

Каждому объекту O_j приписывается уровень защиты $I(O_j)$, принадлежащий множеству L.

Модель Белла – Лападулы

- Множество прав доступа G имеет вид

G{r,a,w,e},

где r – чтение объектом субъекта;

a – модификация данных объекта субъектом без предварительного прочтения;

w – запись-модификация данных после их предварительного прочтения;

e – исполнение субъектом объекта.

Модель Белла – Лападулы

Список текущего доступа b содержит записи вида:

$$(S_i, O_j, X)$$

Если субъекту S_i разрешен доступ $x \in G$ к объекту O_j и это разрешение к настоящему моменту времени не отменено.

Разрешение доступа действительно до тех пор, пока субъект не обратится с запросом на отказ от доступа к монитору.

Модель Белла – Лападулы

Список запросов Z описывает возможности доступа субъекта к объекту, передачи прав доступа другим субъектам, создания или уничтожения объекта.

Модель Белла – Лападулы

В модели рассматриваются 11 следующих запросов:

1) запрос на чтение (r) объекта;

2) запрос на запись (w) в объект;

3) запрос на модификацию (a) объекта;

Модель Белла – Лападулы

11 запросов списка запросов Z :

4) запрос на исполнение (e) объекта;

5) запрос на отказ от доступа;

6) запрос на передачу доступа к другому объекту;

7) запрос на лишение права доступа другого субъекта;

Модель Белла – Лападулы

11 запросов списка запросов Z :

8) запрос на создание объекта без сохранения согласованности;

9) запрос на создание объекта с сохранением согласованности;

10) запрос на уничтожение объекта;

11) запрос на изменение своего текущего уровня защиты.

Модель Белла – Лападулы

Сформулированы два условия защиты для модели:

- простое условие защиты;
- комплексное условие защиты.

Модель Белла – Лападулы

Простое условие защиты предложено для исключения прямой утечки секретных данных и накладывает ограничения на базовые уровни защищенных объектов.

Модель Белла – Лападулы

Комплексные условия защиты предназначены для предотвращения косвенной утечки данных.

Это условие накладывает ограничения на уровни защиты тех объектов, к которым субъект может иметь доступ одновременно.

Модель Белла – Лападулы

Для обеспечения безопасности данных необходимо и достаточно, чтобы изменения состояния системы приводило только к безопасным состояниям, если исходное состояние было безопасным.

Правила выполнения каждого из 11 возможных запросов в модели:

- а) Запрос на чтение субъектом Si объекта Oj разрешается, если выполняется условие $R \in Mij$ V $Is(Si) \geq I(Oj)$ V $It(Si) \geq I(Oj)$;
- б) Запрос на запись субъектом Si в объект Oj разрешается, если выполняется условие $W \in Mij$ V $Is(Si) \geq I(Oj)$ V $It(Si) = I(Oj)$;
- в) Запрос на дополнение субъектом Si объекта Oj разрешается, если выполняется условие $A \in Mij$ V $It(Si) \leq I(Oj)$;
- г) Запрос на исполнение субъектом Si объекта Oj разрешается, если e принадлежит Mij;
- д) Отказ субъекта Si от доступа x принадлежит G к объекту разрешается безусловно;

Правила выполнения каждого из 11 возможных запросов в модели:

- е) Передача субъекту Sk субъектом Si права на доступ x к объекту Oj разрешается, если субъект Sk имеет доступ w к «отцу» Os(j) объекта Oj;
- ё) Лишение субъекта Sk субъектом Si права на доступ x к объекту Oj разрешается, если субъект Sk имеет доступ w к "отцу" Os(j) объекта Oj;
- ж) Создание субъектом Si объекта Ot(j) с уровнем защиты l, являющегося "сыном" объекта Oj, разрешается, если список текущего доступа b содержит записи: Si, Oj, w или Si, Oj, a;
- з) Создание субъектом Si объекта Ot(j) с уровнем защиты l, являюшегося "сыном" объекта Oj, с сохранением согласованности разрешается, если список текущего доступа b содержит записи: Si Oj w или Si Oj a или l больше l(Oj);

- и) Уничтожение субъектом Si объекта Oj (и всех объектов Oj1,Oj2,...Ojk, являщихся «последователями» по структуре дерева) разрешается, если субъект Si имеет доступ w к "отцу" Os(j) объекта Oj, и отвергается - в противном случае. Изменение состояния системы происходит следующим образом: из списка текущего доступа b удаляются все записи, содержащие объекты Oj1,Oj2,...Ojk; из матрицы M удаляются столбцы с номерами j1,j2,...jk;

- к) Изменение субъектом Si своего текущего уровня защиты It(Si) на It' разрешается, если выполняются условия:
  - Is(Si) не меньше It';
  - It' не больше I(Oj), если субъект Si имеет доступ a к какому-либо объекту O;
  - It' равно I(Oj), если субъект Si имеет доступ w к какому-либо объекту Oj;
  - It' не меньше I(Oj), если субъект Si имеет доступ r к какому-либо объекту Oj.
  - Во всех остальных случаях запрос отвергается.

Монитор обработки рассмотренных 11 запросов, созданный на основе модели Белла и Лападулы, был реализован в виде программно-аппаратного ядра защиты ОС Multics.