УДК 004.056.52

Е. В. ГОРКОВЕНКО

ФОРМАЛИЗОВАННОЕ ПРЕДСТАВЛЕНИЕ МЕХАНИЗМОВ ЗАЩИТЫ ПРИ МАНДАТНОМ РАЗГРАНИЧЕНИИ ДОСТУПА

Сформулированы правила и условия выполнения запросов при мандатном разграничении доступа для защищенного состояния вычислительной системы.

Мандатное управление контролем доступа, реализующее полномочную политику безопасности, есть разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. В информационных системах, в которых хранится и обрабатывается критичная информация, политика безопасности основывается на мандатной (или многоуровневой) политике безопасности (МПБ).

Основой многоуровневой политики является решетка ценностей. Политика МПБ считает информационный поток между двумя произвольными объектами X (источник) и Y (получатель) разрешенным тогда и только тогда, когда Y секретнее, чем X. Хотя МПБ делит множество информационных потоков в системе на разрешенные и неразрешенные очень простым условием, эта простота касается огромного количества информационных потоков в системе.

Основная теорема безопасности, доказанная Беллом и Лападуллой, гласит [1], что система будет безопасной, если при переходе из одного состояния в другое не будут нарушены два основных свойства:

свойство простой безопасности (ss-свойство): субъект может только читать объект, если класс доступа субъекта доминирует под классом доступа объекта; другими словами, субъект может читать "вниз", но не может читать "вверх";

свойство ограничения (*-свойство): субъект может только записать в объект, если класс доступа субъекта доминируется классом доступа объекта; субъект может записывать "вверх", но не может записать "вниз".

Несмотря на все достоинства, оказалось, что при использовании модели Белла и Лападула возникает ряд таких технических вопросов, как определение статуса удаленного чтения; определение прав доступа доверенного объекта типа «администратор»; несанкционированная «деклассификация» объекта. Перечисленные ситуации могут привести к «нарушению» безопасного состояния многоуровневой системы доступа, если ориентироваться только на выполнение правил доступа, описанных в [2]. Корректный статус удаленного чтения должен быть реализован через процедуру надежной аутентификации удаленного объекта. Также необходимо расширить список правил разграничения доступом.

Организация мандатного контроля осуществляется через понятия уровня секретности объекта и степени доверия субъекта.

Контроль полномочий доступа, подразумевающий передачу полномочий доступа между субъектами, имеет особенности в соответствии с принятыми в нашей стране процедурами работы с информацией ограниченного пользования. Это накладывает ряд ограничений при формировании правил разграничения доступа и управлении матрицей прав доступа. В предлагаемой модели мандатного разграничения доступа реализованы расширенный список прав доступа и управление доступом с учетом права реализации.

Основными элементами математической модели многоуровневой защиты являются:

множество субъектов $S=\{s_1, s_2, \ldots, s_{m^*}\}$, $j=\overline{1,m^*}$;

множество объектов $O=\{o_1, o_2, \ldots, o_{n^*}\}$, $i=\overline{1,n^*}$;

множество уровней защиты $J=\{j_1, j_2, \ldots, j_L;\}$, $l=\overline{1,L}$;

множество видов доступа и управления ими $A=\{a_1 a_2, \ldots, a_K\}$, $k=\overline{1,K}$;

матрица прав доступа $M=\|m_{ij}\|$, $i=\overline{1,n^*}$, $j=\overline{1,m^*}$,

список текущего доступа $B=\{b_t\}=(s_j, o_i, a)$, $a\in A$;

список запросов $R=\{r_n, n=\overline{1,N}\}$.

Пусть множество объектов $O=\{o_1, o_2, \ldots, o_n\}$ – конечное множество $i=\overline{1,n}$. Объекты как пассивные носители информации могут быть сгруппированы по типам $T(o_t)$, $t=\overline{1,n}^*$. Примеры типов групп объектов: файлы, директории, базы данных, сообщения.

Каждый объект имеет определенный уровень защиты, который соответствует уровню секретности информации, хранящейся в объекте o_i, такому, как «особой важности», «совершенно секретно», «секретно», «ДСП», «конфиденциально», «персональные данные», «для общего пользования». Под уровнем секретности понимают иерархический атрибут, который ассоциирован с сущностью компьютерной системы для обозначения степени ее критичности в смысле безопасности. Это может обозначать степень ущерба от нарушения безопасности в компьютерной системе, или чувствительность — характеристика ресурса, которая определяет его ценность или важность и может учитывать его уязвимость.

Каждому объекту $o_i \in O$ присваивается уровень защиты объекта $J(o_t)$, постоянный для данного объекта. Назовем его базовым $J_b(o_i)$. Он остается неизменным все время существования объекта o_i, вплоть до его уничтожения. В случае изменения статуса хранимой информации, например при понижении уровня секретности информации, вследствие естественного старения информации, базовый уровень объекта также может измениться (понизиться).

Наделим также каждый объект o_i переменным (текущим) уровнем защиты $J_p(o_t)$ на тот случай, когда в процессе функционирования вычислительной системы объект o_i (программа, подпрограмма и т.п.) привлекается субъектом s_j в качестве своего подсубъекта. В этом случае объекту o_i приписывается уровень защиты субъекта s_j, т.е. $J_p(o_t)=J_b(o_t) \cup J(s_j)$, $i \in I$, $j \in J$, где J – множество индексов $\{j \setminus j=1,2,\ldots,m^*\}$ или $J_p(o_t): J(s_j) \to J_b(o_t)$, где $\to$ оператор присвоения. Последнее целесообразно, если $J(s_j) > J_b(o_t)$.

Каждый объект может быть представлен в виде следующей записи:

$$(o_i, s_j, \lambda_j, J_b(o_t)),$$

где o_i – шифр объекта, s_j – шифр субъекта, создавшего объект (владелец o_i), λ_j – классификация субъекта, $J_b(o_t)$ – уровень защиты объекта.

Множество объектов можно наделить структурой дерева. Древовидная структура объектов защиты реализуется через иерархию *прав владения* субъектов объектами. Обозначим соответственно $F(o_i)$ – «отец» объекта o_i, и множество «сыновей» объекта o_i как $H(o_t)=(o_{i1}, o_{i2}, \ldots, o_{ie})$. Формирование древовидной структуры объектов выходит за рамки данной статьи.

Пусть множество субъектов $S=\{s_1, s_2, \ldots, s_m\}$ – конечное частично упорядоченное множество элементов. Каждому субъекту s_j приписывается определенный уровень защиты $J(s_j)$, $j \in J$, остающийся неизменным все время функционирования системы или все время существования субъекта вплоть до лишения его всех прав доступа к объектам системы. Каждый элемент множества $s_j \in S$ представляется парой $\{\lambda_j, \mu_j\}$, где $\{\lambda_j\}$ – конечное множество классификаций субъектов, $\{\mu_j\}$ – конечное множество категорий допуска. Степень доверия — это атрибут, определяющий уровень секретности субъекта. Чем выше степень доверия (категория допуска) субъекта, тем к более секретной информации он имеет доступ. Чем выше секретность объекта, тем более секретная информация хранится в нем. Примеры классификации типов субъектов: куратор проекта, научный руководитель проекта, ответственный исполнитель проекта, гость. Примеры категорий допуска субъектов: 1-я форма допуска, 2-я форма допуска, 3-я форма допуска, для служебного пользования, для общего пользования и т.д.

Множество субъектов наделено структурой дерева: каждому субъекту s_j соответствует список субъектов, непосредственно следующих за ним ("сыновей") и, если субъект $s_j \in S$ отличен от корня дерева s_k, ему соответствует единственный субъект $s_{g(j)}$, непосредственно предшествующий этому субъекту s_j ("отец" субъекта s_j). Обозначим соответственно $F(s_j)$ – «отец» субъекта s_j и множество «сыновей» субъекта s_j как $H(s_j)=(s_{j1}, s_{j2}, \ldots, s_{je})$. Формирование древовидной структуры субъектов выходит за рамки данной статьи.

При этом уровень защиты субъекта s_{j1} выше уровня защиты s_{j2}, т.е. $J(s_{j1}) > J(s_{j2})$, если

1) $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$;
2) $\lambda_{j1} > \lambda_{j2}$, $\mu_{j1} = \mu_{j2}$;
3) $\lambda_{j1} > \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$;
4) $\lambda_{j1} < \lambda_{j2}$, $\mu_{j1} > \mu_{j2}$.

Последнее условие – это особый случай. Уровни защиты субъектов будут равны, т.е.

$J(s_{j1}) = J(s_{j2})$, если $\lambda_{j1} = \lambda_{j2}$, $\mu_{j1} = \mu_{j2}$. Это может иметь место лишь для различных ветвей дерева субъектов, когда субъекты находятся на одной горизонтали, при этом субъекты s_{j1}, $s_{j2} \in S(^1)$ будут относиться к одной подгруппе пользователей с одинаковыми правами доступа.

Будем рассматривать множество S как объединение двух подмножеств $S(^1)$ и $S(^2)$: $S = S(^1) \cup S(^2)$, где $S(^1)$ – подмножество субъектов, имеющих право подписи документов (владельцы объектов), право переписки, право на разрешение доступа к объектам и право ликвидации доступа; $S(^2)$ – подмножество субъектов, не имеющих таких прав.

Каждый субъект может быть представлен в виде следующей записи:

$$(s_j,\ \lambda(s_j),\ J(s_j)),$$

где s_j – шифр субъекта, $\lambda(s_j)$ – его классификация, $J(s_j)$ – уровень защиты субъекта, аналогичный категории допуска μ_j.

Множество уровней защиты J – это конечное упорядоченное множество элементов j_1, j_2, …, j_L: $j_1 > j_2 > \ldots > j_k$. Множество J изоморфно множеству категорий допуска, т.е.

$$\{j_l\} \xrightarrow{is} \{\mu_j\}.$$

С каждой категорией допуска к работам и документам с грифами «особой важности», «совершенно секретно», «секретно», «для служебного пользования», «конфиденциально» соотнесем 5 уровней защиты соответственно. Тогда $J = \{j_k \mid k = \overline{1,5}\}$.

Матрица прав доступа $M = \|m_{ij}^*\|$ – это прямоугольная матрица размерности $m \times n$, каждый элемент m_{ij} которой содержит список видов доступа субъекта $s_j \in S$, $j = \overline{1,m}$, к объекту $o_i \in O$, $i = \overline{1,n}$, на которые он может претендовать и которые ему в данный момент разрешены. Предполагается, что матрица не содержит пустых столбцов, так как при наличии таковых матрица может быть сокращена: $M \setminus \{o_i\}$, $i = \overline{1,n}$. Если матрица содержит пустые строки, это означает, что в данный момент субъекту s_j запрещены все виды доступа ко всем объектам $o_i \in O$, $\forall_i \in I$, которые содержатся в матрице прав доступа.

Каждый элемент $m_{ij} \in M(i,j)$ представляет особый кортеж

$$(s_\nu, a_1, a_2, \ldots, a_n),$$

где $s_\nu \in S^{(1)}$ – шифр субъекта, разрешившего субъекту s_j доступы $a_1, a_2, \ldots, a_n$ к объекту o_i. Если имела место последовательность передачи прав доступа:

$$\lambda_\nu > \lambda_{j1} > \lambda_{j2} > \ldots > \lambda_{jk},$$

то первая компонента кортежа – шифр первого субъекта последовательности, а именно субъекта s_ν.

Множество видов доступа $A = \{a_1, a_2, \ldots, a_K\}$ субъектов к объектам защиты, состоящее из следующих элементов: R – чтение; G – перезапись информации из объекта в объект; D – добавление информации в объект, без предварительного чтения; W – запись, после предварительного чтения; E – исполнение команды; O – отказ в выполнении запроса и видов управления доступом, таких, как C – создание объекта, U – уничтожение объекта, L – лишение прав на доступ, P – передача прав между субъектами, I – изменение уровня защиты, Z –выполнение запроса на доступ, CP – копирование, KL – классификация, Y – разрешение на реализацию запроса, например, может быть определено как:

вид доступа «чтение (R)» состоит в получении субъектом s_j информации, содержащейся в объекте o_i;

вид доступа «отказ от доступа (O)» запрещает субъекту s_j доступ к информации объекта o_i; отказ субъекта s_j от доступа к объекту o_i разрешается безусловно; в этом случае данный вид доступа $a_K \in A$ исключается из множества видов доступа субъекта;

вид управления доступом «передача прав (P)» состоит в передаче полномочий доступа субъектом s_{j1} другому субъекту s_{j2} к объекту o_i по определенным видам доступа;

вид управления доступом «реализации запроса (Y)» состоит в разрешении реализации доступа субъекта s_j к объекту o_i согласно установленной категории допуска субъекта s_j и уровню секретности объекта o_i.

Проверка права реализации субъектом запроса необходима в случае, когда при наличии достаточной категории допуска субъект может быть не наделен полномочиями в ознакомлении с конкретным поступившим документом сравнимой степени секретности.

Рассмотрим расширенный список правил по разрешению запросов, контролю полномочий доступа и изменению состояния системы.

1. Чтение r субъектом s_j объекта o_i разрешается, если для $r \in m_{ij}$ выполняется $J(s_j) \geq J(o_i)$, и отвергается, если не выполняется хотя бы одно из условий. Этот вид доступа соответствует исполнению резолюции «Для ознакомления».

2. Дополнение g субъектом s_j объекта o_v информацией из объекта $o_i (v \neq i)$ разрешается, если для $g \in m_{ij}$, и $r \in m v_j$ выполняются $J(s_j) \geq J(o_v)$, $J(s_j) \geq J(o_i)$, и запрещается, если не выполняется хотя бы одно из условий. При этом происходит изменение состояния системы: если $J(o_i) > J(o_v)$, то $J(o_i) \rightarrow J(o_v)$; если $J(o_i) \leq J(o_v)$, то $J(o_i) = J(o_v)$. Этот вид доступа соответствует исполнению резолюции «Для использования» или «Для реализации» и состоит в чтении объекта o_i и перезаписи информации из него в другой объект o_v.

3. Дополнение d субъектом s_j объекта o_i информацией без предварительного прочтения разрешается, если для $d \in m_{ij}$ выполняется $J(s_j) \geq J(o_i)$ и запрещается, если не выполняется хотя бы одно из условий.

4. Запись w субъектом s_j информации в объект o_i после предварительного прочтения разрешается, если для $w \in m_{ij}$ выполняется при $r \in m_{ij}$, $J(s_j) \geq J(o_i)$, и запрещается, если не выполняется хотя бы одно из условий. Изменение состояния при разрешении $w = a_K \in A: b'' = b \cup \{s_j, o_i, w\}$.

5. Отказ o субъекту s_j от доступа к объекту o_i разрешается безусловно. В этом случае конкретный вид доступа $a_K \in A$ исключается из множества видов доступа $M \backslash \{a_K\}$.

6. Исполнение команды e субъектом s_j над объектом o_i разрешается, если для $e \in m_{ij}$ выполняются при $r \in m_{ij}$, $J(s_j) \geq J(o_i)$, а для вновь созданного объекта $J(o_v) \geq J(o_i)$, $J(s_j) \geq J(o_v)$. Этот вид доступа соответствует исполнению резолюции «Подготовить ответ» и состоит в чтении субъектом s_j объекта o_i и создания нового объекта o_v.

7. Копирование cp субъектом s_j объекта o_i (создание нового объекта o_v, а затем дополнение объекта o_v информацией из объекта o_i) разрешается, если для $cp \in m_{ij}$ выполняются условия $c \in m_{ij}$, $g \in m_{ij'}$, $J(s_j) \geq J(o_i)$, и запрещается, если не выполняется хотя бы одно из условий.

8. Классификация kl объектов и корректировка классификации связаны с формированием древовидной структуры объектов, что выходит за рамки данной статьи. Обозначим $F(o_i)$ – «отец» объекта o_i, $H(o_i)$ – «сын» объекта o_i.

9. Лишение l права доступа субъектом s_j субъекта s_v к объекту o_i разрешается в двух случаях:

1) объект o_i исполнен субъектом s_w $(s_w \neq s_v)$, поэтому отпала необходимость в доступе $a_K \in A$ субъекта s_v к объекту o_i;

2) субъект s_v наказан и поэтому исключается из множества $S \backslash \{s_v\}$.

Субъект s_j лишает права доступа субъекта s_v к объекту o_i при условии $\lambda_j > \lambda_v$, $l = a_K \in m_{ij}$, s_v – «сын» субъекта s_j: $s_v \in H(s_j)$, $J(s_v) \geq J(o_i)$.

10. Передача p субъектом s_j субъекту s_v $(v \neq j)$ права доступа $a_K \in A$ к объекту o_i разрешается, если $p \in m_{ij}$, и выполняется одно из условий:

1) $p = a_K \in m_{ij}$, s_v – «сын» субъекта s_j: $s_v \in H(s_j)$, $J(s_v) \geq J(o_i)$;

2) $p = a_K \in m_{ij}$, $\lambda_j = \lambda_v$, , $J(s_v) \geq J(o_i)$, s_j, $s_v \in S^{(1)}$;

3) $p = a_K \in m_{ij}$, $\lambda_j < \lambda_v$, $s_v \in S^{(1)}$,

и отвергается в противном случае. Происходит изменение состояния системы $p = a_K \in A$: $m_{ij}'' = m_{ij} \cup \{a_K\}$.

11. Создание c субъектом s_j нового объекта $o\alpha(i)$ и задание атрибутов доступа к ним разрешается безусловно. Если для $c \in m_{ij}$, $\exists$ o$\alpha(i)$ – сын объекта o_i то $J(o\alpha(i)) \leq J(o_i)$, если $\exists$ $b_1, b_2 \in B$, где $b_1 = \{s_j, o_i, w\}$, $b_2 = \{s_j, o_i, d\}$, $J(s_j) \geq J(o\alpha(i))$. Изменение состояния системы: расширение множества O и матрицы M: $O' = O \cup o\alpha(i)$; $M' = M \cup M\alpha(i)$; столбец матрицы $M\alpha(i)$ содержит один непустой элемент, значение которого должно быть определено в запросе $c: \{r, w, d\}$, $\{r, w, d, e\}$.

12. Уничтожение субъектом s_j объекта o_i и соответственно всех его «сыновей»: $H(o_i) = (o_{i1}, o_{i2}, \ldots, o_{ie})$ разрешается, если s_j имеет доступ w к «отцу» объекта o_i, т.е. $\exists$ $b \in B$, $b = \{s_v, F(o_i), w\}$, когда s_j – создатель объекта o_i. Изменение состояния: из списка текущего доступа B удаляются все записи, содержащие элементы $o_i, o_{i1}, o_{i2}, \ldots, o_{ie}$, а из матрицы M – столбцы с номерами $i, i_1, i_2, \ldots, i_e$.

13. Запрос z субъекта s_v к субъекту s_j на право доступа $a_K \in A$ к объекту o_i удовлетворяется, если $z \in m_{ij}$ и выполняется одно из условий:

1) $s_v \in \{s_{g(j)}\}$ – "сын" $s_j = F(s_v)$, $J(s_v) \geq J(o_i)$;

2) $\lambda_v = \lambda_j$, $J(s_v) \geq J(o_i)$, $s_j, s_v \in S^{(1)}$;

3) $\lambda_v > \lambda_j$ и отвергается в противном случае.

14. Изменение i субъектом s_j уровня секретности $J(s_j)$ на $J^*(s_j)$ разрешается:

1) при увеличении уровня защиты $J(s_j)<J^*(s_j)$ выполняются все виды запросов к объектам, разрешенных ранее для $J(s_j)$;

2) при уменьшении уровня защиты $J(s_j)>>J^*(s_j)$ – пересмотр всех видов доступа к объектам и разрешении только тех видов, при которых выполняется $J^*(s_j) \geq J(o_i)$.

Изменение состояния системы: $J(s_j)$ на $J^*(s_j)$.

15. Разрешение y на реализацию запроса субъекта s_j выполняется, если для $y \in m_{ij}$, выполняется $J(s_j) \geq J(o_i)$, и отвергается, если не выполняется хотя бы одно из условий. Этот вид доступа соответствует исполнению резолюции «Для ознакомления в соответствии с формой допуска».

Список текущего доступа $B=\{b_t, t=\overline{1,T}\}$ описывает разрешенный в данный момент доступ b_t субъектов s_j к объектам o_i. Он содержит записи вида $b_t=(s_j, o_i, a)$, если субъекту s_j был разрешен доступ $a \in A$ к объекту o_i и это разрешение к настоящему моменту не отменено. Разрешение доступа действует до тех пор, пока субъект не обратится с запросом об отказе от доступа.

Список запросов R^* содержит запросы всех видов доступа: виды доступа субъектов к объектам, создания и уничтожения объектов, передачи и лишения прав доступа, а также отказ от доступа:

$$R^*=\{r,d,g,w,e,o,c,u,l,p,i,z,kl,cp,y\}$$

и соответственно имеет следующий вид:

1) (s_j, o_i, r), 6) (s_j, o_i, c), 11) (s_j, o_i, u),
2) (s_j, o_i, d), 7) (s_j, o_i, e), 12) (s_j, o_i, z),
3) (s_j, o_i, g), 8) (s_j, o_i, p), 13) (s_j, o_i, kl),
4) (s_j, o_i, w), 9) (s_j, o_i, i), 14) (s_j, o_i, cp),
5) (s_j, o_i, o), 10) (s_j, o_i, l), 15) (s_j, o_i, y) .

Разрешение запроса вызывает изменение состояния вычислительной системы. Это изменение должно приводить к защищенному состоянию, если исходное состояние также было защищено. Для этого необходимо строго выполнять решающие правила по разрешению запросов и изменению состояний системы с учетом права на реализацию запроса посредством монитора обработки запросов, реализующего все контрольные функции.

ЛИТЕРАТУРА

1. *LaPadula L., Bell D.* Secure Computer System: Mathematical Foundation, ESD-TR-73-278. V. I, MITRE Corporation.

2. *LaPadula L., Bell D.* Secure Computer System: A Mathematical Model, ESD-TR-73-278. V. II, MITRE Corporation.

Резюме

Есептеуіш жүйенің қорғаныш қалпында мандатты қатынауға шектеу кезінде сұратуларды орындау ережелері мен шарттары анықталған.

Summary

In the paper are formulated rules and conditions of the execution of inquires on the credentials differentiation of the access for protective condition of the computing system.

Институт проблем информатики
и управления МОН РК,
Алматы

Поступила 16.06.06г.