МАНДАТНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ НА ОСНОВЕ АЛГОРИТМОВ ПРИНЯТИЯ РЕШЕНИЯ

С.В. Белим, д.ф.-м.н., профессор
Н.Ф. Богаченко, к.ф.-м.н., доцент
Омский государственный университет им. Ф.М. Достоевского,
г. Омск
E-mail: sbelim@mail.ru, nfbogachenko@mail.ru

Мандатная политика безопасности, получающая все большее распространение, обладает рядом преимуществ по сравнению с дискреционной политикой безопасности. К таким преимуществам можно отнести строгое разделение доступа и перекрытие каналов утечки информации, организуемых троянскими программами [1, 2]. Но существует ряд ограничений на применимость мандатной политики безопасности. Эти ограничения связаны с тем, что множество меток безопасности должно представлять собой алгебраическую решетку. То есть на множестве меток должно быть задано частичное отношение не строгого порядка, одним из свойств которого является транзитивность. Тогда как в реальных компьютерных системах транзитивность разрешений на доступ выполняется не всегда. Рассмотрим два примера.

Во-первых, рассмотрим разрешение на доступ по порождению субъекта, которое соответствует запуску процессов в операционных системах. Пусть разрешены доступы на порождение $S_1 \to S_2$ и $S_2 \to S_3$, но запрещен доступ на порождение $S_1 \to S_3$. То есть первый субъект может породить второй, второй субъект может породить третий, но первый не может породить третий напрямую. В реальных системах такая ситуация может возникнуть для следующей конфигурации: S_1 – операционная система, S_2 – виртуальная JAVA машина, S_3 – исполняемая программа на языке JAVA. Запуск программы возможен только из-под виртуальной машины.

Во-вторых, рассмотрим разрешение на доступ. Пользовательский процесс S_1 имеет право на доступ к API операционной системы S_2 ($S_1 \to S_2$). Функции API имеют право на низкоуровневые операции с жестким диском, объектом O ($S_2 \to O$). Пользовательские процессы не имеют право на низкоуровневые операции с жестким диском, доступ $S_1 \to O$ запрещен.

В обоих случаях при попытке построить мандатную политику безопасности сталкиваемся с ситуацией не транзитивности: $C(S_1) > C(S_2)$, $C(S_2) > C(S_3)$, но $C(S_1) <> C(S_3)$.

Определим на множестве объектов и субъектов системы бинарное отношение, которое возможно не будет транзитивным. Пусть каждому объекту и субъекту этой системы приписана некоторая структура данных $m_i = (x_{i_1}, ..., x_{i_n})$, где x_{i_j} – элемент некоторого множества X_i, причем все X_i могут быть различными. Рассмотрим множество таких структур данных $M = \{m_i\}$.

Определим на M бинарное отношение следующим образом. Пусть в системе задан некоторый алгоритм принятия решений $P(m_i, m_j)$, однозначно выбирающий одну из двух структур $m_i = (x_{i_1}, ..., x_{i_n})$ или $m_j = (x_{j_1}, ..., x_{j_n})$ в зависимости от значения их координат. Естественно потребовать коммутативность функции P: $P(m_i, m_j) = P(m_j, m_i)$.

Будем считать, что $m_i \succ m_j$, если $P(m_i, m_j) = m_i$. То есть алгоритм принятия решений определяет, какая из двух структур является доминирующей. Применяя алгоритм P к всевозможным парам множества M, задается бинарное отношение на M.

Очевидно, это отношение будет антисимметричным: пусть найдется пара различных элементов из M такая, что $(m_i \succ m_j) \wedge (m_j \succ m_i)$, тогда $P(m_i, m_j) = m_i$ и $P(m_j, m_i) = m_j$. В силу коммутативности P: $m_i = m_j$ - противоречие.

Естественно считать это отношение рефлексивным: $P(m_i, m_i) = m_i$. Следует отметить, что введенное бинарное отношение не всегда будет отношением порядка, так как возможны алгоритмы принятия решений, которые приводят к отсутствию транзитивности. Антисимметричное и не обязательно транзитивное отношение принято называть отношением предпочтения.

Еще одно свойство полученного отношения – полнота, так как $\forall m_i, m_j \in M$ либо $(m_i \succ m_j)$, либо $(m_j \succ m_i)$. Это следует из того, что алгоритм принятия решения определен на всем декартовом произведении $M \times M$. Заметим, что ориентированный граф, порожденный заданным отношением предпочтения, при отмене ориентации дуг является полным графом.

Множество M с заданным на нем *полным рефлексивным отношением предпочтения* может быть использовано для построения непротиворечивой мандатной политики безопасности. Действительно, в силу полноты отношения, для каждого доступа может быть принято однозначное решение о разрешении или запрете доступа. При этом элементы множества M будут играть роль меток безопасности. Пусть субъект S имеет метку безопасности m, а объект O метку безопасности m'. Для получения доступа к объекту O субъект S посылает подсистеме безопасности запрос на доступ $S \to_? O$. Подсистема безопасности использует алгоритм принятия решений $P(m, m')$. Если результатом работы алгоритма будет m, то субъект доминирует над объектом и доступ будет разрешен, при противоположном решении – доступ запрещен. Это простейший случай полного доступа. В большинстве систем происходит разграничение доступа, зависящее не только от субъекта и объекта, но и от вида доступа. В этом случае алгоритм принятия решения должен зависеть не только от меток безопасности субъекта и объекта, но и от метки вида доступа p: $P(m, m', p)$.

Список литературы:

1. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.

2. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. 2-е изд., испр. и доп. М.: Научно-техническое издательство «Горячая линия – Телеком», 2013. 338 с.