С. В. Белим, Н. Ф. Богаченко

МОДИФИКАЦИИ ИЕРАРХИЧЕСКОГО ДЕРЕВА ПРИ РОЛЕВОМ РАЗГРАНИЧЕНИИ ДОСТУПА

Политика безопасности компьютерных систем в общем случае задает правила разграничения доступа к информационным объектам. Одним из самых распространенных видов политики безопасности является ролевое разграничение доступа [1]. Ролевая политика безопасности, получившая широкое распространение в системах управления базами данных [1, 2], операционных системах [1, 2] и других вычислительных комплексах, допускает моделирование в рамках теории графов. Однако на сегодняшний день при проектировании подсистемы безопасности компьютерной системы иерархия ролей задается в виде ориентированного дерева [1]. Следует заметить, что математические модели, ориентированные на древовидную организацию иерархии ролей, являются достаточно развитыми [1]. Цель данной работы — развитие модели ролевой политики безопасности для произвольных графов. Основное внимание уделено отображению $R\rho$: $R \to 2^{\rho}$, которое каждой роли из множества R сопоставляет набор полномочий из множества прав на действия в системе ρ.

Иерархия ролей — это отношение частичного нестрогого порядка, заданное на множестве ролей R. При этом если $r_1 \geq r_2$, то r_1 находится в иерархии ролей «выше», чем r_2.

Исходя из этого определения иерархию ролей можно представить в виде ориентированного графа $G = (R, E)$. Множество вершин R — это множество ролей. Дуга $(r_1, r_2) \in E$, если в иерархии ролей $r_1 \geq r_2$[1]. Принято считать, что иерархия ролей имеет вид ориентированного дерева [1, 2], в дальнейшем будем называть его *деревом ролей* и обозначать $T = (R, E)$.

При иерархическом отношении ролей важным является вопрос построения отображения $R\rho$, а именно: возможно ли назначение одного и того же набора полномочий двум ролям, находящимся в иерархическом подчинении. При этом применяется механизм наследования «снизу — вверх»: назначение полномочий начинается с листовых вершин — *листовое распределение прав доступа*.

Пусть иерархия ролей задана в виде ориентированного дерева $T = (R, E)$. Определим разбиение множества листовых вершин R_L дерева ролей T на k подмножеств:

$$R_L = \bigcup_{i=1}^{k} R_L^{(i)}, \forall i, j \in \{1, \ldots, k\} : R_L^{(i)} \cap R_L^{(j)} = \varnothing \ .$$

Данное разбиение задает отношение эквивалентности на множестве листовых вершин. Рассмотрим теперь *классовое распределение прав доступа*. Пусть две роли, относящиеся к одному классу эквивалентности листовых вершин, имеют одинаковые права:

$$\forall r_1, r_2 \in R_L : (r_1 \overset{R_L}{\approx} r_2) \Rightarrow (RP(r_1) = RP(r_2)).$$

По аналогии со случаем неклассового ролевого разграничения доступа [1] возможны три подхода к построению отображения $R\rho$:

1. *Строго таксономический классовый подход*. Разобьем множество ρ на k непересекающихся подмножеств по числу классов эквивалентности листовых вершин дерева ролей:

$$P = \bigcup_{i=1}^{k} P_i, \forall i, j \in \{1, \ldots, k\} : P_i \cap P_j = \varnothing .$$

[1] Если следовать системе обозначений графического языка моделирования UML (Unified Modeling Language), позволяющего представлять различные объектно-ориентированные проекты в единых обозначениях, то дугу надо ориентировать от младшей роли к старшей. Чтобы сохранить терминологию теории графов, будем считать, что дуги направлены от старших ролей к младшим. Очевидно, в обоих случаях отношение порядка, задающее иерархию ролей, и соответствующий неориентированный граф останутся неизменными.

Распределение прав, определяющееся отображением $R\rho$, зададим для листовых вершин в следующем виде:

$\forall r \in R_L^{(i)} : RP(r) = P_i$.

Для нелистовых вершин множество прав будем определять как объединение прав всех вершин, которые являются сыновьями данной вершины:

$\forall r \notin R_L : RP(r) = \bigcup_{r' \in Ch(r)} RP(r')$.

Здесь через $Ch(r)$ обозначено множество всех сыновей вершины r.

2. *Нетаксономический классовый подход*. Аналогично предыдущему случаю, распределение прав изначально производится только между листовыми вершинами, но множества прав различных классов эквивалентности листовых вершин могут пересекаться.

3. *Иерархический охватный классовый подход*. Распределение прав производится между классами эквивалентности листовых вершин и передается по иерархическим принципам. Но, кроме того, нелистовые вершины, унаследовавшие одинаковые наборы прав, могут одновременно получать дополнительные права.

За счет иерархической структуры во всех трех случаях в итоговом наборе полномочий присутствуют все полномочия подчиненных ролей.

Легко показать, что каждый из трех листовых подходов распределения полномочий, определенных в [1], является частным случаем соответствующего классового подхода при условии: $|R_L^{(i)}| = 1$, где $\{R_L^{(i)}\}_{i=1}^{k}$ — начальное разбиение множества листовых вершин, другими словами, каждая листовая вершина образует отдельный класс разбиения.

Разбиение листовых вершин дерева ролей вместе с правилами построения отображения $R\rho$ порождает разбиение всего множества ролей. Будем считать две роли *эквивалентными*, если они наделены одинаковыми правами:

$\forall r_1, r_2 \in R : (RP(r_1) = RP(r_2)) \Rightarrow (r_1 \overset{RP}{\approx} r_2)$.

Полученные классы эквивалентности ролей назовем *$R\rho$-классами*. Каждому узлу r дерева ролей припишем соответствующий данной роли набор полномочий $R\rho(r)$. Результирующее помеченное дерево ролей назовем *$R\rho$-деревом*. Таким образом, в $R\rho$-дереве в один $R\rho$-класс попадают вершины, наделенные одним и тем же набором полномочий.

Обозначим число $R\rho$-классов через K, а число классов эквивалентности листовых вершин через k. Очевидно, что в случае строгого таксономического классового подхода $K \geq k$. При двух других подходах возможен случай $K < k$ в тех ситуациях, когда несколько классов эквивалентности листовых вершин наделяются одним и тем же набором полномочий.

$R\rho$-дерево будем называть *вырожденным*, если на нем существует ровно один $R\rho$-класс, т. е. $K = 1$. *$R\rho$-дерево* будем называть *оптимальным*, если количество заданных на нем $R\rho$-классов совпадает с количеством вершин: $K = |R|$.

Очевидно, что для оптимальности $R\rho$-дерева необходимо потребовать, чтобы в начальном разбиении множества листовых вершин каждый лист составлял отдельный класс. Далее рассмотрим необходимые и достаточные условия оптимальности.

Теорема 1. При строго таксономическом листовом подходе распределения прав $R\rho$-дерево является оптимальным тогда и только тогда, когда полустепень исхода (число исходящих дуг) каждой нелистовой вершины не меньше двух:

$\forall r \notin R_L : d^-(r) \geq 2$. (1)

Доказательство. Пусть $R\rho$-дерево является оптимальным. Тогда

$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow (RP(r_1) \neq RP(r_2))$. (2)

От противного. Пусть $\exists\ r_1 \notin R_L$: $d^-(r_1) < 2$, следовательно, $d^-(r_1) = 1$. Тогда вершина r_1 имеет ровно одного сына, обозначим его r_2. Согласно правилам строго таксономического листового подхода: $R\rho(r_1) = R\rho(r_2)$ — противоречие.

Пусть теперь выполнено неравенство (1). Рассмотрим две различные вершины $r_1, r_2 \in R$. Надо показать справедливость условия (2). Заметим, что требование (1) влечет выполнение следующего неравенства:

$$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow (R_L(r_1) \neq R_L(r_2)), \tag{3}$$

где $R_L(r_i)$ — потомки вершины r_i, являющиеся листовыми вершинами в случае, когда $r_i \notin R_L$, либо сама вершина r_i, если она листовая. Данное утверждение очевидным образом следует из ациклличности принятой иерархии ролей (T — дерево). Согласно введенной системе обозначений, при строго таксономическом листовом подходе:

$$\forall r \in R : RP(r) = \bigcup_{r' \in R_L(r)} RP(r') \tag{4}$$

и

$$\forall r', r'' \in R_L : (r' \neq r'') \Rightarrow (RP(r') \cap RP(r'') = \varnothing). \tag{5}$$

Из (3) и (5) следует:

$$\forall r_1, r_2 \in R : (r_1 \neq r_2) \Rightarrow \left(\bigcup_{r' \in R_L(r_1)} RP(r') \neq \bigcup_{r' \in R_L(r_2)} RP(r') \right). \tag{6}$$

Принимая во внимание равенство (4), получаем условие (2). Что и требовалось доказать.

Теорема 2. При нетаксономическом листовом подходе распределения прав $R\rho$-дерево является оптимальным тогда и только тогда, когда полустепень исхода каждой нелистовой вершины не меньше двух (выполнено условие (1)) и разбиение множества прав ρ на подмножества ρ_i произведено таким образом, что

$$\forall j \in \{1,\ldots,k\} : P_j \not\subseteq \bigcup_{i=1, i \neq j}^{k} P_i . \tag{7}$$

Доказательство. Необходимость доказывается аналогично предыдущей теореме. При доказательстве достаточности условие (5) заменяется условием (7). Пусть I_1, $I_2 \subseteq \{1,\ldots,k\}$: $I_1 \neq I_2$, тогда $\exists\ j$: $(j \in I_1) \wedge (j \notin I_2)$. Согласно (7), $P_j \not\subseteq \bigcup_{i \in I_2} P_i$, следовательно, $\bigcup_{i \in I_1} P_i \not\subseteq \bigcup_{i \in I_2} P_i$. В результате:

$$\forall I_1, I_2 \subseteq \{1,\ldots,k\} : (I_1 \neq I_2) \Rightarrow \left(\bigcup_{i \in I_1} P_i \neq \bigcup_{i \in I_2} P_i \right). \tag{8}$$

Тогда, принимая во внимание неравенство (3) и то, что $\forall\ r_i \in R_L$: $R\rho(r_i) = \rho_i$, получаем (6) и, как следствие, (2). Что и требовалось доказать.

Отметим, что при иерархическом охватном листовом подходе оптимальным может быть $R\rho$-дерево произвольной структуры (например, ориентированная цепь) за счет того, что нелистовые вершины не только наследуют права, но и получают их непосредственно.

В дальнейшем, выбранный подход к построению отображения $R\rho$ будем указывать в названии $R\rho$-дерева. Пусть T — $R\rho$-дерево. *$R\rho$-характеристикой T* называется спецификация, указывающая, какой именно подход был применен при построении отображения $R\rho$. Дерево T называется *таксономическим* (или *нетаксономическим*, или *охватным*), если при распределении прав был использован строго таксономический (или нетаксономический, или иерархический охватный) подход. Если важно подчеркнуть, что было использовано листовое (классовое) распределение полномочий, то T — *листовое* (*классовое*) дерево.

Расширение $R\rho$-дерева T — это процесс построения $R\rho$-дерева T' такого, что T является подграфом T' и $\forall\ r \in R_T$: $R\rho_T(r) = R\rho_{T'}(r)$ — множество $R\rho$-классов T является подмножеством множества $R\rho$-классов T'.

Теорема 3. Произвольное $R\rho$-дерево может быть расширено до таксономического (в общем случае классового) $R\rho$-дерева.

Доказательство. Пусть T — произвольное $R\rho$-дерево. Построим искомое $R\rho$-дерево T'. Все вершины, дуги и полномочия дерева T перенесем в дерево T'. Тем самым T' — расширение дерева T.

Пусть каждой листовой вершине r_i сопоставлен набор полномочий $P_i = \{p_{i1}, \ldots, p_{im_i}\}$. Если $|\rho_i| = m_i > 1$, то в дереве T' к этой вершине присоединим m_i листовых вершин, каждая из которых будет наделена правом ρ_{ij} ($j \in \{1, \ldots, m_i\}$). Двигаясь по дереву T' от листьев к корню, каждую нелистовую вершину r пополним сыновьями-листьями по числу полномочий из набора $R\rho(r)$ дерева T, которые не были унаследованы (каждой новой вершине припишем соответствующее право). В результате, в дереве T' каждая нелистовая вершина не получает ни одного полномочия непосредственно, а лишь наследует их от сыновей:

$\forall r \notin R_L : RP(r) = \bigcup_{r' \in Ch(r)} RP(r')$.

Каждой листовой вершине дерева T' приписано одно-единственное полномочие. Объединяя листовые вершины с одним и тем же значением $R\rho(r) = \{\rho_i\}$ в один класс разбиения листовых вершин $R_L^{(i)}$, получаем:

$\forall r \in R_L^{(i)} : RP(r) = \{p_i\} = P_i, \forall i, j\ (i \neq j) : P_i \cap P_j = \varnothing$.

Итак, отображение $R\rho$ удовлетворяет всем требованиям строго таксономического классового подхода, следовательно, T' — таксономическое $R\rho$-дерево. Что и требовалось доказать.

Расширяя $R\rho$-дерево, мы тем самым строим новую ролевую политику, наследующую все роли и их иерархию из исходной модели.

Одним из преимуществ классового распределения полномочий является возможность расширения нетаксономических или охватных $R\rho$-деревьев до строго таксономических классовых, т. е. возможна смена произвольной $R\rho$-характеристики дерева на таксономическую. Но, к сожалению, при таком преобразовании, как правило, увеличивается количество ролей (и $R\rho$-классов) в системе.

В противовес расширению $R\rho$-дерева можно рассматривать в некотором смысле обратную операцию. Если в $R\rho$-дереве найдется хотя бы один $R\rho$-класс, содержащий несколько ролей, то дерево не *оптимально*, а это свидетельствует о наличии в политике безопасности «дублирующих» ролей. Естественно попытаться преобразовать иерархию ролей так, чтобы результирующее $R\rho$-дерево стало оптимальным и при этом не изменилось множество $R\rho$-классов системы.

Два $R\rho$-дерева T и T' *эквивалентны*, если множества их $R\rho$-классов совпадают (совпадают различные наборы полномочий, встречающиеся в структуре).

Оптимизация $R\rho$-дерева T — это процесс построения $R\rho$-дерева T' такого, что T' эквивалентно T и T' — оптимальное $R\rho$-дерево. Заметим, что $R\rho$-дерево, полученное в результате оптимизации, будет листовым в силу оптимальности.

Попытаемся ответить на следующие вопросы. Любое ли $R\rho$-дерево поддается оптимизации? Как при этом ведет себя $R\rho$-характеристика дерева? Если $R\rho$-дерево является листовым и вершины в пределах одного $R\rho$-класса не связаны дугами (иначе достаточно произвести попарное *стягивание* таких вершин, как эта операция понимается в теории графов [2]), то добиться оптимальности в ряде случаев можно за счет перестройки древовидной структуры и изменения $R\rho$-характеристики на охватную. Этот подход не столь интересен, так как, исходя из практических приложений, желательно получить эквивалентное оптимальное таксономическое $R\rho$-дерево.

Получение эквивалентной оптимальной структуры с той же $R\rho$-характеристикой представляется возможным за счет отказа от древовидности и построения эквивалентного ориентированного графа, задающего иерархию ролей.

Теорема 4. Ориентированный граф задает иерархию ролей (является орграфом ролей) тогда и только тогда, когда в нем отсутствуют ориентированные циклы.

Доказательство. Отсутствие ориентированных циклов необходимо и достаточно для существования отношения частичного порядка, а именно свойств транзитивности и антисимметричности. Что и требовалось доказать.

Заметим, что в орграфе без ориентированных циклов найдется как минимум один сток (вершина с нулевой полустепенью исхода: $d^-(t) = 0$) и как минимум один источник (вершина с нулевой полустепенью захода: $d^+(s) = 0$). Далее будем рассматривать ориентированные графы с одним источником.

Распределение прав по произвольному орграфу ролей, так же как и по дереву ролей, может проводиться одним из трех способов. При этом построение отображения $R\rho$ начинается либо со стоков (листовое распределение), либо с классов эквивалентности, на которые разбиты стоки (классовое распределение).

Определения оптимальности, расширяемости, эквивалентности и оптимизации очевидным образом переносятся на случай $R\rho$-орграфа (помеченного орграфа ролей).

Теорема 5. Произвольное $R\rho$-дерево может быть оптимизировано до $R\rho$-орграфа.

Доказательство. В $R\rho$-дереве достаточно *склеить* вершины, соответствующие эквивалентным ролям, если они не соединены дугами, либо попарно *стянуть*, если такие дуги имеются (операции склейки и стягивания вершин понимаются в соответствии с определениями теории графов [2]). В результате, множество $R\rho$-классов останется прежним, но орграф будет оптимальным. Что и требовалось доказать.

Следствие 5.1. Из алгоритма построения эквивалентного оптимального $R\rho$-орграфа G непосредственно следует ряд свойств этой структуры:

1. G имеет один источник s.
2. Число стоков t_i в G совпадает с числом классов разбиения $R_L^{(i)}$ листовых вершин исходного $R\rho$-дерева T.
3. Если исходное $R\rho$-дерево T являлось оптимальным, то $G = T$.
4. G — листовой $R\rho$-орграф.

Следствие 5.2. Если исходное $R\rho$-дерево таксономическое, то построенный по предложенному алгоритму эквивалентный оптимальный $R\rho$-орграф также таксономический.

Доказательство. Стягивание двух вершин, соответствующих эквивалентным ролям, по дуге, их соединяющей, не изменяет $R\rho$-характеристику. При склейке вершин из одного $R\rho$-класса результирующий набор сыновей будет распределен по тем же $R\rho$-классам, что и в исходном $R\rho$-дереве, тем самым сохранится таксономичность структуры. Что и требовалось доказать.

Следствие 5.3. Если исходное $R\rho$-дерево нетаксономическое, то построенный по предложенному алгоритму эквивалентный оптимальный $R\rho$-орграф также нетаксономический.

Следствие 5.4. Если исходное $R\rho$-дерево охватное, то построенный по предложенному алгоритму эквивалентный оптимальный $R\rho$-орграф может оказаться охватным, нетаксономическим или таксономическим.

Обобщая вышесказанное, получаем следующую возможную последовательность построения ролевой политики безопасности:

1. Исходя из содержательной постановки задачи, построить $R\rho$-дерево T_1 (листовое или классовое).
2. Расширить T_1 до таксономического (в общем случае классового) $R\rho$-дерева T_2 (см. теорему 3).

3. Преобразовать T_2 в эквивалентный оптимальный таксономический $R\rho$-орграф T_3 (см. теорему 5).

Таким образом, любую ролевую модель распределения полномочий можно расширить до политики, в которой иерархия ролей задана орграфом без ориентированных циклов, роли распределены в соответствии со строго таксономическим листовым подходом и $R\rho$-структура оптимальна.

Оказывается, предложенный в теореме 5 алгоритм обратим: по произвольному $R\rho$-орграфу можно построить эквивалентное (но необязательно оптимальное) $R\rho$-дерево.

Теорема 6. Для произвольного $R\rho$-орграфа существует эквивалентное ему $R\rho$-дерево.

Доказательство. Пусть дан $R\rho$-орграф G. Будем строить эквивалентную ему $R\rho$-структуру T. На первом шаге каждому стоку t_i орграфа G сопоставляем $d^+(t_i)$ листьев в T («оригинал» и $(d^+(t_i) - 1)$ «дублей»). Эта операция называется *расщеплением* вершины (если полустепень захода равна единице, то имеется только «оригинал»).

Далее, двигаясь по орграфу G от нижних ярусов к источнику, последовательно расщепляем все вершины. «Оригинал» и «дубли» наделяем теми же правами, что были у вершины, их образующей. К «оригиналу» присоединяем уже существующие вершины структуры T из тех, что не имеют входящих дуг, восстанавливая сыновей расщепляемой вершины орграфа G (такие вершины в T всегда найдутся по построению). К каждому «дублю» добавляем вершины и дуги так, чтобы подграф, порожденный «дублем», представлял собой копию поддерева, порожденного «оригиналом».

Очевидно, что построенная таким образом иерархия T является $R\rho$-деревом и задает те же $R\rho$-классы, что и исходный $R\rho$-орграф G, т. е. ему эквивалентна. Что и требовалось доказать.

Следствие 6.1. Количество вершин $R\rho$-дерева T, эквивалентного $R\rho$-орграфу G и построенного по алгоритму, описанному в теореме, равно

$$\sum_{r \in R_G} \left(1 + (d^+(r) - 1) \mid R_{T(r)} \mid\right),$$

где R_G — множество вершин орграфа G, $R_{T(r)}$ — множество вершин поддерева, порожденного той вершиной дерева T, которая соответствует вершине r орграфа G.

Заметим, что теорема 6 дает возможность свести исследование ролевой политики безопасности на произвольном $R\rho$-орграфе к изучению эквивалентного $R\rho$-дерева.

Таким, образом, теоремы 5 и 6 позволяют выполнять различные эквивалентные преобразования иерархии ролей в зависимости от того, какой признак более значим: древовидность или оптимальность.

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. М.: Издательский центр «Академия», 2005. – 144 с.
3. *Новиков Ф. А.* Дискретная математика для программистов. СПб.: Питер, 2001. – 304 с.