Математические структуры и моделирование
2019. № 1(49). С. 89–96

УДК 004.056
DOI: 10.25513/2222-8772.2019.1.89-96

РАНЖИРОВАНИЕ ПОЛНОМОЧИЙ НА ОСНОВЕ АНАЛИЗА ИЕРАРХИИ РОЛЕЙ В МОДЕЛЯХ РАЗГРАНИЧЕНИЯ ДОСТУПА

Н.Ф. Богаченко
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru
А.В. Филиппова
студент, e-mail: afelia96@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Для оценки вероятности утечки полномочий в ролевой политике разграничения доступа введено понятие «уровень критичности полномочия». Сформулированы постулаты, определяющие зависимость уровней критичности полномочий от структуры ролевой иерархии. Предложена методика (метод и алгоритм) автоматического расчёта уровней критичности полномочий, использующая метод анализа иерархий. Проведён вычислительный эксперимент, выявляющий зависимость уровня критичности полномочия от настраиваемого параметра алгоритма. Настраиваемый параметр позволяет регулировать влияние постулатов на результаты вычислений.

Ключевые слова: роли, полномочия, избыточность, уровень критичности, метод анализа иерархий.

Введение

Ролевое разграничение доступа получило широкое применение во многих современных компьютерных системах. Преимуществами ролевого подхода являются разделение обязанностей, простота администрирования (например, при переназначении пользователю полномочий) и применение иерархии ролей. Модель иерархической организации множества ролей предполагает соблюдение следующих правил:

1) каждая роль наследует полномочия подчинённых ей ролей согласно заданной иерархии;

2) пользователь, авторизованный на некоторую роль, авторизуется и на все роли, подчинённые данной [1].

Управление разграничением доступа в компьютерной системе, в том числе и на основе концепции ролей, должно включать в себя как стадию разработки — проектирование и реализация политики разграничения доступа, так и стадию реконструкции — администрирование, анализ и оптимизация. В свою очередь, анализ реализованной модели разграничения доступа заключается в оценке рисков информационной безопасности. Согласно [2], риск информационной безопасности — это оценка возможного ущерба, наносимого организации

либо активу в результате реализации некоторой угрозы. Основной способ оценки рисков заключается в сочетании вероятности события и его последствий:

$$R(V,T) = P(V,T) \cdot I(T), \tag{1}$$

где $P(V,T)$ — вероятность реализации угрозы T через заданную уязвимость V (для двухфакторного способа оценки рисков) или произведение вероятностей реализации угрозы T и использования уязвимости V (для трёхфакторного способа оценки рисков), $I(T)$ — ущерб от реализации угрозы T [3]. Основной сложностью при решении задач количественной оценки рисков информационной безопасности является качественный характер большинства показателей, влияющих на вероятности реализации угроз и использования уязвимостей, а также определяющих ущерб.

Материалы, представленные в данной работе, получены в результате исследования следующего вопроса: возможно ли при анализе рисков информационной безопасности применительно к ролевой модели разграничения доступа получить какие-либо количественные характеристики, не привлекая механизм экспертных оценок, а исходя из автоматического анализа основных элементов и структур, используемых при построении правил разграничения доступа?

1. Уровень критичности полномочия

При реализации в компьютерной системе подсистемы разграничения доступа возникает задача выявления скрытых каналов передачи информации: возможна ли передача информации между субъектами и объектами в обход политики безопасности. Применительно к ролевому разграничению доступа необходим контроль получения пользователями избыточных полномочий в следствии авторизации на роль, множество полномочий которой шире, чем требуется пользователю. При этом полностью исключить избыточность не всегда возможно. Возникает потребность в выявлении самых значимых полномочий, для которых избыточность наиболее нежелательна. Здесь «нежелательность» оценивается не с точки зрения ущерба, а со стороны вероятностей реализации угроз и использования уязвимостей. Числовая характеристика, отражающая значимость полномочий, названа «уровнем критичности». Содержательный смысл этого термина заключается в следующем: чем выше уровень критичности полномочия, тем больше вероятность его несанкционированного использования (утечки).

Для построения метода расчёта уровней критичности полномочий использована теоретико-графовая формализация ролевой политики разграничения доступа [1]. Рассматриваются такие элементы модели, как множество полномочий $P = \{p_1, \ldots, p_m\}$ и множество ролей $R = \{r_1, \ldots, r_n\}$. Иерархия ролей описывается с помощью ориентированного графа, в котором узлы соответствуют ролям, определённым в системе, метки узлов — наборам их полномочий, направленные ребра (дуги) задают отношение авторизации ролей друг на друга (см. рис. 1).

Уровнем критичности полномочия $p_i \in P$ назовём числовую характеристику $S(p_i)$, отражающую значимость p_i с точки зрения возможности его утечки.

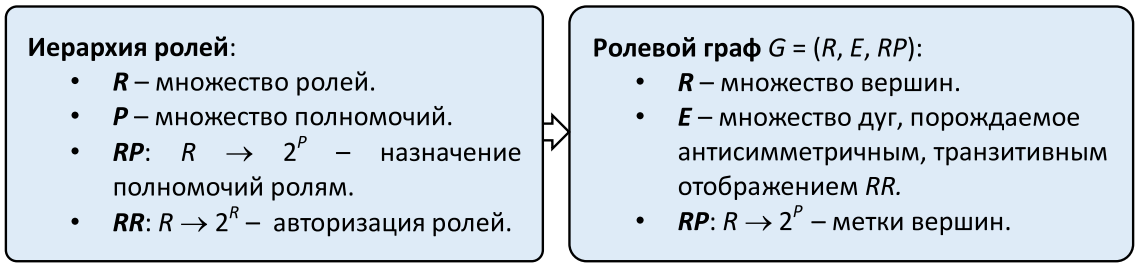


Рис. 1. Теоретико-графовое представление иерархии ролей

Потребуем, чтобы $S(p_i) \in [0,1]$ и $\sum_{i=1}^{m} S(p_i) = 1$. Тогда уровень критичности можно интерпретировать как некоторую априорную вероятность утечки соответствующего полномочия.

Очевидно, что величина $S(p_i)$ зависит как от распространённости полномочия p_i среди наборов полномочий ролей, так и от местоположения ролей, которым сопоставлено это полномочие, в иерархии. Таким образом, уровень критичности полномочия находится в зависимости от отображений RR и RP. Выделены следующие эвристики, определяющие зависимость уровня критичности от структуры ролевого графа.

Постулат 1. *Чем больше полномочий содержит роль, тем выше вероятность атаки (попытки несанкционированной авторизации) на данную роль, тем больше уровни критичности полномочий, сопоставленных роли.*

Постулат 2. *Чем чаще встречается полномочие в наборах полномочий ролей, тем выше вероятность его несанкционированного использования, тем больше его уровень критичности.*

Постулат 3. *Чем ближе роль к вершине иерархии, тем выше вероятность атаки на данную роль, тем больше уровни критичности полномочий, сопоставленных роли.*

2. Методика оценки уровня критичности

К методике расчёта уровней критичности полномочий были предъявлены следующие требования:

1) учёт постулатов 1 – 3;

2) автоматизация процесса вычисления.

Основная идея предложенного метода заключается в интерпретации ролевого графа как дерева решения метода анализа иерархий [4]: за альтернативы метода принимаются полномочия, за критерии — роли. Для этого необходимо провести предобработку ролевого графа:

1) преобразовать ролевой граф G в эквивалентное листовое ролевое дерево T [1];

2) расширить ролевое дерево T до единичного ролевого дерева T_p: каждый листовой узел пополняется узлами-сыновьями по числу его полномочий, каждый новый узел в качестве метки содержит ровно одно полномочие из набора

полномочий своего родителя.

Следует заметить, что в расширенном ролевом дереве T_p листовые узлы теперь ассоциированы не с ролями, а с полномочиями (см. рис. 2).

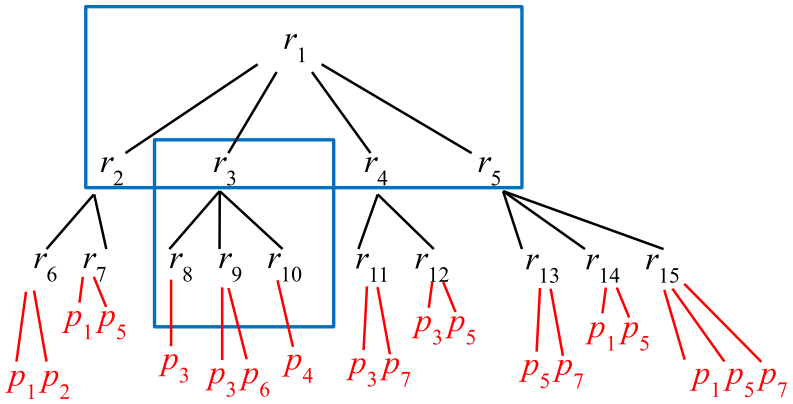


Рис. 2. Пример расширенного ролевого дерева T_p

Алгоритм оценки уровней критичности полномочий состоит из двух этапов:

1) вычисление относительных весовых коэффициентов (весов) для всех узлов дерева T_p, кроме корня;

2) вычисление комбинированных весовых коэффициентов (уровней критичности) для каждого из полномочий.

На первом этапе для каждого узла t_i дерева T_p, начиная с корня и исключая листовые узлы, рассматривается подмножество непосредственно подчинённых ему узлов $\{t_{i_1}, \ldots, t_{i_k}\}$. Для узлов этого подмножества формируется матрица парных сравнений. Но в отличие от классического метода анализа иерархий коэффициенты матрицы заполняются не экспертами, а вычисляются автоматически по формуле

$$m_{i_j i_s} = \frac{|RP(t_{i_j})|}{|RP(t_{i_s})|}, \tag{2}$$

где $|RP(t)|$ — мощность подмножества полномочий, сопоставленных узлу t. С учётом постулата 1 эта величина соотносит уровни критичности полномочий, приписанных узлу t_{i_j}, с уровнями критичности полномочий, приписанных узлу t_{i_s}. Заполненные таким образом матрицы будут идеально согласованными [4], а формула для расчёта относительных весов примет следующий вид:

$$w_{i_j} = \frac{|RP(t_{i_j})|}{\sum_{s=1}^{k} |RP(t_{i_s})|}. \tag{3}$$

На втором этапе для каждого полномочия p_i вычисляется уровень критичности:

$$S(p_i) = \sum_{\rho(t,t_s):(t_s - \text{ лист}) \wedge (RP(t_s)=\{p_i\})} \left(\prod_{j:t_j \in \rho(t,t_s)} w_j \right). \tag{4}$$

Суммирование ведётся по всем ориентированным маршрутам $\rho(t, t_s)$ в дереве T_p, ведущим от корня t к такому листовому узлу t_s, набор полномочий $RP(t_s)$ которого содержит ровно одно полномочие p_i. В каждом произведении используются вычисленные по формуле (3) относительные веса w_j тех узлов t_j, которые составляют ориентированный маршрут $\rho(t, t_s)$ (исключая корень t). Несложно понять, что на втором этапе учтены постулаты 2 и 3: так как для любого допустимого $j : 0 \leqslant w_j \leqslant 1$, то $S(p_i)$ тем больше, чем больше слагаемых и чем меньше множителей, то есть короче путь в формуле (4).

3. Вычислительный эксперимент

Для проверки устойчивости модели в формулу (2) и, как следствие, в формулу (3) был введён параметр α ($\alpha \geqslant 1$):

$$m_{i_j i_s} = \frac{|RP(t_{i_j})|^\alpha}{|RP(t_{i_s})|^\alpha},$$

$$w_{i_j} = \frac{|RP(t_{i_j})|^\alpha}{\sum_{s=1}^{k} |RP(t_{i_s})|^\alpha}. \tag{5}$$

Проведён вычислительный эксперимент с целью исследования влияния параметра α на уровни критичности полномочий. При этом анализировались не только абсолютные величины $S(p)$, а и линейный порядок, порождаемый уровнем критичности на множестве полномочий. Диапазон значений настраиваемого параметра α представлял собой отрезок $[1, 100]$, шаг приращения параметра был равен 1.

Наглядным примером зависимости уровня критичности от параметра α являются графики, представленные на рисунке 4 (а). По оси абсцисс отложены значения параметра α, по оси ординат — значения уровня критичности полномочия $S(p)$. Построение графиков основано на данных для трёхуровневого выровненного ролевого дерева (рис. 3). Заметим, что после некоторого значения α взаимное расположение графиков стабилизируется, что даёт возможность увеличить масштаб построения (см. рис. 4 (б)). Для представленного примера при $\alpha = 1$ последовательность полномочий, упорядоченная по невозрастанию их уровней критичности, имеет вид: $p_8, p_3, p_1, p_5, p_6, p_4, p_2, p_7$. Тогда как для $\alpha = 15$ порядок уже другой: $p_1, p_8, p_7, p_6, p_5, p_4, p_3, p_2$.

Анализ результатов вычислительного эксперимента позволяет сделать следующие выводы.

1. С ростом α наблюдается смена порядка на множестве полномочий. При достижении параметром значения в интервале $[15, 20]$ отношение порядка на множестве полномочий перестаёт изменяться.

2. Параметр α может как совсем незначительно повлиять на ранжирование полномочий (рис. 5 (а)), так и кардинально изменить их порядок (рис. 5 (б)).

Следует отметить, что чем больше значение параметра α, тем меньше величина относительного весового коэффициента w_{i_j} (см. формулу (5)). Зависимость отношения линейного порядка на множестве полномочий, определяемого

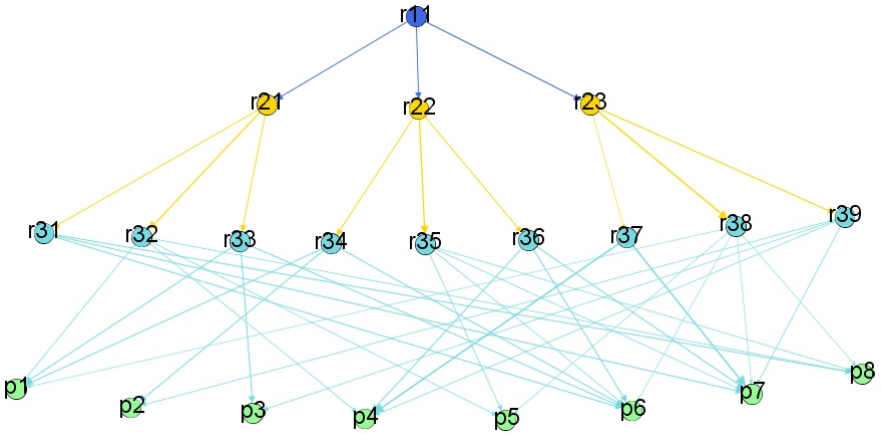
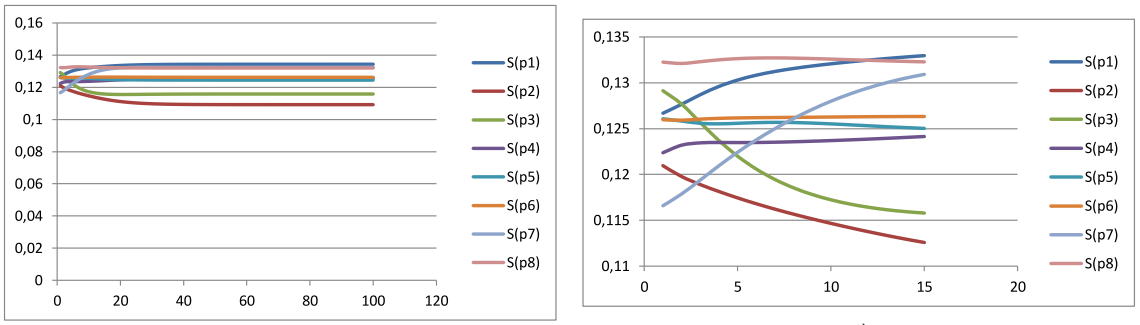


Рис. 3. Пример расширенного ролевого дерева, построенного для трёхуровневой выровненной иерархии ролей



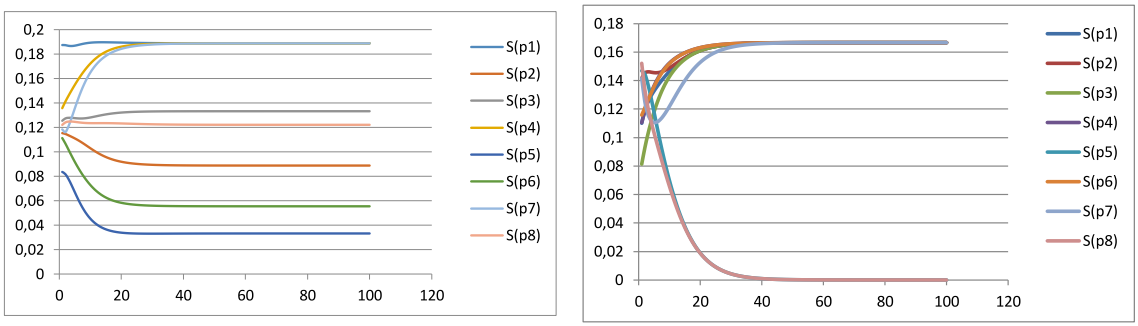
а) б)

Рис. 4. Графики зависимости уровня критичности полномочия от параметра α, полученные для расширенного ролевого дерева, представленного на рисунке 3

их уровнями критичности, от параметра α позволяет управлять значимостью постулатов при расчёте уровня критичности: чем больше α, тем менее значим постулат 1 (число полномочий, приписанных одной роли), а следовательно, большее значение приобретают постулаты 2 и 3 (распространённость полномочия в иерархии и «близость к администратору»). Таким образом, настраиваемый параметр α позволяет администратору безопасности оценить значимость полномочий в различных предположениях об уязвимостях ролевой иерархии.

Заключение

Предлагаемые в статье количественные характеристики полномочий могут являться основой для определения вероятности реализации угроз информационной безопасности через уязвимости, порождаемые структурой ролей политики разграничения доступа (см. формулу (1)). При этом уровень критичности $S(p_i)$ полномочия есть оценка априорной вероятности утечки полномочия p_i через уязвимость, скрытую в ролевом графе.



а) б)

Рис. 5. Графики зависимости уровня критичности от параметра α

Наличие в системе полномочий, уровень критичности которых превышает некоторое пороговое значение, может являться причиной реструктуризации ролевой иерархии с целью уменьшения этих показателей.

Литература

1. Bogachenko N.F. Local Optimization of the Role-Based Access Control Policy // CEUR Workshop Proceedings. 2017. Vol. 1965. URL: `http://ceur-ws.org/Vol-1965/paper14.pdf` (дата обращения: 21.02.2019).
2. NIST SP 800–30 Revision 1. Information Security. Guide for Conducting Risk Assessments. September 2012.
3. Емалетдинова Л.Ю., Аникин И.В. Анализ подходов к оценке рисков информационной безопасности в корпоративных информационных сетях // Вестник Казанского государственного энергетического университета. 2015. № 1(25). С. 55–67.
4. Belim S.V., Belim S.Yu., Bogachenko N.F., Kabanov A.N. User Authorization in a System with a Role-Based Access Control on the Basis of the Analytic Hierarchy Process // IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics). 14–16 Nov., 2017. URL: `http://ieeexplore.ieee.org/document/8239432/` (дата обращения: 21.02.2019).

RANKING OF PERMISSIONS ON THE BASIS OF ANALYSIS OF ROLES HIERARCHY IN ACCESS CONTROL MODELS

N.F. Bogachenko
Ph.D. (Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru
A.V. Filippova
Student, e-mail: afelia96@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The term ”severity level of permissions” is introduced for the probability estimation of the permissions leakage in the role-based access control policy. The

postulates which define the dependence of severity levels of permissions on the structure of the role hierarchy are formulated. The technique (method and algorithm) of automatic calculation of severity levels of permissions is suggested, using analytic hierarchy process. The computing experiment which reveals the dependence of severity level of permission on the algorithm's parameter is made. The algorithm's parameter allows regulating the influence of postulates on results of calculations.

Keywords: roles, permissions, redundancy, severity level, analytic hierarchy process.

References

1. Bogachenko N.F. Local Optimization of the Role-Based Access Control Policy. CEUR Workshop Proceedings, 2017, vol. 1965, URL: `http://ceur-ws.org/Vol-1965/paper14.pdf` (21.02.2019).
2. NIST SP 800–30 Revision 1. Information Security. Guide for Conducting Risk Assessments. September 2012.
3. Emaletdinova L.Yu. and Anikin I.V. Analiz podkhodov k otsenke riskov informatsionnoi bezopasnosti v korporativnykh informatsionnykh setyakh. Vestnik Kazanskogo gosudarstvennogo energeticheskogo universiteta, 2015, no. 1(25), pp. 55–67. (in Russian)
4. Belim S.V., Belim S.Yu., Bogachenko N.F. and Kabanov A.N. User Authorization in a System with a Role-Based Access Control on the Basis of the Analytic Hierarchy Process. IEEE Dynamics of Systems, Mechanisms and Machines (Dynamics), 14–16 Nov., 2017, URL: `http://ieeexplore.ieee.org/document/8239432/` (21.02.2019).

Дата поступления в редакцию: 21.02.2019