

Ранжирование полномочий на основе анализа иерархии ролей в моделях разграничения доступа

Н.Ф. Богаченко
nfbogachenko@mail.ru

А.В. Филиппова
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 уровня критичности полномочий от структуры ролевой иерархии. Предложена методика (метод и алгоритм) автоматического расчёта уровня критичности полномочий, использующая метод анализа иерархий. Проведён вычислительный эксперимент, выявляющий зависимость уровня критичности полномочий от настраиваемого параметра алгоритма. Настраиваемый параметр позволяет регулировать влияние постулатов на результаты вычислений.

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) старшая в иерархии роль наследует полномочия непосредственно подчинённых ей ролей;
- 2) пользователь, авторизованный на некоторую роль, автоматически авторизуется 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:

$$R(V, T) = P(V, T) \cdot I(T), \quad (1)$$

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 трехфакторного способа оценки рисков), $I(T)$ – ущерб от реализации угрозы T [3]. Основной сложностью

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

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 полномочий

При реализации в компьютерной системе подсистемы разграничения доступа возникает так называемая проблема скрытых каналов утечки информации: возможна ли передача информации между субъектами и объектами в обход политики разграничения доступа. Применительно к ролевому разграничению доступа анализ скрытых каналов утечки информации заключается в контроле наличия у пользователей избыточных полномочий. 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 алгоритма расчёта уровня критичности полномочий использована теоретико-графовая формализация ролевой политики разграничения доступа [1]. Рассматриваются такие элементы модели, как множество полномочий $P = \{p_1, \dots, p_m\}$ и множество ролей $R = \{r_1, \dots, r_n\}$. Иерархия ролей описывается с помощью ориентированного графа, в котором вершины соответствуют ролям, определённым в системе, метки вершин – наборам их полномочий, направленные ребра (дуги) задают отношение авторизации ролей друг на друга (см. рис. 1).

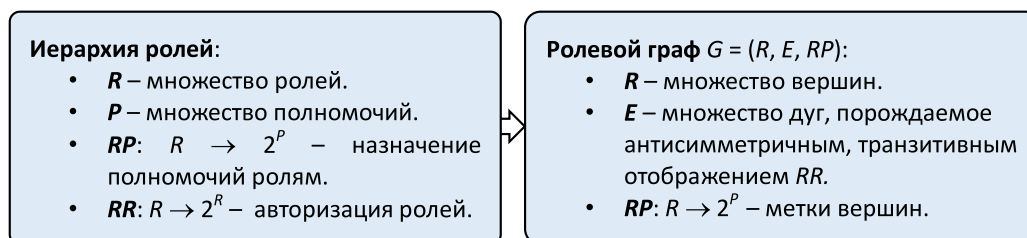


Рис. 1: Теоретико-графовое представление иерархии ролей

Уровнем критичности полномочия $p_i \in P$ назовём числовую характеристику $S(p_i)$, отражающую значимость p_i с точки зрения возможности его утечки. 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 в системе, так и от значимости ролей, которым приписано это полномочие. Тем самым уровень критичности полномочий 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 больше вероятность атаки на неё, тем больше уровень критичности полномочий, сопоставленных этой роли.

Постулат 2. Чем чаще встречается полномочие в списках полномочий ролей, тем больше вероятность его утечки, тем больше его уровень критичности.

Постулат 3. Чем выше роль в иерархии, тем больше вероятность атаки на неё, тем больше уровень критичности полномочий, сопоставленных этой роли.

2 Вычисление уровня критичности

К методике расчёта уровня критичности полномочий были предъявлены следующие требования:

- 1) учёт постулатов 1 – 3;
- 2) автоматизация процесса вычисления.

Основная идея предложенного подхода 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 : каждая листовая вершина пополняется вершинами-сыновьями по числу её полномочий, каждая новая вершина в качестве метки содержит ровно одно полномочие из списка полномочий своего родителя.

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

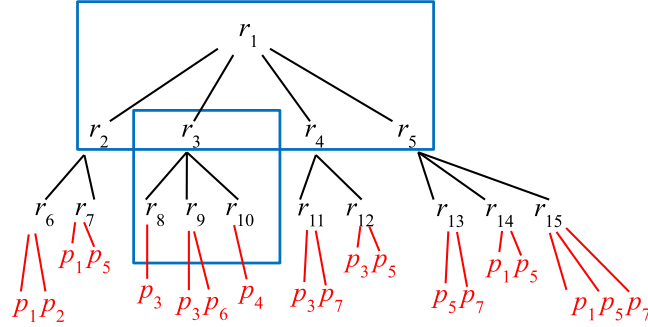


Рис. 2: Пример расширенного ролевого дерева T_p

Алгоритм оценки уровня критичности полномочий состоит из двух этапов:

- 1) вычисление относительных весовых коэффициентов для всех вершин дерева T_p , кроме корневой;
- 2) вычисление комбинированных весовых коэффициентов (уровней критичности) для каждого из полномочий.

На первом этапе для каждой нелистой вершины t_i дерева T_p , начиная с корня, рассматривается подмножество непосредственно подчинённых ей вершин $\{t_{i_1}, \dots, t_{i_k}\}$. Для вершин этого подмножества строится матрица парных сравнений. Но в отличие от классического метода анализа иерархий, коэффициенты матрицы заполняются не экспертами, а вычисляются автоматически по формуле

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

где $|RP(t)|$ – число полномочий, приписанных вершине t . С учётом постулата 1, эта величина соотносит уровень критичности полномочий, приписанных вершине t_{i_j} , с уровнем критичности полномочий, приписанных вершине t_{i_s} . Заполненные таким образом матрицы будут идеально согласованными [4], а формула для расчёта относительных весовых коэффициентов примет следующий вид:

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

На втором этапе для каждого полномочия p_i вычисляется уровень критичности:

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

Здесь сумма берётся по всем ориентированным путям $\rho(t, t_s)$ в дереве T_p , ведущим от корня t к такому листу t_s , список полномочий $RP(t_s)$ которого содержит единственное полномочие p_i . В каждом произведении участвуют вычисленные по формуле (3) относительные весовые коэффициенты w_j тех вершин t_j , которые составляют ориентированный путь $\rho(t, t_s)$ (исключая корень t). Несложно понять, что на втором этапе учтены постулаты 2 и 3: так как для любого допустимого j : $0 \leq w_j \leq 1$, 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 ($\alpha \geq 1$):

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

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

Проведён вычислительный эксперимент с целью исследования влияния параметра α на уровень 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 5 (а). По оси абсцисс отложены значения параметра α , по оси ординат – значения уровня критичности полномочий $S(p)$. Построение графиков основано на данных для трёхуровневого выровненного ролевого дерева (рис. 3 и 4). Столбец «Sum(Si)» в таблице проверяет выполнение условия $\sum_{i=1}^m S(p_i) = 1$. Крайне правый столбец заполняется последовательностью из порядковых номеров полномочий в соответствии с их уровнем критичности: от полномочия, имеющего максимальный уровень критичности, к полномочию с минимальным уровнем. Заметим, что после некоторого значения α , взаимное расположение графиков стабилизируются и возникает необходимость увеличить масштаб построения. Рисунок 5 (б) иллюстрирует зависимость на основе той же таблицы (рис. 4), но для значений параметра от 1 до 15.

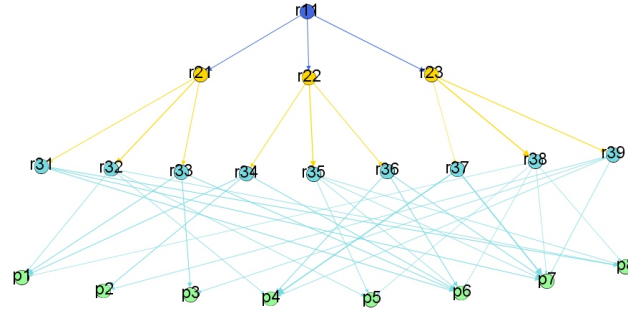


Рис. 3: Пример расширенного ролевого дерева, построенного для трёхуровневой выровненной иерархии ролей

	a	S(p1)	S(p2)	S(p3)	S(p4)	S(p5)	S(p6)	S(p7)	S(p8)	Sum(Si)		max->min
1	0,126674	0,12096	0,129127	0,122366	0,126071	0,125968	0,116587	0,132248		1		8 3 1 5 6 4 2 7
2	0,127648	0,119775	0,127676	0,123191	0,125824	0,125914	0,117871	0,132101		1		8 3 1 6 5 4 2 7
3	0,128694	0,118901	0,125664	0,123446	0,125577	0,126033	0,119391	0,132293		1		8 1 6 3 5 4 7 2
4	0,129594	0,118142	0,123695	0,123484	0,125521	0,126117	0,120951	0,132496		1		8 1 6 5 3 4 7 2
5	0,130292	0,117447	0,121992	0,123478	0,125578	0,126164	0,122421	0,132628		1		8 1 6 5 4 7 3 2
6	0,130821	0,116808	0,120588	0,123486	0,125648	0,12619	0,123766	0,132693		1		8 1 6 5 7 4 3 2
7	0,131228	0,116219	0,119453	0,123517	0,125679	0,126208	0,12499	0,132706		1		8 1 6 5 7 4 3 2
8	0,131554	0,115671	0,118542	0,123566	0,12566	0,126225	0,126099	0,132683		1		8 1 6 7 5 4 3 2
9	0,131827	0,115156	0,117814	0,123625	0,125601	0,126243	0,127097	0,132636		1		8 1 7 6 5 4 3 2
10	0,132063	0,114668	0,117237	0,123694	0,125515	0,126262	0,127985	0,132577		1		8 1 7 6 5 4 3 2
11	0,132274	0,114203	0,116782	0,12377	0,125414	0,12628	0,128765	0,132511		1		8 1 7 6 5 4 3 2
12	0,132466	0,113762	0,116427	0,123853	0,125309	0,126296	0,12944	0,132446		1		1 8 7 6 5 4 3 2
13	0,132643	0,113345	0,116153	0,123943	0,125206	0,126308	0,130018	0,132384		1		1 8 7 6 5 4 3 2
14	0,132805	0,112952	0,115946	0,124038	0,125109	0,126316	0,130505	0,132327		1		1 8 7 6 5 4 3 2
15	0,132955	0,112585	0,115792	0,124138	0,125021	0,126321	0,130912	0,132276		1		1 8 7 6 5 4 3 2

Рис. 4: Таблица зависимости уровня критичности полномочий от параметра α

Анализ результатов вычислительного эксперимента (высота иерархии варьировалась от 2 до 5 уровней, мощность множества полномочий выбиралась равной 8) позволяет сделать следующие выводы.

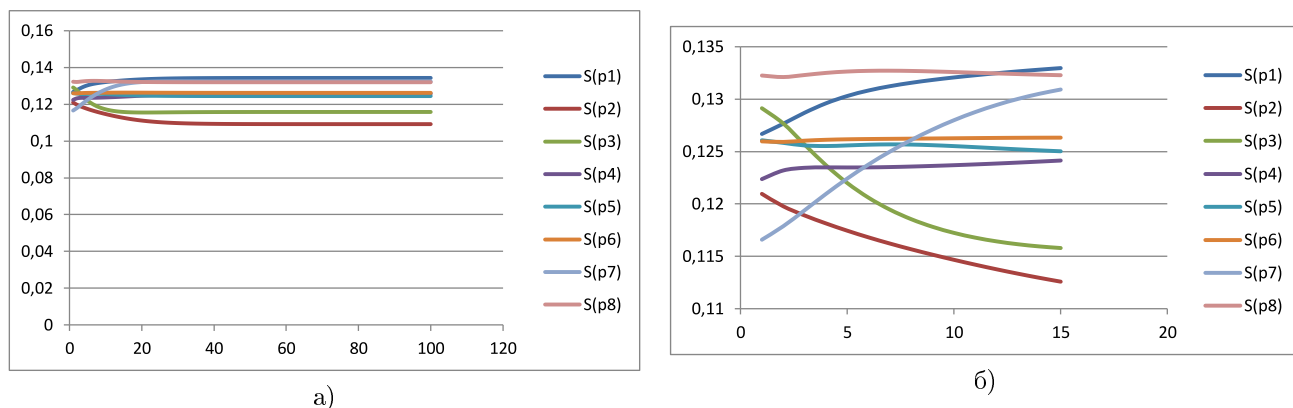


Рис. 5: Графики зависимости уровня критичности полномочий от параметра α , полученные для расширенного ролевого дерева, представленного на рисунке 3

1. С ростом α наблюдается смена порядка на множестве полномочий. При достижении параметром значения в интервале $[15, 20]$ взаимное расположение уровней критичности стабилизируется.
2. Параметр α может как совсем незначительно повлиять на ранжирование уровней критичности полномочий (рис. 6 (а)), так и кардинально изменить их порядок (рис. 6 (б)).

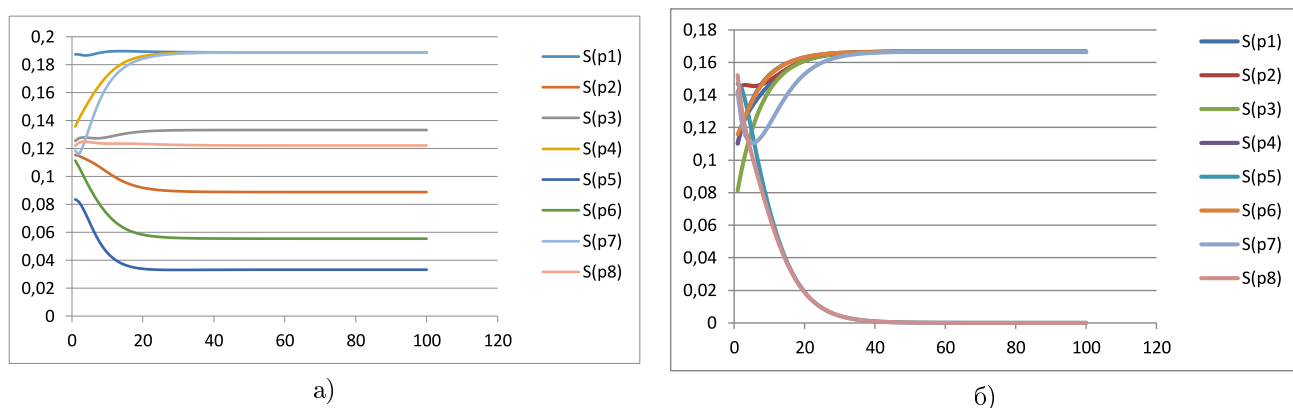


Рис. 6: Графики зависимости уровня критичности от параметра α

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

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

Список литературы

- [1] N.F. Bogachenko. Lokal'naya optimizaciya politiki rolevogo razgranicheniya dostupa (Local Optimization of the Role-Based Access Control Policy). *CEUR Workshop Proceedings*, Vol. 1965, 2017. URL: <http://ceur-ws.org/Vol-1965/paper14.pdf>.
- [2] *NIST SP 800-30 Revision 1. Information Security. Guide for Conducting Risk Assessments*, September 2012.
- [3] L.Yu. Emaletdinova, I.V. Anikin. Risk assessment approaches in telecommunication networks. *Vestnik Kazanskogo gosudarstvennogo energeticheskogo universiteta*, 1(25):55–67, 2015 (In Russian).
- [4] S.V. Belim, S.Yu. Belim, N.F. Bogachenko, A.N. Kabanov. 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/>.

Ranking of Permissions on the Basis of the Analysis of the Roles Hierarchy in Access Control Models

Nadezda F. Bogachenko, Anastasiya V. Filippova

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