Реализация критериев безопасности при построении единой системы разграничения доступа к информационным ресурсам в облачных инфраструктурах

Implementing security criteria when creating a common access isolation system for information resources in cloud infrastructures

Саенко / Saenko I.
Игорь Борисович
(ibsaen@mail.ru)
доктор технических наук, профессор.
ФГКВОУ ВО «Военная академия связи имени Маршала Советского Союза С. М. Буденного» (ВАС им. С. М. Буденного) МО РФ,
профессор.
г. Санкт-Петербург

Бирюков / Birukov M.
Михаил Александрович
(urgent.ma@gmail.ru)
ВАС им. С. М. Буденного,
адъюнкт.
г. Санкт-Петербург

Ясинский / Yasinsky S.
Сергей Александрович
(yasinsky777@mail.ru)
доктор технических наук, доцент.
ЗАО «Институт телекоммуникаций»,
ведущий специалист.
г. Санкт-Петербург

Грязев / Gryazev A.
Андрей Николаевич
(agryazev@zniis.ru)
кандидат технических наук.
ФГУП «Центральный научно-исследовательский институт связи» (ЦНИИС),
генеральный директор.
г. Москва

Ключевые слова: разграничение доступа – access isolation; облачная инфраструктура – cloud infrastructure; управление доступом – access control; критерий безопасности – security criterion; ролевая модель – role model.

Рассматриваются критерии безопасности моделей разграничения доступа в облачных инфраструктурах. Определяются условия их соблюдения при их совместной интеграции. Приводится описание реализации мандатного и дискреционного способа доступа средствами ролевого разграничения доступа. Обсуждаются соблюдение критериев безопасности в облачных инфраструктурах. Предлагается реализовывать разграничение доступа в облачных инфраструктурах средствами ролевой модели доступа.

Access isolation model security criteria in cloud infrastructures are considered. Their compliance conditions at their joint integration are defined. Description of implemented mandatory and discretionary access method using role access control means is shown. Compliance with security criteria in cloud infrastructures using role access model means is discussed.

Введение

Интеграция различных моделей разграничения доступа к информационным ресурсам является перспективным направлением обеспечения кибербезопасности и обусловлена требованиями безопасности к хранению и обработке ресурсов, содержащихся в облачных инфраструктурах [1]. Большинство современных автоматизированных систем используют ролевое разграничение доступа, реализующее концепцию ролей для выдачи полномочий пользователям [2]. Однако в некоторых системах существует необходимость использования меток безопасности и основанного на них мандатного разграничения доступа, а в небольших системах может использоваться дискреционное разграничение доступа. При этом следует учитывать, что интеграция различных частных систем разграничения доступа в единой системе разграничения доступа облачной инфраструктуры предполагает необходимость соблюдения критериев безопасности интегрируемых систем. Рассмотрение способа реализации критериев безопасности в единой системе разграничения доступа облачной инфраструктуры является целью настоящей работы.

1 2018.indd 81 30.03.2018 11:49:42

Критерии безопасности ролевого способа доступа

Ролевая модель разграничения доступа (Role-Based Access Control – RBAC) задает множество ролей пользователей и определяет принадлежность пользователей к одной или нескольким ролям. Предлагается положить модель RBAC в основу построения единой модели разграничения доступа в облачных инфраструктурах. Выбор модели RBAC обусловлен возможностью выражать с ее помощью другие известные модели доступа, а также возможностью доказательства соответствия модели RBAC требованию критерия безопасности ролевой модели.

Для проектирования единой модели RBAC в качестве исходных данных принято использовать [3]:

$U = \{u_i\}, i = 1,...,m, m = |U|$ – множество пользователей;

$PRMS = \{p_j\}, j = 1,...,n, n = |PRMS|$ – множество полномочий;

$ROLES = \{r_l\}, l = 1,...,k, k = |ROLES|$ – множество ролей;

$UA \subseteq U \times ROLES$– бинарное отношение между множествами пользователей и ролей;

$PA \subseteq PRMS \times ROLES$ – бинарное отношение между множествами полномочий и ролей;

$UPA \subseteq U \times PRMS$– бинарное отношение между множествами пользователей и полномочий.

Следует отметить, что результат последовательного применения друг за другом бинарных отношений UA и PA может отличаться от UPA, если ролевая схема имеет некоторые ограничения или она сформирована администратором некорректно. Поэтому для такого бинарного отношения принято использовать обозначение $DUPA$, что означает *Direct UPA*. Пример графа взаимосвязи для ролевой модели доступа приведен на рис. 1.

Иерархическая организация ролей обусловлена установившимся в силовых структурах отношением подчиненности между участниками процессов обработки информации и разделением между ними сфер ответственности. Роли в иерархии упорядочиваются по уровню предоставляемых полномочий [4]. Чем выше в иерархии находится роль, тем больше с ней связано полномочий, поскольку пользователь, имеющий определенную роль, автоматически владеет и всеми подчиненными ей по иерархии ролями [5]. Для ролевой иерархии характерны следующие бинарные отношения:

$RH \subseteq ROLES \times ROLES$– частичное отношение порядка на множестве R, которое определяет иерархию ролей и задает на множестве ролей оператор порядка $\geq$ такой, что если $r_1 \geq r_2$, то роль r_1 находится в иерархии выше, чем роль r_2;

$UA^h \subseteq U \times ROLES$– отношение назначения каждому пользователю набора ролей, причем вместе с каждой ролью в него включаются все роли, подчиненные ей по иерархии, то есть

$$\forall r, r' \in ROLES, u \in U : r > r' \wedge (u, r) \in UA^h \Rightarrow (u, r') \in UA^h;$$

$roles^h : S \to PRMS(ROLES)$– отношение назначения каждому сеансу $s \in S$ набора ролей из иерархии ролей пользователя, работающего в этом сеансе, то есть

$$roles^h(s) \subseteq \left\{ r_l \middle| (\exists r' \geq r_l \Rightarrow (user(s), r') \in UA^h) \right\};$$

$prms^h : S \to PRMS$ – отображение совокупности полномочий, доступных по всем ролям, задействованных пользователем в данном сеансе, с учетом иерархически подчиненных ролей

$$prms^h(s) = U_{r \in ROLES^h(s)} \left\{ p_j \middle| (\exists r'' \leq r(p_j, r) \in PA) \right\};$$

s – сеанс доступа из множества сеансов S;

h – индекс иерархически упорядоченного множества.

При таком способе доступа в качестве критерия безопасности целесообразно использовать следующее правило: система считается безопасной, если любой пользователь системы, работающей в сеансе s, может осуществлять действия, требующие полномочия p, только в том случае, если $p \in prms^h(s)$.

Из формулировки критерия безопасности ролевой модели следует, что управление доступом осуществляется главным образом не с помощью назначения

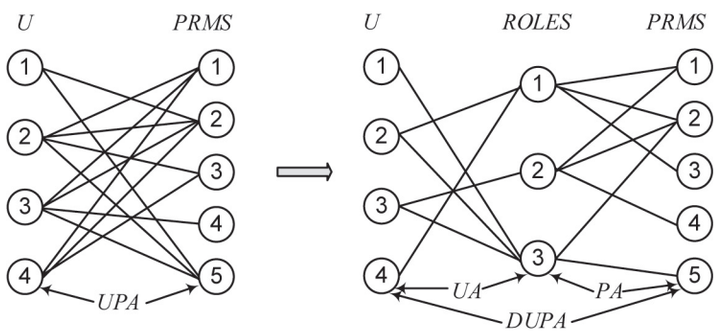


Рис. 1. Пример графа взаимосвязи для ролевой модели доступа

1-2018.indd 82 30.03.2018 11:49:44

полномочий ролям, а путем задания отношения UA^h, назначающего роли пользователям, и функции *roles*, определяющей доступный в сеансе набор ролей. Представление схемы ролевой модели доступа для обеспечения соблюдения выше приведенного критерия безопасности выполним с помощью *UML* (*unified modeling language* – унифицированных язык моделирования).

Управление доступом к информационным ресурсам посредством модели *RBAC* с иерархией ролей осуществляется и в рамках других моделей, выраженных средствами *RBAC*. Это означает, что если ролевая модель не осуществляет контроль доступа к информационным ресурсам системы, то ее безопасность полностью определяется безопасностью тех моделей, которые могут быть выражены ее средствами.

Критерии безопасности дискреционного способа доступа

Дискреционный способ доступа является наиболее простым. Он предназначен для разграничения доступа между субъектами и объектами доступа и позволяет разделить открытую и конфиденциальную информацию без учета категорий конфиденциальности. Классической дискреционной моделью является модель Харрисона-Руззо-Ульмана [6], которая помимо произвольного управления доступом субъектов к объектам осуществляет контроль распространения полномочий на доступ [7].

Дискреционный доступ основывается на выполнении двух условий:

1) все субъекты и объекты идентифицированы;

2) права доступа субъектов к объектам системы определяются некоторым правилом, внешним по отношению к системе.

Такое определение позволяет использовать для представления дискреционного доступа матрицу доступа. Матрица имеет размер $\left|S^{\text{суб}}\right| \times |O|$, где $S^{\text{суб}}$ – множество субъектов компьютерной системы, O – множество объектов. В ячейках матрицы содержится множество прав доступа R, означающих полномочия на выполнение соответствующих действий.

Таким образом, строкам матрицы соответствуют субъекты системы, а столбцам – объекты. Содержимое ячеек матрицы доступа соответствует правам доступа конкретного субъекта к конкретному объекту. Основным достоинством дискреционного доступа является относительная простота реализации системы разграничения доступа.

Очевидно, что ролевой способ доступа по своей сути является модернизацией дискреционного способа, ориентированного на применение в условиях работы с конфиденциальной информацией достаточно большого числа пользователей, каждый из которых может одновременно или попеременно обладать тем или иным заранее установленным набором полномочий относительно объектов доступа (ролями). При этом роли, как определено выше, будут иметь между собой иерархическую подчиненность. Дискреционная матрица доступа в ролевой терминологии есть ни что иное как $UPA \subseteq U \times PRMS$.

В рамках дискреционной модели пространство состояний системы образуется декартовым произведением множества составляющих ее объектов, субъектов и прав – $O \times S^{\text{суб}} \times R$. Текущее состояние системы Q в этом пространстве определяется тройкой, состоящей из множества субъектов, множества объектов и матрицы прав доступа M, описывающей текущие права доступа субъектов к объектам: $Q\,(S^{\text{суб}}, O, M)$. Строки матрицы M соответствуют субъектам, а столбцы – объектам. Поскольку множество объектов включает в себя множество субъектов $S^{\text{суб}} \subset O$, матрица имеет вид прямоугольника. Любая ячейка матрицы $M\,[s^{\text{суб}}, o]$ содержит набор прав субъекта $s^{\text{суб}}$ к объекту o, принадлежащих множеству прав доступа R. Поведение системы во времени моделируется переходами между различными состояниями.

Критерий безопасности дискреционной модели доступа формулируется следующим образом: для заданной системы начальное состояние $Q\,(S^{\text{суб}}, O_0, M_0)$. является безопасным относительно права *right*, если не существует применимой к Q_0 последовательности команд, в результате которой право *right* будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0.

В терминах RBAC можно выразить модель дискреционного управления доступом и ее различные модификации с соблюдением критерия безопасности дискреционного способа. Дискреционная модель обладает высокой детализацией полномочий (с точностью до объекта), поэтому размеры RBAC существенно возрастают.

Учитывая возможность представления дискреционного способа доступа к информационным ресурсам средствами модель RBAC и UML-представления схемы дискреционной модели будет соответствовать частному случаю ролевой модели.

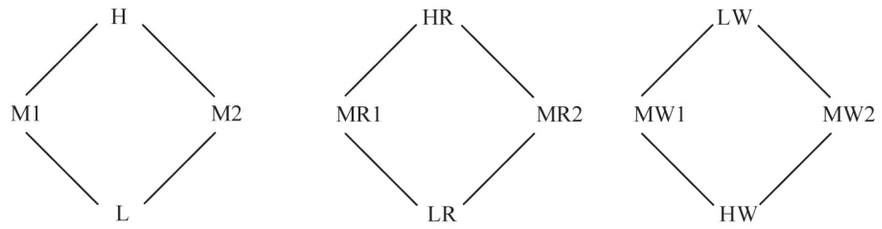
В терминах RBAC можно выразить модель дискреционного управления доступом и ее различные модификации с соблюдением критерия безопасности дискреционного способа. Дискреционная модель обладает высокой детализацией полномочий (с точностью до объекта), поэтому размеры RBAC существенно возрастают.

Учитывая возможность представления дискреционного способа доступа к информационным ресурсам средствами модель RBAC и UML-представления схемы дискреционной модели будет соответствовать частному случаю ролевой модели.

Критерии безопасности мандатного способа доступа

Мандатный способ доступа по сравнению с дискреционным способом является более сложным в реализации и позволяет более эффективно защищать ресурсы. При мандатном способе доступа устанавливаются метки пользователей и ресурсов, регламентирующие доступ

1-2018.indd 83 30.03.2018 11:49:44



а) Ролевая иерархия

б) Ролевая иерархия, нестрогая запись

Рис. 2. Пример схемы РИ мандатной модели доступа

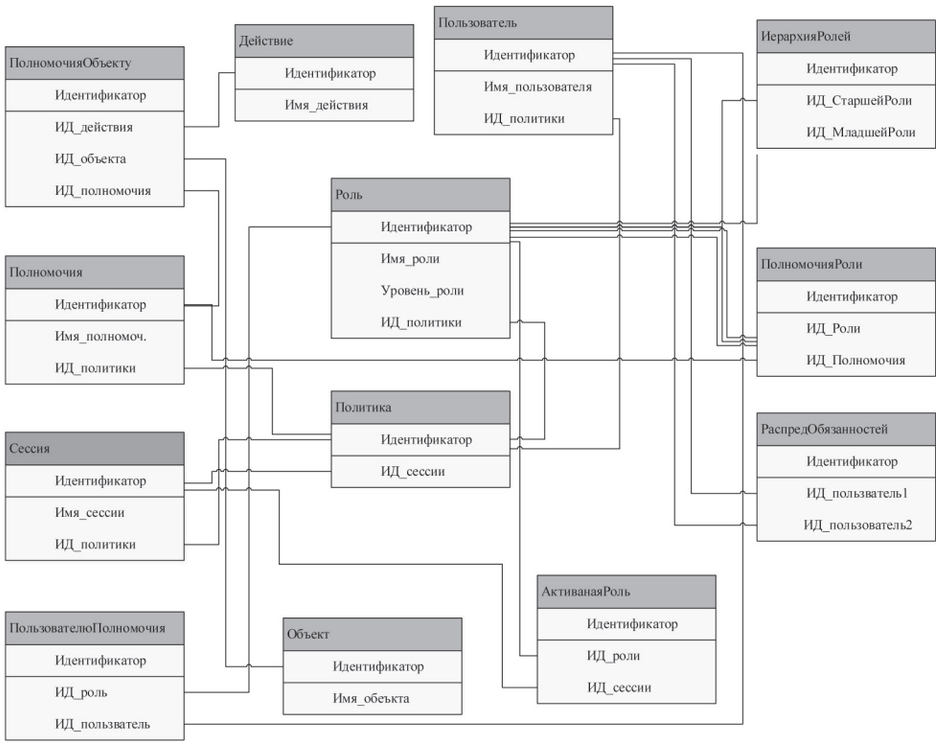


Рис. 3. Пример UML-представление схемы единой системы разграничения доступа

первых ко вторым. Основой мандатных моделей является модель Белла-ЛаПадулы [8], которая основывается на правилах секретного документооборота, обусловленного метками пользователей и ресурсов.

При мандатном способе доступа устанавливаются метки пользователей $M^{\text{п}} = \left\{m_i^{\text{п}}\right\}$ и метки ресурсов $M^{\text{р}} = \left\{m_j^{\text{р}}\right\}$. Доступ i-го пользователя к j-му ресурсу разрешается, если $m_i^{\text{п}} \geq m_i^{\text{р}}$.

Схема разграничения мандатного способа доступа задается матрицей доступа $S^{\text{манд}} = \left\| s_{ij}^{\text{манд}} \right\|$, где

$$s_{ij}^{\text{манд}} = \begin{cases} 0, & \text{если} \quad m_i^{\text{п}} < m_i^{\text{р}} \\ 1, & \text{если} \quad m_i^{\text{п}} \geq m_i^{\text{р}} \end{cases}.$$

Требуемое множество $S^{\text{треб}}$ образуется из единичных элементов требуемой матрицы доступа, реальное множество $S^{\text{реал}}$ – из единичных элементов реализованной матрицы доступа. Для оценки степени совпадения этих схем можно использовать следующий показатель – коэффициент совпадения схем, равный:

$$K^{\text{совп}} = (1 - K^{\text{запр}})(1 - K^{\text{разр}}),$$

где $K^{\text{запр}} \in [0,1]$ – коэффициент избыточного запрещения, а $K^{\text{разр}} \in [0,1]$ – коэффициент избыточного разрешения. Чем выше их значения, тем сильнее схема $S^{\text{реал}}$ отличается от $S^{\text{треб}}$ по соответствующему аспекту.

В [9] предложен способ расчета коэффициентов

1-2018.indd 84 30.03.2018 11:49:45

$K^{разр}$ и $K^{запр}$, который наиболее рационально может быть использован в решении нашей задачи.

Для выражения мандатной модели доступа в терминах RBAC предлагается использовать подход, основанный на решетках классов доступа с частичным отношением порядка. Модифицируемый критерий безопасности типа «звезда» базируется на следующих двух определениях.

Определение 1. Нестрогое *− правило. Субъект может записывать информацию в объект, если $m_i^{п} \geq m_i^{р}$.

Определение 2. Строгое *− правило. Субъект может записывать информацию в объект, если $m_i^{п} = m_i^{р}$.

Основная идея моделирования мандатной решетки состоит в том, чтобы создать ролевую иерархию (РИ), соответствующую схеме мандатной модели. Стоит отметить, что чем выше роль в РИ, тем больше у нее полномочий. На рис. 2 приведен пример схемы РИ мандатной модели доступа, где *Read* − полномочие на чтение (*R*), *Write* − полномочие на запись (*W*), *High* − высокая (*H*), *Medium* − средняя (*M*), *Low* − низкая (*L*) мандатные метки, причем *M*1 и *M*2 − метки, соответствующие правилу 1 и 2. В строгой записи РИ (рис. 2а) доминирующие роли находятся на верхнем уровне иерархии. Для удовлетворения правилам чтения и записи в мандатной модели доступа необходимо использовать две различные РИ (рис. 2б).

В случае моделирования мандатного метода с нестрогим правилом записи получим следующую схему RBAC:

$R = \{HR, M1R, M2R, LR, HW, M1W, M2W, LW\}$ − роли для чтения и записи;

$PRMS = \{(o, read), (o, write) \mid o$ − объект системы$\}$ − полномочия на запись и чтение соответственно.

Существует следующее ограничение на $\{UA = U \times ROLES\}$ − каждому пользователю присваиваются ровно две следующие роли: xR и xW.

Имеется следующее ограничение на сессии − каждая сессия активирует ровно 2 роли: yR и yW.

Существует ограничение на отображение $\{PA = PRMS \times ROLES\}$ в виде

$$xR \mid \exists(o, r) \Leftrightarrow xW \mid \exists(o, w) .$$

При моделировании мандатного способа доступа со строгим правилом записи получим *RBAC*, но РИ для записи станет дискретной, в следующем виде: $R = \{HW, M1W, M2W, LW\}$.

Таким образом, предложенная реализация обеспечивает соблюдение критерия безопасности мандатной модели.

Результатом объединения UML-представлений схем всех рассмотренных моделей доступа будет являться UML-представление схемы единой системы разграничения доступа к ресурсам облачной инфраструктуры с учетом описанных выше механизмов интеграции существующих моделей доступа с моделью *RBAC*. Пример UML-представления схемы единой системы разграничения доступа приведен на рис. 3.

Заключение

Реализация предлагаемой схемы единой системы разграничения доступа станет этапом реализации облачной инфраструктуры, соответствующей особым требованиям безопасности, предъявляемым к информационному обеспечению. Этот результат обеспечивается за счет создания единой системы разграничения доступа к разнородным информационным ресурсам, с учетом соблюдения критериев безопасности частных систем разграничения доступа, интегрируемых в облачной инфраструктуре.

Работа выполнена при поддержке РФФИ (проект 18-07-01369) и бюджетной темы № АААА-А16-116033110102-5.

Литература

1. Котенко, И. В. Аналитический обзор докладов международного семинара «Научный анализ и поддержка политик безопасности в киберпространстве» (SA&PS4CS 2010) / И.В. Котенко, И.Б. Саенко, Р.М. Юсупов // Труды СПИИРАН. − 2010. − № 2 (13). − С. 226−248.

2. Модель администрирования схем разграничения доступа в облачных инфраструктурах / И.Б. Саенко [и др.] // Информация и Космос. − 2017. − № 1. − С. 121−126.

3. Vaidya, J. The Role Mining Problem: Finding a Minimal Descriptive Set of Roles / J. Vaidya, V. Atluri, Q. Guo // 12th ACM symposium on Access control models and technologies. − 2007. − P. 175−184.

4. Clark, D. D. A Comparison of Commercial and Military Computer Security Policies / D.D. Clark, D.R. Wilson // Proceedings of the 1987 Symposium on Security and Privacy. − IEEE Computer Society, Washington, D.C. − 1987. − P. 184−195.

5. Зегжда, Д. П. Контроль доступа к информационным ресурсам в информационно-телекоммуникационных системах высокой доступности / Д.П. Зегжда, А.В. Коротич // Наукоемкие технологии. − 2007. − Т. 8, № 11. − С. 41−46.

6. Ferraiolo, D. Role based access control: Features and motivations / D. Ferraiolo, J. Cugini, D.R. Kuhn // Annual Computer Security Applications Conference. − IEEE Computer Society Press. − 1995.

7. Harrison, M. Monotonic protection systems / M. Harrison, W. Ruzzo // Foundation of secure computation. − 1978.

8. LaPadula, L. J. Secure Computer Systems: A Mathematical Model / L.J. LaPadula, D.E. Bell // MITRE Corporation Technical Report 2547. −Vol. II. − 31 May, 1973.

9. Саенко, И. Б. Генетическая оптимизация схем ролевого доступа / И.Б. Саенко, И.В. Котенко // Системы высокой доступности. − 2011. − Т. 7, № 2. − С. 112−116.

1-2018.indd 85 30.03.2018 11:49:45