

Оптимизация политики безопасности при объединении информационных систем

С.В. Белим
sbelim@mail.ru

С.Ю. Белим
belimsv@gmail.com

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

Аннотация

Проведено моделирование процесса объединения двух информационных систем с различными политиками безопасности. Используется субъектно-объектный подход. Проведена формализация задачи объединения политик безопасности. Сформулирована оптимизационная задача для объединенной политики безопасности. Рассмотрены случаи объединения двух дискреционных политик безопасности и двух мандатных политик безопасности. Выделены критерии оптимальности итоговой политики безопасности.

Введение

В процессе объединения двух информационных систем они становятся подсистемами одной большой системы. При этом возникает необходимость согласования большого количества параметров для их непротиворечивого взаимодействия и обеспечения непрерывности функционирования. Одним из подмножеств таких параметров являются настройки безопасности, определяемые политикой разграничения доступа. Оптимальное решение может быть получено, как правило, только при проектировании всей системы «с нуля». Однако этот подход практически не осуществим в силу требований бизнес-процессов. В связи с этим, актуальной является задача разработки подходов и критериев качества объединения двух политик безопасности.

Можно выделить отдельные ситуации, требующие объединения двух политик безопасности в локальной системе. Во-первых, в настоящее время многие системы прикладного программного обеспечения имеют собственную встроенную политику безопасности. В качестве примера можно привести виртуальные машины, системы управления базами данных, комплексные системы защиты информации и т.д. При этом данные прикладные системы работают под управлением тех или иных операционных систем. Для работы в прикладной системе пользователь должен предварительно авторизоваться в операционной системе. Объекты прикладной системы хранятся в файлах операционной системы. Таким образом, необходимо согласовывать права доступа операционной системы и прикладной среды. Следует отметить, что прикладная система и операционная система могут иметь политики безопасности отличающиеся не только по конфигурации, но и по типу. Например, в большинстве современных СУБД разграничение доступа реализовано на базе ролевой политики безопасности. При этом пользователи работают с табличными пространствами и таблицами, хранящихся в файлах. Доступ к файлам разграничивается средствами операционной системы с использованием дискреционной политики безопасности. Обладая нужными правами в операционной системе злоумышленник может вносить изменения в таблицы, работая с файлами и не имея, при этом

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>

необходимых прав в СУБД. Та же проблема возникает при организации доступа к файлам, хранящимся на виртуальной машине. С одной стороны действует политика безопасности, настроенная на виртуальной машине, с другой стороны виртуальный жесткий диск представляет собой файл, доступ к которому разграничивается базовой операционной системой. Отсюда вытекает необходимость согласования двух политик безопасности, организующих доступ к одним и тем же данным. Кроме этого большое распространение получила технология установки базы данных на виртуальном сервере, которая требует совмещения сразу трех политик безопасности.

На сегодняшний день предложено несколько подходов к описанной проблеме [1, 2, 3, 4], однако все они носят специализированный характер и ориентированы на конкретные программные решения. Общая же постановка задачи на уровне математической модели отсутствует. Целью данной статьи ставится моделирование процесса объединения двух формальных политик безопасности в рамках субъектно-объектного подхода.

1 Субъектно-объектная модель объединения информационных систем

Будем использовать субъектно-объектный подход описания информационных систем. В этом случае все вопросы безопасности описываются в терминах доступов субъектов к объектам. Обозначим множество объектов первой системы через O_1 , а множество объектов второй системы через O_2 . Также введем обозначения для множества активных сущностей (субъектов) первой системы S_1 и второй системы – S_2 . Объединение двух систем приводит к простому объединению множества объектов и множества субъектов. Таким образом, для множества объектов объединенной системы O можем записать:

$$O = O_1 \cup O_2.$$

Аналогично для множества субъектов объединенной системы S будет выполняться равенство:

$$S = S_1 \cup S_2.$$

Второе утверждение является менее очевидным, чем первое. Оно налагает достаточно жесткие требования полного объединения систем. То есть отсутствует механизм имперсонализации, характерный для объединения нескольких операционных систем в домен.

Обозначим политику безопасности, действующую в первой информационной системе через P_1 . Под политикой безопасности понимается множество прав разграничения доступа. В частности, P_1 разграничивает доступ субъектов из множества S_1 к объектам из множества O_1 . Политику безопасности для второй системы обозначим через P_2 . Она разграничивает доступ субъектов из множества S_2 к объектам из множества O_2 . При объединении двух информационных систем необходимо определить политику безопасности P , разграничивающую доступ субъектов из множества S к объектам из множества O . Политика безопасности объединенной системы P не сводится к их прямому объединению:

$$P \neq P_1 \cup P_2.$$

Это утверждение следует из того, что при прямом объединении остаются неопределенными права доступа субъектов из множества S_1 к объектам из множества O_2 и субъектов из множества S_2 к объектам из множества O_1 . Введем две взаимные политики безопасности. Множество правил доступа субъектов из множества S_1 к объектам из множества O_2 обозначим через P_{12} . Множество правил доступа субъектов из множества S_2 к объектам из множества O_1 обозначим через P_{21} . Тогда можно записать следующее равенство:

$$P = P_1 \cup P_2 \cup P_{12} \cup P_{21}.$$

Для принятия решения о разрешении или запрете доступа любая модель безопасности использует некоторые информационные структуры. Например, для дискреционной политики безопасности вся информация о правах доступа хранится в матрице доступов. В мандатной политике безопасности решение принимается на основе сравнения меток безопасности. Ролевая политика безопасности основана на списках полномочий ролей и списках аутентификации пользователей на роли. Эти информационные структуры необходимо дополнить для определения взаимных политик безопасности. При этом следует учитывать возможность возникновения коллизий. Две различные части объединенной политики безопасности могут

принимать различные решения для одного и того же запроса на доступ. Для разрешения коллизий требуются дополнительные процедуры согласования политик безопасности. Причем согласование в ряде случаев представляет собой достаточно серьезную проблему.

Решение задачи согласования политик безопасности может решаться различными способами. Рассмотрим два крайних случая – «жесткий» и «мягкий». Жесткий подход состоит в обеспечении максимальной защищенности от утечек информации. Достичь этого можно с помощью следующего требования: «доступ разрешен тогда и только тогда, когда он разрешен обеими политиками безопасности». Такой подход позволяет избежать появления новых разрешенных доступов в подсистемах, которые ранее были самостоятельными системами. Однако жесткий подход может приводить к новым запретам на доступ, которые ранее отсутствовали, что снижает функциональность объединенной системы. Противоположный ему мягкий подход основывается на принципе: «доступ разрешен, если он разрешен хотя бы одной из политик безопасности». В этом случае не появляются новые запреты на доступ, но могут появляться новые разрешения на доступ. То есть мягкий подход обеспечивает максимальную функциональность путем уступок возможности утечки информации. Таким образом, жесткий подход максимизирует конфиденциальность информации, тогда как мягкий подход максимизирует доступность информации. Доступность и конфиденциальность представляют собой две неотъемлемые составляющие информационной безопасности. Отсюда следует, что выбор алгоритма согласования политик безопасности может быть сформулирован как оптимизационная задача с двумя параметрами – конфиденциальность и доступность. Возможен также промежуточный вариант объединения, в котором правила разграничения доступа частично формулируются по жесткому варианту, частично по мягкому или по каким-то другим алгоритмам. В этом случае нужен некоторый дополнительный алгоритм принятия решения какую из политик безопасности P_1 или P_2 применять в каждом конкретном случае. Такой промежуточный подход будем называть «полужестким».

При каждом варианте построения согласованной политики безопасности будем вычислять две величины: D – количество запрещенных доступов в объединенной информационной системе, которые были разрешены до объединения, A – количество разрешенных доступов в объединенной информационной системе, которые были запрещены до объединения. Оптимизационная задача состоит в минимизации обеих величин D и A . Для строгой формулировки оптимизационной задачи согласования политик безопасности введем целевую двух параметрическую функцию F :

$$F = k_1 D + k_2 A,$$

где k_1, k_2 – весовые коэффициенты, показывающие относительную важность доступности и конфиденциальности в конкретной задаче, причем

$$k_1 + k_2 = 1.$$

Оптимизационная задача в этом случае формулируется следующим требованием:

$$F \rightarrow \min$$

Следует также отметить, что всегда выполняется неравенство $F \geq 0$. Поэтому если какое-то решение обеспечивает нулевое значение целевой функции ($F = 0$), то оно является оптимальным.

При жестком варианте объединения политик безопасности важную роль играет только количество новых запретов, так как новые разрешения отсутствуют. Целевая функция будет определяться одним параметром:

$$F = D.$$

В мягком варианте объединения политик безопасности новые запреты не появляются, поэтому целевая функция будет зависеть только от количества новых разрешенных доступов:

$$F = A.$$

Выбор алгоритма согласования политик безопасности определяется их типом. Одни и те же подходы не всегда применимы для разных типов разграничения доступа. На сегодняшний день строго сформулированы три базовые модели безопасности: дискреционная, мандатная и ролевая. Объединяться могут как две однотипных политики безопасности с различными информационными структурами, так и две политики безопасности разного типа. Таким образом, можно сформулировать шесть оптимизационных задач согласования политик безопасности.

Некоторые задачи согласования политик безопасности были рассмотрены авторами в более ранних работах. Один из подходов совмещения ролевой и мандатной политик безопасности представлен в статье [5].

Объединение двух мандатных политик безопасности рассмотрено в статье [6]. Совмещение ролевых политик с различными иерархиями ролей изучено в [7]. Во всех этих работах используется жесткий вариант объединения информационных систем. Один из возможных полужестких вариантов предложен в статье [8].

2 Примеры объединения политик безопасности

Рассмотрим с точки зрения оптимальности два примера объединения политик безопасности одного типа. Простейшей и в то же время базовой для всех информационных систем является дискреционная политика разграничения доступа. Права доступа в дискреционной политике безопасности объединены в матрицу доступов. Второй случай, который мы рассмотрим, состоит в объединении двух мандатных политик безопасности. Основной информационной структурой мандатной политики безопасности служит решетка ценностей. В обоих случаях будем рассматривать прямое объединение и вычислять для него целевую функцию F .

2.1 Объединение двух дискреционных политик безопасности

Пусть для первой системы с дискреционным разграничением доступа политика безопасности P_1 задана матрицей доступов M_1 . Аналогично для второй системы политика безопасности P_2 задана матрицей доступов M_2 . Объединенная политика безопасности P может быть задана с помощью матрицы доступов следующего вида:

M_1	M_3
M_4	M_2

Ячейки блоков M_3 и M_4 могут быть заданы администратором системы произвольным образом независимо от M_1 и M_2 . Такой вариант объединения является жестким, так как не приводит к появлению новых разрешенных доступов, отсутствующих до объединения ($A = 0$), вследствие того, что исходные матрицы доступа M_1 и M_2 остаются неизменными. По причине неизменности матриц доступа M_1 и M_2 не появляется и новых запретов на доступ ($D = 0$). Следовательно, целевая функция будет иметь нулевое значение $F = 0$ и решение является оптимальным.

2.2 Объединение двух мандатных политик безопасности

Пусть для первой системы с мандатным разграничением доступа политика безопасности P_1 основана на решетке ценностей L_1 , а для второй системы мандатная политика безопасности P_2 основана на решетке ценностей L_2 . Политика безопасности объединенной системы будет основана на прямом объединении двух исходных решеток $L = L_1 \times L_2$. Оценим значение целевой функции F . Новых разрешенных доступов в этом случае возникнуть не может, поэтому $A = 0$ и объединение является жестким. Прямое произведение приводит к тому, что каждому объекту и субъекту будет приписано, по сути, две метки безопасности из разных решеток, что может приводить к коллизиям. Поэтому в общем случае $D > 0$ и, следовательно, $F > 0$. Можно сделать вывод о том, что в общем случае прямое объединение не является оптимальным. Оптимальность может быть достигнута тонкими настройками для конкретных систем, либо полужесткими вариантами объединения.

Заключение

В заключении выделим основные проблемы, возникающие при объединении двух и более политик безопасности:

1. Приведение структур данных политик безопасности различного типа к универсальному виду.
2. Трудности проведения формального анализа безопасности вследствие большого объема и сложности структуры данных политики безопасности.
3. Трудности анализа рисков, связанные с большим количеством прав, привилегий и активных сущностей системы.

4. Выбор политики безопасности, обеспечивающей минимальные угрозы конфиденциальности при минимальном снижении доступности данных.

Все эти проблемы не могут быть решены в едином ключе и требуют рассмотрения большого количества частных случаев.

Список литературы

- [1] P. Bonatti, S. de Capitani di Vimercati, P. Samarati. A modular approach to composing access control policies. *In Proceedings of the 7th ACM conference on Computer and communications security, Athens, Greece, (CCS '00)*.:164–173, 2000.
- [2] A. Filippoupolitis, E. Gelenbe. A distributed decision support system for building evacuation. *In Proceedings of the 2nd conference on Human System Interactions (HSI'09)*. :320–327, 2009.
- [3] I. Flechais, C. Mascolo, M.A. Sasse. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics.*, 1(1):12–26, 2007.
- [4] F. Rezaeibagha, Y. Mu. Access Control Policy Combination from Similarity Analysis for Secure Privacy-Preserved EHR Systems. *IEEE Trustcom/BigDataSE/ICSS.*:386–393, 2017.
- [5] S.V. Belim, N.F. Bogachenko, Yu.S. Rakitsky. Theoretical-Graph Approach to the Problem of Combining Role-Based and Mandatory Security Policies. *Information Security Problems. Computer Systems*, 2:9–17, 2010.
- [6] Yu.S. Rakitsky, S.V. Belim. Model' Sovmesheniya Dvukh Mandatnikh Politik Bezopasnosti. *Bezopasnost' Informatsionnykh Tekhnologiy*, 18(1):125–126, 2011.
- [7] S.V. Belim, N.F. Bogachenko. Building the Role-Based Security Policy on the Directed Graph. *Information Security Problems. Computer Systems*, 3:7–17, 2009.
- [8] S.V. Belim, N.F. Bogachenko, Yu.S. Rakitsky. The Security Policies Joint Implementation Based on Decision Support Algorithms. *Information and Control Systems*, 5(84):66–72, 2016.

Optimization of Security Policy at Information Systems Integration

Sergey V. Belim, Svetlana Yu. Belim

The modeling of integration for two information systems with various security policies is carried out. The subject-object approach is used. The formalization of integration problem for two information system is made. The optimization problem is formulated. Cases of integration for two discretionary security policies and for two mandatory security policies are considered. Criteria of optimality for total security policy are marked out.