Математические структуры и моделирование 2018. № 3(47). С. 126–131

УДК 004.056.5
DOI: 10.25513/2222-8772.2018.3.126-131

ПРОБЛЕМЫ ПОСТРОЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ ПРИ ОБЪЕДИНЕНИИ ИНФОРМАЦИОННЫХ СИСТЕМ

С.В. Белим
профессор, д.ф.-м.н., профессор кафедры информационной безопасности,
e-mail: sbelim@mail.ru
С.Ю. Белим
доцент, к.п.н., доцент кафедры информационной безопасности,
e-mail: svbelim@gmail.com

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

Аннотация. В статье рассмотрена проблема построения политики безопасности при объединении двух информационных систем как оптимизационная задача. В данной задаче выделены два параметра — конфиденциальность и доступность информации. Записана целевая функция. Рассмотрены варианты объединения систем с одинаковыми моделями безопасности. Исследована оптимальность предложенных решений.

Ключевые слова: политика безопасности, дискреционное разграничение доступа, мандатное разграничение доступа.

Введение

Проблема объединения информационных систем с самостоятельными политиками безопасности возникает в большом количестве прикладных задач. Прежде всего такая задача является актуальной при объединении сетей двух независимых организаций с требованием непрерывной работы всех систем. Идеальной будет ситуация полного пересмотра всех правил разделения доступа и создание единой логически выстроенной политики безопасности. Однако в большом количестве случаев ставится требование обеспечения непрерывности всех процессов, что делает невозможной полную пересборку системы.

Существует ряд ситуаций в локальных системах, когда также возникает ситуация двух политик безопасности. Прежде всего необходимость выполнения двух политик безопасности возникает при установке в рамках операционной системы прикладного программного обеспечения с собственными правилами разграничения доступа. К таким прикладным системам можно отнести виртуальные машины, системы управления базами данных, комплексные системы защиты информации и т. д. Например, при подключении к базе данных пользователя СУБД обеспечивает разграничение доступа к табличным пространствам и таблицам, как правило, в рамках ролевой политики безопасности. С другой

стороны СУБД осуществляет хранение таблиц в файлах, к которым пользователь может получить доступ средствами операционной системы. Несмотря на то, что СУБД, как правило, защищает свои файлы от внесения изменений другими процессами, пользователь, обладая определённым набором прав, может это сделать. Аналогичная ситуация с виртуальными машинами, виртуальный жёсткий диск которых для операционной системы представляет собой обычный файл. В связи с развитием технологии виртуализации распространённым явлением стали базы данных, установленные на виртуальном сервере. Для обеспечения безопасности таких систем необходим учёт сразу трёх политик безопасности. Также следует упомянуть о часто встречающейся задаче объединения баз данных.

До настоящего времени проблема построения объединённой политики безопасности решалась преимущественно для специализированных систем [1–4].

Целью данной статьи ставится построение формальной модели объединения двух и более политик безопасности в рамках субъектно-объектной модели.

1. Объединение информационных систем

Рассмотрим процесс объединения информационных систем с точки зрения формального субъектно-объектного подхода построения политики безопасности. Пусть множество объектов первой системы O_1, а второй — O_2. Соответственно, множества субъектов S_1 и S_2. В новой объединённой информационной системе множество объектов $O = O_1 \cup O_2$, а множество субъектов — $S = S_1 \cup S_2$. Пусть в первой системе действует политика безопасности P_1, а во второй — P_2. Необходимо построить политику безопасности P для новой объединённой информационной системы. Все вопросы безопасности решаются рассмотрением доступов субъектов к объектам. Политика безопасности P_1 определяет легитимность доступов субъектов из множества S_1 к объектам из множества O_1. Политика безопасности P_2 определяет легитимность доступов субъектов из множества S_2 к объектам из множества O_2. При объединении необходимо разграничить доступ субъектов из множества S_1 к объектам из множества O_2 и субъектов из множества S_2 к объектам из множества O_1. Каждая политика безопасности использует определённые дополнительные структуры данных, на основе которых определяются права доступа. В дискреционной политике безопасности такой структурой является матрица доступов, в мандатной политике безопасности — метки безопасности, в ролевой политике безопасности — списки полномочий ролей. При расширении множеств объектов и субъектов структуры данных политик безопасности требуют расширения с учётом новых элементов. Так структуры данных политики безопасности P_1 должны быть доопределены для элементов множеств S_2 и O_2, а структуры данных политики безопасности P_2 должны быть доопределены для элементов множеств S_1 и O_1. При этом может возникнуть проблема, связанная с тем, что одни и те же доступы разграничиваются двумя независимыми политиками безопасности. Две политики безопасности могут принимать различные решения для одного и того же доступа. В дальнейшем эту ситуацию будем называть проблемой

согласования политик безопасности.

При решении проблемы согласования политик возможны два различных подхода. Первый подход согласования политик безопасности, будем называть его «жёстким», состоит в том, что доступ разрешён тогда и только тогда, когда он разрешён обеими политиками безопасности. В этом случае не появляется дополнительных разрешённых доступов, однако могут появиться дополнительные запреты на доступ, что может приводить к нежелательным последствиям в вопросах доступности информации и снижать производительность системы. Второй подход, будем называть его «мягким», состоит в том, что доступ разрешён, если он разрешён хотя бы одной из политик безопасности. В этом случае не появляется новых запретов на доступ, что положительно сказывается на доступности информации, однако могут возникнуть дополнительные разрешённые доступы, которые являются потенциальными каналами утечки информации. Таким образом, задачу согласования политик безопасности можно рассматривать как оптимизационную с двумя параметрами — конфиденциальность и доступность.

Кроме рассмотренных двух крайних вариантов согласования, жёсткого и мягкого, возможен и промежуточный вариант, в котором для каждого из доступов выбирается доминирующая политика безопасности. В этом случае система принимает решение, основываясь на политике безопасности P_1 или P_2 в зависимости от параметров доступа и текущего состояния системы. Данный вариант согласования политик безопасности будем называть «полужёстким».

Определим целевую функцию оптимизационной задачи согласования политик безопасности. Необходимо, чтобы минимальным было как количество новых запрещённых доступов D, так и новых разрешённых доступов A. Используем метод весовых коэффициентов, тогда целевая функция будет иметь вид:

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

где k_1, k_2 — весовые коэффициенты, показывающие относительную важность доступности и конфиденциальности в конкретной задаче, причём $k_1 + k_2 = 1$.

Для жёсткого согласования политик безопасности $F = k_1 D$, для мягкого — $F = k_2 A$. Для полужёсткого варианта согласования политик безопасности необходимо выбирать алгоритм принятия решения о доступе, для которого $F \to min$. Следует учитывать, что всегда $F \geqslant 0$. Если какое-то решение обеспечивает нулевое значение целевой функции, то оно является оптимальным.

Проблема согласования политик безопасности существенно зависит от их типа. В различных ситуациях возможны различные проблемы и решения. На сегодняшний день распространены три принципиально разных типа политик безопасности — дискреционная, мандатная и ролевая. Возможно объединение двух однотипных или разнотипных политик безопасности. Всего существует шесть различных вариантов объединения.

Ряд вопросов объединения политик безопасности уже был рассмотрен авторами в более ранних статьях. Проблемы совмещения ролевой и мандатной политик безопасности были рассмотрены в статье [5]. В работе [6] представлен подход к объединению двух мандатных политик безопасности. Объединение

двух ролевых моделей безопасности рассмотрено в статье [7]. Все эти работы связаны с жёстким вариантом совмещения политик безопасности. Полужёсткие варианты совмещения двух политик безопасности рассмотрены в статье [8].

2. Примеры объединения информационных систем

Рассмотрим два примера объединения двух информационных систем с одинаковыми моделями безопасности. Простейшим случаем является объединение двух систем с дискреционной политикой безопасности, права доступа в которых определяются матрицами доступов. Второй случай состоит в объединении двух мандатных политик безопасности, задаваемых различными решётками ценностей. В обоих случаях будем использовать классическое решение и проверять его на оптимальность.

2.1. Объединение двух дискреционных политик безопасности

Рассмотрим случай, когда обе политики безопасности являются дискреционными. Пусть политика безопасности первой системы P_1 определяется матрицей доступов M_1, а политика безопасности второй системы P_2 определяется матрицей доступов M_2. Разграничение доступа в объединённой системе может быть сведено к дискреционной политике безопасности, матрица доступов M которой будет иметь вид:

M_1	M_3
M_4	M_2

Подматрицы M_3 и M_4 определяются произвольно администратором независимо от M_1 и M_2. При таком объединении не возникает ни новых разрешённых доступов ($A = 0$), ни новых запретов на доступ ($D = 0$). Следовательно, целевая функция $F = 0$ и решение является оптимальным.

2.2. Объединение двух мандатных политик безопасности

Пусть для первой системы выполняется политика безопасности P_1 на основе решётки ценностей L_1, а для второй системы — P_2 на основе решётки ценностей L_2. Традиционное решение состоит в построении объединённой политики безопасности P с решёткой ценностей, определяемой как декартово произведение исходных решёток $L = L_1 \times L_2$. Рассмотрим оптимальность такого решения. Очевидно, что «лишних» доступов в этом случае не возникает, поэтому $A = 0$. Однако у каждого объекта возникают метки безопасности от «чужой» решётки ценностей, что может приводить к запрету доступов, существовавших ранее. В связи с этим в общем случае $D > 0$, откуда следует $F > 0$ и решение не является оптимальным. Оптимальности можно добиться, используя «мягкие» методы объединения политик безопасности.

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 объёма 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.

Литература

1. Bonatti P., de Capitani di Vimercati S., Samarati P. A modular approach to composing access control policies // Proceedings of the 7th ACM conference on Computer and communications security, Athens, Greece, (CCS '00). 2000. P. 164–173.
2. Filippoupolitis A., Gelenbe E. A distributed decision support system for building evacuation // Proceedings of the 2nd conference on Human System Interactions (HSI'09). 2009. P. 320–327.
3. Flechais I., Mascolo C., Sasse M.A. Integrating security and usability into the requirements and design process // International Journal of Electronic Security and Digital Forensics. 2007. V. 1(1). P. 12–26.
4. Rezaeibagha F., Mu Y. Access Control Policy Combination from Similarity Analysis for Secure Privacy-Preserved EHR Systems // IEEE Trustcom/BigDataSE/ICESS. 2017. P. 386–393.
5. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Теоретико-графовый подход к проблеме совмещения ролевой и мандатной политик безопасности // Проблемы информационной безопасности. Компьютерные системы. 2010. № 2. С. 9–17.
6. Ракицкий Ю.С., Белим С.В. Модель совмещения двух мандатных политик безопасности // Безопасность информационных технологий. 2011. Вып. 1. С. 125–126.
7. Белим С.В., Богаченко Н.Ф. Построение ролевой политики безопасности на произвольном ориентированном графе // Проблемы информационной безопасности. Компьютерные системы. 2009. Вып. 3. С. 7–17.
8. Белим С.В., Богаченко Н.Ф., Ракицкий Ю.С. Совмещение политик безопасности, основанное на алгоритмах поддержки принятия решений // Информационно-управляющие системы. 2016. № 5(84). С. 66–72.

PROBLEMS OF SECURITY POLICY CREATION AT INFORMATION SYSTEMS ASSOCIATION

S.V. Belim
Dr.Sc. (Phys.-Math.), Professor, e-mail: sbelim@mail.ru
S.Yu. Belim
Ph.D. (Ped.), Associate Professor, e-mail: svbelim@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. In article the problem of security policy creation at two information systems association as an optimizing task is considered. In this task two parameters — confidentiality and availability of information are allocated. Criterion function is make up. Options of systems association with identical security models are considered. The optimality of the proposed solutions is investigated.

Keywords: security policy, discretionary access control, mandatory access control.

Дата поступления в редакцию: 14.03.2018