Анализ формальных понятий для объединения прав пользователей в компьютерных системах

Ю.С. Ракицкий
yrakitsky@gmail.com

Т.Ю. Балашова
t.balaschova@mail.ru

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

Аннотация

В статье рассматривается анализ формальных понятий, как инструмент для изменения политики безопасности в компьютерных системах. Применение анализа формальных понятий позволяет в некоторых случаях объединять пользователей с аналогичными правами для объединения их в группы. Приведены примеры, показывающие, что возможно объединение пользователей с аналогичными правами в группы, что уменьшает количество субъектов в рамках политики безопасности.

Введение

Анализ формальных понятий широко известен как метод обработки данных, извлекающий из этих данных концептуально общие структуры [1, 2, 3]. Он основан на концепции формального контекста, из которого берется таксономическая структура понятий. Задача извлечения знаний из больших баз данных связана с определенными трудностями, в частности с большой размерностью данных, набором хранимых неактуальных данных для обработки и т. Д. На сегодняшний день было реализовано много успешных проектов по применению анализа формальных понятий в промышленных базах данных. Однако анализ формальных концепций не был применен к обработке таким структурам данных, как матрицы доступа в компьютерных системах. Сложность задачи разграничения доступа в больших системах заключается в хранении и управлении структурами данных, хранящими права доступа субъектов к объектам системы. Вопросам разграничения доступа посвящено большое количество работ [4, 5, 6]. При этом, в случае наличия большого количества пользователей (субъектов), объем структур данных увеличивается пропорционально количеству субъектов. Также, в больших системах постоянно меняются наборы объектов, и новые объекты необходимо администрировать с точки зрения безопасности. Описанные условия приводят к тому, что централизованное администрирование безопасности объектов при использовании дискреционной политики безопасности становится практически невозможным. В данной работе рассматривается возможность применения анализа формальных понятий для объединения субъектов с одинаковыми правами доступа в группы. В случае объединения нескольких пользователей в группу, управление правами доступа в системе становится более простой задачей, поскольку уменьшается количество субъектов, которым необходимо устанавливать права. Показаны случаи, в которых применение анализа формальных понятий не дает уменьшения количества сущностей. Рассмотрены простейшие примеры применения анализа формальных понятий при решении задачи объединения пользователей с одинаковыми правами доступа в группы.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2017 (DMS-2017), Omsk, Russia, October 2017, published at http://ceur-ws.org

1 Анализ формальных понятий

Рассмотрим теоретические основы анализа формальных понятий.

Определение 1. Формальный контекст K есть тройка (G, M, I), где G —множество, называемое множеством объектов, M — множество, называемое множеством признаков, $I \subseteq G \times M$ — отношение.

Отношение I можно интерпретировать следующим образом: для $g \in G, m \in M$ имеет место gIm, если объект g обладает признаком m.

Для формального контекста K=(G, M, I) и произвольных $A \subseteq G$ и $B \subseteq M$ определена пара отображений
$A' = m \in M \mid gIm$ для всех $g \in A$
$B' = g \in G \mid gIm$ для всех $m \in B$

Определение 2. Формальное понятие формального контекста $K = (G, M, I)$ есть пара (A, B), где $A \subseteq G$, $B \subseteq M$, $A' = B$, $B' = A$. Множество A называется объемом, а B — содержанием понятия (A, B).

Применим описанные понятия к дискреционной политике безопасности в компьютерной системе. В качестве множества G мы будем рассматривать множество пользователей компьютерной системы. В качестве множества M можно рассматривать множество прав доступа, определенных в матрице доступов (содержимое матрицы доступов). Отношение I показывает обладает ли указанным правом доступа m определенный пользователь g. Множество A, являющееся объемом понятия (A, B), задает набор пользователей, обладающих одинаковыми правами в рамках понятия. Множество B, являющееся содержимым понятия (A, B), задает набор прав, одинаковых для набора пользователей в рамках понятия. Определив таким образом множества, можно применить саму процедуру анализа формальных понятий в случае дискреционной политики безопасности для компьютерной системы.

2 Примеры применения анализа формальных понятий для оптимизации дискреционной политики безопасности

Рассмотрим несколько примеров применения анализа формальных понятий для оптимизации дискреционной политики безопасности. Для простоты в основу примеров положена система, в которой функционирует пять пользователей (Alice, Bob, Charlie, Dave, Eve) и три файла (Text.txt — текстовый файл, Soft.exe — приложение, Pr.ppt — презентация). Матрица доступов строится на предположении, что в системе присутствуют три базовых права доступа (read — чтение, write — запись и execute — выполнение). Построение рисунков выполнялось с помощью [4].

Пример 1. Пусть права в системе назначены следующим образом: все пользователи имеют право читать файл Text.txt, право записи на этот файл имеет только пользователь Dave, право запускать приложение Soft.exe имеют только пользователи Alice и Bob, право на чтение презентации имеют Bob, Charlie и Eve, право на запуск презентации имеют Alice, Bob, Charlie и Eve. Тогда формальный контекст примет вид, указанный (см. рис. 1).

	Text.txt read	Text.txt write	Soft.exe ex...	Pr.ppt read	Pr.ppt execute
Alice	X		X		X
Bob	X		X	X	X
Charlie	X			X	X
Dave	X	X			
Eve	X			X	X

Рис. 1: Формальный контекст, есть пользователи с одинаковыми правами

Из рисунка видно, что пользователи Charlie и Eve имеют одинаковые права в системе, и можно предположить, что их можно объединить в одну группу. Результат анализа представлен на рис. 2.

Из полученных результатов видно, что пользователи Charlie и Eve объединены в один узел решетки контекстов, а для пользователя Bob не имеет смысла выделять отдельную группу, поскольку он будет участником двух групп, находящихся на графе выше (группа для Charlie и Eve, Alice). Это означает, что возможно на базе текущей матрицы доступов создать систему разграничения доступа из трех групп. В результате сложность администрирования значительно снижается, поскольку вместо пяти активных сущностей в системе придется администрировать только три. Проверим, будет ли применение анализа формальных понятий так же эффективно при изменениях в начальной матрице доступов.

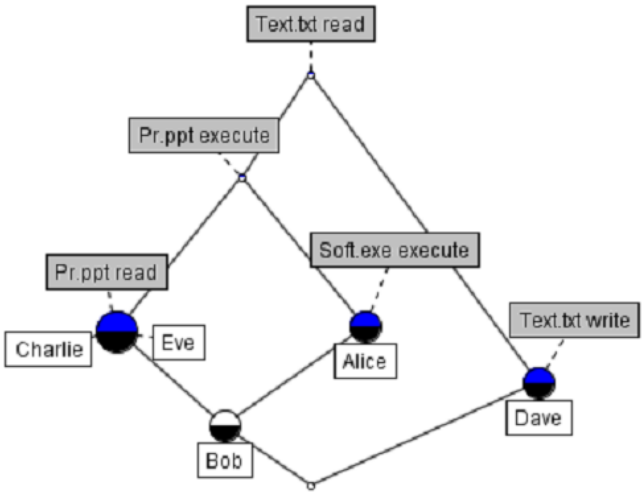

Рис. 2: Решетка контекста

Пример 2. Пусть права в системе назначены следующим образом: все пользователи имеют право читать файл Text.txt, право записи на этот файл имеет только пользователи Charlie и Dave, право запускать приложение Soft.exe имеют только пользователи Alice и Bob, право на чтение презентации имеют Bob, Charlie и Eve, право на запуск презентации имеют Alice, Bob и Charlie. Тогда формальный контекст примет вид, указанный (см. рис. 3).

	Text.txt read	Text.txt write	Soft.exe execute	Pr.ppt read	Pr.ppt execute
Alice	×		×		×
Bob	×		×	×	×
Charlie	×	×		×	×
Dave	×	×			
Eve	×			×	

Рис. 3: Формальный контекст, нет пользователей с одинаковыми правами

Из рисунка видно, что нет пользователей с одинаковыми правами. Результат анализа представлен на рис. 4.

Из полученных результатов видно, что пользователь Bob получит права пользователей Alice и Eve, поскольку он будет участником двух групп, находящихся на графе выше (группы Alice и Eve). Аналогичным образом пользователь Charlie получит права пользователей Dave и Eve, поскольку он будет участником двух групп, находящихся на графе выше (группы Dave и Eve). Это означает, что возможно на базе текущей матрицы доступов создать систему разграничения доступа из трех групп, даже при условии, что изначально не существует пользователей с одинаковыми правами. В результате сложность администрирования значительно снижается, поскольку вместо пяти активных сущностей в системе придется администрировать только три. Приведем еще один пример.

Пример 3. Пусть права в системе назначены следующим образом: Eve имеет право читать файл Text.txt, право записи на этот файл имеет только пользователь Dave, право запускать приложение Soft.exe имеют только пользователь Bob, право на чтение презентации имеет Alice, право на запуск презентации имеет Charlie. Тогда формальный контекст примет вид, указанный (см. рис. 5).

Из рисунка видно, что нет пользователей с одинаковыми правами. Также очевидно, что множества прав пользователей не пересекаются. Исходя из этого можно сделать предположение, что объединить каких-либо пользователей в группы не удастся. Результат анализа представлен на рис. 6.

Из полученных результатов действительно видно, что ни один пользователь не может быть объединен в группу с другим пользователем. Это следствие непересекающихся наборов прав пользователей. В результате сложность администрирования не меняется.

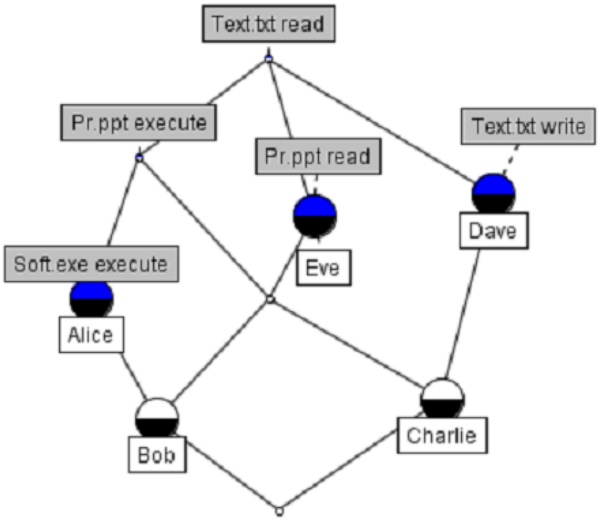

Рис. 4: Решетка контекста

	Text.txt read	Text.txt write	Soft.exe execute	Pr.ppt read	Pr.ppt execute
Alice				×	
Bob			×		
Charlie					×
Dave		×			
Eve	×				

Рис. 5: Формальный контекст, нет пересекающихся прав

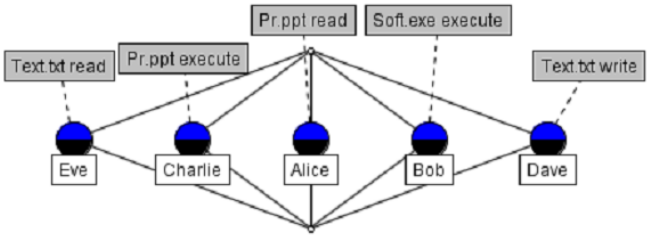

Рис. 6: Решетка контекста

Заключение

Проведенное исследование эффективности анализа формальных понятий применительно к задаче оптимизации дискреционной политики разграничения доступа показывает, что данный метод достаточно эффективен в больших системах. Большие системы характеризуются большим количеством пользователей, которые рассматриваются как объекты формального контекста. Также отличительной особенностью больших систем является большое количество пассивных сущностей (например, файловые объекты) , к каждому из которых назначаются права доступа. При таких условиях вероятность того, что у всех пользователей окажутся неперсекающиеся наборы прав, достаточно мала. Тем не менее, рассмотренные примеры показывают, что в некоторых ситуациях анализ формальных понятий не приводит к существенному улучшению политики безопасности. Также, необходимо учитывать, что в рассмотренных примерах не учитывается многообразие прав доступа в реальных системах и наличие привилегий учетных записей. Поэтому применение анализа формальных понятий в компьютерных системах для улучшения дискреционной политики безопасности требует дальнейшего рассмотрения и совершенствования.

Список литературы

[1] C. Carpineto, G. Romano. *Concept data analysis: Theory and applications.* John Wiley & Sons, 2004.

[2] B. Ganter, R. Wille. *Formal Concept Analysis. Mathematical Foundations.* Springer, 1999.

[3] B. Ganter, G. Stumme, R. Wille. *Formal Concept Analysis. Foundations and Applications.* Springer, 2005.

[4] S.V. Belim, N.F. Bogachenko, J.S. Rakitsky. Theoretical-Graph Approach to the Problem of Combining RoleBased and Mandatory Security Policies. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2:9–17, June 2010 (In Russian).

[5] S.V. Belim, N.F. Bogachenko, J.S. Rakitsky. Combining of Role-Based and Mandatory Security Policies. *Problemy obrabotki i zashchity informatsii. Kniga 1. Modeli politik bezopasnosti komp'iuternykh sistem. Kollektivnaia monografia*, 117–132, 2010 (In Russian).

[6] S.V. Belim, N.F. Bogachenko. Using a Hierarchy Analysis Method to Assess Permission Leakage Risks in Systems with a Role Based Access Control. *Informatsionno-upravliaiushchie sistemy*, 6:67–72, June 2013 (In Russian).

[7] S.A. Yevtushenko. System of data analysis "Concept Explorer". *Proceedings of the 7th national conference on Artificial Intelligence KII-2000*, 127–134, 2000 (In Russian).

Analysis of Formal Concepts for Combining User Rights in Computer Systems

Yuriy S. Rakitsky, Tatyana Yu. Balashova

The article deals with the analysis of formal concepts, as a tool for changing the security policy in computer systems. The use of analysis of formal concepts allows in some cases to combine users with similar rights to group them together. Examples are given showing that it is possible to merge users with similar rights into groups, which reduces the number of subjects within the security policy.