REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 6, Number 304 (2015), 20 – 25

UDC 004.056.5

ACCESS CONTROL MODELS FOR DATABASE SERVERS

E.Zh. Aythozhaeva
Kazakh national research technical university named after K.I.Satpayev, Almaty, Kazakhstan
ait_djam@mail.ru

Keywords: mandatory access control, discretionary access control, formal models of access security.

Abstract. The problem of access control is discussed. The advantages and disadvantages of the most common access control methods are analyzed: Discretionary Access Control (DAC) and Mandatory Access Control (MAC). Overview of general formal models of access security is presented. These models are the basis for the DAC and the MAC. There are models of Goguen-Meseguer, Sutherland, Hoffman, Harrison-Ruzzo-Ulman, Take-Grant, TAM, Clark-Wilson, Biba, Bell-LaPadula, McLean, LWM, Dion. The security aspects that they solve are specified. The issues of implementation of mandatory access control for special and commercial database servers based on the classical model of Bell-LaPadula are discussed. Disadvantages of this model and mandatory access control for commercial servers are indicated. The full and correct access control in commercial servers is possible based on Dion model. The necessity to develop a formal model of mandatory access on the basis of Dion model, taking into account the features of construction and functioning of DBMS, is proved.

УДК 004.056.5

Модели управления доступом в серверах баз данных

Е.Ж. Айтхожаева
Казахский национальный исследовательский технический университет
им. К.И.Сатпаева

Ключевые слова: мандатное управление доступом, дискреционное управление доступом, формальные модели безопасности доступа.

Аннотация. Рассматривается проблема управления правами доступа. Анализируются достоинства и недостатки наиболее распространенных методов управления правами доступа: избирательной политики безопасности (Discretionary Access Control - DAC) и полномочной политики безопасности (Mandatory Access Control - MAC). Выполняется обзор общих формальных моделей безопасности доступа, основные идеи которых послужили основой для DAC и MAC. Указаны аспекты безопасности, которые они решают. Представлены модели Гогена-Мезигера, Сазерлендская, Хоффмана, Харрисона-Руззо-Ульмана, Take-Grant, TAM, Кларка-Вильсона, Биба, Белла-ЛаПадула, Мак-Лина, LWM, Диона. Обсуждаются вопросы реализации принудительного управления доступом в специальных и коммерческих серверах баз данных, в основе которого лежит классическая модель Белла-ЛаПадула. Указываются недостатки этой модели и недостатки принудительного управления доступом в коммерческих серверах. Полное и корректное принудительное управление доступом в коммерческих серверах возможно на основе модели Диона. Обосновывается необходимость разработки формальной модели мандатного доступа на основе модели Диона, учитывающей особенности построения и функционирования СУБД.

К настоящему времени человечеством накоплено огромное количество информации об объектах и явлениях, которые хранятся в электронном виде и используются в базах данных (БД). Согласно законодательству Республики Казахстан компьютерным базам данных предоставляется такая же правовая охрана, как и имущественным и личным неимущественным правам. Обеспечение эффективной защиты информационных ресурсов предполагает соблюдение высоких критериев безопасности, как необходимого условия сохранения конфиденциальности критически важной информации практически в любых областях деятельности. Одним из основных критериев

является политика безопасности организации, которая, в частности, определяет, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать. Таким образом, защита информации напрямую связана с проблемой разграничения доступа пользователей к хранимой информации. Анализ причин нарушений безопасности показывает, что 89% недостатков средств защиты приходится именно на долю системы разграничения доступа [1].

Для решения этой проблемы используется управление правами доступа [2,3]. Существуют различные подходы к управлению правами доступа, но на практике обычно используются два метода управления правами доступа: произвольный (дискреционный, Discretionary Access Control - DAC) и принудительный (MAC - мандатная защита) [4,5].

В большинстве систем реализуется встроенными программными средствами произвольное управление доступом (дискреционная политика безопасности). Главное его достоинство – гибкость, главные недостатки – рассредоточенность управления и сложность централизованного контроля, а также оторванность прав доступа от данных, что позволяет копировать секретную информацию в общедоступные файлы. Существенный недостаток DAC заключается в том, что он не предоставляет полной гарантии того, что информация не станет доступна субъектам, не имеющим к ней доступа. Субъект, имеющий право на чтение информации, может передать ее другим субъектам, которые этого права не имеют, без уведомления владельца объекта. Система DAC не устанавливает никаких ограничений на распространение информации после того как субъект ее получил. Еще одной особенностью DAC, которую можно отнести к недостаткам, является то, что все объекты в системе принадлежат субъектам, которые настраивают доступ к ним для других. На практике оказывается, что в большинстве случаев данные в системе принадлежат не отдельным субъектам, а всей системе. Наиболее распространенным примером такой системы является информационная система.

В DAC доступ выдается к именованным объектам (контейнерам данных), а не к хранящимся в объектах данным. Для реляционной СУБД объектом будет, например, именованное отношение (то есть таблица), а субъектом — зарегистрированный пользователь. В этом случае нельзя в полном объеме ограничить доступ только к части информации, хранящейся в таблице. Частично проблему ограничения доступа к информации в СУБД решают представления и использование хранимых процедур, которые реализуют тот или иной набор бизнес-правил.

Этого недостатка лишена мандатная защита (полномочная политика безопасности). Мандатная защита предназначена для построения систем с более высокой степенью защищенности и представляет собой полномочное (принудительное) управление доступом. Разграничение доступа субъектов к объектам данных основано на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. MAC предполагает наличие четкой неизменяемой классификации информации по типу секретности и пользователей по уровню благонадежности, а это возможно только в организациях с жесткой структурой. Использование СУБД с возможностями мандатной защиты позволяет разграничить доступ собственно к данным, хранящимся в информационной системе, от доступа к именованным объектам данных. Единицей защиты в этом случае будет являться, в частности, запись (строка таблицы), а не таблица или представление, содержащее множество записей.

Самое важное достоинство MAC заключается в том, что пользователь не может полностью управлять доступом к ресурсам, которые он создаёт. Политика безопасности системы, установленная администратором, полностью определяет доступ, и обычно пользователю не разрешается устанавливать более свободный доступ к его ресурсам чем тот, который установлен администратором пользователю. А DAC разрешает пользователям полностью определять доступность их ресурсов, что означает, что они могут случайно или преднамеренно передать доступ неавторизованным пользователям.

В настоящее время существует несколько формальных (абстрактных) моделей безопасности доступа, идеи которых послужили основой для DAC и MAC (модели безопасности в распределенных системах не рассматриваются).

Модель Гогена-Мезигера (Goguen-Meseguer), представленная ими в 1982 г., основана на теории автоматов. Система может при каждом действии переходить из одного разрешенного

состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы - домены. Переход системы из одного состояния в другое выполняется только в соответствии с таблицей разрешений. В таблице указано, какие операции может выполнять субъект, принадлежащий определенному домену, над объектом с учетом домена объекта. Используется для анализа скрытых каналов утечки информации.

Модель Хоффмана является обобщенной математической моделью для анализа защищенности информации, в которой распространение угроз в среде взаимосвязанных объектов описывается с помощью соединенных между собой элементарных зон защиты информации.

Сазерлендская (от англ. Sutherland) модель защиты, опубликованная в 1986 году, делает акцент на взаимодействии субъектов и потоков информации. Используется машина состояний с множеством разрешенных комбинаций состояний и некоторым набором начальных позиций. В данной модели исследуется поведение множественных композиций функций перехода из одного состояния в другое.

Модель Харрисона-Руззо-Ульмана (середина 70-х годов) использует моделирование поведения системы с помощью понятия «состояние», используется теория конечных автоматов [6]. Принятие решения о доступе основывается на критериях, представляющих собой логическую функцию, определенную на множестве условий выполнения перехода, которое определяется политикой безопасности (дискреционный доступ). К моделям дискреционного доступа относятся также модели АДЕПТ-50 (конец 60-х годов), модель пятимерное пространство Хартсона (начало 70-х годов), модель Take-Grant (предложена Джонсом, Липтоном и Шнайдером в 1976 г.), модель Type Access Matrix (TAM).

Существует дискреционная модель Кларка-Вильсона (Clark-Wilson), опубликованная в 1987 г. и модифицированная в 1989 г. [7]. Основана данная модель на использовании транзакций и тщательном оформлении прав доступа субъектов к объектам. В модели Кларка-Вильсона впервые была затронута проблема защищенности третьей стороны - стороны, поддерживающей систему безопасности. Кроме того, транзакции верифицированы, т.е. идентификация субъекта производится не только перед выполнением команды от него, но и повторно после выполнения. Это позволяет избежать подмены субъекта в момент между его идентификацией и собственно командой. Модель Кларка-Вильсона считается одной из самых совершенных в отношении поддержания целостности.

Одной из первых мандатных моделей безопасности доступа является опубликованная в 1977 г. модель К.Биба (Biba), обеспечивающая целостность информации [8]. Согласно ей все субъекты и объекты предварительно разделяются по нескольким уровням доступа, а затем на их взаимодействия накладываются соответствующие ограничения.

Известна классическая модель Белла-ЛаПадула (Bell-LaPadula model - BLP) полномочного управления доступом, основанная на понятии безопасного состояния [9,10,11]. Объектам присваиваются метки секретности. Субъектам присваиваются метки допуска к информации. Субъект не может читать данные с верхнего по отношению к нему уровня допуска и не может передавать (записывать) данные на нижний по отношению к нему уровень допуска. Эти правила являются инверсными по отношению к правилам модели Биба. Модель обеспечивает конфиденциальность информации.

В модели Мак-Лина, которую можно рассматривать, как модификацию модели Белла-ЛаПадула, в отличие от BLP используется понятие безопасного перехода [12].

Модель Low-Water-Mark (LWM) представляет близкий к модели Белла-ЛаПадула подход к определению свойств системы безопасности, реализующей мандатную (полномочную) политику безопасности. В модели LWM предлагается порядок безопасного функционирования системы в случае, когда по запросу субъекта ему всегда необходимо предоставлять доступ на запись в объект.

Модель Диона обобщает известные модели Биба и Белла-ЛаПадула [13]. Модель Диона предполагает использование меток целостности и меток конфиденциальности, обеспечивается целостность и конфиденциальность информации. Является наиболее полной и универсальной.

Все эти модели управления доступом являются общими и могут быть применены как в ОС, так и в СУБД, так как в них никоим образом не отражена специфика отдельных типов

программных продуктов.

Изначально встроенные программные средства защиты информации в коммерческих серверах БД не реализовывали принудительное управление доступом, ограничиваясь реализацией произвольного управления доступом. И этого было достаточно. Но развитие информационных и телекоммуникационных технологий привело к необходимости обеспечения более надежной защиты информации. В открытом информационном пространстве Казахстана при общении граждан между собой, при обращении граждан к электронному правительству, при ведении электронного бизнеса, при работе в корпоративных сетях пользователи рискуют компрометацией своих персональных данных, своей конфиденциальной информацией.

Мандатная защита реализовывалась встроенными программными средствами только в специальных (trusted) серверах БД. Структура конкретной организации учитывается на этапе разработки системы управления базами данных (СУБД) или разработчики адаптируют СУБД с реализованной мандатной защитой под структуру организации заказчика. Например, в СУБД ЛИНТЕР реализована мандатная модель и доступ разграничивается вплоть до значений атрибутов [14]. Права доступа являются неотъемлемой частью и субъектов доступа и объектов доступа. Мандатная модель обеспечивает более высокий уровень защиты, но сложнее в проектировании и реализации. СУБД ЛИНТЕР удовлетворяет требованиям класса безопасности В3 [15,16].

Широкое внедрение информационных технологий в финансовые сферы и необходимость защиты документооборота, особо важной бизнес-информации привело необходимости использования полномочной политики безопасности в государственном и коммерческом секторах, а, следовательно, и ее реализации в коммерческих серверах БД.

Большинство коммерческих серверов БД входят в класс безопасности С2, так как защита данных, основанная на применении произвольного управления доступом, удовлетворяет требованиям только класса безопасности С2. Эти требования, направлены на достижение базового уровня безопасности в условиях невраждебного и хорошо управляемого сообщества пользователей. В современных условиях развития информационных и телекоммуникационных технологий этих требований недостаточно для обеспечения безопасности информации.

Поэтому существует тенденция разработки встроенных платных подсистем в серверах БД, которые дают возможность добавить принудительное управление доступом в коммерческие системы. Такие подсистемы разработаны не для всех серверов БД и не для всех версий. Они имеются в СУБД Oracle (встроенная платная опция Oracle Label Security в Oracle Database Enterprise Edition), Informix OnLine Secure, Sybase Secure SQL Server, Ingres, PostgreSQL, DB2 Viper. Эти серверы удовлетворяют требованиям класса безопасности В1.

В подсистемах мандатной защиты для серверов БД в основном используется классическая модель Белла-ЛаПадула или ее модификации. Мандатная защита в серверах БД, в основном, реализуется через присвоение метки с уровнем конфиденциальности доступа каждой строке таблицы. Используются разные подходы к реализации мандатной защиты в зависимости от особенностей сервера БД.

Например, Oracle Label Security (OLS) использует в своей работе Oracle Virtual Private Database (VPD). В OLS используются метки доступа, которые могут включать следующие компоненты: уровни доступа (levels), разделы (compartments, позволяющие сгруппировать данные по категориям) и группы безопасности пользователей (security groups, позволяющие сгруппировать пользователей данных по принципу общих правил доступа). Для генерации меток по данным и их занесения в таблицу создается функция. Для связи меток, таблицы и авторизации создается политика безопасности (policy). После создания политики она применяется к защищаемым объектам [17].

Можно реализовать мандатную защиту в СУБД с использованием служебных таблиц для профилей пользователей и групп пользователей, представления исходных таблиц данных, триггеров и хранимых процедур [18]. Суть реализации MAC заключается в предоставлении пользователям доступа не непосредственно к данным в таблицах, а к их представлениям, формируемым каждый раз, когда пользователь обращается к ним. Для учета динамических свойств субъектов и объектов используются допустимые и текущие метки безопасности, состоящие из трех компонентов: уровня доступа для чтения записей, уровня доступа для модификации записей,

категории данных.

Недостатком реализации MAC в коммерческих серверах является то, что метка устанавливается на всю строку целиком и на логическом уровне. При этом не учитываются возможные требования на разграничение операций чтения и модификации данных на уровне отдельных свойств класса объектов (атрибутов таблицы). Использование модели Белла-ЛаПадула с ее недостатками определяет и недостатки реализации. В модели Белла-ЛаПадула не предусмотрена защита от изменения уровня секретности объекта вплоть до «не секретно» по желанию «совершенно секретного» субъекта. Например, пусть субъект с высоким уровнем доступа читает информацию из объекта того же уровня секретности. Далее он понижает свой уровень доступа, и записывает считанную ранее информацию в объект низкого уровня секретности. Таким образом, хотя формально модель нарушена не была, безопасность системы нарушена. Для решения этой проблемы необходимо вводить дополнительные правила. Кроме того, субъект с низким уровнем доступа может записать информацию в объект более высокого уровня секретности и, тем самым, модифицировать или даже удалить секретную информацию. Будет нарушена целостность данных, которая является одной из составляющих безопасности баз данных.

Формальные модели мандатного доступа, учитывающие особенности построения и функционирования СУБД отсутствуют, так как их разработка является задачей нетривиальной и трудоемкой и требует детальной проработки правил общей мандатной модели применительно к СУБД. Поэтому разработка средств мандатного контроля доступа в существующих и вновь создаваемых СУБД затруднена и не выполняет полностью свою задачу.

Наиболее полной и отвечающей требованиям безопасности баз данных является модель Диона, которая обеспечивает как конфиденциальность, так и целостность данных. Но она не реализуется в коммерческих СУБД в силу своей сложности. Необходимость полного и корректного принудительного управления доступом в коммерческих серверах приводит к необходимости разработки формальной модели управления доступом, учитывающей особенности реляционных СУБД, на основе модели Диона. Эта формальная модель послужит основой для разработки универсальной технология мандатного управления доступом в коммерческих серверах баз данных встроенными средствами.

ЛИТЕРАТУРА

[1] CERT, www.cert.org

[2] Sandhu R.S., Pierangela Samarati. Access Control: Principles and Practice. IEEE Comunication Magazine, 1994.

[3] Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. - Екатеринбург: Уральский государственный университет, 2003. – 328 с.

[4] Osborn S., Sandhu R., Nunawer Q. Configuring Role-Based Access Control To Enforce Mandatory and Discretionary Access Control Policies //ACM Trans.Info.Syst.Security, 3, 2, 2000.

[5] Щеглов А.Ю., Щеглов К.А. Вопросы и способы реализации полномочного (мандатного) механизма контроля доступа к резервам. http://articles.security-bridge.eom/articles/91/11627.

[6] Harrison M., Ruzzo W., Ulman J. Protection in operating systems // Communication of the ACM. 1976. P. 28-37.

[7] Clark D.D., Wilson D.R. A comparison of commercial and military computer security policies. Proceedings of the 1987 IEEE Sympo sium on Security and Privacy. May 1987. P. 184–194.

[8] Biba K.J. Integrity Considerations for Secure Computer Systems. MTR-3159. The Mitre Corporation. April, 1977.

[9] LaPadula L. J., Bell D. E. Secure Computer Systems: A Mathematical Model. MITRE Corporation Technical Report 2547. Volume II, 31 May 1973.

[10] Bell D. E., LaPadula L.J. Secure Computer Systems: Mathematical Foundations. MITRE Technical Report 2547, 1973. Vol. II.

[11] Bell D.E. Looking Back at the Bell-LaPadula Model. Proceedings of the 21st Annual Computer Security Applications Conference. December 2005. P. 337–351.

[12] McLean J. Security Models // Encyclopedia of software engineering. 1994. P. 246.

[13] Dion L.C. A complete protection model. Proceedings of the 1981 IEEE Symposium on Security and Privacy. April 1981. P. 49–55.

[14] Описание СУБД Линтер. Официальный сайт компании РЕЛЭКС. http://www.relex.ru/ru/projects/dbms.

[15] Department of Defense Trusted Computer System Evaluation Criteria. – DoD 5200.28–STD, 1983.

[16] Критерии оценки безопасности информационных технологий. Международный стандарт ISO/IEC 15408, 2005.

[17] Пржиялковский В. Изучаем метки доступа к строкам: задание свойств столбца доступа к таблице. http://www.citforum.ru/database/oracle/LearnOLS1.

[18] Айтхожаева Е.Ж. Реализация мандатной защиты в системах баз данных // Международная конференция:

Автоматизация и управление: перспективы, проблемы, решения. – Алматы, 2007. - С.317-319.

REFERENCES

[1] CERT, www.cert.org
[2] Sandhu R.S., Pierangela Samarati. Access Control: Principles and Practice. *IEEE Comunication Magazine*, **1994** (in Eng.).
[3] Gaydamakin N.A. Differentiation of access to information in computer systems. - Yekaterinburg: Ural State University, 2003. - 328 p. (in Russ.).
[4] Osborn S., Sandhu R., Nunawer Q. Configuring Role Based Access Control To Enforce Mandatory and Discretionary Access Control Policies. *ACM Trans.Info.Syst.Security,* **2000,** 3, 2 (in Eng.).
[5] Shcheglov A.Yu., Shcheglov K.A. Questions and methods for the implementation of the authorized (mandatory) mechanism to control access to reserves. *http://articles.security-bridge.eom/articles/91/11627* (in Russ.).
[6] Harrison M., Ruzzo W., Ulman J. Protection in operating systems. *Communication of the ACM,* **1976,** 28-37 (in Eng.).
[7] Clark D.D., Wilson D.R. A comparison of commercial and military computer security policies. *Proceedings of the 1987 IEEE Sympo sium on Security and Privacy,* **1987**, 184–194 (in Eng.).
[8] Biba K.J. Integrity Considerations for Secure Computer Systems. *MTR-3159. The Mitre Corporation,* **1977,** (in Eng.).
[9] LaPadula L. J., Bell D. E. Secure Computer Systems: A Mathematical Model. *MITRE Corporation Technical Report 2547,* **1973,** Volume II, 31, (in Eng.).
[10] Bell D. E., LaPadula L.J. Secure Computer Systems: Mathematical Foundations. *MITRE Technical Report 2547*, **1973.** Vol. II (in Eng.).
[11] Bell D.E. Looking Back at the Bell-LaPadula Model. *Proceedings of the 21st Annual Computer Security Applications Conference*, **2005,** 337–351(in Eng.).
[12] McLean J. Security Models. *Encyclopedia of software engineering.* **1994,** 246 (in Eng.).
[13] Dion L.C. A complete protection model. *Proceedings of the 1981 IEEE Symposium on Security and Privacy,* **1981,** 49–55 (in Eng.).
[14] Linter description. RELEX official site. *http://www.relex.ru/ru/projects/dbms* (in Russ.).
[15] Department of Defense Trusted Computer System Evaluation Criteria. *DoD 5200*.28–STD, **1983** (in Eng.).
[16] Criteria for Information Technology Security Evaluation. International Standard ISO / IEC 15408, 2005. (in Russ.).
[17] Przyjalkowski V. Operating tag access lines: Set column properties to access the table. http://www.citforum.ru/database/oracle/LearnOLS1. (in Russ.).
[18] Aythozhaeva E.Zh. The implementation of the protection mandate in database systems // International conference: Automation and Control: Perspectives, problems and solutions. - Almaty, 2007. - p.317-319. (in Russ.).

Деректқорлар серверлерінде қатынас құруды басқару үлгілері

Е.Ж. Айтхожаева
Қ.И. Сәпаев атындағы Қазақ Ұлттық Техникалық Зерттеу университеті

Түйін сөздер: қатынас құруды мандаттық басқару, қатынас құруды дискрециондық басқару, қатынас құру қауіпсіздігінің үлгілері.

Аннотация. Қатынас құру құқықтарын басқарудың ең көп таралған әдістерінің артықшылықтары мен кемшіліктері талданады: таңдаулы қауіпсіздік саясатының (Discretionary Access Control - DAC) және өкілеттілі қауіпсіздік саясатының (Mandatory Access Control - MAC). Негізгі идеялары DAC пен MAC-тың негізі болып табылатын қатынас құру қауіпсіздігінің жалпы формалдық үлгілеріне шолу жасалынады. Классикалық Белла-ЛаПадула үлгісінің кемшіліктері және осы үлгісінің негізінде коммерциялық серверлерде құрылған қатынас құруды мәжбүрлі басқарудың кемшіліктері келтіріледі. ДҚБЖ құрылуы мен жұмыс істеуінің ерекшеліктерін ескеретін Дион үлгісі негізінде мандаттық қатынас құрудың формалық үлгісін әзірлеу қажеттілігі негізделеді.

СВЕДЕНИЯ ОБ АВТОРЕ

Айтхожаева Евгения Жамалхановна - к.т.н. профессор Казахского национального технического университета имени К.И. Сатпаева, г. Алматы, ул. Сатпаева, 22, 8 (727) 257-71-60, e-mail: ait_evg@mail.ru

Поступила 11.09.2015 г.