МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94.056.53

АНАЛИЗ МЕТОДОВ АТРИБУТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

М. Н. Калимолдаев, Р. Г. Бияшев, О. А. Рог

Институт информационных и вычислительных технологий, г. Алматы, Республика Казахстан

Приведён аналитический обзор основных моделей и методов разграничения доступа, начиная от традиционных (DAC, MAC, RBAC) и до последних разработок — многочисленных моделей, реализующих атрибутное разграничение доступа (ABAC). Описана разрабатываемая в настоящее время модель типизированного атрибутного разграничения доступа (ТАРД). Сформулированы требования к методам разграничения доступа, обеспечивающие безопасное совместное использование информационных ресурсов как в локальных, так и в глобальных вычислительных средах. Проанализированы достоинства и недостатки существующих моделей ABAC. Показано, что модели ТАРД отвечают поставленным требованиям универсальности, гибкости, удобства администрирования, способствующим обеспечению безопасности разграничения доступа вне зависимости от типа операционной среды.

Ключевые слова: *атрибутное разграничение доступа (ABAC), типизированное атрибутное разграничение доступа (ТАРД), DAC, MAC, RBAC, политика разграничения доступа, язык спецификации, синтаксис, семантика, моделирование.*

DOI 10.17223/20710410/44/4

ANALYSIS OF THE METHODS FOR ATTRIBUTE-BASED ACCESS CONTROL

M. N. Kalimoldayev, R. G. Biyashev, O. A. Rog

Institute of Information and Computational Technologies, Almaty, Republic of Kazakhstan

E-mail: olga@ipic.kz

The paper contains an analytical overview of the basic models and methods for access control from the traditional ones (DAC, MAC, RBAC) to the latest developments — numerous models implementing attribute based access control (ABAC). The model of typed attribute based access control (TAAC) being developed currently is described. The following disadvantages of traditional models are pointed out: identification of entities with unique names; access rights redundancy ("coarse-grained access control"); difficult managing large number of users; operating in closed environments; the inability to use integrated security policies; lack of built-in administration tools. It is found out that to ensure the safe sharing of information resources in both local and global

computing environments, access control models must meet the requirements of universality, flexibility and ease of administration while performing the following tasks: identification of entities by several features for fine-grained access control; design and use of multiple access control policies to implement the "multiple policy" paradigm and adapt the system to work in various environments; administration as a means for dynamic policy modeling and convenient privilege managing a large number of users. The advantages and disadvantages of different types of ABAC models are considered. The advantages are: identification of entities by sets of attributes; "fine-grained access control"; flexibility and expressiveness of model specification languages; the possibility of creating new and modeling traditional methods of access control; relative ease of administration; managing privileges of groups of users. The main disadvantage of ABAC is the complexity of calculating attribute values. It is shown that the TAAC models meet the above requirements and provide the following: "fine-grained access control" by identifying entities with the sets of typed attributes; decrease in complexity and increase in speed of calculations; management privileges of hierarchical groups of subjects and objects; dynamic policy construction; multi-criteria access control.

Keywords: *attribute-based access control (ABAC), typed attribute-based access control (TAAC), DAC, MAC, RBAC, access control policy, specification language, syntax, semantics, modeling.*

Введение

В результате развития новых технологий вычислительные среды эволюционировали от централизованных систем, основанных на механизмах, обеспечивающих их производительность за счёт различных способов параллельного исполнения команд, до распределённых гетерогенных систем, осуществляющих децентрализованное хранение и обработку данных с помощью эффективно взаимодействующих служб и алгоритмов.

На сегодняшний день распределённые вычислительные среды отходят от понятий высокопроизводительных распределённых вычислений в сторону развития виртуального сотрудничества людей и/или организаций, объединённых общими правилами коллективного доступа к определённым вычислительным ресурсам. Методы предоставления доступа к информации становятся сервисно-ориентированными, что позволяет эксплуатировать одни и те же ресурсы в режиме совместного использования и требует обеспечения их защиты путём организации разграничения доступа.

При этом субъекты получают доступ к объектам системы в соответствии с политикой авторизации, определяющей допуск к ресурсам определённых видов согласно предоставленным полномочиям с одновременным запретом различных видов несанкционированного доступа. Актуальность проблемы защиты растёт по мере увеличения объёмов хранимых данных и роста сложности программного обеспечения для их обработки.

Подавляющее большинство приложений снабжаются средствами контроля доступа в той или иной форме. Системы разграничения доступа, будучи важнейшими компонентами систем защиты, наиболее подвержены рискам из-за возможных ошибок в конфигурации политик разграничения доступа.

1. Недостатки традиционных моделей разграничения доступа и пути их преодоления

В процессе реализации защищённого доступа к данным система выполняет задачи идентификации, аутентификации и авторизации. Идентификация заключается в при-

своении субъекту или объекту идентификатора, ассоциируемого с перечнем разрешённых ему действий. Аутентификация является средством для доказательства права использовать идентификатор, выполнять роль или владеть определёнными атрибутами. На основании результатов операций идентификации и аутентификации осуществляется авторизация как способ выполнения политики посредством предоставления или запрета доступа субъекта к объекту [1].

С начала 1970-х годов было разработано много моделей, основными из которых являются модели дискреционного разграничения доступа DAC (Discretional Access Control), мандатного разграничения доступа MAC (Mandatory Access Control) и ролевого разграничения доступа RBAC (Role Based Access Control) [2 – 4].

Задачи идентификации сущностей в этих моделях выполняются путём присвоения субъектам и объектам уникальных имён, ввиду чего модели называют идентификаторными. Доступ субъекта к объекту осуществляется на основе проверки имён или приписанных им ролей согласно заранее определённым системным политикам.

Идентификаторные модели эффективно работают в замкнутых и относительно неизменных системах, с определённым кругом заранее известных пользователей, имеющих доступ к известным сервисам.

Основным недостатком данных моделей является то, что они не учитывают дополнительных параметров разграничения доступа, таких, как сведения о ресурсах, отношения пользователей к ресурсам, динамической информации — времени суток, IP-адресов и т. д., что ведёт к «грубому» разграничению доступа («coarse-grained access control») и служит причиной появления «избыточности прав доступа» у пользователей. Идентификаторные модели не содержат средств администрирования полномочий, оставляя это «третьей стороне» — системному администратору. В широкомасштабных системах управление правами большого числа пользователей и машин становится слишком сложным и подверженным ошибкам. В работе [5], написанной в 1993 г., проанализированы недостатки существующих моделей и сформулированы проблемы, требующие решения при организации разграничения доступа.

Прежде всего необходимо решить вопросы идентификации с целью избавления от избыточных прав доступа путём обеспечения точного наименования сущностей. Следующим недостатком является недостаток гибкости. Единственной политики безопасности, обеспечиваемой традиционными моделями DAC, MAC и RBAC в автономных приложениях, недостаточно для защиты данных в сложных системах, требующих интегрированных политик разграничения доступа для одновременного выполнения различных критериев защиты с целью обеспечения целостности, конфиденциальности и доступности данных. Одновременное выполнение этих условий требуется при защите сложных приложений в области медицины, финансов, резервирования билетов, научных исследований, цифровых библиотек и др.

Отмечается необходимость введения новой парадигмы — «множественной политики», означающей, что в системе должна быть предусмотрена возможность применения разных политик авторизации в зависимости от требований безопасности среды, в которой функционирует система. Для этого необходимо наличие средств конструирования различных политик без реконфигурации самой системы. Как правило, конкретные политики конструируются на основе единого объекта — политики высокого уровня, или метаполитики, реализуемой в виде фреймворка. Необходимо уточнить аспекты понятия множественной политики, касающиеся порядка применения создаваемых на основе метаполитики механизмов разграничения доступа различных видов.

Одним из путей является поочерёдное применение полученных политик, в результате которого система последовательно меняет применяемый критерий разграничения доступа. Возможность одновременного применения ряда созданных политик для разграничения доступа по различным признакам делает защиту многокритериальной.

В последнее время наблюдается значительный рост числа крупномасштабных распределённых открытых систем, являющихся виртуальными организациями, составленными из множества независимых автономных доменов. Ввиду того, что ресурсы и пользователи зачастую располагаются в разных доменах, связи между субъектами и объектами в таких системах становятся более сложными и динамичными. При этом возникает необходимость идентификации сущностей наборами характеристик, а не предопределёнными именами, так как решения о предоставлении доступа должны приниматься с учётом оценки наборов атрибутов субъектов и объектов, делая традиционные идентификаторные модели разграничения доступа неэффективными.

Для гетерогенных сервисов распределённых виртуальных сред необходимы механизмы авторизации, основанные на идентификации наборами признаков, которые обеспечивают необходимую точность, являются адекватными и надёжно защищают от атак [6].

2. Методы атрибутного разграничения доступа

Для решения этих проблем был предложен атрибутный метод разграничения доступа (Attribute Based Access Control — ABAC). Его основу составляет безыдентификаторный подход, который заключается в обозначении субъектов и объектов совокупностями атрибутов и позволяет принимать решение по управлению доступом без предварительного знания субъектов или их отношения к поставщику услуг.

Наиболее общим определением ABAC является следующее. Атрибутное разграничение доступа — это метод, посредством которого запросы субъекта на выполнение определённых операций над объектом удовлетворяются или отвергаются на основе приписанных им атрибутов, условий среды выполнения и набора политик, сформулированных с учётом этих условий и атрибутов.

Атрибутное разграничение доступа является многообещающей альтернативой традиционным моделям. Оно привлекает внимание как академических исследователей, так и создателей промышленных приложений [7–9].

Преимущество ABAC состоит в том, что оно позволяет создавать политики доступа на основе атрибутов пользователей и объектов, а не назначать роли, права собственности или метки безопасности вручную системным администратором. Это упрощает администрирование в сложных системах с большим числом пользователей, устраняя необходимость ручного вмешательства при авторизации пользователей для определённых ролей или уровней безопасности, а также создавая возможность автоматизации решения по управлению доступом для удалённых пользователей из других доменов.

Система именования сущностей атрибутами обеспечивает точность идентификации и, следовательно, «точное» разграничение доступа (fine-grained access control) в процессе организации защищённого использования ресурсов, не допуская избыточных прав доступа у пользователей. Языки спецификации моделей ABAC дают гибкость и выразительную мощность описаниям политик безопасности. При этом многие из них разрешают моделировать традиционные методы разграничения доступа — DAC, MAC, RBAC.

Модели атрибутного разграничения доступа находят применение в самых разных областях современных вычислений для защиты приложений, баз данных, файловых серверов, в облачных средах и больших данных.

За последнее время разработано множество ABAC-моделей, как базовых, так и специализированных [10 – 12]. Их объединяет то, что они могут рассматриваться в качестве основополагающих моделей нового направления защиты, способных решать задачи разграничения доступа, поставленные в [5].

Типичная ABAC-модель содержит следующие компоненты:

— атрибуты пользователей;
— атрибуты объектов;
— атрибуты контекста или вычислительной среды;
— политики авторизации, основанные на этих атрибутах.

Атрибуты обычно определяются в виде функций, аргументами которых служат субъекты или объекты, а результатом — значения их атрибутов. Политика авторизации предоставляет группам пользователей определённые виды доступа (такие, например, как чтение и запись) к заданным объектам на основе оценки значений их атрибутов.

В [13, 14] описываются две техники спецификации политик авторизации. Наиболее распространённой из них считается спецификация, определяющая политики с помощью формул логики, содержащих атрибуты в качестве своих переменных (LAP — Logical-formula Authorization Policy). LAP задаётся с помощью булевых выражений, состоящих из подвыражений, соединённых логическими операторами и операторами отношений. LAP предоставляет доступ субъекта к объекту, если в результате вычисления логическое выражение принимает значение «истина». Примерами моделей LAP-ABAC служат [10, 11, 15, 16]. Гибкость этих моделей продемонстрирована их способностью моделировать традиционные DAC, MAC и RBAC. Альтернативной техникой представления атрибутных политик разграничения доступа является перечисление. Примерами этой категории служат Policy Machine (PM) [17] и 2-sorted-RBAC [18].

Неформально перечислимая политика авторизации (Enumerated Authorization Policy, EAP) определяется как множество кортежей (uai, OP, oai), где uai и oai — значения атрибутов пользователя и объекта соответственно; OP — множество операций, доступных пользователю. В EAP кортежи различны и независимы, а значения атрибутов могут быть как атомарными, так и в виде множеств.

Полезность перечислимых политик авторизации продемонстрирована на многих примерах. Так, в Policy Machine [17] определены перечислимые атрибутные политики с использованием одного атрибута пользователя, одного атрибута объекта и набора возможных действий. Простая структура политики перечисления не делает её менее выразительной. Показано, что посредством PM могут быть сконфигурированы политики MAC и RBAC.

Преимущество логического подхода для представления атрибутных политик разграничения доступа в виде формул логики заключается в его простоте и лёгкости использования. Создание новых правил авторизации не представляет трудностей, так как не включает дополнительных расходов, требуемых, например, для инжиниринга ролей в RBAC. Эти правила способны гибко и в сжатой форме описывать даже сложные политики. Не существует ограничений на количество используемых в них атрибутов и сложность языка описания правил [7].

С другой стороны, создание выразительных вычислительных языков для спецификации атрибутных правил разграничения доступа делает задачи вычисления зна-

чений разнородных атрибутов в процессе конструирования и выполнения политик NP-полными или даже неразрешимыми, что служит, вместе с отсутствием формальных определений моделей и сложностью администрирования, главным препятствием широкому применению метода ABAC.

Относительно политик перечисления, разработка которых начата сравнительно недавно, сделано предположение о полиномиальном времени, требуемом для оценки атрибутов.

3. Виды моделей ABAC

В [6, 9, 13] приводятся описания многочисленных моделей атрибутного разграничения доступа, разработанных за последнее время. Их можно разделить на две категории — модели общего назначения и специализированные, предназначенные для применения в определённых вычислительных средах, таких, как облачные вычисления, веб-сервисы и т. д.

Примерами моделей общего назначения служат:

- логический фреймворк для ABAC (A Logic-Based Framework for Attribute-Based Access Control) — модель в форме фреймворка, основанного на логическом программировании, в которой политики определяются в виде логических программ, а атрибуты и операции — как объекты теории перечислимых множеств;
- атрибутная матрица доступа (Attribute-Based Access Matrix Model, ABAM). В ней строки представляют собой пары, состоящие из субъектов и множеств их атрибутов, а столбы содержат пары объектов и их атрибутов. Клетка матрицы содержит множество прав доступа субъекта к объекту в соответствии с принятой политикой безопасности;
- модель Rubio-Medrano, отображающая атрибуты сущностей в маркеры безопасности, соотнесённые с привилегиями, путём обхода графа маркеров, определяемого администратором. В результате обхода осуществляется принятие/отказ решения о доступе;
- ABAC-alpha — ещё одна недавно созданная модель (2012), предназначенная специально для моделирования DAC, MAC и RBAC. Для этого даётся формальное определение основных элементов ABAC (пользователей, объектов, политик и т. д.), их отношений и ограничений, позволяющее эмулировать традиционные модели;
- модель Policy Machine предлагает инновационный подход к разграничению доступа. Она предоставляет архитектуру и фреймворк для спецификации и реализации обобщённых атрибутных политик разграничения доступа, составляющие унифицированный механизм для реализации широкого круга различных политик;
- модель атрибутного разграничения доступа на основе иерархических групп (Hierarchical Group and Attribute-Based Access Control — HGABAC) создает обобщённую модель ABAC с иерархическим представлением групп атрибутов субъектов и объектов.

К числу специализированных моделей ABAC относятся следующие: модель CA-ABAC, предназначенная для организации разграничения доступа в облаках; T-ABAC, применяемая в системах реального времени; MPABAC — в объединённых рабочих и образовательных средах. Специальные модели разработаны для сред мобильных приложений, грид-вычислений, веб-сервисов, цифровых библиотек и т. д.

В [9] приводится анализ этих моделей и делается вывод о том, что большинство из них ориентировано на специфические условия использования и не отвечают требо-

ваниям, обеспечивающим универсальность, удобство администрирования и гибкость управления безопасностью.

Для выполнения данных требований модели должны обладать следующими характеристиками:

— иметь формальное определение;
— содержать средства администрирования;
— обеспечивать возможность применения множественных политик и включать способы их конструирования;
— язык описания модели должен быть высокоуровневым, т. е. не зависеть от операционной среды.

4. Задача спецификации моделей ABAC

Типичный механизм разграничения доступа содержит данные, описывающие политики разграничения доступа и атрибуты, а также набор функций для приёма и обработки запросов на доступ согласно этим политикам.

Реализация разграничения доступа осуществляется по-разному в различных операционных средах. Особенности распределённых гетерогенных сред ставят дополнительные задачи, требующие учитывать круг контролируемых объектов (пользователей и ресурсов), различные типы операций (такие, например, как чтение, пересылка, одобрение, выбор), а также типы данных (записи, файлы, сообщения, рабочие заметки). Администраторы вынуждены принимать во внимание наличие разных доменов безопасности, управляемых различными политиками на основании характерных атрибутов.

Необходимость осуществления глобального контроля безопасности ставит задачу разработки высокоуровневых средств, позволяющих конструировать различные политики на основе метаполитики как единого высокоуровневого объекта, с помощью соответствующих средств администрирования, которые не зависели бы от операционной среды.

В настоящее время разработан ряд языков спецификации политик авторизации и основанных на них систем разграничения доступа. К их числу относятся XACML, NGAC, Ponder, Akenti, dRBAC и др. [19, 20].

Многие из рассмотренных моделей ABAC используют собственные встроенные языки описания политик или вовсе не имеют языков.

В работах [21 – 30] приводится описание различных аспектов, а также формальное представление модели разрабатываемого метода типизированного атрибутного разграничения доступа (ТАРД). В данной работе кратко рассмотрены общие положения ТАРД, даны определения его модели на нескольких уровнях, описан порядок функционирования основанных на ней систем.

Модель ТАРД принадлежит классу моделей ABAC, но, в отличие от ABAC, атрибутам безопасности сущностей ТАРД приписаны определённые типы. Решение о возможности доступа принимается на основе обработки однотипных атрибутов пары субъект — объект.

Данная модель может быть отнесена к разряду моделей разграничения доступа общего назначения, основанной на логических формулах (LAP-ABAC). В её состав входят:

— средства определения возможности доступа субъектов к объектам в соответствии с их полномочиями;

— средства двухступенчатого администрирования — для конструирования политик авторизации и для управления идентификацией сущностей в процессе разграничения доступа.

В соответствии с определением типа атрибутов T модель ТАРД имеет многоуровневое представление, которое делает её инструментом конструирования механизмов разграничения доступа в виде типов, моделирующих различные политики безопасности, включая DAC, MAC и RBAC. Создаваемые политики могут применяться как по очереди, так и одновременно, что обеспечивает выполнение всех аспектов парадигмы «множественной политики».

Идентификация сущности ТАРД осуществляется путём присвоения ей метки безопасности в виде значения определённого типа или множественной метки безопасности в виде ряда значений различных типов.

Тип T определяется как математический объект, содержащий домен типа — конечное множество всевозможных значений атрибутов в виде полного частично упорядоченного множества, структурированного отношением предшествования, и определённых на нем операций типизации Type, представленных непрерывными монотонными функциями, а также операцией доступа Acc [21, 23, 27, 28]. Операция типизации присваивает сущности e метку безопасности T:

$$T(e) = \mathrm{Type}(e).$$

Множественная метка безопасности в виде кортежа $T_1(e), \ldots, T_K(e)$ присваивается в результате применения нескольких операций типизации типов $T_1, \ldots, T_K$.

Предикат Acc осуществляет сравнение меток безопасности типа T субъекта и объекта, разрешая/отвергая возможность доступа. Истинностное значение означает разрешение на доступ субъекту s к объекту o:

$$\mathrm{Acc}(T(s), T(o)) = \texttt{true/false}.$$

Набор операций типа T образует механизм разграничения доступа, а также служит средством реализации политики типизированного атрибутного разграничения доступа $P(T)$, задаваемой типом T [23].

Спецификация политики безопасности $P(T)$ задаётся конкретным видом структуры и значениями узлов домена типа T, а также соответствующими этой структуре операциями. Тип T служит ограничением на значения атрибутов и круг операций с атрибутами данного типа. Данное обстоятельство лежит в основе принципа безопасности моделей ТАРД [26].

Метод ТАРД имеет многоуровневое определение в виде метауровня META, объектного уровня OBJ и уровня матрицы доступа AM. В соответствии с этим даётся многоуровневое определение типа T.

На уровне META тип представлен метатипом T_{META}, являющимся обобщённым представлением политики $P_{\mathrm{META}}(T)$. Он служит для порождения политик типизированного атрибутного разграничения доступа объектного уровня $P_{\mathrm{OBJ}}(T)$.

Типы объектного уровня T_{OBJ} представляют собой ряд конкретных политик разграничения доступа $P_{\mathrm{OBJ}}(T)$, получаемых из метаполитики $P_{\mathrm{META}}(T)$. При этом T_{OBJ} является интенсиональным представлением типа T.

Тип T_{AM} уровня AM — это реализация политики типизированного атрибутного разграничения доступа $P_{\mathrm{OBJ}}(T)$ в виде множества типизированных переменных, образующих матрицу доступа и являющихся экстенсиональным представлением типа T.

Построена модель $M(T)$, которая является формальным представлением типа T. Она предназначена для конструирования и представления предметной области ТАРД на этапах работы системы разграничения доступа. Модель, так же как и тип, имеет многоуровневое определение. Переход на следующий уровень производится путём моделирования семантики предыдущего уровня в процессе функционирования системы разграничения доступа.

Уровень метамодели $M_{\text{META}}(T)$ представляет метатип T_{META} и играет роль фреймворка, или инструмента для создания конкретных моделей ТАРД. Объектная модель $M_{\text{OBJ}}(T)$ — это объектный тип T_{OBJ}, который является средством реализации конкретной политики безопасности типа T, полученной из метатипа T_{META}.

Матрица доступа $M_{\text{AM}}(T)$ — сложноструктурированная область типизированных значений атрибутов в виде меток безопасности сущностей, содержит результаты выполнения политики безопасности $P(T)$ в процессе функционирования модели $M_{\text{OBJ}}(T)$.

В процессе работы на разных уровнях модель выполняет различные функции.

На уровне META осуществляется конструирование семантических значений типа T_{OBJ} специальной операцией интерпретации I, которое заключается в определении вида структуры домена типа T_{OBJ} как подструктуры домена типа T_{META} и присвоении значений его элементам. В результате создаются различные виды моделей $M^i_{\text{OBJ}}(T)$, предназначенные для выполнения соответствующих политик разграничения доступа $P^i_{\text{OBJ}}(T)$:

$$M_{\text{META}}(T, I) \to M^i_{\text{OBJ}}(T).$$

Формирование матрицы доступа осуществляется операциями Type сконструированных моделей $M^i_{\text{OBJ}}(T)$. При этом производится присвоение полномочий сущностям в виде их меток безопасности:

$$M^i_{\text{OBJ}}(T, \text{Type}(e)) \to M^i_{\text{AM}}(T).$$

На уровне AM производится обработка создаваемой матрицы доступа путём выдачи разрешения на доступ согласно критерию, задаваемому типом T_{OBJ}, в результате выполнения операции доступа Acc модели $M^i_{\text{OBJ}}(T)$:

$$M^i_{\text{OBJ}}(T, \text{Acc}(T(s), T(o)) \to \{\texttt{true}, \texttt{false}\}.$$

Модели $M^i_{\text{OBJ}}(T)$ могут выполняться как последовательно, так и параллельно, реализуя все аспекты множественной политики.

Обозначим $M^i_{\text{OBJ}}(T) = M_{\text{OBJ}}(T_i)$ и рассмотрим множество различных моделей $\{M_{\text{OBJ}}(T_i) : i = 1, \ldots, K\}$, где типы T_i семантически независимы. Одновременное использование этих моделей в рамках одной системы обеспечивает разграничение доступа по ряду критериев, определяемых политиками $T_1, \ldots, T_K$.

Предикат $MM_{\text{AM}}(T_1, \ldots, T_K)$ предоставляет доступ субъекту s к объекту o при условии одновременного выполнения критериев $T_1, \ldots, T_K$:

$$MM_{\text{AM}}(T_1, \ldots, T_K) = M_{\text{AM}}(T_1, \text{Acc}_1) \wedge \ldots \wedge M_{\text{AM}}(T_K, \text{Acc}_K). \quad (1)$$

Построено формальное представление модели ТАРД, определяемое на уровнях META, OBJ и AM в виде языковых спецификаций T^{AS} и T^{LS}, взаимосвязь которых обусловливает её функционирование [27, 28].

В работе [27] приводится представление типа атрибутов в виде алгебраической системы, в [28] содержится обзор возможностей применения логики для разграничения

доступа, используемых в настоящее время, а также описание языка T^{LS} для представления типа атрибутов ТАРД в виде логики.

Модель ТАРД представима в виде пары

$$M(T) = (T^{AS}, T^{LS}),$$

где $T^{AS} = (D, \sigma)$ — многоуровневое определение многосортной алгебраической системы, состоящей из домена D и сигнатуры σ операций типа T, служащей для представления состояния каждого уровня модели:

$$T^{AS} = (T^{AS}_{\text{МЕТА}}, T^{AS}_{\text{OBJ}}, T^{AS}_{\text{AM}});$$

T^{LS} — многосортная логическая система, включающая язык L с алфавитом, представленным доменом D и правилами грамматики — операциями типа T, а также аксиомами Ax и правилами вывода Inf:

$$T^{LS} = (L, Ax, Inf).$$

Функционирование многоуровневой модели ТАРД заключается в моделировании семантики следующего уровня путём интерпретации модели, представляющей предыдущий уровень. При этом T^{LS}, представленная в виде тройки $(T^{LS}_{\text{МЕТА}}, T^{LS}_{\text{OBJ}}, T^{LS}_{\text{AM}})$, образует систему семантического моделирования.

Ввиду того, что определение T^{LS} включает функции интерпретации, схему взаимодействия спецификаций модели ТАРД можно представить следующим образом:

Метауровень МЕТА: $T^{LS}_{\text{МЕТА}}(T^{AS}_{\text{МЕТА}}) \to T^{AS}_{\text{OBJ}}$.

Объектный уровень OBJ: $T^{LS}_{\text{OBJ}}(T^{AS}_{\text{OBJ}}) \to T^{AS}_{\text{AM}}$.

Уровень матрицы доступа АМ: $T^{LS}_{\text{AM}}(T^{AS}_{\text{AM}}) \to \{\texttt{true}, \texttt{false}\}$.

В целях реализации модели ТАРД для каждого её уровня даётся формальное определение системы типизированного атрибутного разграничения доступа как программы (или программной системы) $S(T)$, построенной на основе модели $M(T)$. Она обеспечивает разграничение доступа в соответствии с политикой, представленной типом T [29].

Программа S является общим представлением функции семантического моделирования состояний предметной области ТАРД. Многокритериальное разграничение доступа осуществляется программой S, построенной на основе моделей $M(T_1), \ldots, M(T_K)$ согласно формуле (1).

Архитектура системы ТАРД состоит из модуля настройки и модуля выполнения, соответствующих мета- и объектным уровням определения модели ТАРД.

Модуль настройки (Администратор 1) осуществляет конфигурирование системы путём задания одного типа T или нескольких типов $T_1, \ldots, T_K$ атрибутов (которое заключается в задании их структуры и определении значений элементов доменов), служащих критериями разграничения доступа. Критерий или набор критериев, обеспечиваемых сконструированными типами, должен отвечать требованиям защиты данной информационной системы.

Модуль выполнения осуществляет две функции — функцию администрирования (Администратор 2), которая присваивает сущностям (субъектам и объектам) значение типа $T(e)$ или кортежи значений типов $(T_1(e), \ldots, T_K(e))$ в качестве их меток безопасности, и функцию разграничения, которая обеспечивает доступ субъектов к объектам на основе сравнения меток безопасности одинаковых типов.

Необходимо отметить, что выразительность метода ТАРД несколько ограничена по сравнению с общепринятыми ABAC-методами.

Описанная модель ТАРД обладает следующими характеристиками:

— принцип обработки однотипных атрибутов является предпосылкой обеспечения скорости вычислений их значений;
— модель имеет возможность формально доказывать правильность решений о предоставлении доступа, используя дедуктивный аппарат логической спецификации;
— обеспечивает наглядность и контроль процесса администрирования;
— способна динамически конструировать новые модели разграничения доступа вместе с возможностью моделировать традиционные DAC, MAC, RBAC и применять их в системе как одну за другой, так и одновременно;
— модель непосредственно реализуема на языках функционального и логического программирования с использованием аппарата программирования в ограничениях.

Перечисленные особенности позволяют использовать системы типизированного атрибутного разграничения доступа в качестве центров управления политиками безопасности, создаваемых в локальных и глобальных вычислительных средах. На основе этих центров, рассматриваемых в качестве виртуальных организаций, могут создаваться домены администрирования, поддающиеся локализации и обеспечивающие в силу этого полную защиту информации на контролируемых ими участках распределённых гетерогенных вычислительных сред [30].

Заключение

Рассмотрены основные методы разграничения доступа в их развитии — от традиционных моделей DAC, MAC и RBAC до последних разработок — моделей, основанных на методе атрибутного разграничения доступа ABAC.

Приведён перечень недостатков традиционных моделей и пути их преодоления. Сформулированы требования, обеспечивающие гибкость управления безопасностью, универсальность и удобство администрирования, которым должны отвечать модели разграничения доступа, функционирующие как в локальных, так и в распределённых гетерогенных средах.

Перечислены основные разработанные к настоящему времени модели атрибутного разграничения доступа, отмечены их достоинства и недостатки. Описана модель типизированного атрибутного разграничения доступа, показано, что она отвечает основным требованиям построения моделей, обеспечивающим безопасное пользование разделяемыми ресурсами.

ЛИТЕРАТУРА

1. *Karp A., Haury H., and Davis M.* From ABAC to ZBAC: The evolution of access control models // ISSA J. 2010. No. 8. P. 22–30.
2. *Sandhu R. S. and Samarati P.* Access control: principle and practice // IEEE Commun. Mag. 1994. No. 32(9). P. 40–48.
3. *Девянин П. Н.* Модели безопасности компьютерных систем: учеб. пособие для вузов. М.: Академия, 2005. 144 с.
4. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
5. *Hosmer H.* The multipolicy paradigm for trusted systems // Proc. NSPW '92-93. ACM, N.Y.: ACM, 1993. P. 19–32.
6. *Lang B. et al.* A flexible attribute based access control method for grid computing // J. Grid Comput. 2009. No. 7(2). P. 169–180.

7. *Hu V. C., Ferraiolo D., Kuhn R., et al.* Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication, 800:162, 2014. http://dx.doi.org/10.6028/NIST.SP.800-162
8. https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-3c_ABAC_0.pdf — NCCOE. Attribute Based Access Control How-to Guides for Security Engineers. Accessed November 25, 2015.
9. *Servos D. and Osborn S.* Current research and open problems in attribute-based access control // ACM Computing Surveys. 2017. V. 49. Iss. 4. Art. 65.
10. *Jin X., Krishnan R., and Sandhu R. S.* A unified attribute-based access control model covering DAC, MAC and RBAC // LNCS. 2012. V. 7371. P. 41–55.
11. *Servos D. and Osborn S.* HGABAC: Towards a formal model of hierarchical attribute-based access control // Foundations and Practice of Security. Springer, 2014. P. 187–204.
12. *Yuan E. and Tong J.* Attributed based access control (ABAC) for web services // Proc. ICWS'2005. Washington, 2005. P. 561–569.
13. *Biswas R., Sandhu R., and Krishnan R.* Label-based access control: An ABAC model with enumerated authorization policy // Proc. ABAC'16. N.Y.: ACM, 2016. P. 1–12.
14. *Biswas P., Sandhu R., and Krishnan R. A.* A comparison of logical-formula and enumerated authorization policy ABAC models // LNCS. 2016. V. 9766. P. 122–129.
15. *Shen H. and Hong F.* An attribute-based access control model for web services // Proc. PDCAT'06. IEEE, 2006. P. 74–79.
16. *Wang L., Wijesekera D., and Jajodia S.* A logic-based framework for attribute based access control // Proc. FMSE'04. ACM, 2004. P. 45–55.
17. *Ferrailo D., Atluri V., and Gavrila S.* The Policy Machine: A novel architecture and framework for access control policy specification and enforcement // J. Systems Architecture. 2011. V. 57(4). P. 412–424.
18. *Kuijper W. and Ermolaev V.* Sorting out role based access control // Proc. 19th ACM SACMAT. ACM, 2014. P. 63–74.
19. *Ferraiolo D., Chandramouli R., Hu V. C., and Kuhn R. A.* A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications, Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). Natl. Inst. Stand. Technol. Spec. Publ. 800-178, 2016. 68 p.
20. *Wakefield R.* Policy Management in a Distributed Computing Environment. http://www.cs.colostate.edu/~waker/papers/CS556_Policy_Management_in_Distributed_Computing.pdf. 2008.
21. *Калимолдаев М. Н., Бияшев Р. Г., Рог О. А.* Формальное представление функциональной модели многокритериальной системы разграничения и контроля доступа к информационным ресурсам // Проблемы информатики. 2014. № 1(22). С. 43–55.
22. *Rog O. A.* Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types // Inform. Technologies, Management and Society. 12th Intern. Scientific Conf. Riga, April 16–17, 2014. P. 66.
23. *Бияшев Р. Г., Калимолдаев М. Н., Рог О. А.* Полиморфная типизация сущностей и задача конструирования механизма многокритериального разграничения доступа // Изв. НАН РК. Сер. физ.-мат. 2014. № 5. С. 33–41.
24. *Бияшев Р. Г., Калимолдаев М. Н., Рог О. А.* Конструирование систем многокритериального атрибутного разграничения доступа в облачных структурах // 11 Междунар. Азиатская школа-семинар «Проблемы оптимизации сложных систем». Чолпон-Ата, 27 июля–7 августа 2015. С. 148–152.

25. *Бияшев Р. Г., Калимолдаев М. Н., Рог О. А.* Логический подход к организации многокритериального атрибутного разграничения доступа // Int. Conf. «Computational and Informational Technologies in Science, Engineering and Education» (September 24–27, 2015). Almaty: Казак университеті, 2015. P. 86.
26. *Бияшев Р. Г., Калимолдаев М. Н., Рог О. А.* Представление ограничений моделей атрибутного разграничения доступа // Изв. НАН РК. Сер. физ.-мат. 2016. № 1. С. 58–65.
27. *Бияшев Р. Г., Калимолдаев М. Н., Рог О. А.* Моделирование семантики типизированного атрибутного разграничения доступа // Проблемы информатики. 2017. № 1. С. 25–37.
28. *Калимолдаев М. Н., Бияшев Р. Г., Рог О. А.* Применение логики для построения моделей разграничения доступа к информации // Докл. НАН РК. 2017. № 3. С. 48–54.
29. *Калимолдаев М. Н., Бияшев Р. Г., Рог О. А.* Основы архитектуры программных систем для осуществления типизированного атрибутного разграничения доступа // Современные проблемы информатики и вычислительных технологий: Материалы науч. конф. (29–30 июня 2017). Алматы, 2017. С. 88–95.
30. *Калимолдаев М. Н., Бияшев Р. Г., Рог О. А.* О применении типизированного атрибутного разграничения доступа в глобальных вычислительных средах // Изв. науч.-технич. общества «КАХАК». Алматы, 2017. № 3(58). С. 30–36.

REFERENCES

1. *Karp A., Haury H., and Davis M.* From ABAC to ZBAC: The evolution of access control models. ISSA J., 2010, no. 8, pp. 22–30.
2. *Sandhu R. S. and Samarati P.* Access control: principle and practice. IEEE Commun. Mag., 1994, no. 32(9), pp. 40–48.
3. *Devyanin P. N.* Modeli bezopasnosti kompyuternyh sistem. Ucheb. posobie dlja stud. vyssh. ucheb. zavedenij) [Models of security of computer systems: Textbook for students of higher educational institutions]. Moscow, Akademija Publ., 2005. 144 p. (in Russian)
4. *Gaydamakin N. A.* Razgranichenie dostupa k informatsii v komp'yuternykh sistemakh) [Differentiation of Access to Information in Computer Systems]. Ekaterinburg, USU Publ., 2003. 328 p. (in Russian)
5. *Hosmer H.* The multipolicy paradigm for trusted systems. Proc. NSPW '92-93, N.Y., ACM, 1993, pp. 19–32.
6. *Lang B. et al.* A flexible attribute based access control method for grid computing. J. Grid Comput., 2009, no. 7(2), pp. 169–180.
7. *Hu V. C., Ferraiolo D., Kuhn R., et al.* Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publ., 800:162, 2014. `http://dx.doi.org/10.6028/NIST.SP.800-162`
8. `https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-3c_ABAC_0.pdf` — NCCOE. Attribute Based Access Control How-to Guides for Security Engineers. Accessed November 25, 2015.
9. *Servos D. and Osborn S.* Current research and open problems in attribute-based access control. ACM Computing Surveys, 2017, vol. 49, iss. 4, art. 65.
10. *Jin X., Krishnan R., and Sandhu R. S.* A unified attribute-based access control model covering DAC, MAC and RBAC. LNCS, 2012, vol. 7371, pp. 41–55.
11. *Servos D. and Osborn S.* HGABAC: Towards a formal model of hierarchical attribute-based access control. Foundations and Practice of Security, Springer, 2014, pp. 187–204.
12. *Yuan E. and Tong J.* Attributed based access control (ABAC) for web services. Proc. ICWS'2005, Washington, 2005, pp. 561–569.

13. *Biswas R., Sandhu R., and Krishnan R.* Label-based access control: An ABAC model with enumerated authorization policy. Proc. ABAC'16, N.Y., ACM, 2016, pp. 1–12.
14. *Biswas P., Sandhu R., and Krishnan R. A.* A comparison of logical-formula and enumerated authorization policy ABAC models. LNCS, 2016, vol. 9766, pp. 122–129.
15. *Shen H. and Hong F.* An attribute-based access control model for web services. Proc. PDCAT'06, IEEE, 2006, pp. 74–79.
16. *Wang L., Wijesekera D., and Jajodia S.* A logic-based framework for attribute based access control. Proc. FMSE'04, ACM, 2004, pp. 45–55.
17. *Ferrailo D., Atluri V., and Gavrila S.* The Policy Machine: A novel architecture and framework for access control policy specification and enforcement. J. Systems Architecture, 2011, vol. 57(4), pp. 412–424.
18. *Kuijper W. and Ermolaev V.* Sorting out role based access control. Proc. 19th ACM SACMAT, ACM, 2014, pp. 63–74.
19. *Ferraiolo D., Chandramouli R., Hu V. C., and Kuhn R. A.* A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications, Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). Natl. Inst. Stand. Technol. Spec. Publ. 800-178, 2016. 68 p.
20. *Wakefield R.* Policy Management in a Distributed Computing Environment. `http://www.cs.colostate.edu/~waker/papers/CS556_Policy_Management_in_Distributed_Computing.pdf`. 2008.
21. *Kalimoldayev M. N., Biyashev R. G., and Rog O. A.* Formal'noe predstavlenie funkcional'noj modeli mnogokriterial'noj sistemy razgranichenija i kontrolja dostupa k informacionnym resursam [Formal representation of the functional model of a multi-criteria system of the access control to information resources]. Problemy Informatiki, 2014, no. 1(22), pp. 43–55. (in Russian)
22. *Rog O. A.* Polymorphic typing of entities in the multi-criteria system of access control and a task of constructing types. Inform. Technologies, Management and Society, 12th Intern. Scientific Conf., Riga, April 16–17, 2014, p. 66.
23. *Biyashev R. G., Kalimoldayev M. N., and Rog O. A.* Polimorfnaja tipizacija sushhnostej i zadacha konstruirovanija mehanizma mnogokriterial'nogo razgranichenija dostupa [Polymorphic typing of entities and a task of constructing a mechanism for multi-criteria access control]. Izv. NAN RK, Ser. fiziko-matematicheskaja, 2014, no. 5, pp. 33–41. (in Russian)
24. *Biyashev R. G., Kalimoldayev M. N., and Rog O. A.* Konstruirovanie sistem mnogokriterial'nogo atributnogo razgranichenija dostupa v oblachnyh strukturah [Designing of systems of multi-criteria attribute-based access control in cloud structures]. 11 Mezhdunar. Aziatskaja Shkola-seminar "Problemy optimizacii slozhnyh sistem", Cholpon-Ata, 27 July – 7 August 2015, pp. 148–152. (in Russian)
25. *Biyashev R. G., Kalimoldayev M. N., and Rog O. A.* Logicheskij podhod k organizacii mnogokriterial'nogo atributnogo razgranichenija dostupa [Logical approach to the organization of multi-criteria attribute-based access control]. Intern. Conf. "Computational and Informational Technologies in Science, Engineering and Education" (September 24–27, 2015), Almaty, Kazak University, 2015, p. 86. (in Russian)
26. *Biyashev R. G., Kalimoldayev M. N., and Rog O. A.* Predstavlenie ogranichenij modelej atributnogo razgranichenija dostupa [Representation of the constraints of models of attribute-based access control]. Izv. NAN RK, Ser. fiziko-matematicheskaja, 2016, no. 1, pp. 58–65. (in Russian)
27. *Biyashev R. G., Kalimoldayev M. N., and Rog O. A.* Modelirovanie semantiki tipizirovannogo atributnogo razgranichenija dostupa [Modeling of semantics of typed attribute-based access control]. Problemy Informatiki, 2017, no. 1, pp. 25–37. (in Russian)

28. *Kalimoldayev M. N., Biyashev R. G., and Rog O. A.* Primenenie logiki dlja postroenija modelej razgranichenija dostupa k informacii [The use of logic for constructing models for the control of access to information]. Dokl. NAN RK, 2017, no. 3, pp. 48–54. (in Russian)
29. *Kalimoldayev M. N., Biyashev R. G., and Rog O. A.* Osnovy arhitektury programmnyh sistem dlja osushhestvlenija tipizirovannogo atributnogo razgranichenija dostupa [Fundamentals of the architecture of software systems for the implementation of typed attribute-based access control]. Proc. "Sovremennye Problemy Informatiki i Vychislitel'nyh Tehnologij" (29–30 Juny 2017), Almaty, 2017, pp. 88–95. (in Russian)
30. *Kalimoldayev M. N., Biyashev R. G., and Rog O. A.* O primenenii tipizirovannogo atributnogo razgranichenija dostupa v global'nyh vychislitel'nyh sredah [On the application of typed attribute-based access control in global computing environments]. Izv. Nauchno-Tehnicheskogo Obshhestva "KAHAK", Almaty, 2017, no. 3(58), pp. 30–36. (in Russian)