УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004

Построение шаблонов для решения задачи контроля целостности конфигурации на основе атрибутной модели контроля доступа

Ф. М. Ерин
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская область, Россия

Осуществлено объединение атрибутных моделей контроля доступа, контроля целостности и шаблонов безопасности в единую концепцию. Описывается, каким образом связаны эти аспекты информационной безопасности между собой, а также какие преимущества применение такой концепции имеет перед существующими решениями.

Ключевые слова: атрибутная модель контроля доступа (ABAC), контроль целостности конфигурации, шаблоны безопасности, стандарт XACML, стандарт NGAC.

Ранее такие аспекты безопасности информационных систем, как модели контроля доступа, контроль целостности и шаблоны безопасности, рассматривались достаточно обособленно и относились к разным функциям систем обеспечения информационной безопасности. В каждом из трех направлений было разработано много эффективных подходов к обеспечению защиты информации, но концепции, связывающей эти аспекты в одно целое и открывающей новый подход к решению задачи контроля целостности конфигурации, не было. В данной работе, обосновывается существование, дается формулировка и демонстрируется перспективность применения такой концепции, рассматривается построение и применение шаблонов безопасности для решения задачи контроля целостности конфигурации на основе атрибутной модели контроля доступа.

Атрибутные модели контроля доступа

Системы разграничения доступа к ресурсам информационных систем (ИС) строятся на основе различных моделей: дискреционной (Discretionary Access Control, DAC), мандатной (Mandatory Access Control, MAC), ролевой (Role Based Access Control, RBAC), атрибутной (Attribute Based Access Control, ABAC) и других. Модель ABAC считается наиболее перспективным [1] видом логического управления доступом и информационными потоками в ИС [2]. Разграничение доступа в атрибутной модели устроено следующим образом. В ИС имеется множество сущностей (объекты), субъектов, прав доступа и объектов-параметров (атрибуты объектов). Каждая из сущностей имеет ряд атрибутов. Тройке субъект—сущность—право доступа соответствуют набор объектов-параметров и предикат, который зависит от всех этих логических элементов таким образом, что субъект получает право доступа к конкретной сущности, когда истинен предикат. По инициативе субъекта доступ может быть ему предоставлен (авторизация). Состояние ИС в атрибутной модели управления доступом определяют сущности, текущие состояния прав доступа субъектов к сущностям вместе со значениями атрибутов [1].

Разработаны два стандарта реализации атрибутной модели безопасности: Extensible Access Control Markup Language (XACML) и Next Generation Access Control (NGAC). Эти стандарты имеют существенные различия, но перед ними стоят аналогичные цели и задачи. Применение обоих стандартов позволяет обеспечить стандартизированный способ описания и применения разнообразных политик контроля доступа для различных типов ИС. Однако стандарты по-разному определяют политики контроля доступа, которые отображают набор правил разграничения доступа, заданных для ИС, и их реализации [3]. Стандарт XACML, основанный на Extensible Markup Language (XML), разработан

Ерин Федор Михайлович, студент.
E-mail: fedor.erin@phystech.edu

Статья поступила в редакцию 13 июня 2018 г.

© Ерин Ф. М., 2018

для описания политик безопасности, запросов доступа и ответов, необходимых для обращения к системе политик и принятия решения о предоставлении доступа (авторизации). Политики определяются XML-структурой PolicySet, в которой содержатся правила предоставления доступа. Стандарт NGAC основывается на отношениях (связях между сущностями) и архитектуре ИС, предназначен для описания, управления и применения политик контроля доступа путем конфигурирования связей. Политики определяются отношениями (их виды: Assignments, Associations, Prohibitions, Obligations), которые выражаются классами политик и их атрибутами, вместе составляющими контейнеры. Наборы политик, так же как и группы объектов/субъектов, могут быть объединены и охарактеризованы контейнерами [3]. Указанные стандарты также отличаются по:

- степени разделимости используемого программного пространства между функциями управления доступом и собственной операционной средой;
- операционной эффективности;
- способу управления атрибутами и политиками;
- многообразию и типам поддерживаемых политик;
- возможности поддержки административного надзора за исполнением рабочих функций [3].

Несмотря на существенные различия в подходах, оба стандарта осуществляют контроль доступа к ИС путем контроля атрибутов объектов и взаимосвязей между сущностями ИС.

Контроль целостности

Рассмотрим другой важный аспект информационной безопасности — контроль целостности [4]. Для определенности будем использовать следующее понятие целостности: целостность — это "состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право" [5]. В [6] под контролем целостности (КЦ) понимается процесс вычисления контрольной суммы (КС) и сравнения ее с эталонным значением. Поскольку контролировать непосредственно саму информацию нельзя, контролируют объекты, ее хранящие и обрабатывающие. Контрольная сумма вычисляется исходя из состояния того объекта ИС [7], чью целостность необходимо контролировать. Это может быть программа, персональный компьютер, конфигурация виртуальной инфраструктуры (ВИ) и т. д. Состояние системы (защищаемого объекта) представляет собой набор параметров и их значений, определяющих текущую конфигурацию системы. Контроль целостности позволяет своевременно обнаружить несанкционированные модификации программ и данных и предотвратить их использование [6], поскольку такие действия могут нанести вред, например, компании (ее финансам, репутации), взявшей на себя обязательства по хранению и обработке данной информации. Если, например, сотрудник организации, обрабатывающей личные данные (паспортные данные, кредитные карты, медицинская история и т. п.), некоторое время отсутствовал за компьютером, являющимся защищаемым объектом, а этот объект подвергся атаке хакеров и часть важных данных была стерта или изменена, то КЦ, осуществленный в момент возобновления работы сотрудником за своим компьютером, позволит зафиксировать изменение состояния ИС и сообщить пользователю о нарушении. Если в процессе КЦ контрольные суммы совпадают, то целостность объекта сохранена, если нет, то защищаемый объект был несанкционированно модифицирован.

Существующие подходы к КЦ не лишены недостатков. Если в ИС есть несколько разрешенных состояний (например, как в ВИ), то для каждого из них нужно иметь эталонное значение, что противоречит традиционному представлению о целостности, где эталон всего один (согласно [6] эталон – это контрольная сумма защищаемого объекта, рассчитываемая на основании значений атрибутов, критически важных для целостности; КС текущего состояния объекта рассчитывается в момент проверки целостности, например в момент включения персонального компьютера). Эталон не может пониматься как нечто неизменное, так как современные ИС динамичны и могут изменять свое состояние в течение времени, это допустимо и не должно вызывать нарушение целостности. При таких условиях эталон должен быть гибким и легко модифицируемым (разумеется, только имеющими на это право субъектами). КЦ с использованием КС не дает детализации: несовпадение контрольных сумм не позволяет определить, какие конкретно параметры ИС изменились. Необходим новый подход к КЦ.

Применение атрибутных моделей контроля доступа к КЦ

Для принятия решения о предоставлении доступа в атрибутных моделях контроля доступа используются наборы атрибутов объекта, субъекта и условий среды (не зависящие от объекта и субъекта характеристики среды, в которой выполняется запрос субъекта на доступ к объекту, например время или день недели), характеризующие текущее их состояние. Доступ предоставляется в соответствии с

действующими политиками безопасности, которые определяют, какими атрибутами должен быть наделен субъект доступа, чтобы ему был предоставлен доступ к объекту, имеющему свой определенный набор атрибутов, при текущих значениях атрибутов условий среды. Подобный подход может быть применен к КЦ [8]. Действительно, состояние ИС и среды описывается атрибутами. Аналогичным образом можно описать эталон. Следовательно, можно их соотнести на предмет совпадения, что проверит корректность состояния ИС. Тем самым будет произведен КЦ. В [8] данная тема уже поднималась, рассматривался КЦ конфигурации ВИ. Однако концепция применения атрибутных моделей контроля доступа для КЦ ВИ может быть обобщена и на КЦ ИС в целом. Применимость стандарта XACML для КЦ на практике была доказана в [9], и так как стандарты XACML и NGAC лишь реализуют атрибутную модель безопасности, то будем подразумевать применение именно XACML. Однако остаются открытыми вопросы построения и хранения эталонов: если КЦ с использованием КС не является лучшим подходом и вместо этого следует представлять эталон(ы) набором атрибутов, то как строить и перестраивать (в случае изменения) такие эталоны, и каким образом должно задаваться множество разрешенных состояний ИС?

Шаблоны безопасности

Существуют различные способы построения шаблонов для КЦ. В данной работе понятие шаблона безопасности отличается по смыслу от понятия эталона: под шаблоном понимается определённый допустимый набор настроек ИС, который может отражать как одно допустимое состояние ИС, так и несколько. Рассмотрим существующие решения по созданию шаблонов безопасности, чтобы выявить их сильные стороны и недостатки. Это позволит показать, что существующие решения по созданию шаблонов «заточены» именно под идею единственности эталонного состояния и не рассматривают эталон, как нечто гибкое и легко перестраиваемое, поэтому шаблон безопасности единственен и отождествлен с эталоном.

В продукте vGate, сертифицированном средстве защиты платформ виртуализации, эталоном является контрольная сумма ВИ, рассчитанная на основании параметров конфигурации ВИ [10]. Для расчета контрольной суммы используется вспомогательная утилита guest-chsum-calc, в которую передается конфигурационный файл, содержащий пути до всех файлов, контрольные суммы которых необходимо посчитать. В результате обработки входного файла с путями генерируется файл в формате JSON, содержащий контрольные суммы заданных файлов ОС, контрольные суммы главной загрузочной записи (MBR) всех найденных дисков, а также серийные номера разделов дисков, в которых хранятся заданные файлы. Путем расчета контрольных сумм формируются эталоны еще, например, в средстве защиты информации "Аккорд-В" [11]. В продукте HyTrust, также защищающем ВИ, эталон конфигурации ВИ представляется набором фиксированных значений корректных параметров, определяющих конфигурацию ВИ [12]. При проверке целостности состояние ВИ сравнивается с эталонным, и администратор безопасности получает уведомление о том, какие параметры расходятся со своими эталонными значениями. Данные решения формируют эталоны, но не позволяют расширить эталон новыми разрешенными значениями подконтрольных параметров безопасности: если некоторое новое состояние ИС необходимо начать считать разрешенным, то оно будет представлено другим эталоном, и при этом прежнее состояние уже не будет проходить проверку КЦ. В результате необходимо будет хранить два и более эталона, что не оптимально для ИС с множеством разрешенных состояний.

Атрибутное описание шаблонов безопасности

Шаблоны безопасности могут быть выражены языком атрибутов [8], т. е. шаблон можно представить как набор пар вида атрибут—значение, использование которого позволяет создавать, изменять и применять шаблоны безопасности для КЦ ИС. Построенные таким образом шаблоны обладают высокой детализацией и гибкостью, поскольку могут быть модифицированы и расширены для проверки множества корректных состояний ИС. В этом случае нет необходимости хранить для каждого состояния свой эталон, вместо этого при появлении нового корректного состояния предыдущий эталон будет модифицирован и будет поддерживать новую конфигурацию ИС. Такой шаблон будет соответствовать всему множеству разрешенных состояний ИС, так как атрибутные модели безопасности подразумевают использование сложных булевых (логических) функций над множеством атрибутов и условий, а это множество может содержать сколько угодно допустимых конфигураций ИС. Однако в случае появления нового разрешенного состояния ручная правка атрибутов в шаблоне администратором безопасности трудоемка, велик шанс ошибиться, поэтому необходимо создать алгоритм автоматического перестроения шаблонов.

Заключение

Рассмотрение трех описанных аспектов как единой концепции открывает принципиально новый подход к КЦ. Использование атрибутной модели контроля доступа для КЦ ИС позволяет детально сравнивать состояние ИС с эталоном, который может быть легко модифицирован (расширен) до нового корректного. Язык атрибутного описания хорошо подходит не только для описания состояний объектов КЦ и эталонов, но и для формирования гибкого шаблона безопасности, который поддерживает ИС (например, ВИ) с множеством разрешенных состояний. Для обеспечения высокой эффективности такого подхода к КЦ необходимы механизмы автоматического перестроения эталонов безопасности.

Литература

1. *Чернов Д. В.* О моделях логического управления доступом на основе атрибутов. // ПДМ. Приложение. 2012. № 5. https://cyberleninka.ru/article/n/o-modelyah-logicheskogo-upravleniya -dostupom-na-osnove-atributov
2. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. — М.: Горячая линия-Телеком, 2011. — 320 с.
3. *Ferraiolo D. et al.* A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Application [Электронный ресурс]. URL: http://dx.doi.org/10.6028/NIST.SP.800-178 (дата обращения: 23.05.2018).
4. ГОСТ Р ИСО/МЭК 17799—2005 [Электронный ресурс]. URL: https://www.niisva.su/wp-content/uploads/2014/09/ГОСТ_Р_ИСО-МЭК_17799-2005.pdf (дата обращения: 20.05.2018).
5. Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения [Электронный ресурс]. URL: http://www.altell.ru/ legislation/standards/50.1.056-2005.pdf (дата обращения: 23.05.2018).
6. *Конявский В. А., Лопаткин С. В.* Компьютерная преступность. В 2 томах. Т. 2. — М.: РФК-Имидж Лаб, 2006. — 840 с.
7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения [Электронный ресурс]. URL: https://www.niisva.su/wp-content/uploads/2014/ 09/ ГОСТ_Р_ 50922-2006-Защита-информации. -Основные-термины-и-определения.pdf (дата обращения: 23.05.2018).
8. *Ерин Ф. М.* Представление эталона конфигурации ВИ в виде наборов политик языка FACPL: отчет по НИР. — М.: МФТИ (ГУ). 2017.
9. *Мозолина Н. В.* Разработка средства контроля целостности виртуальной инфраструктуры и её конфигураций: выпускная квалиф. работа. — М.: МФТИ (ГУ). 2017.
10. Документация vGate R2. Руководство администратора. Принципы функционирования [Электронный ресурс]. URL: http://www.securitycode.ru/products/vgate/documentation/ (дата обращения: 24.05.2018).
11. ПАК «Аккорд-В.» [Электронный ресурс]. URL: http://www.accord.ru/accord-v.html (дата обращения: 24.05.2018).
12. Управление доступом к виртуальной инфраструктуре с помощью продукта HyTrust [Электронный ресурс]. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-virtualnykh-sred/upravlenie-dostupom-k-virtualnoj-infrastrukture-s-pomoschyu-produkta-hytrust/2012 (дата обращения: 25.05.2018).

Building templates for solving configuration integrity monitoring task constructed on the attribute-based access control

F. M. Erin
Moscow Institute of Physics and Technology (State University),
Dolgoprudny, Moscow region, Russia

The article combines attribute attribute-based access control, integrity monitoring and security templates into a single concept. It describes how these aspects of information security relate to each other, also what advantages the application of such a concept has over existing solutions.

Keywords: attribute-based access control (ABAC), configuration integrity monitoring, security templates, XACML standard, NGAC standard.

Bibliography — 12 references. *Received June 13, 2018*