УДК 004.056.52

Выработка требований к децентрализованной системе разграничения доступа

А. Ю. Чадов
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская обл., Россия

Сформированы требования к системе разграничения доступа, в которой основные функциональные элементы разнесены на разные рабочие станции. На основе полученных требований предложен пример архитектуры системы. Выделены особенности такой системы, которые необходимо исследовать.

Ключевые слова: разграничение доступа, централизация, децентрализация, модульная система.

Одной из основных задач защиты информации является разграничение доступа. Существует большое количество различных систем разграничения доступа к информации. Среди основных решений на рынке систем защиты информации (СЗИ) от несанкционированного доступа (НСД) можно выделить следующие наиболее распространенные продукты:

- Secret Net ("Код Безопасности"): степень охвата рынка 52 %
- "Аккорд" (ОКБ САПР): степень охвата рынка 25,8 %
- Dallas Lock ("Конфидент"): степень охвата рынка 5,8 % [1].

Во всех этих решениях система, принимающая решения о запрете или разрешении доступа, располагается на самом подконтрольном объекте (ПКО). Таким образом машина, отвечающая за обработку данных, отвечает и за безопасность [2—7].

Проанализируем, что будет, если построить систему, в которой эти функции выполняют разные машины.

Далее описывается концепция новой системы разграничения доступа, в которой элемент, отвечающий за принятие решений о разрешении доступа, вынесен на другую машину.

При создании концепции новой системы сначала определим модель контроля доступа, которая будет использоваться в этой системе. Наиболее популярными и распространёнными являются подход к разграничению доступа на основе ролей (Role-Based Access Control, RBAC) [8] и подход к разграничению доступа на основе атрибутов (Attribute-Based Access Control, ABAC) [9]. Однако роль в понимании стандарта RBAC может быть назначена субъекту в рамках ABAC в качестве одного из атрибутов, что делает RBAC в некотором смысле частным случаем и лишает его всех преимуществ перед ABAC [10, 11]. Поэтому новая система должна базироваться на атрибутной модели контроля доступа контроля целостности отчужденного выполнения сервисов. В первом разделе описываются первые теоретические попытки разрешения указанного противоречия. Во втором разделе речь идет о подходе, на который опираются основные исследования в этой области, и методах, реализующих данный подход. В третьем разделе проводятся обзор и сравнение реализованных систем, основанных на описанных методах, по указанным ранее требованиям.

Чадов Антон Юрьевич, аспирант.
E-mail: "barrens"@okbsapr.ru

Статья поступила в редакцию 13 июня 2018 г.

Проектирование новой системы

Определение архитектуры новой системы: в спецификации NIST стандарта ABAC приведены два варианта архитектуры системы для двух стандартов, NGAC и XACML (рис. 1, 2).

В обоих вариантах предложена модульная система. Модульные системы обладают рядом достоинств: возможность резервного дублирования отдельных критичных модулей, лёгкая заменимость модулей при необходимости, удобное управление и настройка.

В соответствии со стандартом новая система — модульная. В новой системе элемент, отвечающий за принятие решений, вынесен на отдельную рабочую станцию. При этом на ПКО остается агент, перехватывающий запросы субъектов к объектам и отправляющий их к удалённому элементу, принимающему решения о доступе. Поскольку модуль принятия решений вынесен отдельно, имеет смысл сделать его одним для всех ПКО, контролируемых данной системой разграничения доступа в рамках одной информационной системы, чтобы избежать ненужного дублирования.

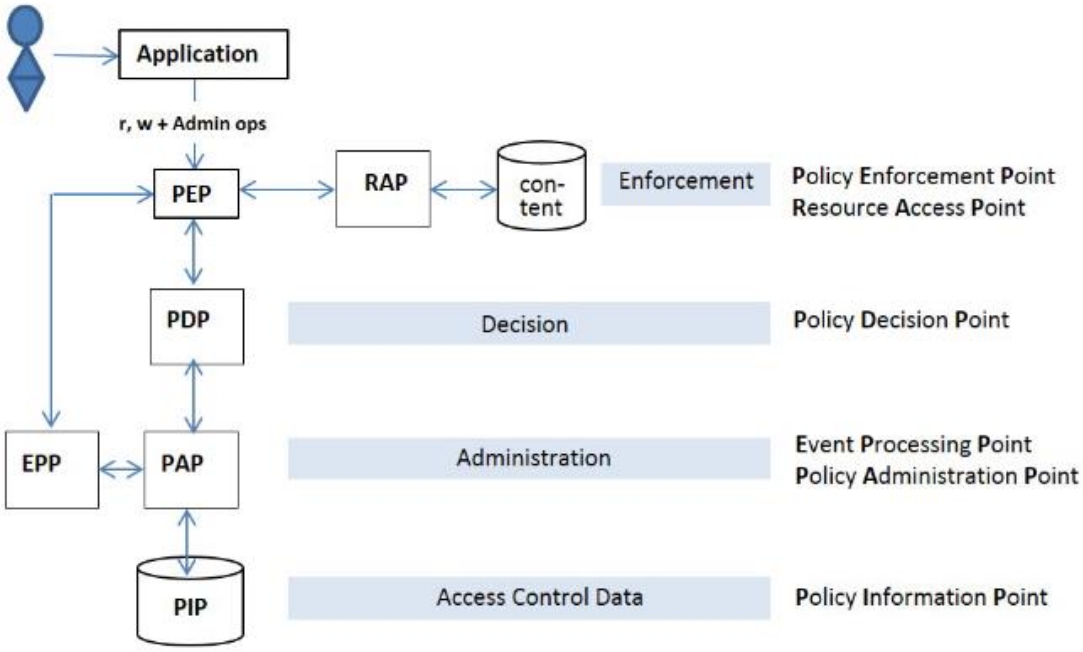

Рис. 1. Функциональная архитектура NGAC (см. [12], С. 34)

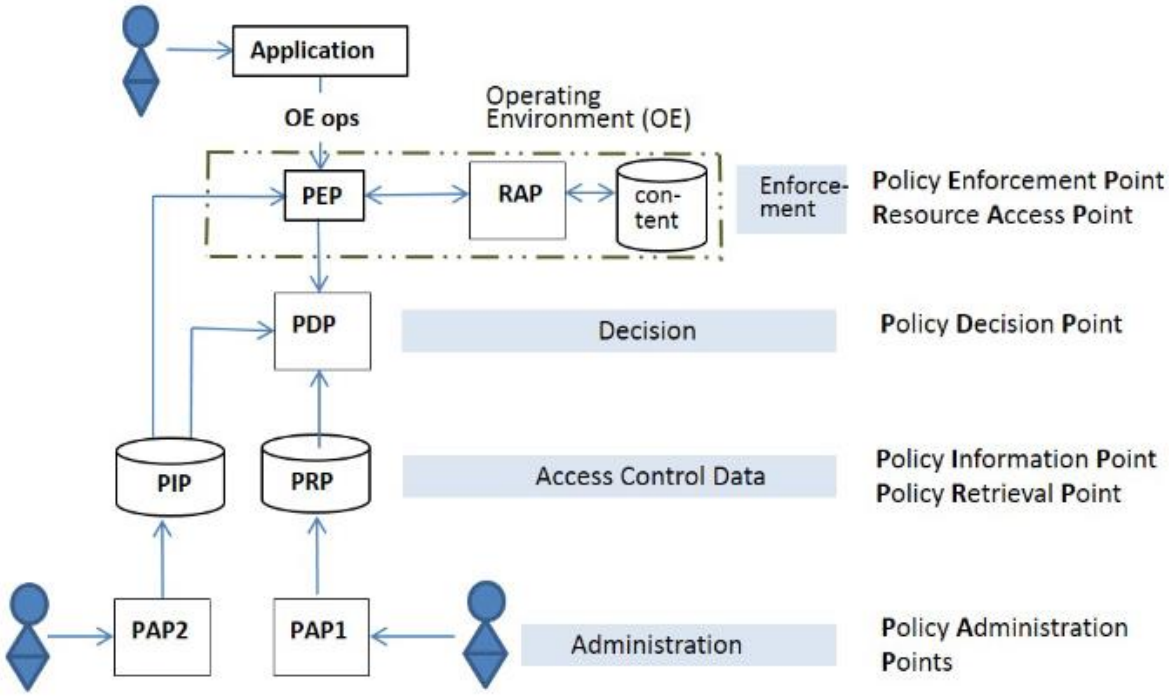

Рис. 2. Функциональная архитектура XACML (см. [12], С. 21)

Модульная система разграничения доступа будет более универсальной: если, например, операционную систему (ОС) на рабочих станциях нужно будет сменить на несовместимую с модулем перехвата данных, достаточно будет сменить только этот модуль на совместимый с нужной ОС.

Выделим два элемента, которые должны быть в новой системе разграничения доступа. В стандарте в обеих архитектурах помимо уже обозначенных модулей есть отдельный модуль хранения политик доступа и модуль управления политиками. Включим их в новую систему. Итак, среди модулей в новой системе должны быть модуль принятия решений о доступе, модуль хранения политик доступа, модуль-перехватчик запросов доступа субъектов к объектам, модуль управления политиками. Также

нужна транспортная система для передачи сообщений между модулями и хранения их в очередях в случае необходимости. Она также должна являться модулем. При дальнейшем развитии можно будет при необходимости добавлять новые модули. Например систему журналирования тоже можно вынести в отдельный модуль.

Трудности, возникающие при построении модульной системы

Сама концепция модульной системы привносит особенности, которые необходимо учитывать.

Во-первых, если решения теперь принимаются на удалённой машине, то ко времени принятия решения о предоставлении доступа добавляется время на передачу сообщений между модулями; как следствие может возрасти время отклика системы. При проектировании нужно учесть особенности передачи данных по сети и минимизировать задержку. Возможно, для этого придётся объединять некоторые модули в рамках одной рабочей станции либо делать локальный кэш. *Задержка работы системы не должна превышать времени чтения данных с диска.* Современные сетевые технологии позволяют построить такую систему: задержка передачи по сети достаточно мала по сравнению со скоростью чтения данных с диска [13].

Во-вторых, необходима защита данных, передаваемых между модулями. Поскольку теперь части системы разграничения доступа находятся не в рамках одной рабочей станции, для некоторых типов сообщений (нужно исследовать, для каких именно) *придётся обеспечивать конфиденциальность или целостность данных*. Для этого можно использовать шифрование, подпись либо протоколы защиты канала. Следует учесть, что всё это также повлияет на скорость отклика и должно быть учтено в проектировании. Также нужно *предусмотреть механизм аутентификации элементов при общении друг с другом*.

Требования к системе и пример архитектуры

В примере, приведенном на рис. 3, все модули общаются друг с другом через менеджер сообщений. Работа строится следующим образом. Сначала администратор через автоматизированное рабочее место (АРМ) управления настраивает базу данных политик. Затем в процессе работы агенты, перехватывая события, обращаются к серверу принятия решений. Он делает запрос в базу данных (БД) политик и на основе полученных оттуда данных даёт агенту ответ.

В итоговый вариант схемы могут добавиться новые модули, может появиться локальный кэш на ПКО, что приведёт к изменению схемы работы с системой.

Суммируя сказанное, получаем следующий список требований к новой системе разграничения доступа:

- Система должна состоять из отдельных модулей, общающихся друг с другом через определённое API. Среди этих модулей обязательно должны быть модуль принятия решений о доступе, модуль хранения политик доступа, модуль-перехватчик запросов доступа субъектов к объектам, модуль управления политиками, модуль транспортной системы для передачи сообщений.

Рис. 3. Возможный вид новой системы

- Решения о доступе субъектов к объектам принимает центральный модуль, политики также хранятся централизовано.
- Задержка, вносимая работой системы, не должна ощущаться пользователем: она должна быть того же порядка, что и время обращения к диску, или меньше.
- Модули должны уметь проводить взаимную аутентификацию.
- Данные, передаваемые в запросах модулей друг к другу, должны быть защищены.

В дальнейшем планируется решить вопросы, поднятые во втором разделе: безопасность и быстродействие системы. Необходимо провести исследование, каким будет время отклика у такой системы, какие методы защиты данных нужно применить в этой системе и для каких именно данных, также проработать технические моменты реализации агента. Например, при генерации события доступа субъекта к объекту агент должен будет отправить запрос к модулю принятия решений, а для этого агенту нужно будет получить доступ к сетевым ресурсам, что сгенерирует событие доступа. С учётом результатов этих исследований можно будет приступить к созданию итогового проекта.

Литература

1. *Комаров А.* Рынок систем защиты информации (СЗИ) от несанкционированного доступа (НСД) в России. 2013 [Электронный ресурс]. URL: https://www.anti-malware.ru/node/11728# (дата обращения: 02.04.2018).
2. Документы Компании "Код безопасности". Средство защиты информации SecretNet 7. Руководство администратора. Принципы построения [Электронный ресурс]. URL: https://www.securitycode.ru/upload/documentation/secret_net/Secret_Net_Admin_Guide_Construction_Principles.pdf (дата обращения: 15.03.2018).
3. Документы Компании "ОКБ САПР". Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа "АККОРД-Win32" (версия 4.0). Описание применения [Электронный ресурс]. URL: http://www.accord.ru/accwin32-prim.html (дата обращения: 15.03.2018).
4. Документы Компании "ОКБ САПР". Система удаленного централизованного управления СЗИ от НСД АККОРД. Руководство администратора [Электронный ресурс]. URL: http://www.accord.ru/accwin32-admin.html (дата обращения: 15.03.2018).
5. Документы Компании "ОКБ САПР". СУЦУ [Электронный ресурс]. URL: http://www.accord.ru/sucu.html (дата обращения: 15.03.2018).
6. Документы Центра защиты информации ООО "Конфидент". Система защиты информации от несанкционированного доступа "Dallas Lock 8.0-K". Описание применения [Электронный ресурс]. URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-01%2031%20-%20Описание%20применения%20DL%208.0-K.pdf (дата обращения: 15.03.2018).
7. Документы Центра защиты информации ООО "Конфидент". Система защиты информации от несанкционированного доступа "Dallas Lock 8.0-K". Руководство по эксплуатации [Электронный ресурс]. URL: https://www.dallaslock.ru/upload/medialibrary/cp/documents/RU.48957919.501410-02%2092%20-%20Руководство%20по%20эксплуатации.pdf (дата обращения: 20.11.2016).
8. *Ferraiolo D., Kuhn R.* Role-Based Access Controls: Proceedings of the 15th National Computer Security Conference. — Gaithersburg: NIST Gaithersburg MD, 1992. P. 554—563.
9. *Sandhu R., Ferraiolo D., Kuhn R.* The NIST model for role-based access control: towards a unified standard // Proceedings of the 5th ACM Workshop on Role-based Access Control. — N.Y: ACM New York, 2000. P. 47–63.
10. *Coyne E., Weil T. R.* ABAC and RBAC: Scalable, Flexible, and Auditable Access Management // IT Professional. 2013. № 3. P. 14–16.
11. *Угрюмов С.* Проект подсистемы централизованной обработки событий контроля доступа: вып. квалифик. работа. — М.: Кафедра "Защита информации" ФРТК МФТИ, 2017. — 23 с.
12. *Ferraiolo D., Chandramouli R., Hu V., Kuhn R.* NIST Special Publication 800-178 A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications.
13. Latency Numbers Every Programmer Should Know [Электронный ресурс] URL: https://gist.github.com/jboner/2841832 (дата обращения: 01.04.2018).

Requirements engineering for decentralized computer access control system

A. Yu. Chadov

Moscow Institute of Physics and Technology (State University), Dolgoprudny, Moscow region, Russia

In the article requirements to computer access control system were formed. Based on the received requirements the architecture of system was proposed. The special aspects of such a system which should be investigated further were marked.

Keywords: computer access control, centralization, decentralization, modular system.

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