Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ИСПОЛЬЗОВАНИЕ АТРИБУТНОЙ МОДЕЛИ КОНТРОЛЯ ДОСТУПА В ЗАДАЧЕ КОНТРОЛЯ ЦЕЛОСТНОСТИ КОНФИГУРАЦИИ

Н.В. МОЗОЛИНА

Закрытое акционерное общество «ОКБ САПР»

Введение

В последние годы стремительно развивается модель безопасности, в которой решение о предоставлении доступа субъекта к объекту или отказе в нём принимается на основе атрибутов, присвоенных этим субъекту и объекту, условий среды, а также наборов политик доступа, – атрибутная модель контроля доступа (Attribute-Based Access Control, ABAC) [1]. Разработаны стандарты реализации и применения этой модели – XACML [2] и NGAC [3].

На основе данной модели может быть реализовано как разграничение доступа, например, в медицинских учреждениях[4], так и решён ряд задач, напрямую с разграничением доступа не связанных: балансировка нагрузки (числа включённых виртуальных машин) на хостах-гипервизорах [5] или динамическое создание правил межсетевого экрана [6].

В данной статье рассмотрим применение ABAC при решении задачи контроля целостности конфигурации.

Задача контроля целостности конфигурации

Целостность, наряду с конфиденциальностью и доступностью, – одно из основных свойств информации с точки зрения безопасности [7], обеспечение которого является общепринятой практикой защиты информации.

В настоящее время контроль целостности в рамках некоторого средства вычислительной техники (СВТ) или информационной системы (ИС), в целом, состоит из следующих этапов:

1. Контроль физического оборудования.
2. Контроль BIOS, MBR, файлов операционной системы (ОС).
3. Контроль пользовательских файлов, а также запускаемых программ.

Например, это может быть осуществлено с помощью продуктов «Аккорд-АМДЗ» и «Аккорд-Win32/64» (или «Аккорд-X», если мы работаем на ОС семейства Linux). Так, с помощью «Аккорд-АМДЗ» контролируется, что при включении компьютера управление передаётся именно тому BIOS, который соответствует принятому эталону, что загружается именно та ОС, которая и должна быть загружена, и что её загрузка происходит именно на том оборудовании, которое и должно быть. Затем начинает свою работу «Аккорд-Win32/64»: это средство защиты информации от несанкционированного доступа контролирует не только доступ субъектов к объектам, но и целостность файлов ОС и пользовательских файлов, контролирует, какие процессы, какие программы в системе могут быть запущены [8-9].

Однако одна и та же программа при различных настройках может работать поразному, и некоторые из настроек могут создавать угрозы безопасности.

Так возникает ещё один этап контроля целостности – контроль настроек программного обеспечения (ПО), проверка его конфигурации на соответствие некоторому эталону, при котором программа работает корректно и не создаёт угрозы безопасности.

При контроле целостности конфигурации следует учитывать, что может существовать несколько конфигураций, которые будут считаться корректными – удовлетворять как требованиям по функциональности используемого программного обеспечения, так и требованиям безопасности.

Возникает противоречие с традиционным подходом к контролю целостности, когда разрешённым может быть лишь одно состояние, совпадающее с эталоном.

Задача контроля конфигурации ПО с учётом нескольких разрешённых состояний находится за гранью возможностей, существующих на текущий момент средств защиты информации.

Для того чтобы понять, как решить задачу контроля целостности конфигурации, на данном этапе ограничимся её частным случаем – контролем конфигурации виртуальной инфраструктуры (ВИ).

Контроль целостности конфигурации ВИ

Под конфигурацией ВИ при этом будем понимать совокупность её объектов, связей между этими объектами и их параметры (атрибуты) [10].

Контроль целостности предполагает сравнение текущего состояния некоторого объекта с эталоном, то есть выделенным состоянием объекта, которое считается корректным и безопасным.

Но при контроле целостности конфигурации виртуальной инфраструктуры следует учитывать, что ВИ – динамическая система в том смысле, что некоторые её связи, атрибуты объектов могут быть изменены и при этом состояние системы останется корректным (не нарушающим целостность). Например, для виртуальной машины может быть определён набор хостов-гипервизоров, перемещение между которыми (миграция) разрешено.

Если рассматривать эталонную конфигурацию ВИ в традиционном понимании, то есть как некоторый «снимок» конкретного состояния системы, то мы столкнёмся с тем, что выбор такого эталона зачастую невозможен – например, одним «снимком» нельзя охватить сразу несколько разрешённых состояний. Необходимо задать такое представление эталона и текущей конфигурации, такое их сопоставление, которое позволит учесть множество разрешённых состояний [11-12].

Для решения этой проблемы воспользуемся атрибутной моделью контроля доступа. В данной статье качестве конкретного примера ABAC будет использован стандарт XACML[2] и его реализация – язык FACPL[4,5,13].

Применение ABAC для контроля целостности конфигурации ВИ

Согласно стандарту XACML по запросу пользователя на доступ к объекту формируется запрос («request»), в который включаются необходимые для принятия решения о предоставлении доступа атрибуты субъекта, объекта и среды, в которой происходит запрос. Каждый запрос проверяется на соответствие политикам доступа («PolicySet»), иными словами, политики применяются к запросу. Если запрос политикам соответствует, то результатом применения политики будет значение «permit», в этом случае доступ субъекта к объекту разрешён. Если же результатом применения политик к запросу является значение «deny» – доступ запрещён.

Каждому объекту виртуальной инфраструктуры можно поставить в соответствие XACML-запрос («request»). Этот запрос будет состоять из всех атрибутов, которые соответствуют рассматриваемому объекту в ВИ, а также из дополнительных атрибутов, обозначающих связи с другими объектами. Совокупность запросов для всех объектов ВИ будет являться представлением текущей конфигурации.

В качестве эталона будет задано «PolicySet» – множество политик, построенных таким образом, что целостность конфигурации виртуальной инфраструктуры сохранена тогда и только тогда, когда получен результат «permit» при обработке абсолютно всех запросов («requests»), составляющих представление о текущей конфигурации ВИ. Если хотя бы 1 запрос получит значение «deny» – имеет место нарушение целостности конфигурации ВИ.

Работоспособность такого решения проверена на практике через создание тестового средства контроля целостности конфигурации ВИ, построенной на платформе виртуализации VMware vSphere.

Созданное средство состоит из двух компонентов – первый предназначен для работы на автоматизированном месте администратора безопасности системы, второй – на выделенном сервере проверки.

Общая схема работы выглядит следующим образом:

1. Администратор безопасности на языке FACPL пишет множество политик, определяющие эталон виртуальной инфраструктуры, - «PolicySet».Эти политики должны быть переданы на выделенный сервер проверки.

2. По запросу модуль, работающий на автоматизированном рабочем месте администратора, получает данные из виртуальной инфраструктуры, определяющие её текущее состояние, и формирует на их основе запросы («requests»).

3. После передачи этих запросов на сервер проверки, начинается их проверка на соответствие созданным ранее политикам.

4. Если проверка всех запросов на соответствие политикам прошла успешно (с результатом «permit»), то целостность конфигурации ВИ сохранена. В противном случае имеет место нарушения целостности.

Заключение

Атрибутная модель контроля доступа может применяться в решении как задачи разграничения доступа, так и в задаче контроля целостности конфигурации ВИ.

Представление текущей конфигурации ВИ через множество XACML-запросов, эталона – через набор политик безопасности, сопоставление текущей конфигурации с эталоном – через применение политик к запросам – всё это позволяет учесть, что разрешёнными, не нарушающими целостность может быть несколько конфигураций.

Таким образом, при применении атрибутной модели контроля доступа решается основная проблема контроля целостности конфигурации – противоречие с традиционным подходом, при котором разрешённым может быть лишь одно состояние, совпадающее с эталоном.

Список литературы

1. Hu V. C., et al. Guide to Attribute Based Access Control (ABAC) Definition and Considerations // NIST Approved: Special Publication (SP) 800-162. 2014 [Электронный ресурс]. URL: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf (дата обращения: 16.01.2017).

2. eXtensible Access Control Markup Language (XACML) Version 3.0 OASIS Standard [Электронный ресурс]. URL: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf (дата обращения: 16.01.2017).

3. Information technology - Next Generation Access Control - Functional Architecture (NGAC-FA) // INCITS 499-2013. American National Standard for Information Technology, American National Standards Institute. 2013.

4. Margheri A., Masi M., Pugliese R., Tiezzi F. On a Formal and User-Friendly Linguistic Approach to Access Control of Electronic Health Data // Proc. of the International Conference on Health Informatics (HEALTHINF 2013), SCITEPRESS – 2013

5. Margheri A., Masi M., Pugliese R., Tiezzi F. Developing and Enforcing Policies for Access Control, Resource Usage, and Adaptation. A Practical Approach. // Proc. of the 10th International Workshop on Web Services and Formal Methods (WS-FM 2013), Springer – 2013.

6. Berger S., Vensmer A., Kiesel S. An ABAC-based policy framework for dynamic firewalling //International Conference on Systems and Network Communications (ICSNC 2012), 2012. – С. 118-123.

7. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005. С. 5.

8. Аккорд-АМДЗ // [Электронный ресурс] URL: http://www.accord.ru/amdz.html (дата обращения: 10.04.2017).

9. ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) [Электронный ресурс] URL: http://www.accord.ru/acwin32.html (дата обращения: 10.04.2017)

10.Мозолина Н. В. Контроль целостности виртуальной инфраструктуры и её конфигураций. // Комплексная защита информации. Материалы XXI Международной конференции. Смоленск 2016. С. 167–170.

11.Мозолина Н. В. Задание эталона при контроле целостности конфигурации виртуальной инфраструктуры // Новые Информационные Технологии и Системы. Сборник научных статей XII Международной научно-технической конференции г. Пенза. 2016 г. С. 219–225.

12.Мозолина Н. В. Выбор способа задания эталона при контроле целостности конфигурации виртуальной инфраструктуры // 59-я Всероссийская научная конференция МФТИ [Электронный ресурс]. URL: http://conf59.mipt.ru/static/prog.html (дата обращения: 16.01.2017).

13.Margheri A. et al. A rigorous framework for specification, analysis and enforcement of access control policies //arXiv preprint arXiv:1612.09339. – 2016.

ОБЗОР ПЕРСПЕКТИВНЫХ РЕШЕНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.П. ПАНАСЕНКО

ООО Фирма «АНКАД»

Фирма «АНКАД» основана в 1991 г. и известна как одна из ведущих компаний-производителей решений по обеспечению информационной безопасности. Основные направления деятельности компании включают в себя разработку, производство и поставку аппаратных и программных средств криптографической защиты информации, электронной подписи, защиты от несанкционированного доступа и разграничения доступа к компьютерным ресурсам, построения защищенных телекоммуникационных сетей и обеспечения безопасности персональных данных [1].

В качестве примеров продуктового ряда Фирмы можно привести:

семейство аппаратно-программных модулей доверенной загрузки (АПМДЗ) «КРИПТОН-ЗАМОК» (рис. 1);

компоненты защищенной архитектуры «тонкого клиента» «КРИПТОН-ТК»;

абонентские шифраторы серии «КРИПТОН».

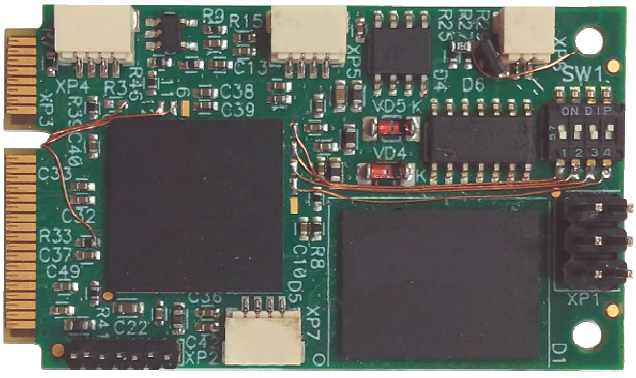

Рис. 1 – АПМДЗ «КРИПТОН-ЗАМОК/mini-E»