НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2015 Том 15 № 6 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2015 Vol. 15 No 6 ISSN 2226-1494 http://ntv.ifmo.ru/en
УНИВЕРСИТЕТ ИТМО

УДК 004.056.53

МЕТОД И АБСТРАКТНАЯ МОДЕЛЬ КОНТРОЛЯ И РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА ПЕРЕНАПРАВЛЕНИЕМ (ПЕРЕАДРЕСАЦИЕЙ) ЗАПРОСОВ ДОСТУПА

М.Г. Ковешников[a], К.А. Щеглов[a], А.Ю. Щеглов[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: info@npp-itb.spb.ru

Информация о статье
Поступила в редакцию 20.04.15, принята к печати 17.09.15
doi:10.17586/2226-1494-2015-15-6-1122-1129
Язык статьи – русский

Ссылка для цитирования: Ковешников М.Г., Щеглов К.А., Щеглов А.Ю. Метод и абстрактная модель контроля и разграничения прав доступа перенаправлением (переадресацией) запросов доступа // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 6. С. 1122–1129.

Аннотация

Исследованы вопросы реализации контроля и разграничения прав доступа субъектов к объектам в современных вычислительных системах. Предложен метод контроля доступа, реализуемый перенаправлением (переадресацией) запросов доступа к объектам. Определено его принципиальное отличие от метода дискреционного контроля доступа – запрос доступа субъекта к объекту, в том случае, когда субъекту необходимо запретить запись в объект (модифицировать объект), не запрещается, он перенаправляется (право доступа сохраняется, но доступ при этом реализуется уже к иному объекту), что позволяет реализовывать разграничительные политики доступа к системным объектам без нарушения работоспособности системы и приложений и корректно разделять объекты доступа между субъектами. Данная важнейшая особенность предложенного метода контроля доступа позволяет решать принципиально новые задачи защиты системных объектов, в том числе реализовывать виртуализацию системных средств, с целью защиты системных объектов от атак со стороны пользователей и приложений. Построена абстрактная модель, на которой показано, что метод контроля доступа субъектов к объектам, реализуемый перенаправлением запросов доступа, может позиционироваться в качестве полноценного самостоятельного метода контроля, с использованием которого может быть реализована любая разграничительная политика доступа субъектов к объектам, т.е. в качестве альтернативы методу дискреционного контроля доступа.

Ключевые слова

информационная безопасность, контроль и разграничение прав доступа, запрос доступа, правило доступа, право доступа, субъект и объект доступа, перенаправление (переадресация) запроса.

METHOD AND ABSTRACT MODEL FOR CONTROL AND ACCESS RIGHTS BY REQUESTS REDIRECTION

M.G. Koveshnikov[a], K.A. Shcheglov[a], A.Yu. Shcheglov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: info@npp-itb.spb.ru

Article info
Received 20.04.15, accepted 17.09.15
doi:10.17586/2226-1494-2015-15-6-1122-1129
Article in Russian

For citation: Koveshnikov M.G., Shcheglov K.A., Shcheglov A.Yu. Method and abstract model for control and access rights by requests redirection. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2015, vol. 15, no. 6, pp. 1122–1129.

Abstract

We have researched implementation problems of control and access rights of subjects to objects in modern computer systems. We have suggested access control method based on objects access requests redirection. The method possesses a distinctive feature as compared to discretional access control. In case when a subject needs to deny writing (object modification), it is not denied but redirected (access rights are not changed, but operation is performed with another object). This gives the possibility to implement access policies to system objects without breaking the system and applications operability, and share correctly access objects between subjects. This important property of suggested access control method enables to solve fundamentally new system objects securing problems like system resources virtualization aimed to protect system objects from users' and applications attacks. We have created an abstract model, and it shows that this method (access control from subjects to objects based on requests redirection) can be used as self-sufficient access control method, implementing any access control policy (from subjects to objects), thus being an alternative to discretional access control method.

Keywords

information security, control and access rights, access request, access rule, access right, access subject and object, request redirection.

Введение

Наиболее широко сегодня на практике используется метод дискреционного контроля доступа (его еще называют избирательным при принудительном управлении информационными потоками – при исключении возможности создателем объекта самому назначать к нему правила доступа [1]), что позволяет реализовать контроль и разграничение прав доступа субъектов к объектам на основе матрицы доступа, формализующей представление назначаемых правил доступа. К правам доступа субъекта к объекту, используемым при задании соответствующих правил, относятся разрешение/запрет чтения, записи, удаления и т.д.

В современных условиях требования к реализации дискреционного контроля доступа, являющегося основой построения ролевой модели контроля доступа (Role-Based Access Control Models) [2], существенно расширяются, что позволяет реализовать эффективную защиту от актуальных угроз атак[1]. В частности, субъект доступа требуется уже идентифицировать двумя сущностями: пользователь, процесс [3], что позволяет решать задачи защиты от угроз атак на приложения [4, 5], в том числе и создаваемых при выявлении в программных средствах ошибок программирования. С целью защиты от атак на повышение привилегий при идентификации субъекта доступа должна учитываться возможность смены исходного идентификатора пользователя, запустившего процесс, запрашивающий доступ к защищаемому ресурсу. Субъект доступа в этом случае уже идентифицируется следующей совокупностью признаков: исходный пользователь, эффективный пользователь, процесс [6], что, например, реализовано и апробировано в [7]. Реализация подобных, на взгляд авторов, необходимых в современных условиях требований, выполнение которых направлено на решение задач защиты от актуальных угроз атак, существенно усложняет практическую реализацию разграничительной политики доступа, что, например, проиллюстрировано в [8]. Как видим, упрощение задачи администрирования становится одной из ключевых современных задач, требующих решения при разработке методов контроля доступа к защищаемым ресурсам. Однако метод дискреционного контроля доступа обладает и еще одним, куда более значимым недостатком, уже ограничивающим его практическое применение (в предположении корректности реализации разграничительной политики доступа). Состоит данный недостаток в том, что далеко не всегда возможно реализовать необходимый с точки зрения безопасности запрет доступа к каким-либо объектам, в первую очередь к системным файловым объектам, без нарушения корректности работы системы и соответствующих приложений [1]. В результате подобного противоречия в системе создается соответствующая угроза уязвимости.

В настоящей работе рассмотрим метод реализации контроля и разграничения прав доступа (далее контроля доступа) субъектов к объектам перенаправлением (переадресацией) запросов доступа, разграничительная политика доступа для которого уже формально описывается не матрицей доступа субъектов к объектам, а матрицей перенаправлений запросов доступа, к правам же доступа субъекта к объекту, используемым при задании соответствующих правил, уже относятся перенаправление в такой-то объект запроса доступа к такому-то объекту/отсутствие перенаправления. Покажем, что данный метод не имеет ключевого недостатка, присущего методу дискреционного контроля доступа, поскольку при его реализации не используется права запрета доступа – запрет доступа реализуется перенаправлением соответствующего запроса доступа к иному объекту. Метод может позиционироваться как полноценный самостоятельный метод контроля и разграничения прав доступа (как альтернатива методу дискреционного контроля доступа). При этом оценим появляющиеся при его практическом применении дополнительные возможности защиты вычислительных систем.

Метод и абстрактная модель дискреционного контроля доступа

Дискреционный контроль доступа при принудительном управлении информационными потоками [1] (Discretionary Access Control – DAC), основан на реализации абстрактной модели Харрисона–Руззо–Ульмана [10]. Основу построения разграничительной политики доступа при его использовании составляет задание администратором матрицы доступа, включающей списки правил доступа каждого субъекта к объектам.

Представим абстрактную модель. Если считать, что множества C {C1, …, C*l*} и O = {O1, …, O*k*} – соответственно линейно упорядоченные множества субъектов и объектов доступа, а R – конечное множество прав доступа $R = \{w,r,x,d\}$ (чтение, запись, исполнение, удаление, отсутствие прав доступа 0). Будем рассматривать наиболее общий набор прав доступа субъекта к объекту на примере контроля доступа к файловым объектам, понимая при этом, что все сказанное с учетом особенностей объекта, в том числе возможных наборов (множеств) задаваемых прав доступа к нему, относится и к иным объектам – защищаемым ресурсам. Тогда разграничительная политика доступа субъектов к объектам описывается матрицей доступа **M**, где M[C,O] – ячейка матрицы, которая содержит набор прав доступа

[1] Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.

субъекта из множества C = {C1, …, Cl} к объекту из множества O = {O1,…, Ok}. В любой момент времени система контроля доступа описывается своим текущим состоянием Q = (C,O,M).

$$\mathbf{M} = \begin{array}{c} \\ \text{C1} \\ \text{C2} \\ . \\ . \\ . \\ \text{C}l-1 \\ \text{C}l \end{array} \begin{array}{c} \begin{array}{cccc} \text{O1} & \text{O2} & & \text{O}k \end{array} \\ \begin{bmatrix} r,w,d & w & & 0 \\ r & r,w,d & & 0 \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ \dots & \dots & & \dots \\ 0 & 0 & & r \\ 0 & w & & r,w,d \end{bmatrix} \end{array}.$$

Замечание 1. Использование именно матрицы доступа в рассматриваемой модели крайне важно и определяет различные способы отображения назначения правил доступа. Матрица **M** отображает назначение правил доступа субъектов к объектам. Транспонируем ее и получим матрицу доступа **M**тр, отображающую назначения правил доступа к объектам субъектов (это два принципиально отличающихся способа реализации метода дискреционного контроля доступа [1]):

$$\mathbf{M}\text{тр} = \begin{array}{c} \\ \text{O1} \\ \text{O2} \\ . \\ . \\ . \\ \text{O}k \end{array} \begin{array}{c} \begin{array}{cccc} \text{C1} & \text{C2} & \text{C}l-1 & \text{C}l \end{array} \\ \begin{bmatrix} r,w,d & r & 0 & 0 \\ w & r,w,d & 0 & w \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & r & r,w,d \end{bmatrix} \end{array}.$$

Данная абстрактная модель на практике используется для формирования требований к безопасности системы и для оценки их выполнения средствами защиты, реализующими методы контроля доступа. Требование к безопасности системы в рассматриваемом случае может быть сформулировано следующим образом: «Для заданной системы состояние Q0 = (C0,O0,M0) следует считать безопасным относительно некоторого права R, если не существует применимой к Q0 последовательности действий, в результате выполнения которых субъектом C0 приобретается право R доступа к объекту O0, исходно отсутствующее в ячейке матрицы M0[C0,O0]». Если же право R, отсутствующее в ячейке матрицы M0[C0,O0], приобретается субъектом C0, то следует говорить, что произошла утечка права R, а система небезопасна относительно права R.

Замечание 2. К аналогичной абстрактной модели (с соответствующими формализациями правил доступа на основе меток безопасности) могут быть сведены модели Белла–ЛаПадулы [11] и Биба [11].

Пример формирования соответствующих требований и оценки их выполнения приведен в [12].

Задача и метод разделения объектов между субъектами доступа

В [1] дано обоснование того, что о корректной реализации метода контроля доступа можно говорить только в том случае, если заданием соответствующих правил доступа может быть реализована разграничительная политика, формально описываемая диагональной (в [1] названной канонической) матрицей доступа, **M**к:

$$\mathbf{M}\text{к} = \begin{array}{c} \\ \text{C1} \\ \text{C2} \\ . \\ . \\ . \\ \text{C}l-1 \\ \text{C}l \end{array} \begin{array}{c} \begin{array}{ccc} \text{O1} & \text{O2} & \text{O}k \end{array} \\ \begin{bmatrix} r,w,d & 0 & 0 \\ 0 & r,w,d & 0 \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ 0 & 0 & 0 \\ 0 & 0 & r,w,d \end{bmatrix} \end{array}.$$

Данное важнейшее требование к корректности реализации метода контроля доступа на практике не может быть выполнено ввиду присутствия в системе объектов, не разделяемых системой и приложениями как между пользователями, так и между процессами. Если, например, в качестве подобного объекта рассмотреть каталог временного хранения файлов, то файлов на момент задания разграничительной политики доступа в нем нет – временные файлы создаются в процессе работы

системы, как следствие, права доступа могут устанавливаться только на данный каталог коллективного пользования в целом. Но именно заданием права записи на каталог применительно к методам контроля доступа субъектов к объектам могут разграничиваться права доступа к объектам между субъектами. Получаем следующее противоречие: не разграничивать права доступа к подобному объекту нельзя (невозможно будет изолировать работу как пользователей, так и приложений), а разграничение приведет к возможности разрешения права доступа к подобному объекту (при попытке полностью изолировать обработку информации между субъектами доступа) только для одного субъекта, что, естественно, приведет к усечению функционала системы или соответствующего приложения для иных субъектов доступа (в том числе это может сказаться на корректности работы некоторых приложений).

Проиллюстрируем описанную проблему с использованием соответствующей матрицы доступа.

Если обозначить объект доступа, не разделяемый системой между субъектами доступа, через Он, то диагональная матрица доступа с учетом наличия в системе неразделяемого объекта преобразуется к следующему виду:

$$\mathbf{M}\text{к} = \begin{array}{c} \\ \text{С1} \\ \text{С2} \\ . \\ . \\ . \\ \text{С}l-1 \\ \text{С}l \end{array} \begin{array}{c} \begin{array}{cccc} \text{О1} & \text{О2} & \text{Он} & \text{О}k \end{array} \\ \begin{bmatrix} r,w,d & 0 & r,w,d & 0 \\ 0 & r,w,d & r,w,d & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & r,w,d & 0 \\ 0 & 0 & r,w,d & r,w,d \end{bmatrix} \end{array}.$$

Как видим, задача обеспечения корректности реализации метода дискреционного контроля доступа состоит в разделении между субъектами доступа не разделяемых системой объектов доступа. Данная задача может быть решена методом перенаправления (переадресации) запросов доступа, реализация которого авторами запатентована [13].

Для каждого субъекта доступа Сi, i=1,...,l (в зависимости от реализуемого контроля доступа субъектов к объектам – для пользователя или для процесса) для неразделяемого объекта Он администратором создается соответствующий собственный объект Онi, i=1,...,l. При запросе доступа субъектом Сi к объекту Он, записи информации системой или приложением в неразделяемый каталог (соответственно чтения из каталога) Он не осуществляется – каталог Он становится виртуальным, к нему невозможно получить доступ ни одному субъекту, запрос доступа перенаправляется в (из) соответствующий каталог Онi субъекта Сi, запросившего доступ к объекту Он. В результате неразделяемый каталог (объект доступа) полностью разделяется между всеми субъектами доступа, а матрица доступа **М**к принимает следующий вид:

$$\mathbf{M}\text{кр} = \begin{array}{c} \\ \text{С1} \\ \text{С2} \\ . \\ . \\ . \\ \text{С}l-1 \\ \text{С}l \end{array} \begin{array}{c} \begin{array}{ccccc} \text{О1} & \text{О2} & \text{Он1} & \text{Он}l & \text{О}k \end{array} \\ \begin{bmatrix} r,w,d & 0 & r,w,d & 0 & 0 \\ 0 & r,w,d & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & r,w,d & r,w,d \end{bmatrix} \end{array}.$$

Перенаправление запроса доступа заключается в анализе поступающего запроса на наличие в нем обращения к объекту Он и в замене в исходном запросе доступа объекта Он на объект Онi, который определяется задаваемыми правилами перенаправлений, в результате чего реализуется переадресация запроса доступа к другому объекту.

Средствами же дискреционного контроля доступа субъектов к объектам могут быть установлены правила запрета доступа к объектам, в которые перенаправлены запросы доступа, исходя из следующего условия: Сi(R=0)Онj, $j\neq i$, i=1,...,l, j=1,...,l.

Метод и абстрактная модель контроля доступа, реализуемого перенаправлением (переадресацией) запросов доступа

Контроль доступа к неразделяемым объектам формально описывается матрицей перенаправлений запросов доступа. В ячейке матрицы перенаправлений запросов доступа, реализуемых для разделения объектов между субъектами, может задаваться одно из следующих двух правил: Сi(Онi)Он, что означает

перенаправление запросов доступа от субъекта С*i* к объекту Он в объект Он*i*; отсутствие перенаправления – С*i*(0)О*j*.

Матрица перенаправлений запросов доступа **М**п для матрицы доступа **М**кр имеет следующий вид:

$$\mathbf{M}\text{п} = \begin{array}{c} \\ \text{С1} \\ \text{С2} \\ . \\ . \\ . \\ \text{С}l-1 \\ \text{С}l \end{array} \begin{array}{c} \begin{array}{cccc} \text{О1} & \text{О2} & \text{Он} & \text{О}k \end{array} \\ \begin{bmatrix} 0 & 0 & \text{Он1} & 0 \\ 0 & 0 & \text{Он2} & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \text{Он}l-1 & 0 \\ 0 & 0 & \text{Он}l & 0 \end{bmatrix} \end{array}.$$

Выше мы отмечали, что контроль доступа, реализуемый перенаправлением (переадресацией) запросов доступа, требует совместного его использования с дискреционным контролем доступа, который применяется для разграничения прав доступа к объектам, в которые перенаправляются запросы доступа.

Рассмотрим применение данного метода контроля доступа с целью полноценного разделения между субъектами доступа неразделяемого объекта Он – полноценного разделения в том смысле, что средствами перенаправления запросов доступа требуется выполнить следующее условие: С*i*(*R*=0)Он*j*, *j*≠*i*, *i*=1,...,*l*, *j*=1,...,*l*. С этой целью зададим правила перенаправления запросов доступа, иллюстрируемые следующей матрицей:

$$\mathbf{M}\text{п} = \begin{array}{c} \\ \text{С1} \\ \text{С2} \\ . \\ . \\ . \\ \text{С}l-1 \\ \text{С}l \end{array} \begin{array}{c} \begin{array}{cccc} \text{Он} & \text{Он1} & \text{Он}i & \text{Он}l \end{array} \\ \begin{bmatrix} \text{Он1} & 0 & \text{Он1} & \text{Он1} \\ \text{Он2} & \text{Он2} & 0 & \text{Он2} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \text{Он}l-1 & \text{Он}l-1 & \text{Он}l-1 & \text{Он}l-1 \\ \text{Он}l & \text{Он}l & \text{Он}l & 0 \end{bmatrix} \end{array}.$$

Видим, что реализацией подобных правил перенаправлений запросов доступа может быть выполнено требуемое условие: С*i*(*R*=*r*,*w*,*d*)Он*i*, С*i*(*R*=0)Он*j*, *j*≠*i*, *i*=*1*,...,*l*, *j*=1,...,*l*, исходный же разделяемый объект доступа Он при этом становится виртуальным – для него справедливо: С*i*(*R*=0)Он, *i*=1,...,*l*.

Естественно, что, если рассматривать контроль доступа перенаправлением (переадресацией) запросов доступа, в качестве самостоятельного полноценного метода контроля и разграничения прав доступа (в качестве альтернативы дискреционному методу контроля доступа субъектов к объектам), а не только применительно к разделению между субъектами доступа не разделяемых системой объектов, то в этом случае следует говорить о том, что перенаправление запросов доступа может задаваться администратором применительно к любым объектам доступа. При этом в ячейке матрицы перенаправлений запросов доступа применительно к любому объекту может задаваться одно из следующих правил перенаправлений: С*i*(О*k*)О*j*, что означает перенаправление запросов доступа от субъекта С*i* к объекту О*j* в объект О*k*, либо отсутствие подобного перенаправления С*i*(0)О*j*.

Построим матрицу перенаправлений запросов доступа **М**п, реализующую диагональную матрицу доступа **М**к (при этом для наглядности представления будем считать, что множества С = {С1, …, С*l*} и О = {О1, …, О*l*}):

$$\mathbf{M}\text{п} = \begin{array}{c} \\ \text{С1} \\ \text{С2} \\ . \\ . \\ . \\ \text{С}l-1 \\ \text{С}l \end{array} \begin{array}{c} \begin{array}{ccc} \text{О1} & \text{О2} & \text{О}l \end{array} \\ \begin{bmatrix} 0 & \text{О1} & \text{О1} \\ \text{О2} & 0 & \text{О2} \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \text{О}l-1 & \text{О}l-1 & \text{О}l-1 \\ \text{О}l & \text{О}l & 0 \end{bmatrix} \end{array}.$$

Данный пример иллюстрирует, что разграничительная политика доступа данным методом контроля заданием правил перенаправлений запросов доступа может быть реализована в полном объеме.

Принципиальным отличием данного метода контроля доступа от дискреционного метода является то, что запрос доступа субъекта к объекту в том случае, когда субъекту необходимо запретить запись в объект (модифицировать объект), не запрещается, что не всегда можно реализовать применительно к системным объектам без нарушения корректности работы системы и приложений, он перенаправляется (право доступа сохраняется, но доступ при этом реализуется уже к иному объекту). Данное отличие можно позиционировать как принципиальное преимущество данного метода контроля доступа применительно к защите системных объектов как в части защиты системных объектов одного субъекта от атак со стороны другого объекта, так и в части создания различных конфигураций для субъекта, исходно создаваемых единой для системы в целом. Его же практическое использование позволяет решать принципиально новые задачи защиты, например, реализовывать виртуализацию системных средств [14]. Реализация данного метода защиты позволяет принципиально упростить создание в системе разграничительной политики доступа к защищаемым ресурсам, в первую очередь, к системным объектам [14].

Построим абстрактную модель. Если считать, что множества C = {C1, …, C*l*} и O = {O1, …, O*l*} – соответственно линейно упорядоченные множества субъектов и объектов доступа, а право перенаправления запросов доступа *P* задается как C*i*(O*k*)O*j*, что означает перенаправление запросов доступа от субъекта C*i* к объекту O*j* в объект O*k* (C*i*(0)O*j* – отсутствие перенаправления), то разграничительная политика доступа субъектов к объектам описывается матрицей перенаправлений запросов доступа **M**, где *M*[C,O] – ячейка матрицы, которая содержит право перенаправлений запросов доступа субъекта из множества C = {C1, …, C*l*} к объекту из множества O = {O1, …, O*k*}. В любой момент времени система контроля доступа описывается своим текущим состоянием Q= (C,O,*M*).

При назначении правил перенаправлений запросов доступа для субъектов, а не для объектов (прямая, а не транспонированная матрица, по аналогии с методом дискреционного контроля доступа), объекты доступа в правилах могут назначаться масками. Маски при этом задаются и применяются следующим образом [13]. В общем случае маска при задании в правиле объекта доступа имеет вид *Oj*. Например, если в правилах перенаправлений запросов доступа задать исходный объект маской *.com, а объект, в который перенаправляется доступ, маской *.exe, то любое обращение к файлу с расширением com будет перенаправляться к файлу с тем же полным именем, но уже с расширением exe – вместо расширения com в имени объекта в запросе доступа будет подставляться расширение exe (пример защиты от замещающих вирусов).

Ограничения данной модели состоят в том, что рассмотренным методом контроля доступа невозможно разграничивать отдельные права доступа субъекта к объекту (чтение, запись, удаление, исполнение) – при любом виде запроса к объекту, как на чтение, так и на запись, этот запрос будет перенаправлен в соответствии с заданными правилами. Расширим возможности предлагаемого метода контроля доступа введением следующих правил перенаправления запросов: C*i*(O*k*,*w*)O*j* – перенаправление запросов доступа на запись (*w*) от субъекта C*i* к объекту O*j* в объект O*k*, C*i*(O*k*,*r*)O*j* – перенаправление запросов доступа на чтение (*r*) от субъекта C*i* к объекту O*j* в объект O*k*, C*i*(0)O*j* – отсутствие перенаправления.

Замечание 3. Мы строим абстрактные модели. На практике, как правило, вместе с правом записи обязательно разрешается и право чтения, т.е. разрешается либо только *r*, либо одновременно *w*, *r*, поскольку для модификации файла приложению нужно сначала его прочитать.

При использовании данных правил уже анализируется не только объект, к которому запрошен доступ, но и тип запрашиваемого доступа (чтение или запись, в общем случае могут анализироваться и иные типы доступа), соответствующим образом и перенаправляются либо нет запросы доступа с учетом типа запрашиваемого доступа.

Абстрактная модель приобретает в данном случае (уже в общем случае для предлагаемого метода контроля доступа) следующий вид. Если считать, что множества C = {C1, …, C*l*} и O = {O1, …, O*l*} – соответственно линейно упорядоченные множества субъектов и объектов доступа, а *R* – конечное множество прав доступа *R* = {*w*,*r*,*x*,*d*} (чтение, запись, исполнение, удаление), право перенаправления запросов доступа *P* задается как C*i*(O*k*,*R*)O*j*, означает перенаправление запросов доступа, затребовавших соответствующее право доступа из множества *R* от субъекта C*i* к объекту O*j*, в объект O*k*, (C*i*(0)O*j* – отсутствие перенаправления), то разграничительная политика доступа субъектов к объектам описывается матрицей перенаправлений запросов доступа **M**, где *M*[C,O] – ячейка матрицы, которая содержит право перенаправлений запросов доступа субъекта из множества C = {C1, …, C*l*} к объекту из множества O = {O1, …, O*k*}. В любой момент времени система контроля доступа описывается своим текущим состоянием Q= (C,O,*M*).

Проиллюстрируем построение разграничительной политики доступа с использованием метода перенаправлений запросов доступа на примере. Рассмотрим произвольную матрицу доступа **M** (с заданными правилами доступа дискреционным методом контроля доступа):

$$\mathbf{M} = \begin{array}{c} \\ \mathrm{C}1 \\ \mathrm{C}2 \\ . \\ . \\ . \\ \mathrm{C}l-1 \\ \mathrm{C}l \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{O}1 & \mathrm{O}2 & \mathrm{O}l \end{array} \\ \begin{bmatrix} r,w,d & w & 0 \\ r & r,w,d & 0 \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ 0 & 0 & r \\ 0 & w & r,w,d \end{bmatrix} \end{array}.$$

Реализуем эту же разграничительную политику доступа с использованием метода перенаправлений запросов доступа. Получим матрицу перенаправлений запросов доступа, **М**п:

$$\mathbf{M}\text{п} = \begin{array}{c} \\ \mathrm{C}1 \\ \mathrm{C}2 \\ . \\ . \\ . \\ \mathrm{C}l-1 \\ \mathrm{C}l \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{O}1 & \mathrm{O}2 & \mathrm{O}l \end{array} \\ \begin{bmatrix} 0 & \mathrm{O}1,r,d & \mathrm{O}1,r,w,d \\ \mathrm{O}2,w,d & 0 & \mathrm{O}2,r,w,d \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \\ \mathrm{O}l-1,r,w,d & \mathrm{O}l-1,r,w,d & \mathrm{O}l-1,w,d \\ \mathrm{O}l,r,w,d & \mathrm{O}l,r,d & 0 \end{bmatrix} \end{array}.$$

Данный пример наглядно иллюстрирует, что методом контроля доступа перенаправлением запросов доступа с учетом в правилах перенаправлений типа запрашиваемого доступа может быть реализована любая разграничительная политика доступа субъектов к объектам, что позволяет сделать вывод о том, что предложенный метод контроля доступа перенаправлением запросов доступа является полноценным самостоятельным методом контроля доступа субъектов к объектам и может рассматриваться в качестве альтернативы методу дискреционного контроля доступа.

Заключение

В заключение отметим, что предложенный метод контроля доступа обладает крайне важным отличительным свойством – запрос доступа субъекта к объекту в том случае, когда субъекту необходимо запретить запись в объект (модифицировать объект), не запрещается, он перенаправляется (право доступа сохраняется, но доступ при этом реализуется уже к иному объекту), что позволяет реализовывать разграничительные политики доступа к системным объектам без нарушения работоспособности системы и приложений. Это позволяет решать принципиально новые задачи защиты в области информационной безопасности, например, как отмечали, реализовывать виртуализацию системных средств [14]. Другие, не менее важные задачи защиты и реализуемые для их решения разграничительные политики доступа (правила перенаправления запросов доступа) авторы предполагают рассмотреть в последующих работах.

Литература

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. 384 с.
2. Sandhu R.S., Coyne E.J., Feinstein H.L., Youman C.E. Computer role-based access control models // Computer. 1996. V. 29. N 2. P. 38–47. doi: 10.1109/2.485845
3. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к ресурсам компьютерной системы с субъектом доступа «пользователь, процесс» // Патент РФ №2534599. Бюл. 2014. № 33.
4. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. 2013. № 2 (101). С. 36–43.
5. Щеглов К.А., Щеглов А.Ю. Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. 2012. № 4 (99). С. 31–36.
6. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к ресурсам компьютерной системы с субъектом «исходный пользователь, эффективный пользователь, процесс». Патент РФ №2534488. Бюл. 2014. № 33.
7. Щеглов А.Ю., Павличенко И.П., Корнетов С.В., Щеглов К.А. Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Свидетельство о государственной регистрации программы для ЭВМ №2014660889.
8. Щеглов К.А., Щеглов А.Ю. Контроль доступа к статичным файловым объектам // Вопросы защиты информации. 2012. № 2(97). С. 12–20.

9. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in operating systems // Communication of the ACM. 1976. V. 19. N 8. P. 461–471. doi: 10.1145/360303.360333
10. Bell D.E., LaPadula L.J. Security Computer Systems: Unified Exposition and MULTICS Interpretation. MITRE Technical Report MTR-2997 Rev. 1. Bedford, Massachusetts, MITRE Corp., 1976. 129 p. Режим доступа: http://csrc.nist.gov/publications/history/bell76.pdf (дата обращения 24.10.2015)
11. Biba K.J. Integrity Consideration for Security Computer System. MITRE Technical Report MTR-3153. Bedford, Massachusetts, MITRE Corp., 1975. 61 p. Режим доступа: http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf (дата обращения 24.10.2015)
12. Щеглов К.А., Щеглов А.Ю. Модели контроля доступа к создаваемым файловым объектам. Требования к построению безопасной системы // Вопросы защиты информации. 2013. № 3(102). С. 60–67.
13. Щеглов А.Ю., Щеглов К.А. Система переформирования объекта в запросе доступа. Патент РФ № 2538918. Бюл. 2015. № 1.
14. Ковешников М.Г., Щеглов К.А., Щеглов А.Ю. Абстрактные модели виртуализации системы // Научно-технический вестник информационных технологий, механики и оптики. 2015. Т. 15. № 3. С. 483–492. doi: 10.17586/2226-1494-2015-15-3-483-492

Ковешников Михаил Геннадьевич – студент, Университет ИТМО, Санкт-Петербург, Российская Федерация, Mike_35_92@mail.ru

Щеглов Константин Андреевич – аспирант, Университет ИТМО, Санкт-Петербург, Российская Федерация, scheglov.konstantin@gmail.com

Щеглов Андрей Юрьевич – доктор технических наук, профессор, профессор, Университет ИТМО, Санкт-Петербург, Российская Федерация, info@npp-itb.spb.ru

Michail G. Koveshnikov – student, ITMO University, Saint Petersburg, 197101, Russian Federation, Mike_35_92@mail.ru

Konstantin A. Shcheglov – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, scheglov.konstantin@gmail.com

Andrey Yu. Shcheglov – D.Sc., Professor, Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, info@npp-itb.spb.ru