4. *Ou X., Govindavajhala S., and Appel A.* MulVAL: A logic-based network security analyzer // SSYM'05 Proc. 14th Conf. USENIX Security Symp. 2005. V. 14. P. 113–128.
5. *Ingols K., Lippmann R., and Piwowarski K.* Practical attack graph generation for network defense // ACSAC'06: Proc. 22nd Ann. Computer Security Appl. Conf. 2006. P. 121–130.
6. *Danforth M.* Models for Threat Assessment in Networks. PhD Thesis, University of California-Davis, 2006.
7. *Девянин П. Н.* Модели безопасности компьютерных систем. М.: Academia, 2005.
8. *Горбатенко Д. Е., Кочемазов С. Е., Семёнов А. А.* О дискретно-автоматных моделях атак в компьютерных сетях // Прикладная дискретная математика. Приложение. 2016. № 9. С. 80–83.

УДК 004.94 DOI 10.17223/2226308X/11/29

ПОДХОДЫ К МОДЕЛИРОВАНИЮ УПРАВЛЕНИЯ ДОСТУПОМ В СУБД PostgreSQL В РАМКАХ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

Широкое применение СУБД PostgreSQL в защищённых операционных системах, в том числе в операционной системе специального назначения (ОССН) Astra Linux Special Edition, требует разработки научно-обоснованных подходов к исследованию безопасности реализованного в этой СУБД механизма управления доступом. Для этого необходимо проанализировать как изначально используемое в СУБД PostgreSQL ролевое управление доступом, так и востребованные в практике создания защищённых систем мандатное управление доступом и мандатный контроль целостности. Известно, что научной основой при разработке механизма управления доступом в ОССН стала мандатная сущностно-ролевая ДП-модель (МРОСЛ ДП-модель), включающая перечисленные три вида управления доступом, имеющая иерархическое представление (позволяющее дополнять модель новыми элементами без её полной переработки), а также прошедшая проверку на корректность с применением инструментальных средств дедуктивной верификации. В связи с этим предлагаются подходы к построению в рамках иерархического представления МРОСЛ ДП-модели новых уровней, соответствующих механизму управления доступом в СУБД PostgreSQL. При этом из-за наличия существенных отличий этого механизма в ОССН и СУБД на первом этапе моделирования основное внимание уделено ролевому управлению доступом.

Ключевые слова: *компьютерная безопасность, формальная модель, управление доступом, PostgreSQL.*

С введением в действие ФСТЭК России с июня 2017 г. [1] профилей защиты операционных систем (ОС) общего назначения (типа «А»), включающих, начиная с третьего класса защиты, компоненты доверия ADV_SPM.1 «Формальная модель политики безопасности», AVA_CCA_EXT.1 «Анализ скрытых каналов» и ADV_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках» [2], разработка научных подходов по формированию модели безопасности управления доступом, верификации её реализации, анализа на её основе безопасности информационных потоков (скрытых каналов) стала актуальной задачей для специалистов в области защиты информации. Можно ожидать, что в ближайшей перспективе ФСТЭК России будут введены аналогичные требования для систем управления базами данных (СУБД).

В этой связи в 2012 г. был начат процесс научного сопровождения разработки отечественной защищённой ОССН Astra Linux Special Edition [3, 4], в рамках которого удалось достичь следующих результатов:

— в математической нотации разработано иерархическое представление мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели) [5], включающее в настоящее время девять уровней, дающих строгое формальное описание мандатного контроля целостности (*Mandatory Integrity Control — MIC*) с невырожденной решеткой уровней целостности [6], мандатного управления доступом (*Mandatory Access Control — MAC*) с обеспечением безопасности информационных потоков по памяти и по времени [7] и ролевого управления доступом (*Role-Based Access Control — RBAC*) с использованием запрещающих ролей [8];
— в рамках МРОСЛ ДП-модели сформулированы и обоснованы условия безопасности механизма управления доступом в ОССН в смыслах мандатного контроля целостности, Белла — ЛаПадулы (безопасности информационных потоков по памяти) и безопасности информационных потоков по времени [5];
— четыре первых уровня МРОСЛ ДП-модели представлены в формализованной нотации Event-B и прошли верификацию с использованием инструментальных средств среды Rodin Platform [9];
— эти четыре уровня (за исключением элементов ролевого управления доступом) реализованы в ОССН версии 1.5 в программном коде, который прошел дедуктивную верификацию с применением инструментальных средств Frama-C и Why3;
— МРОСЛ ДП-модель, материалы по её верификации и внедрению в ОССН были использованы в качестве свидетельств при её сертификации в сентябре 2017 г. по второму классу защиты ОС типа «А» [10].

Вместе с тем управление доступом в СУБД, в том числе в СУБД PostgreSQL, устроено существенно иначе, чем в ОССН. В отличие от изnthereачально дискреционного относительно простого для анализа и модификации механизма управления доступом в ОС семейства Linux, ролевое управление доступом в СУБД, разработка которого на основе стандарта SQL ведётся несколько десятилетий, является достаточно громоздким, трудно поддающимся модификации для обеспечения соответствия модели управления доступом в ОССН. При этом путь разработки для СУБД независимой формальной модели, например, как это было предложено в работах [11, 12], имеет существенный недостаток, заключающийся в том, что тем самым будет чрезвычайно затруднён научный анализ безопасности информационных потоков (особенно по времени), возникающих при кооперации субъектов, например, при их одновременном доступе к сущностям ОССН и СУБД. В этом смысле разработка единой модели управления доступом для ОССН и СУБД представляется более перспективной.

По этой причине автором было начато формирование в рамках иерархического представления МРОСЛ ДП-модели новых уровней, соответствующих СУБД PostgreSQL. Первым был разработан базовый уровень СУБД, основанный на уровне запрещающих ролей МРОСЛ ДП-модели [8]. Его назначение — создать фундамент для моделирования на последующих уровнях мандатного управления доступом и мандатного контроля целостности, в том числе для обеспечения безопасности информационных потоков. Поэтому на этом уровне не были учтены многие детали реализации в СУБД ролевого управления доступом, так как излишняя детализация затруднит разработку подходов по противодействию запрещённым информационным потокам

по времени или потребует использования для их применения существенных ресурсов СУБД, что может негативно сказаться на её производительности.

В результате на базовом уровне СУБД PostgreSQL МРОСЛ ДП-модели использованы:

— множества: ролей СУБД, административных привилегий СУБД (*SUPERUSER*, *CREATEROLE*, *CREATEDB*, *LOGIN*, *REPLICATION*, *INHERIT*), административных ролей СУБД, специальных ролей СУБД, общих ролей СУБД, элементов СУБД, элементов-объектов СУБД (каталоги по событию, расширения, сопоставления, домены, конфигурации, словари, парсеры, шаблоны, функции, последовательности, строки, ограничения, индексы, правила, триггеры, триггерные функции, репликации), элементов-контейнеров СУБД (кластеры, базы данных, схемы, таблицы, столбцы, представления, табличные пространства), видов привилегий СУБД (*SELECT*, *INSERT*, *UPDATE*, *DELETE*, *TRUNCATE*, *REFERENCES*, *TRIGGER*, *USAGE*, *CREATE*, *CONNECT*, *TEMPORARY*, *TEMP*, *EXECUTE*, *OWN*), сущностей СУБД (на этом уровне модели сущностями являются элементы СУБД от её схем и далее выше по иерархии, например, базы данных, кластеры), привилегий к элементам СУБД;
— функции: административных привилегий ролей СУБД, ролей входа субъект-сессий в СУБД, наследования привилегий ролей к элементам СУБД, управления подчинённостью ролей в иерархии, административных прав доступа административных ролей ОССН и СУБД к ролям СУБД, привилегий к элементам СУБД ролей СУБД, соответствия административных привилегий и видов привилегий к элементам СУБД правам доступа, эффективных прав доступа ролей СУБД.

Кроме того, переопределены:

— множество доступов субъект-сессий к ролям, запрещающим ролям, административным ролям или ролям СУБД;
— функции: имён сущностей и элементов СУБД, имён ролей, запрещающих ролей, административных ролей, ролей СУБД, доступа субъект-сессий к сущностям или элементам СУБД в контейнерах;
— иерархия сущностей и элементов СУБД;
— иерархия ролей, запрещающих ролей, административных ролей и ролей СУБД;
— состояние системы.

Сформулированы 30 условий, которым должно удовлетворять единое ролевое управление доступом в СУБД и ОССН, в том числе определяющие порядок:

— использования административных прав доступа, привилегий ролей и специальных административных ролей СУБД;
— создания, удаления, изменения иерархии ролей СУБД;
— администрирования иерархии сущностей и элементов СУБД;
— управления доступом к сущностям СУБД;
— использования административных доступов субъект-сессий к ролям СУБД.

При этом по аналогии с уровнями модели для ОССН описание условий, касающихся порядка реализации в СУБД мандатного контроля целостности и мандатного управления доступом, будет осуществлено на последующих уровнях модели.

На базовом уровне СУБД PostgreSQL иерархического представления МРОСЛ ДП-модели по сравнению с уровнем запрещающих ролей не было задано новых де-юре правил преобразования состояний, их осталось 35, хотя большая их часть была модифицирована путём добавления в правила новых параметров, условий и результатов

применения, учитывающих специфику управления доступом в СУБД. Несмотря на существенные отличия механизмов управления доступом в ОССН и СУБД, это было сделано целенаправленно, чтобы создать условия для формирования единых подходов к их реализации, в том числе для противодействия в перспективе запрещённым информационным потокам. Однако, так как на этом уровне модели информационные потоки ещё не рассматриваются, в него не были включены де-факто правила преобразования состояний.

В итоге было сформулировано и обосновано утверждение о соответствии (корректности) правил преобразования состояний системы условиям, которым должно удовлетворять ролевое управление доступом, заданным как на текущем уровне МРОСЛ ДП-модели, так и на двух предшествующих уровнях: базовом и запрещающих ролей.

Таким образом, удалось разработать и апробировать подходы к моделированию ролевого управления доступом в СУБД PostgreSQL, совместимые с использованными при разработке иерархического представления МРОСЛ ДП-модели, изначально предназначавшегося для моделирования безопасности мандатного и ролевого управления доступом, мандатного контроля целостности в ОССН Astra Linux Special Edition. Это создаёт предпосылки для дальнейшего использования этих видов управления доступом при развитии модели управления доступом в СУБД, её верификации с использованием инструментальных средств, практической реализации единого механизма управления доступом в ОССН и СУБД, а также сертификации СУБД по профилям защиты, включающим компоненты доверия ADV_SPM.1, AVA_CCA_EXT.1 и ADV_FSP.5.

ЛИТЕРАТУРА

1. Информационное сообщение об утверждении Требований безопасности информации к операционным системам от 18 октября 2016 г. № 240/24/4893 / ФСТЭК России. `http://fstec.ru/component/attachments/download/1051`
2. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
3. Операционные системы Astra Linux. `http://www.astralinux.com/`
4. Astra Linux. `https://ru.wikipedia.org/wiki/Astra\_Linux`
5. *Буренин П. В., Девянин П. Н., Лебеденко Е. В. и др.* Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов / под ред. П. Н. Девянина. 2-е изд., стереотип. М.: Горячая линия — Телеком, 2016. 312 с.
6. *Девянин П. Н.* Реализация невырожденной решётки уровней целостности в рамках иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2017. № 10. С. 111–114.
7. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. 2-е изд., испр. и доп. М.: Горячая линия — Телеком, 2013. 338 с.
8. *Девянин П. Н.* Уровень запрещающих ролей иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. 2018. № 39. С. 58–71.
9. *Девянин П. Н., Кулямин В. В., Петренко А. К., и др.* О представлении МРОСЛ ДП-модели в формализованной нотации Event-B // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 7–15.
10. Astra Linux сертифицирована по требованиям ФСТЭК России к операционным системам. `http://astralinux.com/home/novosti/437-rbt-fstec.html`

11. *Шумилин А. В.* Основные элементы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в СУБД PostgreSQL ОС специального назначения Astra Linux Special Edition // Прикладная дискретная математика. 2013. № 3(21). С. 52–67.

12. *Смольянинов В. Ю.* Анализ условий предоставления и получения прав доступа в модели управления доступом MS SQL Server // Прикладная дискретная математика. 2014. № 2(24). С. 48–78.

УДК 004.934 DOI 10.17223/2226308X/11/30

АВТОМАТИЗИРОВАННОЕ ПРОХОЖДЕНИЕ GOOGLE RECAPTCHA V2

И. Н. Манашев

Показана неактуальность текущего подхода к решению задачи разграничения реальных пользователей и компьютерных ботов. Приводится способ автоматизированного прохождения теста Google reCAPTCHA v2.

Ключевые слова: *распознавание captcha, автоматизация, reCAPTCHA v2.*

1. Общие сведения

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart, далее — капча) — один из вариантов теста Тьюринга, который позволяет различить реальных пользователей и компьютерных ботов. В его основе лежит задача, лёгкая для человека, но трудоёмкая для компьютера [1]. Этот механизм защиты должен оградить сайты от спама, автоматических регистраций, накруток, DDoS-атак и прочих дел, которыми обычно занимаются боты. На данный момент самой популярной реализацией капчи является Google reCAPTCHA v2.

Классическая (текстовая) капча представляет собой картинку с последовательностью искажённых символов (букв, цифр и спецсимволов). Решением текстовой капчи считается получение изображённых на картинке символов в текстовом виде [2]. Технология Google отходит от стандартной концепции автоматизированного теста Тьюринга и оценивает поведение пользователя, а не его способность разгадывания слов.

Пользователю нужно выполнить простейшее действие — отметить галочкой утверждение «Я не робот». В этот момент капча оценивает косвенные параметры, указывающие на возможного бота: время, проведённое на странице, траекторию движения курсора, IP-адрес и пр. Если у капчи закрадываются сомнения в том, что пользователь — человек, то она предложит выполнить одно из двух заданий: образный или аудиотест.

Образная капча — это тест, для прохождения которого требуется решить задачу классификации образов: нужно выбрать из нескольких изображений те, которые соответствуют заранее объявленному критерию (например, выбрать изображения, на которых есть автомобиль).

Аудиокапча представляет собой аудиозапись, в которой проговаривается какая-либо фраза, содержащая последовательность слов или цифр. Как правило, в аудиозаписи присутствуют различные искажения: варьируемая тональность, фоновый шум, паузы. Решением аудиокапчи считается получение фразы в текстовом виде.

Одна из главных проблем любой капчи — её исполнение. Боты — проблема не для пользователей, а для администраторов сайта. Перекладывать её решение на обычных