

ального вида в графе доступов) с субъект-сессией или недоверенным пользователем z через недоверенную субъект-сессию или недоверенного пользователя x .

При этом при задании простых мостов и мостов в граф доступов добавлены вершины, соответствующие ролям, и ребра, задающие: принадлежность роли права доступа к сущности, принадлежность роли множеству авторизованных ролей пользователя или субъект-сессии, принадлежность роли множеству текущих ролей субъект-сессии, возможность административной роли изменять принадлежащие роли права доступа к сущности, принадлежность пользователей или субъект-сессий к островам.

Теорема 1. Пусть G_0 — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь $x \in N_U$ и субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, такие, что $x \neq y$. Предикат $simple_can_access_own(x, y, G_0)$ является истинным тогда и только тогда, когда существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \dots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \dots, y_m \in N_U \cup S_0$, где $m \geq 1$, таких, что $x_1 = x$, $y_m = y$, $y_i \in island(x_i)$, где $1 \leq i < m$, и выполняются следующие условия:

- 1) Если $m \geq 2$, то справедливо равенство $is_bridge(x_m, y_{m-1}, y) = true$.
- 2) Если $m \geq 3$, то для каждого $2 \leq i < m$ справедливо равенство или $is_bridge(x_i, y_{i-1}, y_i) = true$, или $is_simple_bridge(x_i, y_{i-1}, y_i) = true$.

Таким образом, в рамках БР ДП-модели обосновываются необходимые и достаточные условия получения субъект-сессией, функционирующей от имени недоверенного пользователя, доступа владения к другой субъект-сессии для случая, когда в системе взаимодействуют произвольное число субъект-сессий и они не используют информационные потоки по памяти.

ЛИТЕРАТУРА

1. Sandhu R. Role-Based Access Control // Advanced in Computers. Academic Press, 1998. V. 46.
2. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.
3. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005. 144 с.
4. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
5. Девянин П. Н. О разработке моделей безопасности информационных потоков в компьютерных системах с ролевым управлением доступом // Материалы Третьей Междунар. науч. конф. по проблемам безопасности и противодействия терроризму. МГУ им. Ломоносова. 25–27 октября 2007 г. М.: МЦНМО, 2008. С. 261–265.
6. Девянин П. Н. Базовая ролевая ДП-модель // Прикладная дискретная математика. 2008. № 1(1). С. 64–70.

УДК 004.94

ПРЕПОДАВАНИЕ МОДЕЛЕЙ УПРАВЛЕНИЯ ДОСТУПОМ И ИНФОРМАЦИОННЫМИ ПОТОКАМИ В РАМКАХ ДИСЦИПЛИНЫ «ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ»

П. Н. Девянин

Одной из актуальных проблем теории компьютерной безопасности является анализ безопасности логического управления доступом и информационными потоками в компьютерных системах (КС). Как правило, для описания условий передачи прав до-

ступа и реализации информационных потоков в КС используются формальные модели безопасности КС, основными из которых являются модели систем дискреционного управления доступом, изолированной программной среды (ИПС), систем мандатного управления доступом, безопасности информационных потоков, ролевого управления доступом [1, 2]. Данные модели являются фундаментом теории компьютерной безопасности, и их целесообразно изучать в рамках дисциплин ГОС ВПО третьего поколения по специальностям 090102 — «Компьютерная безопасность» и 090105 — «Информационная безопасность автоматизированных систем».

В дискреционной модели Харрисона – Руззо – Ульмана (ХРУ) основное внимание уделено правилам преобразования матрицы доступов. При этом обосновывается алгоритмическая неразрешимость задачи проверки безопасности произвольных КС с дискреционным управлением доступом. Результаты анализа КС, используемые в модели ХРУ, получили развитие в модели типизированных матриц доступов (ТМД), в которой рассматриваются подходы к обеспечению безопасности КС, имеющие большие, чем у модели ХРУ, возможности практической реализации. В модели *Take-Grant* с применением графов доступов наглядно описываются условия передачи прав доступа и реализации информационных потоков.

В субъектно-ориентированной модели ИПС рассматриваются вопросы определения порядка безопасного взаимодействия субъектов системы, описания и обоснования необходимых условий реализации ИПС, которая обеспечивает выполнение в КС требований априорно заданной политики безопасности.

Мандатное управление доступом чаще всего описывают в терминах, понятиях и определениях свойств классической модели Белла – ЛаПадулы и ее основных интерпретаций. На основе модели Белла – ЛаПадулы строится большинство описанных в литературе формальных моделей КС с мандатным управлением доступом, например, модель безопасности систем военных сообщений (СВС), которая более эффективно, чем классическая модель Белла – ЛаПадулы, позволяет учитывать особенности функционирования современных КС.

Часто в рассматриваемых моделях наряду с исследованием условий передачи прав доступа анализируется безопасность информационных потоков. В то же время существуют модели, в основном ориентированные только на анализ условий реализации информационных потоков. Таковыми являются автоматная модель безопасности информационных потоков, программная модель контроля информационных потоков и вероятностная модель безопасности информационных потоков.

Моделирование КС с ролевым управлением доступом является в настоящее время одним из самых динамично развивающихся направлений компьютерной безопасности. На основе базовой модели ролевого управления доступом *RBAC* созданы модель ролевого мандатного управления доступом, ролевая мандатная модель защиты от угрозы целостности информации, модель ролевого администрирования и другие модели.

Как правило, классические модели не позволяют в полной мере учесть следующие особенности функционирования современных КС:

- возможность кооперации части субъектов при передаче прав доступа и реализации информационных потоков;
- возможность реализации доверенных и недоверенных субъектов;
- возможность противодействия доверенными субъектами передаче прав доступа или реализации информационных потоков недоверенными субъектами;
- различие условий реализации информационных потоков по памяти и по времени;
- наличие иерархической структуры сущностей;

- возможность изменения функциональности субъекта при реализации информационного потока по памяти на функционально ассоциированные с ним сущности;
- необходимость в ряде случаев определения различных правил управления доступом и информационными потоками для распределенных компонент КС.

В связи с этим при наличии возможности при преподавании дисциплины «Теоретические основы компьютерной безопасности» целесообразно рассмотреть подходы, примененные при разработке семейства моделей безопасности логического управления доступом и информационными потоками (ДП-моделей) КС с дискреционным, мандатным или ролевым управлением доступом [3]. При этом наиболее существенными моделями семейства являются дискреционная базовая ДП-модель, ДП-модель с функционально ассоциированными с субъектами сущностями (ФАС ДП-модель), мандатная ДП-модель и базовая ролевая ДП-модель.

Все рассмотренные модели войдут в разрабатываемое автором учебное пособие «Модели безопасности компьютерных систем», второе издание которого планируется в 2010 году.

ЛИТЕРАТУРА

1. Девянин П. Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005. 144 с.
2. Bishop M. Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.
3. Девянин П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.

УДК 004.94

ЗАМЫКАНИЕ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ

М. А. Качанов

При анализе базовой ролевой (сокращенно: БР) ДП-модели в работе [1] были рассмотрены условия передачи прав доступа ролей в случае взаимодействия только двух субъект-сессий двух пользователей. В рамках обозначений и определений, введенных в указанной работе, рассмотрим случай взаимодействия субъект-сессий произвольного числа пользователей и предложим алгоритм, используя который можно осуществлять проверку истинности предиката *can_share()* для всех пользователей, сущностей и прав доступа одновременно, а вместе с ней и возможности получения недоверенным субъектом права доступа владения к доверенному субъекту в компьютерных системах с дискреционным управлением доступом и информационными потоками. Такой алгоритм реализует преобразование начального состояния компьютерной системы (КС) в его замыкание. Дадим определения замыканий базовой ролевой ДП-модели, предложим и обоснуем алгоритмы их построения.

В соответствии с [1], в рамках БР ДП-модели при анализе условий передачи прав доступа, реализации информационных потоков по памяти или по времени возможно использование только монотонных правил преобразования состояний.

Введем подмножество правил преобразования БР ДП-модели $OP_{acs} = \{take_role(), grant_right(), create_first_session(), control(), access_own(), take_access_own(), access_write(), access_append(), post()\}$. Этих правил преобразования, согласно [1], достаточно для анализа условий передачи прав доступа ролей.