Секция 3

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94

РЕЗУЛЬТАТЫ АНАЛИЗА УСЛОВИЙ ПОЛУЧЕНИЯ ДОСТУПА ВЛАДЕНИЯ В РАМКАХ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ БЕЗ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ПАМЯТИ

П. Н. Девянин

На основе семейства ролевых моделей *RBAC* [1 – 3] и семейства ДП-моделей компьютерных систем (КС) с дискреционным или мандатным управлением доступом [4] построена базовая ролевая ДП-модель (БР ДП-модель) [5, 6]. Данная модель ориентирована на анализ в КС с ролевым управлением доступом условий передачи прав доступа ролей и реализации информационных потоков по памяти и по времени.

В настоящее время в рамках БР ДП-модели не удалось завершить исследования КС с ролевым управлением доступом, на условия функционирования которых не наложено ограничений. В связи с этим в [5, 6] с применением БР ДП-модели выполнен анализ необходимых и достаточных условий передачи прав доступа для случая, когда в системе существуют только две субъект-сессии двух пользователей.

В докладе исследуется БР ДП-модель, в которой взаимодействуют произвольное число субъект-сессий, и они не получают доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям. Для этого определяется предикат $simple\_\,can\_\,access\_\,own(x,\ y,\ G_0)$, истинный тогда и только тогда, когда существует траектория функционирования системы с начальным состоянием G_0 и с некоторым конечным состоянием, в котором субъект-сессия, функционирующая от имени недоверенного пользователя x, получает доступ владения к субъект-сессии, функционирующей от имени пользователя y.

Для упрощения записи алгоритмически проверяемых необходимых и достаточных условий истинности предиката $simple\_\,can\_\,access\_\,own(x, y, G_0)$ определятся предикат $simple\_\,directly\_\,access\_\,own(x,\ y,\ G_0)$, задающий легкопроверяемые условия, при выполнении которых субъект-сессия, функционирующая от имени недоверенного пользователя x, может непосредственно получить доступ владения к субъект-сессии, функционирующей от имени пользователя y. По аналогии с моделью *Take-Grant* [2, 3] также определяются:

island: $N_U \cap S \to 2^{N_u} \cup 2^S$ — функция, задающая остров (подграф графа доступов, соответствующего состоянию системы) для субъект-сессии или недоверенного пользователя;

$is\_\,simple\_\,bridge$: $(N_U \cup (N_S \cap S)) \times (N_U \cup S) \times (N_U \cup S) \to \{true,\ false\}$ и $is\_\,bridge$: $(N_U \cup (N_S \cap S)) \times (N_U \cup S) \times (N_U \cup S) \to \{true,\ false\}$ — функции, для которых справедливы соответственно равенства $is\_\,simple\_\,bridge(x,\ y,\ z) = true$ или $is\_\,bridge(x,\ y,\ z) = true$ тогда и только тогда, когда субъект-сессия или недоверенный пользователь y соединен соответственно простым мостом или мостом (путями специ-

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 $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 1$, таких, что $x_1 = x$, $y_m = y$, $y_i \in island(x_i)$, где $1 \leqslant i < m$, и выполняются следующие условия:

1) Если $m \geqslant 2$, то справедливо равенство $is\_bridge(x_m,\ y_{m-1},\ y) = true$.

2) Если $m \geqslant 3$, то для каждого $2 \leqslant i < m$ 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-