ступ к сущностям, защищенным ЭПС, и кодирование в них данных в случае, когда оно осуществляется ЭПС. Эти доверенные субъекты реализуют информационные потоки по памяти между каждой сущностью, защищенной ЭПС, и соответствующей ей сущностью-образом, не являющейся субъектом.

Условие 4. Доверенные или недоверенные субъекты, не реализующие доступ к сущностям, защищенным ЭПС, не обладают правами доступа и не могут получать доступ к этим сущностям. При этом они могут обладать правами доступа или получать доступ к сущностям-образам сущностей, защищенных ЭПС.

Условие 5. Недоверенный субъект-задача может создать доверенного субъекта в случае, когда недоверенный субъект реализовал к себе информационные потоки по памяти от всех сущностей, параметрически ассоциированных с некоторым потенциальным доверенным субъектом.

При анализе безопасности ЭПС представляют интерес вопросы, связанные с возможностью получения нарушителем доступа к документам в обход правил политики безопасности. Для разрабатываемой ЭПС ДП-модели строятся формальные описания моделей нарушителя различных видов, а именно:

— нарушителя, являющегося зарегистрированным пользователем ЭПС;
— нарушителя, не являющегося зарегистрированным пользователем ЭПС, но имеющего возможность запускать процессы в ОС сервера ЭПС;
— нарушителя, не являющегося зарегистрированным пользователем ЭПС, но имеющего возможность прослушивать каналы связи между клиентами и сервером ЭПС и выступать в роли клиента ЭПС.

На основе ЭПС ДП-модели с использованием данных моделей нарушителя производится анализ возможности получения недоверенными субъектами доступа к сущностям, защищенным ЭПС, а также реализации от данных сущностей запрещенных информационных потоков. В результате предполагается разработать рекомендации по проектированию защищенных ЭПС.

ЛИТЕРАТУРА

1. *Девянин П Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
2. *Колегов Д Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнева. 2009. Вып. 1(22). Ч. 1. С. 49–54.
3. *Буренин П В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. № 1(3). С. 93–112.

УДК 004.94

РЕЗУЛЬТАТЫ АНАЛИЗА БЕЗОПАСНОСТИ СИСТЕМ С ПРОСТЫМИ ТРАЕКТОРИЯМИ ФУНКЦИОНИРОВАНИЯ В РАМКАХ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ[1]

П. Н. Девянин

На основе базовой ролевой ДП-модели (БР ДП-модели) [1, 2] рассматриваются условия передачи прав доступа и реализации информационных потоков по памяти для случая, когда на траекториях функционирования системы субъект-сессии не получают

[1]Работа выполнена при поддержке гранта МД № 2.2010.10.

доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям.

Определение 1. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют пользователь $x \in U_0$ и право доступа к сущности $(e, \alpha) \in P_0$. Определим предикат $simple\_can\_share((e, \alpha), x, G_0)$, который будет истинным тогда и только тогда, когда существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $s_x \in S_N$, такая, что $user_N(s_x) = x$ и выполняется условие $(e, \alpha) \in de\_facto\_rights_N(s_x)$.

Определение 2. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют сущности или недоверенные пользователи $x, y \in N_U \cup E_0$, где $x \neq y$. Определим предикат $simple\_can\_write\_memory(x, y, G_0)$, который будет истинным тогда и только тогда, когда существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и выполняется условие $(x', y', write_m) \in F_N$, где верно следующее: если $x \in E_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_N$ и $user_N(x') = x$; если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_N$ и $user_N(y') = y$.

В рамках определений 1 и 2 возможно обоснование следующих теорем.

Теорема 1. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь $x \in N_U$ и право доступа к сущности $(e, \alpha) \in P_0$. Предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным тогда и только тогда, когда выполняется одно из следующих условий:

1. Выполняется условие $(e, \delta) \in PA_0(UA_0(x))$, где $\delta \in \{\alpha, own_r\}$.

2. Существует субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, истинен предикат $simple\_can\_access\_own(x, y, G_0)$, и выполняется одно из условий:

— или $y \in N_U$ и $(e, \alpha) \in PA_0(UA_0(y))$;
— или $y \in N_S \cap S_0$ и $(e, \alpha) \in PA_0(UA_0(user_0(y)))$;
— или $y \in L_S \cap S_0$ и $(e, \alpha) \in PA_0(roles_0(y))$.

3. 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 $m \geqslant 2$, таких, что $x_1 = x$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и выполняется одно из условий:

— или $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— или $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— или $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_m, y_{m-1}, y_m) = \text{true}$, и для каждого $2 \leqslant i \leqslant m$ справедливо равенство или $is\_bridge(x_i, y_{i-1}, y_i) = \text{true}$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Теорема 2. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют сущности или недоверенные пользователи $x, y \in N_U \cup E_0$, где $x \neq y$. Предикат $simple\_can\_write\_memory(x, y, G_0)$ истинен

тогда и только тогда, когда существует последовательность недоверенных пользователей или сущностей $e_1, \ldots, e_m \in N_U \cup E_0$, где $e_1 = x$, $e_m = y$ и $m \geqslant 2$, таких, что выполняется одно из условий:

1. $m = 2$ и $(x', y', write_m) \in F_0$, где выполняются условия:

— если $x \in E_0$, то $x' = x$;
— если $x \in N_U$, то $x' \in S_0$ и $user_0(x') = x$;
— если $y \in E_0$, то $y' = y$;
— если $y \in N_U$, то $y' \in S_0$ и $user_0(y') = y$.

2. Для каждого $i = 1, \ldots, m-1$ выполняется одно из условий:

— $e_i \in N_U \cup S_0$, $e_{i+1} \in N_U \cup E_0$ и $(e'_i, e'_{i+1}, write_m) \in F_0$, где верно следующее:
  - если $e_i \in S_0$, то $e'_i = e_i$;
  - если $e_i \in N_U$, то $e'_i \in S_0$ и $user_0(e'_i) = e_i$;
  - если $e_{i+1} \in E_0$, то $e'_{i+1} = e_{i+1}$;
  - если $e_{i+1} \in N_U$, то $e'_{i+1} \in S_0$ и $user_0(e'_{i+1}) = e_{i+1}$;
— $e_i \in N_U \cup S_0, e_{i+1} \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((e_{i+1}, \alpha), e'_i, G_0)$, где $\alpha \in \{write_r, append_r\}$, и верно следующее:
  - если $e_i \in N_U$, то $e'_i = e_i$;
  - если $e_i \in S_0$, то $e'_i = user_0(e_i)$;
— $e_{i+1} \in N_U \cup S_0, e_i \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((e_i, read_r), e'_{i+1}, G_0)$, где верно следующее:
  - если $e_{i+1} \in N_U$, то $e'_{i+1} = e_{i+1}$;
  - если $e_{i+1} \in S_0$, то $e'_{i+1} = user_0(e_{i+1})$;
— $e_i \in N_U \cup (N_S \cap S_0)$, $e_{i+1} \in N_U \cup S_0$ и истинен $simple\_can\_access\_own(e'_i, e_{i+1}, G_0)$, где верно следующее:
  - если $e_i \in N_U$, то $e'_i = e_i$;
  - если $e_i \in N_S \cap S_0$, то $e'_i = user_0(e_i)$;
— $e_{i+1} \in N_U \cup (N_S \cap S_0)$, $e_i \in N_U \cup S_0$ и истинен предикат $simple\_can\_access\_own(e'_{i+1}, e_i, G_0)$, где верно следующее:
  - если $e_{i+1} \in N_U$, то $e'_{i+1} = e_{i+1}$;
  - если $e_{i+1} \in N_S \cap S_0$, то $e'_{i+1} = user_0(e_{i+1})$.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Базовая ролевая ДП-модель // Прикладная дискретная математика. 2008. № 1(1). С. 64–70.
2. *Девянин П. Н.* Анализ условий получения доступа владения в рамках базовой ролевой ДП-модели без информационных потоков по памяти // Прикладная дискретная математика. 2009. № 3(5). С. 69–84.