УДК 004.94

О РЕЗУЛЬТАТАХ РАЗРАБОТКИ РОЛЕВОЙ ДП-МОДЕЛИ ДЛЯ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА LINUX[1]

П. Н. Девянин

Рассматривается развивающая ролевые ДП-модели [1, 2] ролевая ДП-модель управления доступом и информационными потоками в операционных системах (ОС) семейства *Linux* (или, сокращенно, РОСЛ ДП-модель), в которую по сравнению с БРОС ДП-моделью внесены следующие основные изменения.

Виды прав доступа ($read_r$, $write_r$, $execute_r$, own_r) и доступов ($read_a$, $write_a$, own_a) заданы в соответствии с реализуемыми в ОС семейства *Linux* правилами дискреционного управления доступом. При задании иерархии сущностей (отношения частичного порядка $\leqslant$ на множестве сущностей E) и функции иерархии сущностей (H_E) учтено наличие механизма создания «жестких» ссылок (*hard link*) в файловой системе ОС рассматриваемого семейства, обеспечивающего возможность размещения сущностей-объектов одновременно в нескольких сущностях-контейнерах.

В РОСЛ ДП-модели впервые по существу анализируется механизм ограничений (описанный в БР ДП-модели) на значения множеств авторизованных ролей учетных записей пользователей ($Constraint_U$), прав доступа ролей ($Constraint_P$) и текущих ролей субъект-сессий ($Constraint_S$). Этот механизм включен в модель для реализации в перспективе на основе ролевого управления доступом востребованного во многих защищенных ОС мандатного управления доступом.

Наибольшие изменения по сравнению с БРОС ДП-моделью внесены в описания условий и результатов применения правил преобразования состояний, в которых учтено наличие механизма ограничений и «жестких» ссылок. Правило создания сущности заменено двумя правилами — создания объекта и создания контейнера; добавлены правила создания и удаления «жесткой» ссылки, удаления доступа и получения субъект-сессией при наличии доступа владения к другой субъект-сессии всех ее информационных потоков.

В рамках РОСЛ ДП-модели по аналогии с существующими ДП-моделями рассматриваются монотонные правила преобразования состояний, которые по определению не приводят к удалению из состояний: ролей из множества текущих ролей субъект-сессий; прав доступа ролей к сущностям; субъект-сессий, сущностей или «жестких» ссылок на сущности-объекты; доступов субъект-сессий к сущностям; информационных потоков. Наличие в модели механизма ограничений в общем случае требует использования монотонных и немонотонных правил при передаче прав доступа ролей или возникновения информационных потоков. С учетом этого формулирование и обоснование алгоритмически проверяемых условий передачи прав доступа ролей или возникновения информационных потоков между сущностями целесообразно осуществлять для некоторых заданных в конкретных системах множеств ограничений. Для этого предлагается рассматривать ограничения, инвариантные относительно немонотонных правил преобразования состояний, каждое из которых по определению обладает следующим свойством: если в системе задано только ограничение данного вида, то для любой траектории системы применение или неприменение на ней любого немонотонного правила не влияет на выполнение ограничений у последующих за ним правил преобразования

[1]Работа выполнена при поддержке гранта МД-2.2010.10.

состояний. С использованием обозначений БРОС ДП-модели [2] дадим определение и сформулируем утверждение.

Определение 1. Ограничение инвариантно относительно немонотонных правил преобразования состояний в системе $\Sigma(G^*, OP)$, если при условии, что в ней задано только данное ограничение, для любых состояния системы G_0, немонотонного правила преобразования состояний op_1, правил преобразования состояний op_2, …, op_N, где $N > 1$, справедливо следующее: если $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{N-1}} G_{N-1}$, $G_0 \vdash_{op_2} G'_2 \vdash_{op_3} \ldots \vdash_{op_{N-1}} G'_{N-1}$ и в состоянии G_{N-1} выполнены ограничения, заданные в условиях применения правила op_N, то эти ограничения выполнены в состоянии G'_{N-1}.

Утверждение 1. Пусть G_0 — начальное состояние системы $\Sigma(G^*, OP, G_0)$, в котором все ограничения инвариантны относительно немонотонных правил преобразования состояний, и функции $(i_u, i_e, i_r, i_s)_0$ удовлетворяют условиям предположения 7 БРОС ДП-модели [2]. Пусть также существуют состояния системы G_1, …, 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 $N \geqslant 0$. Тогда существуют состояния G'_1, …, G'_M, где $M \geqslant 0$, и монотонные правила преобразования состояний op'_1, …, op'_M, такие, что $G_0 \vdash_{op'_1} G'_1 \vdash_{op'_2} \ldots \vdash_{op'_M} G'_M$ и выполняются следующие условия:

1. Верно включение $S_N \subset S'_M$ и для каждой субъект-сессии $s \in S_N$ выполняются условия $user_N(s) = user'_M(s)$, $roles_N(s) \subset roles'_M(s)$.

2. Верно включение $E_N \subset E'_M$, для каждой сущности $e \in E_N \setminus S_N$, не являющейся субъектом, выполняется условие $H_{E_N}(e) \subset H'_{E_M}(e)$, и для любых сущностей e, $e' \in E_N$ если в состоянии G_N выполняется условие $e < e'$, то данное условие выполняется в состоянии G'_M.

3. Для каждой роли $r \in R$ выполняется условие $PA_N(r) \subset PA'_M(r)$.

4. Верно включение $A_N \subset A'_M$.

5. Верно включение $F_N \subset F'_M$.

6. Функции $(i_u, i_e, i_r, i_s)'_M$ удовлетворяют условиям предположения 7 БРОС ДП-модели [2].

Из утверждения 1 следует, что при наличии в системе только ограничений, инвариантных относительно немонотонных правил преобразования состояний, при анализе условий передачи прав доступа ролей, реализации информационных потоков достаточно использовать только монотонные правила преобразования состояний.

Таким образом, РОСЛ ДП-модель позволяет анализировать перспективные для ОС семейства *Linux* механизмы защиты: ролевое управление доступом, включая ограничения, и мандатный контроль целостности. В дальнейшем планируется развитие модели с целью включения в нее новых элементов, более точно учитывающих особенности функционирования ОС рассматриваемого семейства, и выработки научно-обоснованных технических решений, направленных на совершенствование механизмов защиты информации в ОС.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.

2. *Девянин П. Н.* Правила преобразования состояний базовой ролевой ДП-модели управления доступом и информационными потоками в операционных системах // Прикладная дискретная математика. 2011. № 1(11). С. 78–95.