УДК 004.94

КОРРЕКТНОСТЬ ПРАВИЛ ПРЕОБРАЗОВАНИЯ СОСТОЯНИЙ СИСТЕМЫ В РАМКАХ МАНДАТНОЙ СУЩНОСТНО-РОЛЕВОЙ ДП-МОДЕЛИ ОС СЕМЕЙСТВА LINUX

П. Н. Девянин

Рассматриваются де-юре и де-факто правила преобразования состояний системы мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в операционных системах (ОС) семейства Linux и формулируется утверждение об их корректности относительно заданных в рамках модели требований к реализации мандатного контроля целостности, мандатного и ролевого управления доступом.

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

Для строгого формального обоснования безопасности защищённой операционной системы Astra Linux Special Edition [1] автором разрабатывается мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в ОС семейства Linux [2, 3] (МРОСЛ ДП-модель). В рамках модели описываются требования к реализации механизмов мандатного контроля целостности, мандатного и ролевого управления доступом, в том числе:

— для уровней доступа и целостности учётной записи пользователя;
— для текущих уровней доступа и целостности субъект-сессии;
— для уровней конфиденциальности и целостности сущности, входящей в состав сущности-контейнера;
— для уровней конфиденциальности и целостности роли или административной роли;
— для уровней конфиденциальности и целостности сущностей, параметрически ассоциированных с учётной записью пользователя, ролью или административной ролью;
— для доступов субъект-сессии к сущности с учётом атрибутов конфиденциальности и целостности сущностей-контейнеров CCR и $CCRI$, для создания, удаления сущности или «жёсткой» ссылки на сущность, для сущностей-«дырок», в которых данные «не сохраняются», для доступов субъект-сессии на владение к субъект-сессии, на активизацию из сущности субъект-сессии;
— для специальных сущностей, используемых для получения доступа к сущностям с высоким уровнем целостности;
— для доступов субъект-сессии к роли или административной роли;
— для индивидуальных ролей и административных ролей учётной записи пользователя;
— для изменения атрибутов CCR, $CCRI$, переименования роли, административной роли или сущности-контейнера;
— для получения субъект-сессией данных о числе «жёстких» ссылок к сущности;
— для предоставления имён сущностей, ролей или административных ролей;
— для возможности нарушения отдельных условий мандатного управления доступом (при администрировании защищённой ОС).

После этого задаются 20 де-юре и 10 де-факто правил преобразования состояний системы, для каждого из которых детально описываются условия и результаты применения. В таблице приведены примеры задания де-юре правила $grant\_rights(x, x'$,

r, $\{(y,\ \alpha_{rj})\colon 1 \leqslant j \leqslant k\}$), позволяющего субъект-сессии x при кооперации с субъект-сессией x' дать роли r права доступа к сущности y, и де-факто правила $control(x, y, z)$, при реализации которого субъект-сессия x получает фактическое владение субъект-сессией y, используя сущность z, функционально ассоциированную с y.

Примеры задания правил преобразования состояний

Правило	Исходное состояние $G = (PA, user, A, AA, F, H_E)$	Результирующее состояние $G' = (PA', user', A', AA', F', H'_E)$
$grant\_rights(x,\ x',\ r,\ \{(y,\ \alpha_{rj})\colon 1 \leqslant j \leqslant k\})$	$x, x' \in S$, $y \in E$, $r \in R \cup AR$, $(x,\ r,\ write_a) \in AA$, $Constraint_{PA}(PA') =$ `true`, $(x, y, own_a) \in A$, [если $y \in S$, то $\alpha_{rj} = own_r$ и $i_s(y) \leqslant i_r(r)$], [если $y \in E \setminus S$ и $\alpha_{rj} \in \{own_r, write_r\}$, то $i_e(y) \leqslant i_r(r)$], [если ($y \in S$ и $i_s(y) = i\_high$) или ($y \in E \setminus S$ и $i_e(y) = i\_high$), то $(x', f_s(x)\_i\_entity, write_a) \in A$], где $1 \leqslant j \leqslant k$	$S' = S$, $E' = E$, $A' = A$, $AA' = AA$, $user' = user$, $H'_E = H_E$, $F' = F$, $PA'(r) = PA(r) \cup \cup\{(y, \alpha_{rj}) : 1 \leqslant j \leqslant k\}$ и для $r' \in R \setminus \{r\}$ выполняется равенство $PA'(r') = PA(r')$
$control(x,\ y,\ z)$	$x \in N_S \cap S$, $y \in S$, $x \neq y$, $z \in [y]$ и или $x = z$, или $(x, z, write_m) \in F$, или [$z \in S$ и $z \in de\_facto\_own(x)$]	$S' = S$, $E' = E$, $PA' = PA$, $A' = A$, $AA' = AA$, $user' = user$, $H'_E = H_E$, $de\_facto\_own'(x) = de\_facto\_own(x) \cup \{y\}$, $F' = F \cup \{(x, y, write_t), (y, x, write_t)\}$

В результате формулируется и обосновывается утверждение о корректности правил преобразования состояний системы относительно заданных в рамках модели требований к реализации мандатного контроля целостности, мандатного и ролевого управления доступом, т. е. эти требования должны выполняться в состояниях и при переходах между состояниями на всех траекториях функционирования системы.

Утверждение 1. Пусть G_0 — состояние системы $\Sigma(G^*, OP)$, удовлетворяющее требованиям к реализации мандатного контроля целостности, мандатного и ролевого управления доступом. Тогда для любой траектории $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 1$, эти требования выполняются в состоянии G_N и при переходе $G_{N-1} \vdash_{op_N} G_N$.

Таким образом, обеспечивается основа для дальнейшего теоретического исследования и обоснования в рамках МРОСЛ ДП-модели свойств рассматриваемых защищённых ОС семейства Linux.

ЛИТЕРАТУРА

1. Операционные системы Astra Linux // `http://www.astra-linux.ru/`.
2. *Девянин П. Н.* О разработке мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в операционных системах семейства Linux // Методы и технические средства обеспечения безопасности информации: Материалы 21-й науч.-технич. конф. 24–29 июня 2012 г. СПб.: Изд-во Политехн. ун-та, 2012. С. 91–94.
3. *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.