Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94 DOI 10.17223/2226308X/10/44

РЕАЛИЗАЦИЯ НЕВЫРОЖДЕННОЙ РЕШЁТКИ УРОВНЕЙ ЦЕЛОСТНОСТИ В РАМКАХ ИЕРАРХИЧЕСКОГО ПРЕДСТАВЛЕНИЯ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

В рамках иерархического представления мандатной сущностно-ролевой ДП-модели, являющейся научной основой при реализации механизма управления доступом в отечественной защищённой операционной системе специального назначения *Astra Linux Special Edition*, строится новый уровень — «боковая ветвь» для уже существующих четырёх иерархически упорядоченных уровней. Он развивает уровень мандатного контроля целостности (второй уровень) модели и использует вместо элементарной решётки, состоящей всего из двух уровней целостности — высокого (системного) и низкого (пользовательского), невырожденную решетку целостности, включающую произвольное множество уровней. Новый уровень ориентирован на моделирование мандатного контроля целостности при использовании технологий виртуализации или в рамках сетевой доменной архитектуры.

Ключевые слова: *компьютерная безопасность, формальная модель, мандатный контроль целостности.*

Мандатный контроль целостности — важнейший, хорошо зарекомендовавший себя механизм безопасности, который, аналогично мандатному управлению доступом [1], направлен на задание и применение чётких, понятных для пользователей и администраторов современных операционных систем правил обеспечения целостности их программной среды. Поэтому теоретическое описание и строгое научное обоснование свойств этого механизма изначально стало частью мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели) [2], реализованной в отечественной операционной системе специального назначения (ОССН) *Astra Linux Special Edition* [3 – 5].

До настоящего момента для представления мандатного контроля целостности в МРОСЛ ДП-модели использовались всего два уровня целостности — высокий (i_high) и низкий (i_low). Этого было вполне достаточно для разделения всех элементов ОССН на системные (доверенные компоненты ОССН, обеспечивающие функционирование процессов её ядра и системных процессов, в том числе механизмов защиты и администрирования), обладающие высоким уровнем целостности, и пользовательские (недоверенные компоненты ОССН, выполняющие функции процессов непривилегированных пользователей, в том числе нарушителей), обладающие низким уровнем целостности. Именно в таком виде мандатный контроль целостности реализован в версиях 1.4 и 1.5 ОССН.

При переходе от «монолитного» к иерархическому представлению МРОСЛ ДП-модели [6] в ней также были использованы два уровня целостности. При этом само иерархическое представление задаёт модель по уровням (слоям), где каждый нижний

уровень модели представляет абстрактную систему, элементы которой не зависят от новых элементов, принадлежащих более высокому уровню модели, который, в свою очередь, наследует, а при необходимости корректирует или дополняет элементы нижнего уровня. Первоначально иерархическое представление включало четыре уровня (рис. 1):

— первый уровень — модель системы ролевого управления доступом (1);
— второй уровень — модель системы ролевого управления доступом и мандатного контроля целостности (2);
— третий уровень — модель системы ролевого управления доступом, мандатного контроля целостности и мандатного управления доступом только с информационными потоками по памяти (3.1);
— четвёртый уровень — модель системы ролевого управления доступом, мандатного контроля целостности и мандатного управления доступом с информационными потоками по памяти и по времени (4.1).

Рис. 1. Иерархическое представление МРОСЛ ДП-модели и его возможные расширения

Однако такое представление создавалось не только с целью структурирования описания модели, обеспечения его большего соответствия механизму управления доступом ОССН или упрощения её теоретического анализа. По своему замыслу иерархическое представление должно было позволить добавлять в МРОСЛ ДП-модель новые «альтернативные» уровни без переработки её целиком. Например, в качестве «альтернативного» третьего уровня предполагалось построить модель системы ролевого управления доступом, мандатного контроля целостности и гипервизора или, наоборот, среды виртуализации в самой ОССН. Очевидно, что в таких случаях для адекватного описания

механизмов управления доступом в ОССН явно недостаточно двух уровней целостности. Одним из возможных решений здесь может быть использование трёх уровней целостности: высокого, соответствующего системному для основной ОССН, среднего, соответствующего системному для ОССН, запущенной в среде виртуализации (виртуализированной), и низкому — пользовательскому для основной и виртуализированной ОССН.

Кроме того, в перспективе уровней целостности может потребоваться больше, в том числе для реализации невырожденной (состоящей из более чем двух уровней, где не каждый уровень сравним с каждым) решётки уровней целостности. Такая решётка может оказаться востребованной при моделировании управления доступом в компьютерной сети, использующей доменную архитектуру.

В связи с изложенным в качестве первого шага формирования таких уровней иерархического представления МРОСЛ ДП-модели автором разработан «альтернативный» третий уровень, названный моделью мандатного контроля целостности с невырожденной решёткой уровней целостности (3.2).

Хотя может показаться, что корректировка второго уровня модели с целью замены двухуровневой решётки на невырожденную не требует внесения в модель значительного числа изменений, при его описании оказалось, что необходимо переопределить множества доверенных и недоверенных субъект-сессий (доверенные субъект-сессии, как и на предыдущем уровне, обладают наивысшим уровнем целостности i_high, а недоверенные — не обязательно самым низким i_low, таковыми являются все субъект-сессии с уровнем целостности ниже наивысшего); функции, задающие для субъект-сессий субъект-сессии и сущности, относительно которых они функционально или параметрически корректны (соответственно функции $f\_correct$ и $p\_correct$, которые теперь определены не только на множестве доверенных субъект-сессий, а на множестве всех субъект-сессий, уровень целостности которых выше минимального). Кроме того, потребовалось внесение изменений в определение иерархии индивидуальных административных ролей, индивидуальных ролей учётных записей пользователей и общих ролей, так как они должны быть созданы для каждого уровня целостности. В связи с этим из де-юре правил преобразования состояний наибольшие изменения коснулись правил, выполняющих создание учётной записи пользователя ($create\_user$) или изменение её уровня целостности (set_user_labels).

Наибольший интерес при использовании невырожденной решётки уровней целостности представляют изменения в условиях безопасности системы в смысле мандатного контроля целостности. Несмотря на то, что применяемые для этого определения безопасного начального состояния и траектории без кооперации доверенных и недоверенных субъект-сессий текстуально не изменились, это означает, что безопасность системы обеспечивается в том числе за счёт возможности получения в качестве текущих специальных административных ролей только доверенными (обладающими наивысшим уровнем целостности) субъект-сессиями и их возможным участием на рассматриваемых траекториях только в создании некоторых информационных потоков по памяти (использовании только некоторых де-факто правил вида $flow\_memory\_access$, *find*, *post* и *pass*). При этом, в отличие от предыдущего уровня, любые де-юре или де-факто правила могут применять не только субъект-сессии с минимальным уровнем целостности i_low, но и выше него.

В результате достаточными условиями безопасности системы в смысле мандатного контроля целостности, кроме оставшихся без изменений условий к корректному определению уровней целостности сущностей, функционально или параметриче-

ски ассоциированных с субъект-сессиями, на уровне мандатного контроля целостности с невырожденной решёткой уровней целостности МРОСЛ ДП-модели являются функциональная и параметрическая корректность всех субъект-сессий с уровнями целостности выше минимального i_low (а не только наивысшего i_high) относительно субъект-сессий с меньшим уровнем целостности.

Таким образом, во-первых, построенный новый уровень («альтернативный» третьему) МРОСЛ ДП-модели позволил впервые непосредственно показать преимущество иерархического представления модели над «монолитным», заключающееся в возможности добавления в неё существенных изменений без переработки всей модели целиком; во-вторых, создана основа для разработки востребованных практикой уровней модели, ориентированных на описание и строгий теоретический анализ безопасности управления доступом и информационными потоками для гипервизора, среды виртуализации, а также сетевой доменной архитектуры ОССН *Astra Linux Special Edition*. Перечисленное создаёт предпосылки к тому, что для всё более широкого спектра защищённых отечественных операционных систем будет научно обоснована безопасность реализуемых в них технических решений. Это представляется особенно важным с учётом начавшегося процесса внедрения ФСТЭК России «Требований безопасности информации к операционным системам» [7], в которых, а также в разработанных на их основе в соответствии с ГОСТ Р ИСО/МЭК 15408 [8] профилях защиты и заданиях по безопасности для некоторых, возможно, высоких классов защиты операционных систем, как предполагается, будут явно указаны требования наличия представления формальной модели политики безопасности.

ЛИТЕРАТУРА

1. *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.
2. *Буренин П. В., Девянин П. Н., Лебеденко Е. В. и др.* Безопасность операционной системы специального назначения Astra Linux Special Edition: учеб. пособие для вузов. 2-е изд., стереотип. М.: Горячая линия — Телеком, 2016. 312 с.
3. *Девянин П. Н., Куликов Г. В., Хорошилов А. В.* Комплексное научно-обоснованное решение по разработке отечественной защищенной ОССН Astra Linux Special Edition // Методы и технические средства обеспечения безопасности информации: Материалы 23-й науч.-технич. конф. 30 июня – 03 июля 2014 г. СПб.: Изд-во Политех. ун-та, 2014. С. 29–33.
4. Операционные системы Astra Linux. `http://www.astralinux.com/`
5. Astra Linux. `https://ru.wikipedia.org/wiki/Astra\_Linux`
6. *Девянин П. Н.* О результатах формирования иерархического представления МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2016. № 9. С. 83–87.
7. Информационное сообщение об утверждении Требований безопасности информации к операционным системам от 18 октября 2016 г. № 240/24/4893. `http://fstec.ru/component/attachments/download/1051`
8. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. М.: Стандартинформ, 2014.