В рамках описанной модели мы рассмотрели ряд задач, связанных с анализом и блокированием атак в компьютерных сетях. В частности, рассмотрены задачи выбора злоумышленником нескольких хостов для атаки. При этом на возможности злоумышленника накладывались различные ограничения: например, требовалось получить root-право на некотором компьютере сети не более чем за фиксированное число моментов времени. Дополнительно предполагалось, что в процессе атаки злоумышленник не может в каждый момент времени иметь root-права более чем на заданном числе хостов сети. Такого рода задачи «подбора множеств хостов» являются комбинаторными из-за значительного в общем случае числа различных альтернатив, требующих проверки. Задачи описанного типа решались за счёт их сведения к задаче о булевой выполнимости (SAT). При этом использованы кодировки и общие идеи, представленные в работе [7], в которой методами SAT исследована активационная динамика в сетях. Если удавалось подобрать множество хостов, с которого злоумышленник успешно атаковал рассматриваемую систему, то для этой ситуации рассматривалась обратная задача: запретить те или иные уязвимости на некоторых хостах сети, чтобы в результате найденная атака стала невозможной. Эту задачу М. Данфорт называет задачей расстановки патчей. В рамках развитого вычислительного аппарата можно накладывать ограничения на число расставляемых патчей и их вид (например, предполагать, что блокирование некоторых уязвимостей невозможно). Все вычислительные эксперименты проводились на сетях, сгенерированных случайным образом в соответствии с моделью Барабаши — Альберт [8]. Перечисленные комбинаторные задачи удалось успешно решить для сетей с несколькими сотнями хостов.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем: учеб. пособие для вузов. М.: Издательский центр «Академия», 2005.
2. *Jha S., Sheyner O., and Wing J.* Two formal analysis of attack graphs // Proc. 15th IEEE Workshop on Computer Security Foundations (CSFW '02). 2002. P. 49–63.
3. *Sheyner O., Haines J. W., Jha S., et al.* Automated generation and analysis of attack graphs // Proc. 2002 IEEE Symposium on Security and Privacy. 2002. P. 273–284.
4. *Колегов Д. Н.* Проблемы синтеза и анализа графов атак. `http://www.securitylab.ru/contest/299868.php`. 2009.
5. *Danforth M.* Models for Threat Assessment in Networks. PhD Thesis, University of California-Davis, 2006.
6. *Kauffman S.* Metabolic stability and epigenesis in randomly constructed genetic nets // J. Theoretical Biology. 1969. No. 22. P. 437–467.
7. *Kochemazov S. and Semenov A.* Using synchronous Boolean networks to model several phenomena of collective behavior // PLoS ONE. 2014. No. 9: e115156. P. 1–28.
8. *Barabasi A-L. and Albert R.* Emergence of scaling in random networks // Science. 1999. No. 286. P. 509–512.

УДК 004.94 DOI 10.17223/2226308X/9/32

О РЕЗУЛЬТАТАХ ФОРМИРОВАНИЯ ИЕРАРХИЧЕСКОГО ПРЕДСТАВЛЕНИЯ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

«Монолитное» представление мандатной сущностно-ролевой ДП-модели, являющееся основой механизма управления доступом в отечественной защищённой опе-

рационной системе специального назначения (ОССН) *Astra Linux Special Edition*, ввиду своего значительного объёма и сложности стало неудобно как для научного анализа, верификации и дальнейшего развития самой модели, так и для непосредственного применения в ОССН. По этой причине предлагается полностью переработанное иерархическое представление модели, описывающее её по уровням. В текущем таком представлении заданы четыре иерархически упорядоченных уровня, соответствующих: 1) ролевому управлению доступом; 2) мандатному контролю целостности; 3) мандатному управлению доступом с информационными потоками по памяти и 4) по времени. В дальнейшем возможно добавление новых, в том числе «боковых» уровней, например 3') для модели гипервизора.

Ключевые слова: *компьютерная безопасность, формальная модель, иерархическое представление, Linux.*

Разработанная автором мандатная сущностно-ролевая ДП-модель (МРОСЛ ДП-модель) [1, 2] является частью комплексного научно-обоснованного решения [3] по разработке отечественной защищенной ОССН *Astra Linux Special Edition* [4, 5]. Для получения гарантий адекватности реализации МРОСЛ ДП-модели в ОССН Институтом системного программирования РАН [6, 7] она была сначала переведена в формализованную нотацию *Event-B* (*Rodin Platform*), которая позволила верифицировать описание модели и осуществить дедуктивные доказательства её свойств. Затем на основе формализованного представления модели с использованием инструмента дедуктивной верификации кода *Why* (в среде разработки *Frama-C*) были заданы и проверено выполнение спецификаций (предусловий и постусловий) функций механизма управления доступом ОССН, что позволило обосновать адекватность реализации модели в программном коде.

В то же время существующее описание МРОСЛ ДП-модели имеет значительный объём и является «монолитным», т. е. в нём элементы модели приводятся в порядке, принятом несколько лет назад в начале формирования модели. Первыми делаются предположения о базовых свойствах задаваемой в рамках модели абстрактной системы, потом даются определения элементов состояний системы, далее описываются требования к реализации в системе мандатного и ролевого управления доступом и мандатного контроля целостности, затем приводятся правила преобразования состояний системы, и в заключение формулируются и обосновываются условия безопасности системы, а также рассматриваются подходы к применению модели в ОССН.

В итоге по мере получения новых теоретических результатов и всё большей адаптации модели к условиям функционирования ОССН модель становится всё труднее корректировать, так как каждое изменение в каком-либо её элементе требует учёта во всех других связанных с ним элементах модели, а также проверки справедливости большинства обоснованных в модели утверждений. Кроме того, из-за большого объёма и «монолитности» модели, невозможности в таком виде её поэтапной реализации затрудняется использование модели разработчиками ОССН, а также создание на её основе новых моделей (например, модели гипервизора для ОССН).

В связи с этим автором реализуется переход от «монолитного» описания модели к иерархическому, позволяющему представить модель по уровням (слоям). При этом каждый нижний уровень модели представляет абстрактную систему, элементы которой не зависят от новых элементов, принадлежащих более высокому уровню, который, в свою очередь, наследует, а при необходимости корректирует или дополняет элементы нижнего уровня.

Таким образом, при иерархическом описании МРОСЛ ДП-модели в настоящее время задаются следующие уровни (рис. 1):

— первый уровень — модель системы ролевого управление доступом;
— второй уровень — модель системы ролевого управление доступом и мандатного контроля целостности;
— третий уровень — модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом только с информационными потоками по памяти;
— четвёртый уровень — модель системы ролевого управление доступом, мандатного контроля целостности и мандатного управления доступом с информационными потоками по памяти и по времени.

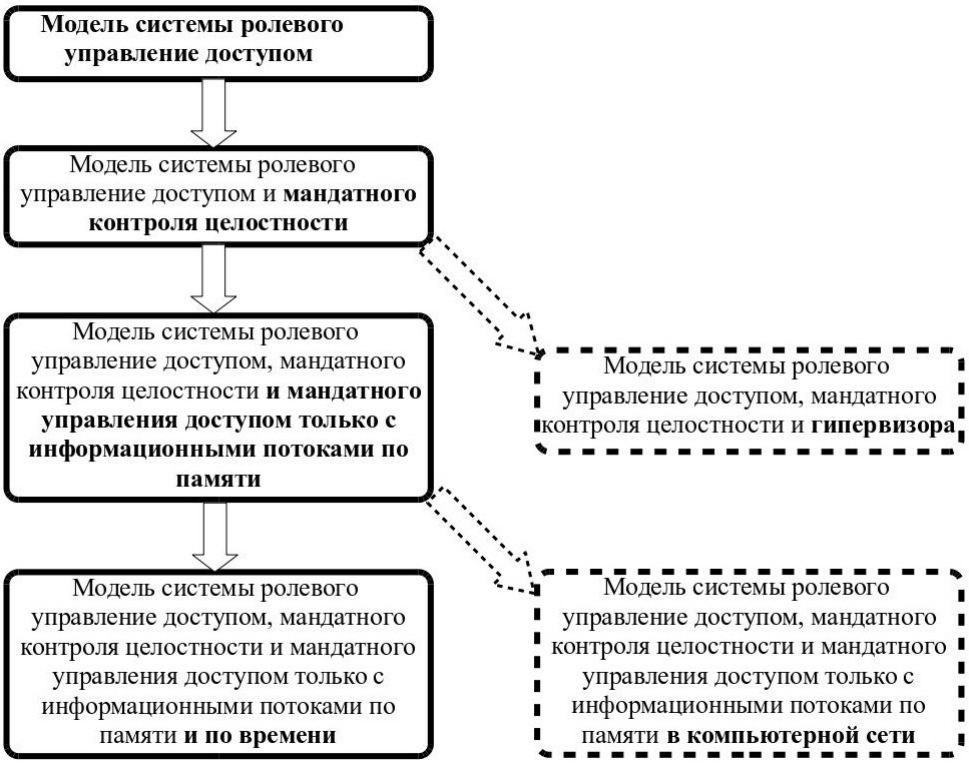

Рис. 1. Иерархическое представление МРОСЛ ДП-модели и его возможные расширения

Этот подход позволяет постепенно усложнять формулировки определений и утверждений модели по мере включения в неё соответствующих очередному рассматриваемому уровню элементов. Например, на третьем уровне (мандатного управления доступом с информационными потоками по памяти) с использованием обозначений из [1] даётся следующая формулировка определения безопасного начального состояния системы. При этом идентификаторы определения и его условий дополнительно показывают последовательность их формирования при переходе от уровня к уровню (Ц — второй уровень, КП — третий уровень).

Определение о.Ц.06.КП. Начальное состояние G_0 системы $\Sigma(G^*, OP, G_0)$ назовём безопасным, если оно удовлетворяет следующим условиям.

Условие Ц.1.КП. Для каждых субъект-сессий $x, y \in S_0$, таких, что $y \in de\_facto\_own_0(x)$, верно $f_{s_0}(y) = f_{s_0}(x)$ и $i_{s_0}(y) \leqslant i_{s_0}(x)$ (по сравнению со вторым уровнем добавляется требование равенства текущих уровней доступа субъект-сессий x и y, одна из которых де-факто владеет другой).

Условие Ц.2.КП. Для каждых недоверенной субъект-сессии $x \in N_{S_0}$, субъект-сессии $y \in S_0$ и сущности $e \in E_0$, таких, что либо $(e \in [y]$ и $(x, e, write_m) \in F_0)$, либо $(e \in]y[$ и либо $(e, x, write_m) \in F_0$, либо $(x, e, read_a) \in A_0)$, верно $f_{s_0}(y) \leqslant f_{s_0}(x)$ и $i_{s_0}(y) \leqslant i_{s_0}(x)$ (по сравнению со вторым уровнем добавляется требование, чтобы текущий уровень доступа к сущностям, параметрически или функционально ассоциированным с сущностью y, недоверенной субъект-сессии x был не ниже текущего уровня доступа этой субъект-сессии y и субъект-сессия x либо имела информационные потоки по памяти, либо обладала доступом на чтение).

Условие Ц.3. (На третьем уровне в это условие не дополняется новых требований.)

Условие Ц.4.КП. Для каждого информационного потока $(x, y, write_m) \in F_0$ справедливо $f_{x_0}(x) \leqslant f_{y_0}(y)$**, где** f_{x_0} **и** f_{y_0} **— соответствующие функции** f_{e_0} **или** f_{s_0}, и справедливо $i_{x_0}(x) \leqslant i_{y_0}(y)$, где i_{x_0} и i_{y_0} — соответствующие функции i_{e_0} или i_{s_0} (по сравнению со вторым уровнем добавляется требование, чтобы при наличии информационного потока по памяти уровень конфиденциальности источника x был не выше уровня конфиденциальности приемника y).

Условие КП.5. **Для доверенных субъект-сессий** $x, y \leqslant L_{S_0}$**, таких, что** $y \in de\_facto\_own_0(x)$**,** $(y, downgrade\_admin\_role, read_a) \in AA_0$**, верно** $(x, downgrade\_admin\_role, read_a) \in AA_0$ (новое условие, добавленное на третьем уровне, заключающееся в запрете получения через де-факто владение специальной административной роли $downgrade\_admin\_role$, позволяющей нарушать правила мандатного управления доступом).

Аналогично задаются 34 де-юре и 10 де-факто правил преобразования состояний, когда на каждом очередном уровне добавляются, корректируются или остаются без изменений условия и результаты их применения.

При таком иерархическом описании модель гипервизора для ОССН (рис. 1) рассматривается как альтернативный (дополнительный) третий уровень (модель системы ролевого управления доступом, мандатного контроля целостности и гипервизора), так как можно предположить, что гипервизор для ОССН должен обеспечивать корректность функционирования её мандатного контроля целостности, а мандатное управление доступом в ОССН не должно реализовываться средствами гипервизора. Аналогично модель ролевого управления доступом в компьютерной сети целесообразно считать альтернативной четвёртому уровню представления МРОСЛ ДП-модели, так как в этой модели существенным является мандатный контроль целостности и мандатное управление доступом только с информационными потоками по памяти.

Таким образом, переход от «монолитного» к иерархическому представлению МРОСЛ ДП-модели за счёт более ясного, структурированного её изложения способствует развитию самой модели, улучшению результатов её верификации при переводе модели в формализованную нотацию *Event-B*, а также позволяет повысить качество реализации модели непосредственно в ОССН.

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. *Девянин П. Н.* Необходимые условия нарушения безопасности информационных потоков по времени в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2015. № 8. С. 81–83.

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 Политехн. ун-та, 2014. С. 29–33.
4. Операционные системы Astra Linux. `http://www.astra-linux.ru/`
5. Astra Linux. `https://ru.wikipedia.org/wiki/Astra\_Linux`
6. *Девянин П. Н., Кулямин В. В., Петренко А. К. и др.* О представлении МРОСЛ ДП-модели в формализованной нотации Event-B // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 7–15.
7. *Devyanin P., Khoroshilov A., Kuliamin V., et al.* Formal verification of OS security model with Alloy and Event-B // LNCS. 2014. V. 8477. P. 309–313.

УДК 517.19 DOI 10.17223/2226308X/9/33

СХЕМА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ В АЛГОРИТМЕ RAID-PIR

М. Р. Кащеев, Ю. В. Косолапов

Рассматривается задача обеспечения конфиденциальности информационной базы данных в схеме анонимного получения информации (private information retrieval) с удалённых серверов. Предполагается, что для хранения базы используются r серверов (r — нечётное), а для анонимного доступа к информации используется алгоритм RAID-PIR. Построен способ шифрования и распределения базы данных таким образом, чтобы, во-первых, по зашифрованным данным, хранящимся на каждом из серверов, нельзя было нарушить конфиденциальность базы данных, и, во-вторых, чтобы при чтении или перезаписи блока данных ни один из серверов не мог узнать, какой блок соответственно считывался или перезаписывался.

Ключевые слова: *анонимность данных, PIR, распределение данных.*

Под анонимностью в сетях передачи данных, как правило, понимается либо невозможность идентификации сервером пользователей, отправивших запрос (анонимность пользователя), либо невозможность идентификации сервером запрашиваемой пользователями информации (анонимность запроса) [1]. В настоящей работе рассматривается обеспечение второго варианта анонимности. Предполагается, что для хранения информационной базы данных используется несколько серверов. Пользователь заинтересован в получении некоторой части базы данных таким образом, чтобы серверы, участвующие в хранении, по отдельности не смогли идентифицировать, какая именно часть базы была запрошена пользователем. В подобных схемах серверы могут рассматриваться как недобросовестные наблюдатели, цель которых заключается в выяснении, в получении какой информации из базы данных заинтересован пользователь. Простейшим случаем обеспечения анонимности является схема с одним сервером, когда пользователь с сервера запрашивает всю базу полностью [2]. Обычно в системах обеспечения анонимности запроса предполагается, что серверу может быть известно (частично или полностью) информационное содержимое базы. В работе рассматривается ситуация, когда знание сервером базы нежелательно, при этом необходимо также защититься от получения сервером информации о расположении или доле запрашиваемой информации в базе. Таким образом, ставится задача построения схемы защиты