УДК 004.94 DOI 10.17223/2226308X/8/30

НЕОБХОДИМЫЕ УСЛОВИЯ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ВРЕМЕНИ В РАМКАХ МРОСЛ ДП-МОДЕЛИ

П. Н. Девянин

В рамках мандатной сущностно-ролевой ДП-модели, ориентированной на реализацию в отечественной защищённой операционной системе специального назначения (ОССН) *Astra Linux Special Edition*, формулируется теорема о необходимых условиях нарушения безопасности информационных потоков по времени (создания таких потоков «сверху вниз»), из которой следует, что эти условия легко устранить на практике, после чего для безопасности управления доступом ОССН в целом достаточно обеспечить в ней безопасность информационных потоков по памяти в смысле Белла — ЛаПадулы и мандатный контроль целостности.

Ключевые слова: *компьютерная безопасность, формальная модель, информационный поток, Linux.*

Анализ условий безопасности информационных потоков по времени (или, наоборот, её нарушения) при построении формальных моделей механизмов управления доступом часто является наиболее сложной задачей, решение которой начинается после того, как исследованы условия безопасности информационных потоков по памяти. Этим традиционным путём разрабатывалась мандатная сущностно-ролевая ДП-модель (сокращённо МРОСЛ ДП-модель) [1 – 3], большая часть элементов которой уже реализована в отечественной защищённой ОССН *Astra Linux Special Edition* [4]. После задания в модели элементов состояния системы, описания порядка функционирования мандатного и ролевого управления доступом и мандатного контроля целостности, де-юре и де-факто правил преобразования состояний системы и обоснования их корректности была сформулирована и доказана базовая теорема безопасности (БТБ-ДП) о достаточных условиях безопасности в смысле Белла — ЛаПадулы (предотвращения возможности реализации информационных потоков по памяти «сверху вниз») и мандатного контроля целостности (предотвращения возможности захвата контроля недоверенными субъект-сессиями над доверенными субъект-сессиями) [5], которые определяются следующим образом (с использованием обозначений из [1] даётся определение трёх смыслов нарушения безопасности, под безопасностью в каждом из этих смыслов понимается отсутствие соответствующего её нарушения).

Определение 1. Пусть G_0 — безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$ и существует траектория без кооперации доверенных и недоверенных субъект-сессий $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 1$. Будем говорить, что в состоянии G_N произошло нарушение безопасности системы, когда в нём выполняется одно из следующих условий, при этом они не выполняются в состояниях G_i траектории для $0 \leqslant i < N$:

— существуют недоверенная субъект-сессия $x \in N_{S_N}$ и доверенная субъект-сессия $y \in de\_facto\_own_N(x) \cap L_{S_N}$, такие, что $i_{s_N}(y) = i\_high$ (нарушение безопасности в смысле мандатного контроля целостности);

— существует информационный поток по памяти $(x, y, write_m) \in F_N$, такой, что $x, y \in E_N$ и неверно неравенство $f_{e_N}(x) \leqslant f_{e_N}(y)$ (нарушение безопасности в смысле Белла — ЛаПадулы);

— существует информационный поток по времени $(x, y, write_t) \in F_N$, такой, что $x, y \in$ $\in E_N$ и неверно неравенство $f_{e_N}(x) \leqslant f_{e_N}(y)$ (нарушение безопасности в смысле контроля информационных потоков по времени).

Для формулирования теоремы о необходимых условиях нарушения безопасности в смысле контроля информационных потоков по времени потребовалось уточнить заданные в модели условия использования имеющихся в реальной защищённой ОССН некоторых «особенных» сущностей. Изначально сущности — специальные объекты-«дырки», не позволяющие хранить данные или быть использованными для создания информационных потоков по памяти (например, сущности, соответствующие портам вывода на графические устройства, «слушающие» сокеты), в модели были включены в множество E_HOLE. Однако практическая реализация модели потребовала разделения этого множества на объекты-«дырки» первого вида (например, файлы `dev/null` или `dev/zero`), которые полностью не сохраняют данных, их нельзя использовать для создания любых информационных потоков (сущности из множества MT_HOLE), и объекты-«дырки» второго вида (сущности из множества M_HOLE), которые изначально входили в множество E_HOLE (таким образом, стало $E\_HOLE = MT\_HOLE \cup$ $\cup\, M\_HOLE$, $MT\_HOLE \cap M\_HOLE = \varnothing$).

Теорема 1. Пусть G_0 — безопасное начальное состояние системы $\Sigma(G^*, OP, G_0)$. Пусть на всех траекториях системы без кооперации доверенных или недоверенных субъект-сессий $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 1$, каждое состояние G_i безопасно в смыслах условия 1 и 2 определения 1, где $1 \leqslant i \leqslant N$, и безопасно в смысле условия 3 определения 1, где $1 \leqslant i < N$. Пусть также в состоянии G_N происходит нарушение безопасности в смысле условия 3 определения 1. Тогда выполняется одно из условий:

— существуют субъект-сессия $x \in N_{S_N} \cup NF_{S_N}$ и сущность $y \in M\_HOLE$, такие, что $(x, y, write_a) \in A_N$ и верно неравенство $f_{s_N}(x) < f_{e_N}(y)$ (найдётся недоверенная или некорректная относительно информационных потоков по времени доверенная субъект-сессия с низким уровнем доступа, имеющая доступ на запись к объекту-«дырке» второго вида с высоким уровнем доступа, через который возможно создание информационных потоков по времени);

— существуют сущность-контейнер $c \in C_N$ и сущность $e \in E_N$, такие, что $CCR_N(c) =$ $= CCRI_N(c) =$ `true`, $e < c$ и $f_{e_N}(e) < f_{e_N}(c)$ (найдётся сущность-контейнер с мандатными атрибутами конфиденциальности CCR и целостности $CCRI$, равными `true`, в состав которого входит сущность с меньшим уровнем конфиденциальности, что может позволить недоверенной субъект-сессии, изменяя параметры этой сущности-контейнера, через входящую в него сущность создавать информационные потоки по времени).

Из теоремы следует, что для предотвращения запрещённых информационных потоков по времени «сверху вниз» в реальной ОССН достаточно обеспечения её безопасности в смыслах условия 1 и 2 определения 1, исключения создания (особенно при установке или администрировании ОССН) сущностей-контейнеров с мандатными атрибутами конфиденциальности и целостности, равными `true`, в состав которых входят сущности с меньшим уровнем конфиденциальности, а также либо полный запрет на использование сущностей из множества M_HOLE (задание $M\_HOLE = \varnothing$), либо такую реализацию этих сущностей, когда их нельзя будет применять для создания информационных потоков по времени.

Таким образом, закончен очередной этап разработки комплексного научно-обоснованного технического решения [6], направленный на создание отечественной защи-

щённой ОССН *Astra Linux Special Edition* и заключающийся в теоретическом обосновании алгоритмически проверяемых и реализуемых на практике условий безопасности в ОССН информационных потоков по памяти и по времени.

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.* Адаптация мандатной сущностно-ролевой ДП-модели к условиям функционирования ОС семейства Linux // Системы высокой доступности. 2013. № 3. С. 98–102.
3. *Девянин П. Н.* Администрирование системы в рамках мандатной сущностно-ролевой ДП-модели управления доступом и информационными потоками в ОС семейства Linux // Прикладная дискретная математика. 2013. № 4(22). С. 22–40.
4. Операционные системы Astra Linux. `http://www.astra-linux.ru/`
5. *Девянин П. Н.* Условия безопасности информационных потоков по памяти в рамках МРОСЛ ДП-модели // Прикладная дискретная математика. Приложение. 2014. № 7. С. 82–85.
6. *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.

УДК 004.94 DOI 10.17223/2226308X/8/31

О ВОМОЖНОСТИ РЕАЛИЗАЦИИ СКРЫТЫХ КАНАЛОВ ПО ВРЕМЕНИ НА ОСНОВЕ ЗАГОЛОВКОВ КЭШИРОВАНИЯ ПРОТОКОЛА HTTP В ОБЛАЧНЫХ СЕРВИСАХ ХРАНЕНИЯ ФАЙЛОВ

Д. Н. Колегов, О. В. Брославский, Н. Е. Олексов

Показывается, как скрытые каналы по времени на основе заголовков кэширования протокола HTTP могут быть реализованы в облачных сервисах хранения файлов.

Ключевые слова: *HTTP, скрытые каналы, безопасность веб-приложений, ботсети.*

В [1] впервые предложено семейство скрытых каналов по времени на основе заголовков кэширования протокола HTTP, а также базовые сценарии их реализации. В [2] исследуются практические вопросы реализации таких скрытых каналов в современных компьютерных системах. Одним из сценариев реализации рассматриваемых скрытых каналов является сценарий в модели M_1, в рамках которой рассматривается взаимодействие доверенного веб-сервера и двух субъектов-нарушителей, кооперирующих друг с другом путём обращения к этому серверу с целью обмена вредоносными данными. Данный сценарий обеспечивает свойство анонимности скрытого канала, но может обеспечить лишь пропускную способность не более 1 бит/с. В данной работе в рамках рассматриваемого сценария предлагается метод реализации скрытого канала по времени, позволяющий повысить его пропускную способность и сохранить свойство анонимности.