ной СУБД имеет следующую архитектуру. На стороне клиента приложению посредством специальной библиотеки предоставляется NoSQL-интерфейс доступа к данным. На стороне сервера MySQL реализован модуль расширения (`plagin`), который преобразует NoSQL-запросы приложения в низкоуровневые операции подсистемы хранения данных (`storage engine`). В дополнение к стандартному MySQL-протоколу взаимодействия клиента и сервера БД реализован дополнительный NoSQL-протокол с поддержкой выборки по диапазону над зашифрованными данными. Отличительными характеристиками NoSQL-протокола являются: 1) асинхронность (работа клиента на время обработки запроса сервером не приостанавливается); 2) поддержка интерактивного алгоритма шифрования (на сервере хранится промежуточное состояние взаимодействия); 3) обход SQL-уровня MySQL-сервера, что позволяет избежать временных затрат на синтаксический анализ и оптимизацию запросов. Наиболее близким аналогом разработанной СУБД можно назвать исследовательский проект CryptDB [4], в котором подсистема, реализующая шифрование данных, является настройкой (прокси-сервером) над СУБД MySQL.

ЛИТЕРАТУРА

1. *Жиров А. О., Жирова А. О., Кренделев С. Ф.* Безопасные облачные вычисления с помощью гомоморфной криптографии // БИТ. 2013. Т. 1. С. 6–12.
2. *Popa R. A., Li F. H., and Zeldovich N.* An ideal-security protocol for order-preserving encoding // IEEE Symp. Security and Privacy. San Francisco, CA, USA, May 23–24, 2013. P. 463–477.
3. *Boldyreva A., Chenette N., Lee Y., and O'Neill A.* Order-preserving symmetric encryption // EUROCRYPT'09. LNCS. 2009. V. 5479. P. 224–241.
4. *Popa R. A., Redfield C. M. S., Zeldovich N., and Balakrishnan H.* CryptDB: protecting confidentiality with encrypted query processing // Proc. Twenty-Third ACM Symp. Operating Systems Principles (SOSP'11). New York, NY, USA, 2011. P. 85–100.

УДК 004.94

УСЛОВИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ПАМЯТИ 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 *Astra Linux Special Edition*, анализируются условия безопасности информационных потоков по памяти в смысле Белла — ЛаПадулы и мандатного контроля целостности.

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

Фундаментальным требованием безопасности операционных систем, реализующих мандатное управление доступом, является предотвращение возможности реализации информационных потоков по памяти «сверху вниз» (безопасность в смысле Белла — ЛаПадулы [1]). Кроме того, современную защищённую операционную систему трудно представить без мандатного контроля целостности, основой которой является предотвращение возможности модификации (через создание соответствующих информационных потоков по памяти) сущностей с высоким уровнем целостности субъект-сесси-

ями с низким уровнем целостности. Таким образом, важным этапом при разработке мандатной сущностно-ролевой ДП-модели (МРОСЛ ДП-модели) [1 – 3], реализуемой в настоящее время в отечественной защищенной операционной системе специального назначения (ОССН) *Astra Linus Special Edition* [4], стало формулирование и обоснование достаточных условий безопасности в смысле Белла — ЛаПадулы и мандатного контроля целостности.

Дополнительно к использованным в перечисленных работах дадим следующие определения и обозначения.

Определение 1. Доверенную субъект-сессию y назовем функционально корректной относительно доверенной субъект-сессии y' и сущности или субъект-сессии e, когда y не реализует информационный поток по памяти от e к некоторой сущности e', функционально ассоциированной с y'. Субъект-сессию y назовем абсолютно функционально корректной относительно субъект-сессии y' и сущности или субъект-сессии e, когда y не реализует информационный поток по памяти от e к некоторой сущности e', функционально ассоциированной с y'. При этом используем следующие обозначения:

— $f\_correct : L_S \to 2^{L_s \times (E \cup S)}$ — функция, задающая для каждой доверенной субъект-сессии множество пар вида (доверенная субъект-сессия, сущность или субъект-сессия), относительно которых она функционально корректна;

— $af\_correct : S \to 2^{S \times (E \cup S)}$ — функция, задающая для каждой субъект-сессии множество пар вида (субъект-сессия, сущность или субъект-сессия), относительно которых она абсолютно функционально корректна.

Определение 2. Доверенную субъект-сессию y назовем параметрически корректной относительно доверенной субъект-сессии y' и сущности или субъект-сессии e, когда y не реализует информационный поток по памяти от или к e от или к некоторой сущности e', параметрически ассоциированной с y'. Субъект-сессию y назовем абсолютно параметрически корректной относительно субъект-сессии y' и сущности или субъект-сессии e, когда y не реализует информационный поток по памяти от или к e от или к некоторой сущности e', параметрически ассоциированной с y'. При этом используем следующие обозначения:

— $p\_correct : L_S \to 2^{L_s \times (E \cup S)}$ — функция, задающая для каждой доверенной субъект-сессии множество пар вида (доверенная субъект-сессия, сущность или субъект-сессия), относительно которых она параметрически корректна;

— $ap\_correct : S \to 2^{S \times (E \cup S)}$ — функция, задающая для каждой субъект-сессии множество пар вида (субъект-сессия, сущность или субъект-сессия), относительно которых она абсолютно параметрически корректна.

Определение 3. Назовём траекторию $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$ системы $\Sigma(G^*, OP, G_0)$, где $N \geqslant 0$, на которой доверенные субъект-сессии не инициируют выполнение де-юре правил преобразования состояний, траекторией без кооперации доверенных и недоверенных субъект-сессий. Таким образом, по определению в системе $\Sigma(G^*, OP, G_0)$ на траекториях без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа доверенные субъект-сессии могут инициировать выполнение только де-факто правил вида $flow\_memory\_access(x, y, \alpha_a)$, $flow\_time\_access(x, y)$, $find(x, y, z)$, $post(x, y, z)$ и $pass(x, y, z)$.

Определение 4. Состояние G системы $\Sigma(G^*, OP, G_0)$ назовём безопасным, когда оно удовлетворяет следующим условиям:

— для каждых субъект-сессий $x, y \in S$, таких, что $y \in de\_facto\_own(x)$, выполняется $f_s(y) = f_s(x)$ и $i_s(y) \leqslant i_s(x)$;
— для каждых недоверенной субъект-сессии $x \in N_S$, субъект-сессии $y \in S$ и сущности $e \in E$, таких, что либо ($e \in [y]$ и $(x, e, write_m) \in F$), либо ($e \in]y[$ и либо $(e, x, write_m) \in F$, либо $(x, e, read_a) \in A$), верны условия $f_s(y) \leqslant f_s(x)$ и $i_s(y) \leqslant i_s(x)$;
— для каждой доверенной субъект-сессии $y \in L_S$ и каждой сущности $c\_i\_entity \in E\_HOLE$, где $c \in LC$, верно условие $(y, c\_i\_entity, write_a) \notin A$;
— для каждого информационного потока $(x, y, \alpha_f) \in F$, где $\alpha_f \in \{write_m, write_t\}$, справедливо $f_x(x) \leqslant f_y(y)$, где f_x и f_y — соответствующие функции f_e, f_r или f_s, и, если $\alpha_f = write_m$, то справедливо $i_x(x) \geqslant i_y(y)$, где i_x и i_y — соответствующие функции i_e или i_s.

Определение 5. 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, где $0 \leqslant i < N$:

— 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 не верно 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 $x, y \in E_N$ и не верно неравенство $f_{e_N}(x) \leqslant f_{e_N}(y)$ (нарушение безопасности в смысле контроля информационных потоков по времени).

В следующей базовой теореме безопасности (БТБ-ДП) сформулированы достаточные условия безопасности системы, заданной в рамках МРОСЛ ДП-модели, в смыслах Белла — ЛаПадулы и мандатного контроля целостности. При этом анализ условий безопасности информационных потоков по времени как существенно более сложный планируется осуществить при проведении дальнейших исследований.

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 $N \geqslant 0$, и в каждом состоянии G_N для каждой субъект-сессии $s \in S_N$ и сущности $e \in E_N$ выполняются следующие условия:

— если $e \in [s]$, то выполняются условия $i_{s_N}(s) \leqslant i_{e_N}(e)$ и ($f_{s_N}(s) = f_{e_N}(e)$ или $i_{e_N}(e) = i\_high$) (корректность уровней конфиденциальности и целостности сущностей, функционально ассоциированных с субъект-сессиями);
— если $e \in]s[$, то выполняется равенство $f_{s_N}(s) = f_{e_N}(e)$ и для каждой роли или административной роли $r \in R_N \cup AR_N$, такой, что $(e, read_r) \in PA_N(r)$, выполняются условия $i_{s_N}(s) \leqslant i_{e_N}(e) \leqslant i_{r_N}(r)$ (корректность уровней конфиденциальности и целостности, а также прав доступа на чтение к сущностям, параметрически ассоциированным с субъект-сессиями);
— для всех доверенных субъект-сессий $s \in L_{S_N}$ верны равенства $f\_correct_N(s) = p\_correct_N(s) = L_{S_N} \times (E_N \cup S_N)$ (функциональная и параметрическая кор-

ректность всех доверенных субъект-сессий относительно всех доверенных субъект-сессий и сущностей);

— для всех субъект-сессий $s \in S_N$ выполняются равенства $\{s' \in S_N : f_{s_N}(s') = f_{s_N}(s)\} \times (E_N \cup S_N) \subset af\_correct_N(s) = ap\_correct_N(s)$ (абсолютная функциональная и параметрическая корректность субъект-сессии относительно всех сущностей и субъект-сессий с совпадающим уровнем конфиденциальности).

Тогда система $\Sigma(G^*, OP, G_0)$ безопасна в смыслах Белла — ЛаПадулы и мандатного контроля целостности.

Условия теоремы БТБ-ДП требуют от ОССН функционально и параметрически корректной (абсолютно корректной) реализации всех субъект-сессий и корректного задания соответствующих уровней конфиденциальности и целостности функционально или параметрически ассоциированных с ними сущностей. Если, например, субъект-сессия, имеющая высокий уровень доступа, некорректно обрабатывает данные («заражается») в сущностях с низким уровнем конфиденциальности и это приводит к получению фактического владения над нею субъект-сессией с низким уровнем доступа, то система защиты ОССН не сможет этому воспрепятствовать. Таким образом, условия теоремы БТБ-ДП указывают на необходимость повышения качества разработки прикладного программного обеспечения 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.* 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/`.

УДК 004.94

ОБЩИЙ МЕТОД АУТЕНТИФИКАЦИИ HTTP-СООБЩЕНИЙ В ВЕБ-ПРИЛОЖЕНИЯХ НА ОСНОВЕ ХЕШ-ФУНКЦИЙ

Д. Н. Колегов

Предлагается метод аутентификации HTTP-сообщений в веб-приложениях, построенный на основе криптографических протоколов с ключевыми хеш-функциями. Данный метод может быть использован для защиты от многих атак на веб-приложения, использующих уязвимости в реализации механизмов аутентификации или авторизации.

Ключевые слова: *криптографические протоколы, аутентификация сообщений, веб-приложения.*

Одним из свойств, характеризующих безопасность протоколов, является свойство аутентификации сообщений, заключающееся в обеспечении аутентификации источника данных и целостности передаваемого сообщения. Аутентификация источника данных означает, что протокол обеспечивает гарантии того, что полученное сообщение или