Секция 5

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.65, 004.056.55

ЗАЩИЩЁННАЯ СУБД С СОХРАНЕНИЕМ ПОРЯДКА

И. Н. Глотов, С. В. Овсянников, В. Н. Тренькаев

Работа посвящена разработке защищённой клиент-серверной СУБД при недоверенном сервере БД. Конфиденциальные данные шифруются на стороне клиента с помощью специализированных шифров, позволяющих производить операции над данными без их предварительного расшифрования. Для этого используется шифр mOPE с сохранением порядка, который позволяет производить операции сравнения над зашифрованными данными. Разработан и реализован асинхронный NoSQL-протокол взаимодействия клиента и сервера БД, поддерживающий простой набор операций над конфиденциальными данными. Разработанный протокол интегрирован в свободно распространяемую СУБД MySQL.

Ключевые слова: *защищённая СУБД, недоверенный сервер БД, шифр с сохранением порядка, NoSQL-протокол.*

Рассматривается задача построения защищённой клиент-серверной СУБД в случае, когда сервер БД неподконтролен пользователю БД. Такая ситуация имеет место, например, при использовании облачных услуг, когда хранение и обработка данных производится на серверах, предоставляемых в пользование третьей стороной. Предполагается, что возможна пассивная атака, когда корректно выполняются все запрашиваемые операции, но при этом ведётся наблюдение за данными, обращаемыми на сервере БД.

Проблему недоверенного сервера предлагается решать с помощью шифрования конфиденциальных данных на доверенном клиенте с последующей их передачей в неконтролируемую БД. Для этого следует использовать специализированные шифры, позволяющие выполнять безопасные вычисления — шифры, сохраняющие вычислительные операции над данными [1] и (или) порядок данных в базе [2]. В этом случае не требуется расшифрования при манипуляции с данными.

В настоящей работе используется шифр mOPE с сохранением порядка [2], так как он является единственным, для которого доказана безопасность в смысле отсутствия утечки информации об открытых текстах по шифртекстам, кроме их порядка, — стойкость к атаке IND-OCPA [3]. Шифр mOPE ненамного увеличивает длину шифртекста по сравнению с длиной открытого текста (в отличие от других шифров с сохранением порядка, для которых длина шифртекста экспоненциально зависит от длины открытого текста). Особенностями шифра mOPE являются интерактивность (алгоритм шифрования распределён между клиентом и сервером) и изменяемость шифртекстов (в процессе шифрования текущего открытого текста могут измениться шифртексты других данных).

В качестве основы при разработке защищённой СУБД с сохранением порядка взята свободно распространяемая СУБД MySQL. Экспериментальный образец защищён-

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-