ЗАЩИТА ДАННЫХ С ПОМОЩЬЮ ЗАКРЫТЫХ ЗАПРОСОВ

А.А. Кашкароева, *канд. социол. наук, доцент*
С.С. Субанбекова, *преподаватель*
Институт социального развития и предпринимательства
(Кыргызстан, г. Бишкек)

Аннотация. *В данной статье исследована пользовательская техническая компьютерная угроза и предложены способы защиты от нее на основе обработки закрытых запросов к базам данных.*

Ключевые слова: *база данных, зашифрованная информация, коммерческая безопасность, информационные ресурсы, обработка данных.*

В настоящее время компьютерной разведкой (КпР) называют добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [1]. Пользовательская КпР позволяет получать данные непосредственно о пользователях (людях и программах) компьютерных систем и сетей, то необходимо разработать методы защиты от нее. Напомним, что пользователями компьютерных сетей являются не только люди, но и отдельные программы или программно-аппаратные комплексы.

Пользовательская КпР - это добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной легендируемой (заманивающей) информационной инфраструктуре (приманка). Итак, рассмотрим более подробно обращение пользователей к различным информационным ресурсам и базам данных (БД). Суть пользовательской КпР заключается в анализе интересов пользователей по их запросам к БД. Следовательно, для защиты от пользовательской КпР необходимо, например, скрывать сами запросы. При "легальных" применениях возникает проблема того, как при известном запросе скрыть только содержание запроса. В работах Дмитрия Валерьевича Асонова [2-3] предложен оригинальный подход к решению этой проблемы путем применения "обработки закрытых запросов" (ОЗЗ).

Рассматриваются две нестандартные проблемы обработки запросов к базам данных (БД). Первая проблема ОЗЗ заключается в обработке запроса к БД так, что: сервер (и владелец) базы данных не может получить никакой информации о содержании и результате запроса пользователя и пользователь не получает никакой информации о БД, за исключением ответа на свой запрос. Подчеркнем, что доступ к БД нам разрешен, но никто, кроме нас, не должен в принципе знать ни о нашем вопросе, ни о полученном ответе. Администратор БД видит только факт самого запроса и размер полученных по этому запросу данных. Это позволяет владельцу БД выставить соответствующий счет на оплату услуг. Известны три категории решения данной проблемы [2]: теоретические, криптографические и обработка закрытых запросов на защищенном вычислительном устройстве.

Теоретические методы в разных вариациях рассматривают копирование всей БД. Криптографические решения существуют на основе доработок нестандартными методами, но для них обязателен доступ в реальном времени и перебор всей базы данных. Например, владелец БД пересылает заказчику всю БД в зашифрованном виде, что исключает возможность воровства информации. Заказчик через каталог или аннотации выбирает из БД требуемую ему одну запись и также шифрует ее "поверх" шифра владельца. Используемые

шифры должны быть гомоморфными (или коммуникативными), что позволяет осуществлять замену шифров. Заказчик не может прочесть запись, так как она зашифрована владельцем. Заказчик отправляет зашифрованную запись владельцу БД, который также не может прочесть эту запись, ведь ему не известен шифр заказчика. Далее, владелец "снимает" свой шифр, выставляет счет на оплату и, после получения денег, пересылает запись заказчику. Заказчик после оплаты и получения записи, расшифровывает ее и использует для своих целей. Получаем, что заказчик получает только одну запись, но ее содержание не известно никому, ведь она зашифрована самим заказчиком. Владелец БД отдает заказчику только одну запись, ведь все остальные записи зашифрованы именно владельцем. По каналам связи передается только зашифрованная информация, что исключает доступ к ней посторонних лиц. У этого класса криптографических решений существует огромный недостаток, обусловленный необходимостью перебора всей БД, что значительно увеличивает время между заказом и получением требуемой записи. Учитывая огромные размеры современных БД, этот недостаток делает невозможным реальное использование криптографических методов для решения проблемы обработки закрытых запросов к большим и/или часто обновляемым БД.

Обработка закрытых запросов на защищенном вычислительном устройстве (ЗВУ). Защищенные вычислительные устройства - ЗВУ, представляют собой специальный класс устройств для хранения защищенных данных и исключения доступа к ним людей, даже системных администраторов и владельцев. При попытке проникновения в ЗВУ все данные на нем немедленно физически уничтожаются и проводится оповещение соответствующих служб. Это устройство выполняет функции "третьего доверенного лица", которому доверяют и владелец, и заказчик. Если любого человека хотя бы теоретически можно подкупить, то ЗВУ подкупить невозможно. Отметим, что ЗВУ используются для решения различных задач и достаточно большим количеством способов. В данной работе целесообразно для примера проанализировать только несколько способов. В целом, ЗВУ представляют собой "черный ящик", который встраивается в оборудование владельца информационного ресурса. Возможно, что такое "встраивание" является рискованным и психологически сложным для владельца.

Рассмотрим запрос заказчика на получение конкретной записи от владельца БД. Заказчик посылает свой зашифрованный запрос к ЗВУ, которое его расшифровывает. Далее, ЗВУ получает поочередно все записи из БД, но "откладывает", запоминает у себя внутри только одну - нужную заказчику. После выполнения финансовых действий, владелец разрешает ЗВУ отослать зашифрованную этим ЗВУ запись заказчику. Этот шифр знают только ЗВУ и заказчик, который после получения самостоятельно расшифровывает требуемую ему запись и использует ее. Таким образом, никто кроме ЗВУ не знает какую запись получил заказчик, а заказчик не видит остальных записей БД владельца.

Вторая проблема ОЗЗ заключается в обработке запроса на пересечение двух баз данных таким образом что: владельцы баз данных не могут получить никакой информации о БД партнера, а также о результате запроса на пересечение; пользователь не может получить никакой информации из баз данных, за исключением результата запроса на пересечение.

В этом случае заказчик не узнает ничего лишнего о БД, кроме прямого ответа на свой запрос. ОЗЗ позволяет получать заказчикам такие ответы и не показывает никому содержание самих БД. Например, две компании могут проводить статистические исследования пересечений своих пользователей, но исходные данные о своих клиентах эти компании друг другу не показывают (только обобщенные статистические результаты и зависимости). Другой

пример, когда транспортные компании перевозят пассажиров и собирают все данные на них, а внешние службы безопасности имеют списки "злоумышленников" ("стоп-списки"). Задача состоит в том, что бы при решении совместных задач по обеспечению безопасности пассажиров никто из злоумышленников, включенных в "стоп-списки" не мог попасть на транспорт и при этом, чтобы транспортные компании не знали самих "стоп-списков", а службы безопасности не знали о перемещениях лиц, не входящих в "стоп-списки". Таким образом, формально решается задача получения взаимного доступа только к пересечениям двух баз данных, но владельцы этих БД не знают ничего другого о чужих БД.

Решение этой проблемы так же возможно криптографическими способами, аналогичными выше указанным способам. К недостаткам этих способов можно отнести то, что они способны выявлять только полное равенство (совпадение) признаков записей из разных баз данных. Более перспективным является применение защищенных вычислительных устройств. Такие ЗВУ внутри себя получают доступ ко всем базам данных и могут не только выявлять полное равенство (совпадение) записей из разных БД, но и определять степень их близости (находить близкие записи или подобные).

Потенциальные приложения этих двух проблем ОЗЗ очень разнообразны и включают, помимо технической защиты от пользовательской КпР, такие области, как коммерческая безопасность, антитеррористические меры, экономика (банковское дело, трейдинг, маркетинг, реклама, электронные магазины, и т.д.), биомедицина, патентное дело, и т.д. В настоящее время проводятся исследования по следующим основным направлениям в области обработки закрытых запросов: комбинирование криптографических методов и защищенных вычислительных устройств; закрытые запросы к сверхбольшим базам данных в режиме времени, близком к реальному; закрытые запросы к нескольким базам данных, а также по другим направлениям.

Вывод: Для защиты от пользовательской технической компьютерной разведки можно применять технологию обработки закрытых запросов к базам данных, предложенную Д.В. Асоновым. Наиболее перспективным является метод защиты путем обработки закрытых запросов на основе защищенных вычислительных устройств.

Библиографический список

1. *Варламов О.О. О* системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ТРТУ, Тематический выпуск "Информационная безопасность". 2006. №7 (62). С. 216-223.

2. *Асонов Д.В.* Обработка закрытых запросов. Доклад на семинаре Московской секции ACM SIGMOD, ВМК МГУ. 26.04.2007

3. *DmitriAsonov:* PrivateInformationRetrieval. GI Jahrestagung (2) 2001: 8

PROTECTION OF DATA WITH HELP OF CLOSED REQUESTS

A.A. Kashkaroyeva, *candidate of social sciences, associate professor*
S.S. Subanbekova, *lecturer*
Institute for social development and entrepreneurship
(Kyrgyzstan, Bishkek)

Abstract. *This article explores the user's technical computer threat and suggests ways to protect against it by processing closed queries against databases.*

Keywords: *database, encrypted information, commercial security, information resources, data processing.*