значит, в общем случае ее решение является вычислительно трудной задачей. Данный подход приемлем в случае корректного доказательства требования неразличимости (свойства виртуального "черного ящика"), а затем сведения задачи построения разрешенного полинома $p(\cdot)$ к задаче SAT.

Таким образом, в статье представлены различные подходы к определению стойкости обфускации и установлена возможность построения универсального обфускатора, удовлетворяющего требованиям стойкости в модели виртуального "черного ящика".

Литература

1. Варновский Н.П., Захаров В.А., Кузюрин Н.Н. Математические проблемы обфускации // Математика и безопасность информационных технологий. Материалы конференции в МГУ 28–29 октября 2004 г. Москва: 2005. С. 65–91.

2. Barak B., Goldreich O., Impagliazzo R., Rudich S., Sahai A., Vadhan S., Ke Yang. On the (im)possibility of obfuscating programs // Advances in Cryptology - CRYPTO'01, Lecture Notes in Computer Science, v. 2139, 2001, p. 1-18.

3. Dalla Preda M., Giacobazzi R. Semantic-based code obfuscation by abstract interpretation // International Colloquium on Automata, Language and Programming, Lecture Notes in Computer Science, v. 3580, 2005, p.1325-1336.

4. Козачок, А. В., Аналитическая модель защиты файлов документальных форматов от несанкционированного доступа / А. В. Козачок, М. В. Бочков, Р. Р. Фаткиева, Л. М. Туан. // Труды СПИИРАН (Санкт-Петербург), 2015.– Вып. 43. – С. 228–252.

5. Della Preda M., Giacobazzi G. Semantic-based code obfuscation by abstract interpretation // Journal of Computer Security, 2009, v. 17, N 6, p. 855-908.

6. Garg S., Gentry C., Halevi S., Raykova M., Sahai A., Waters B. Candidate indistinguishability obfuscation and functional encryption for all circuits // In FOCS, 2013. pp. 40–49.

7. Козачок А.В., Туан Л.М. Комплекс алгоритмов контролируемого разграничения доступа к данным, обеспечивающий защиту от несанкционированного доступа // Системы управления и информационные технологии. 2015. № 3(61). С. 58–61.

8. Ananth P., Gupta D., Ishai Y., Sahai A. Optimizing obfuscation: Avoiding barrington's theorem // In Proceeding of the 2014 ACM SIGSAC, 2014. pp. 646-658.

9. Pass R., Seth K., Telang S. Indistinguishability obfuscation from semantically-secure multilinear encodings // In Advances in Cryptology – CRYPTO, 2014. pp. 500–517.

10. Kilian J. Founding cryptography on oblivious transfer // In 20th Annual ACM Symposium on Theory of Computing 1988. pp. 20–31.

11. Garg S., Gentry C., Halevi S. Candidate multilinear maps from ideal lattices // In Advances in Cryptology – EUROCRYPT 2013. pp. 1–17.

12. Козачок А.В., Теоретическое обоснование стойкости неразличимой обфускации / А. В. Козачок, М. В. Бочков, Лай Минь Туан // Вопросы кибербезопасности. – 2016.– Вып. 1 (14).– С. 36–46.

А.Н. Крутов

ОПЫТ ВНЕДРЕНИЯ ЗАЩИЩЕННОЙ СИСТЕМЫ РЕПЛИКАЦИИ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

В работе описывается опыт внедрения модуля «Бастион-2 – Репликация», являющегося частью аппаратно-программного комплекса «Бастион-2». Данный аппаратно-программный комплекс позволяет объединить системы безопасности различных производителей в области видеонаблюдения, контроля доступа и пожарной сигнализации в единую систему, удобным образом настраиваемую и надежно функционирующую. По своей сути аппаратно-программный комплекс «Бастион-2» является качественным развитием АПК «Бастион» с дополнительными возможностями. К ним относятся:

1. Переход от хранения данных в СУБД Firebird к СУБД Oracle. Для работы на относительно небольших объектах достаточно наличия бесплатной версии СУБД Oracle XE 11g и выше.
2. Существенные доработки ядра системы, позволяющие увеличить количество одновременно подключаемых драйверов.
3. Поддержка большего количества устройств, таких как биометрические считыватели, системы охраны периметра, модули аварийного освещения и т.п.

Кроме этого, АПК «Бастион-2» разрабатывался как масштабируемый продукт, способный к стабильной работе на объектах разного масштаба – от небольших офисов до крупных предприятий, с развитой филиальной сетью. Все вышесказанное послужило основанием для создания модуля «Бастион-2 – Репликация», основной функцией которого являлась бы передача электронных пропусков между объектами (филиалами) одного предприятия.

При анализе существующих решений по репликации данных в СУБД Oracle просматривались два решения, а именно технологий Oracle Streams и Golden Gate. Было отмечено, что использование технологии Oracle Streams требует весьма тщательной настройки сервера базы данных, требующей наличие на объекте администратора базы данных весьма высокой квалификации [1]. Сопровождение такой системы репликации неизбежно привело бы к необходимости привлечения существенных дополнительных ресурсов у службы технической поддержки. Кроме этого в работах [2,3] отмечается весьма ограниченные существующие средства по разрешению конфликтов репликации, что тре-

бует написания дополнительных программных модулей. Поэтому использование технологии Oracle Streams было признано нецелесообразным.

Анализ программного продукта Oracle Golden Gate показал [4], что в настоящее время это лучшее решение по репликации данных для Oracle. Однако высокая стоимость продукта не позволяет его использовать в составе АПК «Бастион-2». Учитывая все вышесказанное, было принято решение по написанию самостоятельной системы репликации данных между серверами Oracle. Ниже приводится список первоначальных требований к системе репликации и то, какими способами удалось удовлетворить этим требованиям.

1. **Возможность работы в бесплатных версиях СУБД Oracle**

Основное ядро в модуле «Бастион-2 – Репликация» реализовано на уровне базы данных. Для того, чтобы организовать связь между различными участниками репликации во всех участниках-филиалах создается database link к серверу-центру, а на сервере-центре создаются соединения со всеми его филиалами. Непосредственные соединения филиалов между собой отсутствуют. Технология создания соединений между базами Oracle доступна даже в бесплатной версии XE.

2. **Простота установки и первоначальной настройки**

Принципиальная схема разработанной системы репликации описана в работе [5]. Для упрощения установки модуль «Бастион-2 – Репликация» собран в инсталляционный пакет. При первом запуске системы модуль запускается в режиме мастера, с помощью которого осуществляется быстрая настройка модуля без необходимости ввода большого количества технических параметров базы данных.

3. **Совместимость со всеми разработанными ранее модулями системы**

Совместимость со всеми разработанными ранее модулями системы обеспечивается тем, что очередная версия модуля «Бастион-2 – Репликация» поставляется вместе со всеми другими модулями очередного релиза АПК «Бастион-2». Если по каким-то причинам будут установлены продукты несовместимых версий, то их запуск будет невозможен.

4. **Обеспечение взаимно-однозначного соответствия данных у различных участников репликации.**

Для организации взаимно-однозначного соответствия данных у различных участников репликации используются статически уникальные 128-битные идентификаторы (GUID). Для этого в каждую реплицируемую таблицу добавляется поле REPL_GUID, являющееся ключом-кандидатом, а также поле MEMBER_GUID_OWNER для указания владельца записи. При настройке репликации в Центре данные поля REPL_GUID заполняются значениями функции SYS_GUID, и в качестве владельца всем записям проставляется Центр. При настройке системы репликации в конкретном филиале сопоставляются его данные с данными, имеющимися в Центре. При обнаружении одинаковых записей значения полей REPL_GUID заполняются значениями идентификаторов из Центра и он же указывается в качестве владельца записей. После завершения процедуры идентификации все незаполненные значения полей REPL_GUID заполняются значениями функции SYS_GUID, и в качестве владельца записей проставляется конкретный филиал. При первичном сопоставлении данных поиск одинаковых значений осуществляется по информационным полям соответствующих таблиц (для справочников – наименование, для карт доступа их полный номер и т.п.)

5. **Репликация с учетом всех существующих в системе бизнес-правил и ограничений.**

Все существующие в АПК «Бастион-2» бизнес-правила реализованы на уровне сервера СУБД в виде соответствующих триггеров и хранимых процедур. При репликации данных из одной СУБД в другую, данные заносятся через те же хранимые процедуры, которые используются всеми другими модулями АПК «Бастион-2» для своей работы, например, «Бастион-2 –АРМ Бюро пропусков». При этом осуществляется доставка полученных данных до контроллеров оборудования имеющимися штатными средствами системы.

6. **Отслеживание конфликтов репликации.**

Для отслеживания и последующего разрешения конфликтов на компьютере-источнике ведется протокол посылки/применения записи, т.е. используется обратная связь с компьютером-приемником, а на компьютере-приемнике ведется только протокол применения записи. Приведенная схема протоколирования обеспечивает возможность отследить возможные ошибки репликации на любых ее узлах.

7. **Сокращение вероятности появления логических ошибок.**

Ввиду того, что репликация происходит не в режиме реального времени, при её работе возможно появление логических ошибок, когда с двух различных участников репликации происходит редактирование одного и того же пропуска. После проведения репликации они обмениваются своими изменениями, и значения перестают быть одинаковыми. Такие ошибки являются трудоемкими для обнаружения, т.к. формально процедура репликации завершилась успешно, а по факту – нет. Для того, чтобы максимально сократить вероятность появления таких ошибок используется правило, что данные в Центре имеют более высокий приоритет, чем в филиале. Данное правило также будет работать в случае, если происходит одновременное редактирование данных в двух разных филиалах, т.к. репликация осуществляется транзитом через Центральный офис.

8. Возможность работы при нестабильной связи между различными филиалами организации.

Ввиду того, что репликация происходит не в режиме реального времени, при её работе возможно появление логических ошибок, когда с двух различных участников репликации происходит редактирование одного и того же пропуска. После проведения репликации они обмениваются своими изменениями, и значения перестают быть одинаковыми. Такие ошибки являются трудоемкими для обнаружения, т.к. формально процедура репликации завершилась успешно, а по факту – нет. Для того, чтобы максимально сократить вероятность появления таких ошибок используется правило, что данные в Центре имеют более высокий приоритет, чем в филиале. Данное правило также будет работать в случае, если происходит одновременное редактирование данных в двух разных филиалах, т.к. репликация осуществляется транзитом через Центральный офис.

9. Обеспечение защищенной передачи данных

Для безопасного соединения удаленных серверов баз данных между собой рекомендуется организации VPN-соединения. Для дополнительной защиты информации данные промежуточных таблиц могут шифроваться любым современным алгоритмом шифрования, как симметричным, так и асимметричным. Проблема передачи ключей для расшифровки информации в данном случае не стоит, так как информация реплицируется внутри одной, пусть и распределенной организации.

Опыт внедрения полученной системы репликации свидетельствует о том, что все заявленные цели, поставленные при ее проектировании, были достигнуты. В настоящее время ведется мониторинг возможных конфликтов репликации с тем, чтобы предложить пользователям автоматические средства по их разрешению.

Литература

1. Kirtikumar Deshpande. Oracle Streams 11g Data Replication. - McGraw-Hill Osborne Media, 2011. – 546 с.

2. Базилевский Е.В. Альтернативный способ разрешения конфликтов репликации в распределенных базах данных Oracle // Современные проблемы науки и образования. - 2012. №2. - С. 266

3. Гришмановский П.В., Базилевский Е.В. Анализ технологий репликации данных и методы повышения эффективности разрешения конфликтов репликации // Вестник Волжского университета им. В.Н. Татищева. - 2012. №2[19]. - С. 98-106

4. B. Prusinski, S. Phillips, R. Chung. Expert Oracle GoldenGate. - Apress, 2011. – 352 с.

5. Крутов А.Н. Разработка защищенной системы репликации // Информационное противодействие угрозам терроризма, 2015, №24, С. 81-85

А.Б. Кузьмичев

АЛГОРИТМ ИДЕНТИФИКАЦИИ СУБЪЕКТА ПО БИОМЕТРИЧЕСКИМ ПРИЗНАКАМ НА ОСНОВЕ ТЕОРИИ СИСТЕМ СО СЛУЧАЙНОЙ СТРУКТУРОЙ

(Тольяттинский государственный университет, г. о. Тольятти)

Идентификация субъекта по биометрическим признакам возможно реализовать при различиях в параметрах, которые можно измерить по характеристикам, присущих человеку. Такими параметрами могут являться такие как лицо, голос, отпечатки пальцев, клавиатурный почерк и т.д. В основе идентификации лежит вычисление выбранных биометрических параметров χ на основе измерений по идентифицируемому субъекту, и сравнение их на степень совпадения с априорно известными или измеренными ранее биометрическими параметрами по выбранным субъектам. При малых различиях вычисляемых параметров и наличии ошибок в оценке измерений по идентифицируемым субъектам, увеличивается вероятность принятия ошибочного решения $P_{o\text{р}}$ при простом сравнении полученной оценки параметра с некоторой границей принятия решения. Одним из путей уменьшения $P_{o\text{р}}$ является увеличение количества измерений χ и их усреднении с целью уменьшения ошибки в оценке выбранного параметра.

В данной работе предлагается использовать алгоритма идентификатора, построенного с применением теории систем со случайно изменяющейся структурой. Данный алгоритм по известным законам распределения биометрических параметров для субъектов идентификации позволяет оценить вероятность того, что данный субъект является требуемым субъектом идентификации. Рассмотрим в качестве примера алгоритм идентификации субъекта по одному измеряемому биометрическому параметру. Для этого используем математический аппарат, предложенный в [1] и рассмотренный в [2].

Постановка задачи. Имеются априорные данные о распределении биометрического параметра для вероятных субъектов, подлежащих идентификации. В процессе измерений от *m* обнаруженных субъектов производятся вычисления биометрических параметров χ_{j} (j=1,m) с ошибкой, априорно известной исходя из конкретного типа измерителей характеристик человека и их условий применения.

Принятые допущения:

1. Уравнения объекта имеют вид :

$$\dot{\chi} = 0\,,$$

$$\chi(0) = \chi_0\ ,\ \chi_0 = \mathrm{N}_{\text{усеч}}\{m_x(s_k), \sigma_x(s_k)\}, \quad (1)$$