УДК 519.254

В.С. Русецкий, Е.А. Русецкая, Р.Т. Файзуллин, Р.Р. Файзуллин

Процедура отсроченного приема сообщения в задаче защиты продукции от фальсификации

Предложена процедура идентификации продукции несколькими кодами. Коды генерировались с помощью композиции 2 и 3 датчиков случайных чисел. Схема стойка к попыткам вскрытия. Проведенные тесты NIST показывают, что выдача удовлетворяет требованиям случайности.

Ключевые слова: случайная последовательность, имитовставка.

Защита от фальсификации. Переход на новый технологический уровень приводит к тому, что некоторые виды несанкционированной обществом деятельности становятся экономически невыгодными. Например, уход от оплаты наличными, кредитование, гарантийное обслуживание ограничивают уличную преступность эффективней, чем любые силовые методы.

Можно предположить, что имеющиеся нерегулируемые лакуны, используемые криминальными сетевыми структурами, можно элиминировать с помощью внедрения современных информационных технологий в повседневную жизнь. Одной из наиболее болевых точек является фальсификация различного рода продуктов.

Рассмотрим проблему фальсификации в криптографических терминах. У нас имеется два абонента: производитель (Алиса) и покупатель продукта (Боб). Сам продукт можно интерпретировать как сообщение P, пересылаемое от производителя продуктов покупателю по открытому каналу связи. Продавец априори выступает как атакующая сторона, задача которой – подменить сообщение имитовставкой [1].

Мы не будем рассматривать организационные и правовые меры по защите передачи, сводящиеся к защите канала связи, а будем считать, что производитель и покупатель как наиболее заинтересованные стороны производят процедуру аутентификации продукта при различного рода атаках со стороны продавца.

Очевидно, что первый и самый примитивный уровень аутентификации заключается в нанесении различного рода марок, кодов и т.п. на продукт, определяющих производителя.

Опыт применения такого рода меток показал, что атакующий легко справляется с задачей подмены сообщения. Так, попытки усложнить задачу подделки путем нанесения сложных технологических меток легко преодолеваются атакующим, причем иногда даже более быстро, чем защита реализуется самим производителем. Например, нанесение литеры М (Массандра) на дно бутылок было осуществлено нарушителями ранее, чем производителем.

Следующим шагом в усложнении процедуры аутентификации является нанесение различного рода уникальных кодов (номера, QR коды и т.п.) на упаковку и сам продукт, которые аутентифицируют не только производителя, но и сам продукт или упаковку партии продукта. В этом случае покупатель может обратиться непосредственно к производителю и узнать, что продукт с такой маркировкой действительно произведен Алисой. Насколько в этом случае высока защищенность? Очевидно, что возможно дублирование меток и без процедуры обратной связи, т.е. увеличения числа обменов сообщениями между Алисой и Бобом, защита не эффективна.

У Алисы имеется база данных с номерами продуктов и на обращение со стороны Боба с просьбой подтвердить N Алиса реагирует высылкой сообщения M_1 о том, что данный номер имеется в базе. Алиса может дополнить сообщение направлением продаж и любой другой сопутствующей информацией, что влияет на окончательное решение Боба о приеме сообщения (покупке). Но самое главное, что у Алисы нет информации о факте покупки данного продукта, что не позволяет полностью исключить имитовставку.

Мы имеем ситуацию, не совсем свойственную классической схеме. Алиса должна поощрить Боба в продолжении процедуры аутентификации и вынудить к формированию сообщения M_2 о факте приема P (покупки), не раскрывая информацию о предыдущем сеансе связи с другим поку-

пателем, завершившимся фактом приема. В ответ Алиса высылает сообщение M_3, которое несет информацию о том, был или не был куплен продукт ранее. Очевидно, что Боб решает задачу определения баланса между затратами на формирование сообщения M_2 и возможного риска приема имитовставки.

Так, предложенный в одном патенте [2] способ нанесения двух уникальных кодов на упаковку и сам продукт казалось бы полностью решает проблему. Но сама процедура вскрытия упаковки после покупки представляет собой затратную процедуру и ставит под сомнение доказательство факта имитовставки при разборе ситуации перед арбитром.

Возможно и другое решение задачи, т.е. неклассический отсроченный прием сообщения P. Боб фиксирует факт приема сообщения предъявлением Алисе сертификата, идентифицирующего продавца I, например фотографии чека. Алиса же хранит в базе данных не только поля под N_1, N_2, M_1, M_2, но и поле под I. Факт приема сообщения фиксирует факт продажи, а код N_2 уже может служить дополнительным аргументом для арбитра при доказательстве факта имитовставки. В случае если продажа или прием сообщения были осуществлены ранее другим получателем, Боб информируется об этом.

В данной ситуации Боб может выбирать между инициацией процедуры доказательства перед арбитром и быстрым отказом от приема сообщения. То есть Боб может осуществить возврат продукта, не отходя от кассы и не вскрывая упаковку, или предъявить иск продавцу за продажу фальсифицированного продукта. Заметим, что в этом случае код N_2 уже не является необходимым, а лишь достаточным, что существенно снижает затраты производителя при маркировке.

Включение в схему независимого арбитра и хранение у него I, обеспечивает юридическую поддержку в случае факта фальсификации и при атаке со стороны внутреннего нарушителя.

Насколько предложенная схема будет стойкой при попытке восстановления генератора кодов N_i при их наличии в ограниченном числе у Кларка?

Пусть даны два датчика ПСВ D_1, D_2. Будем считать, что период первого датчика равен 2^{N_1}, а период второго 2^{N_2}, $a_1,..,a_{2^{N_1}}$, $b_1,..,b_{2^{N_2}}$ – это строки из нулей и единиц, результат работы генераторов.

Сформируем последовательность чисел $P_1,..,P_q$ по следующему правилу:

$$P_1 = \sum_{k=0}^{K} a_k 2^k, \quad P_i = \sum_{k=0}^{K} a_{k+m_i} 2^k, \quad m_i = \sum_{v=1}^{i} S_v, \quad S_v = \sum_{q=0}^{L} b_{q+L(v-1)} 2^q.$$

Первый датчик генерирует числа P_i, а второй – длины лакун S_v между P_i.

Числа P_i используются для маркировки некоторых объектов. Предложенная конструкция позволяет маскировать выход как первого датчика, так и второго и затрудняет восстановление структур генераторов ПСВ.

Попытаемся оценить снизу число операций, необходимых для восстановления структур генераторов в наиболее благоприятном для атакующего случае.

Пусть у атакующего имеется в наличии некоторое число Ω экземпляров $P_i, i = r_1,..,r_\Omega$. Очевидно, что порядок генерации не совпадает с порядком экземпляров P_i.

1) Будем считать, что генераторы представляют собой линейные регистры сдвига с обратной связью.

2) Будем считать, что какие-то два P_i из $P_i, i = r_1,..,r_\Omega$ генерируются последовательно, т.е. соответствующее S_v, определяющее лакуну между ними, равно нулю.

3) Будем считать, что длина первого регистра равна N_1, а второго N_2.

4) Будем считать, что значения каждых двух лакун S_v генерируются последовательно.

При всех этих условиях для восстановления D_1, D_2 необходимо рассмотреть все пары из $P_i, i = r_1,..,r_\Omega$ и в каждом случае получить $a_1,..,a_{2^{N_1}}$. Заметим, что последовательно генерируемые P_{i1}, P_{i2} позволяют полностью восстановить структуру линейного регистра сдвига.

Выделяя среди $a_1,..,a_{2^{N1}}$ остальные P_i, мы получим предполагаемые m_i. Число вариантов перебора пар будет равно C_2^{Ω}. Согласно 4 можно найти пару S_{v1},S_{v2}, которая позволяет получить именно такие m_i между $P_i, i = r_1,..,r_\Omega$. Число перебираемых пар S_{v1},S_{v2} равно $C_2^{\Omega-1}$.

Окончательно оценка на число операций, необходимых для восстановления структуры регистров, можно оценить величиной $C_2^{\Omega-1}C_2^{\Omega}2^{N_1}$. Минимальное значение Ω, при котором возможно восстановление регистров, равно 4.

Таким образом, число операций и память, необходимая для хранения промежуточных данных, для восстановления регистров сдвига, оценивается величиной $C2^{N_1}$ с небольшой по величине константой C. Любое изменение условий 1–4 приводит к существенному росту числа необходимых операций. Например, если для вычисления лакун использовать не весь выход второго регистра, а лишь некоторую часть, то значение Ω, необходимое для восстановления структуры регистров, растет факториально.

Ситуацию с датчиками ПСВ можно усложнить, добавив 3-й датчик, согласно которому последовательность $a_1,..,a_{2^{N1}}$ будет переставляться сгенерированной им перестановкой. Перестановка a_{k+m_i} и $a_{k+m_{i+1}}$ проводится, если датчик на данном шаге выдал 1, в противном случае не проводится. Для сгенерированных датчиками последовательностей битов были проведены тесты NIST [3, 4]. Кроме теста на равномерность в подпоследовательностях, все тесты были пройдены успешно.

Своё наглядное воплощение процедура отсроченного приёма сообщения получила в разработанном программном продукте «ПродМарка». Продукт предназначен для комплексного решения задачи защиты от фальсификации.

Архитектура продукта «ПродМарка» построена на клиент-серверном принципе, т.е. база данных продукции и обработчики обращений размещены на сервере владельца системы защиты, а клиенты, в данном случае покупатели, обращаются на сервер из различных коммуникационных сред.

Основой системы является база данных формата «MySQL», в которую посредством специального программного обеспечения производитель записывает информацию о поступающих в торговую сеть единицах продукции. Выбранный тип хранения данных – «InnoDB» позволяет при обновлении юридического статуса единицы продукции, в отличие от более распространённого «MyISAM», использовать блокировку на уровне строки, а не всей таблицы, что, в общем итоге, обеспечивает многократное повышение скорости работы клиентов с базой данных. К записываемой информации относятся наименование товара, изображение, описание и характеристики, направление распространения. Структура базы данных является оптимизированной, что позволяет отказаться от дублирования общей для видов или партий продукции информации. Стандартная сборка продукта позволяет без привлечения дополнительных средств распределённого хранения данных обрабатывать до десяти миллионов единиц продукции. При оценке быстродействия системы за расчётную нагрузку принимался месячный оборот продукции в количестве одного миллиона единиц, было смоделировано усреднённое значение 23 запроса в секунду, использован мобильный интернет-канал с пропускной способностью 200 кбит/с. Время ответа системы не превышало 4 с, а среднее чистое машинное время обработки запроса сервером составило 0,3 с. При этом система имеет возможность наращивания мощности с увеличением количества обрабатываемых единиц путём кластеризации.

Регистрацию продукции в базе данных выполняет комплекс программных средств, обеспечивающий валидацию и оптимизацию данных. Результатом регистрации, помимо непосредственной записи в базу данных, является генерация уникального номера и контрольного значения для каждой единицы. Уникальный номер используется для автоматизированного нанесения на упаковку продукции, в том числе в сочетании с машиночитаемым графическим кодом для быстрого распознавания портативными устройствами. Контрольные значения могут быть сгенерированы в том числе и с использованием генератора псевдослучайной последовательности. Тестирования, проведённые с применением стандарта программирования OpenMP [5], подтверждают возможность применения такой генерации.

Сценарий двусторонней связи с покупателем реализован посредством препроцессора гипертекста. Интерфейс служит для мгновенного обмена сообщениями с покупателями, обращений в базу данных, описания закрытых классов обслуживания датчиков ПСВ и связи с внешними библиотека-

ми. Обращения происходят на виртуальный хост системы, зарегистрированный в глобальном адресном пространстве.

После поступления продукции в торговую сеть покупатель приобретает возможность совершения первичных запросов характеристик товара в базу данных производителя, производя в ручном или автоматическом режиме отправку индивидуального номера упаковки в публичный интерфейс системы «ПродМарка». Ответом на запрос является текстово-графическая информация, содержащая наименование, описание, изображение и характеристики товара, служащая двум задачам: начальной идентификации и получению сведений о потребительских свойствах. При совпадении информации, отправленной системой, с информацией, нанесённой на упаковку, покупатель принимает решение о покупке.

Непосредственно в момент совершения покупки покупатель отправляет вторичный запрос в базу данных производителя, передавая либо фотографию кассового чека, либо контрольный код, скрытый внутри упаковки товара. После распознавания принятой от покупателя информации система возвращает юридический статус продукта: была ли вскрыта упаковка ранее или нет, одновременно совершая регистрацию покупки данной единицы продукции, вскрытия упаковки. Оперирование юридическим статусом является основополагающим инструментом системы, поскольку исключает возможность массового контрафактного дублирования продукции.

Литература

1. Дубнов И.А. Использование имитовставок для контроля целостности контента цифрового телевизионного вещания./ И.А. Дубнов, Ю.А. Дубнов // Труды НИИР. – 2013. – № 2. – С. 45–50.

2. Пат. 2463656 РФ, МПК G06F21/24, G06K9/00. Способ аутентификации продукта в контейнере и соответствующий способ для проверки аутентичности продукта и его контейнера / О. Дангманн (FR), Ж. Дешеро (FR). – Патентообладатель ОИ ЭРОП САРЛЬ (FR). – № 2011118612/08 ; заявл. 10.10.2008 ; опубл.: 10.10.2012.

3. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf, свободный (дата обращения: 24.04.14).

4. Вильданов Р.Р. Тесты псевдослучайных последовательностей и реализующее их программное средство / Р.Р. Вильданов, Р.В. Мещеряков, С.С. Бондарчук // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 108–111.

5. Вильданов Р.Р. Применение стандарта OpenMP для тестирования псевдослучайных последовательностей / Р.Р. Вильданов, В.В. Маркин, Р.В. Мещеряков // Сборник статей региональной научно-практической конференции «Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов» (28 февраля 2012 г. на базе Алтайского государственного университета). – 2012. – С. 153–158.

Русецкий Владимир Сергеевич
Инженер-программист центра телекоммуникаций и вычислительной техники Омского государственного технического университета (ОмГТУ)
Тел.: +7-983-117-15-51
Эл. почта: vladimir@omgtu.ru

Русецкая Елена Александровна
Начальник отдела АСУ–ВУЗ центра телекоммуникаций и вычислительной техники ОмГТУ
Тел.: +7-913-617-94-31
Эл. почта: elena@omgtu.ru

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, зав. каф. «Комплексная защита информации» ОмГТУ
Тел.: 8 (381-2) 21-77-02
Эл. почта: r.t.faizullin@mail.ru

Файзуллин Рамиль Рашитович
Ст. преподаватель каф. «Комплексная защита информации» ОмГТУ
Тел.: 8 (381-2) 72-17-19
Эл. почта: strannik11@list.ru

Rusetskiy V.S., Rusetskaya E.A., Faizullin R.T., Faizullin R.R.
Procedure of the delayed reception of the message in a problem of protection of production from falsification

A procedure for the identification of several product codes. Codes are generated using the compositions 2 and 3 random numbers. The scheme is resistant to tampering. NIST tests have shown that the issuance satisfies the requirements of randomness.
Keywords: random sequence, message authentication code.