Обеспечение безопасности передаваемых данных с помощью кодов аутентификации сообщений

Т.А. Билык, А.Ю. Потехонченко, Н.Н. Дацун (ЦБ РФ)

Предлагается алгоритм кода аутентификации сообщений, обеспечивающий подлинность и целостность передаваемых данных в системах доверяющих друг другу абонентов. Приводится описание программной реализации алгоритма и анализ его эффективности.

Ключевые слова: код аутентификации и код аутентичности сообщения, ключевая функция хэширования.

Введение

Коды аутентификации сообщений используются как средство, гарантирующее подлинность источника данных и целостность самих данных при их передаче и хранении в системах с доверяющими друг другу пользователей.

В этих системах для каждого набора данных вычисляется значение кода аутентификации: на вход поступает два аргумента (сообщение произвольной длины и известный отправителю и получателю секретный ключ фиксированной длины), на выходе выдается результат фиксированной длины, называемый имитовставкой. Имитовставка передается или хранится вместе с самими данными. При получении данных пользователь вычисляет значение имитовставки и сравнивает ее с имеющимся контрольным значением. Несовпадение говорит о том, что данные были изменены либо подделаны.

Таким образом, код аутентификации предназначен не только для обнаружения случайных ошибок в наборах данных, возникающих при их хранении и передаче, как при использовании хэш-функции, но и сигнализации об активных атаках злоумышленника, пытающегося осуществить навязывание ложной информации. Значение имитовставки зависит от секретного, неизвестного злоумышленнику ключа, поэтому злоумышленник не может самостоятельно вычислить контрольное значение имитовставки и тем самым осуществить успешную имитацию или подмену данных.

Из-за не устоявшейся терминологии в различных источниках коды аутентификации сообщений также называются ключевыми функциями хэширования или кодами аутентичности сообщений.

За рубежом данная тема изучалась с 70-х годов XX века и получила особо бурное развитие в последнее время. Был предложен целый ряд подходов построения кодов аутентификации, основанных на зарубежных криптографических алгоритмах, из которых несколько были стандартизированы NIST (National Institute of Standards). Иная ситуация сложилась в нашей стране. Рекомендации ГОСТ 28147-89 о режиме выработки имитовставки, по сути являющемся алгоритмом кода аутентификации, на текущий момент не удовлетворяет требованиям безопасности, так как длина формируемых по нему имитовставок равна 32 бита, и злоумышленник за весьма короткий период времени может реализовать атаку полного перебора. Помимо данного устаревшего алгоритма в России нет стандартов на коды аутентификации, а также нет серьезных исследований по этой теме, за исключением работы [1].

Таким образом, в настоящее время актуальна проблема разработки алгоритма кода аутентификации, основанного на российских криптографических стандартах, и позволяющего строить имитовставки достаточной длины для обеспечения заданного уровня безопасности.

Примеры использования

Сегодня практически любая информационная система использует коды аутентификации. Классическим примером является протокол HTTPS, использующий протокол TLS или SSL для шифрования канала и подтверждения подлинности передаваемых данных с помощью кодов аутентификации.

Другим примером может служить сетевой протокол SSH, позволяющий производить удаленное управление ОС и передачу файлов. Этот протокол схож по функциональности с протоколами Telnet и rlogin, но в отличие от них благодаря использованию криптографических средств обеспечивает конфиденциальность и подлинность передаваемых данных.

Кроме того стандарт сотовой связи GSM использует алгоритм COMP128 для аутентификации пользователей в сети. Для успешной аутентификации пользователю на запрос необходимо предоставить корректную имитовставку.

В связи с тем, что применяемые в данных примерах алгоритмы кодов аутентификации используют зарубежные криптографические алгоритмы, российские организации в соответствии с законодательством РФ не могут применять их в системах, обрабатывающих и/или хранящих информацию, относящуюся к государственной тайне, что безусловно тормозит внедрение подобных передовых технологий в автоматизированные системы на российском рынке.

Зарубежные подходы построения кодов аутентификации

В настоящее время существует два основных подхода построения кодов аутентификации:

– превращение однонаправленной устойчивой к коллизиям хэш-функции в код аутентификации;

– построение кода аутентификации на основе блочного шифрования.

Для каждого подхода был разработан стандартизированный NIST алгоритм кода аутентификации: для первого подхода – алгоритм HMAC (The Keyed-Hash Message Authentication Code), описанный в

стандарте FIPS 198 [2], для второго – CMAC (Cipher Message Autentication Code), описанный в стандарте SP 800-38B [3]. Рассмотрим подробнее два этих подхода и исследуем на возможность их применения для построения кода аутентификации на основе российских криптографических стандартов.

Построение кода аутентификации на основе алгоритма блочного шифрования

В основе данного подхода лежит использование блочного шифра в режиме сцепления блоков шифротекста (режим, при котором каждый последующий блок входного сообщения перед шифрованием складывается операцией XOR с результатом шифрования предыдущего блока). При этом используется секретный ключ, известный отправителю и получателю, и два рабочих ключа, вычисляемых от него. Перед шифрованием последнего блока он складывается операцией XOR с одним из рабочих ключей, в зависимости от того является ли последний блок текста полным либо дополняется нулевыми байтами. Все промежуточные блоки шифрованного текста отбрасываются, а последний берется в качестве имитовставки.

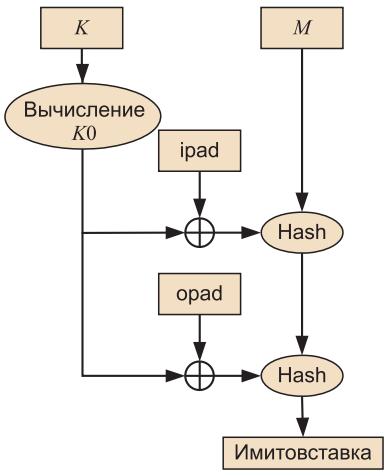

Рис. 1. Алгоритм кода аутентификации на основе хэш-функции

В стандарте SP 800-38B предлагается использовать алгоритма шифрования Advanced Encryption Standard, хотя также может использоваться алгоритм блочного шифрования ГОСТ 28147-89. При такой реализации длина имитовставки будет равна длине выходного блока шифра, то есть 64 бита. С учетом современных вычислительных возможностей злоумышленнику не составит труда реализовать атаку полного перебора. Поэтому данное решение может использоваться только в системах с очень коротким периодом актуальности пар сообщение-имитовставка.

Построение кода аутентификации сообщения на основе хэш-функции

Подход заключается в преобразовании однонаправленной хэш-функции в код аутентификации путем вычисления хэша от сообщения, особым образом дополненного ключом. В стандарте FIPS 198 в качестве хэш-функции предлагается использовать алгоритм SHA-1, однако можно применить и любой другой известный алгоритм однонаправленной функции хэширования, например ГОСТ Р 34.11-94. Таким образом, в алгоритме кода аутентификации HMAC в качестве хэш-функции будет использоваться ГОСТ Р 34.11-94. Ранее совместное использование этих двух алгоритмов не предлагалось и возможность такого совмещения не исследовалась. Опишем реализацию данного алгоритма.

Алгоритм на входе получает секретный ключ K, на основе которого вычисляется ключ K0. Производится проверка равенства длины ключа K длине входного блока хэш-функции (256 бит). Если длина K больше, то для K вычисляется хэш-функция. Если длина секретного ключа меньше длины блока хэш-функции, секретный ключ дополняется нулевыми байтами до необходимого размера входного блока. Полученный ключ K0 считается секретным ключом алгоритма. Далее на основе K0 путем его сложения операцией XOR с двумя константами opad и ipad вырабатываются два рабочих ключа. Имитовставка вычисляется по следующей формуле: $Hash[(K0 \oplus opad)\| Hash((K0 \oplus ipad) \| M)$, где M – входное сообщение, *Hash* – значение хэш-функции, вычисленное по алгоритму ГОСТ Р 34.11-94. На выходе получаем имитовставку длины 256 бит, что в 1,6 раза длиннее, чем для HMAC, построенного на основе хэш-функции SHA-1. Блок-схема работы алгоритма представлена на рис. 1.

В соответствии с результатами, полученными в [4], уровень стойкости алгоритма кода аутентификации, у которого длина ключа t бит, а длина выходной имитовставки m бит, вычисляется как $\min(t, m/2)$. Таким образом, предложенный алгоритм вычисления кода аутентификации с использованием ГОСТ Р 34.11-94 имеет 128-битный уровень стойкости, что на сегодняшнее время считается безопасным (то есть злоумышленнику вычислительно сложно подобрать корректную имитовставку для сообщения или подобрать ключ).

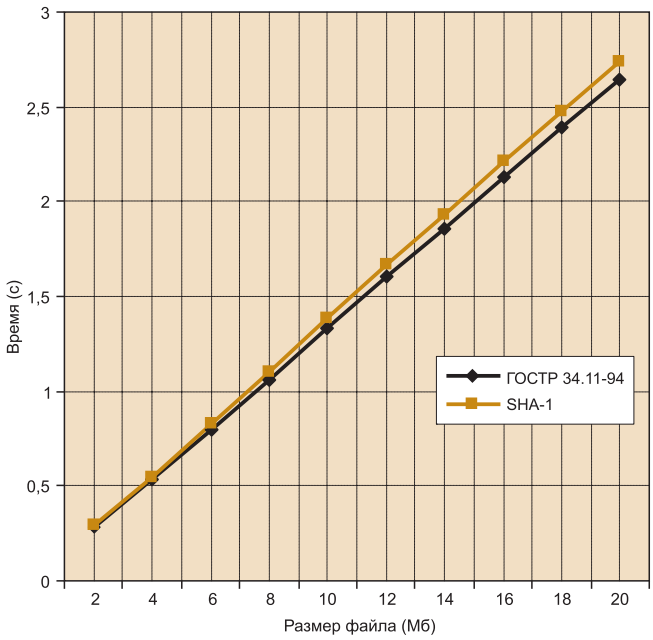

Рис. 2. Результат экспериментов

Программная реализация и оценка эффективности

Предложенный алгоритм был программно реализован и протестирован. Для проведения экспериментов были выбраны несколько файлов различной длины (2...20 Мб). Для каждого файла измерялось время вычисления имитовставок для предложенного алгоритма на основе ГОСТ Р 34.11-94 и зарубежного аналога на основе SHA-1. На рис. 2 приведен график, построенный на основе полученных результатов.

Время вычислений для обоих алгоритмов растет линейно с увеличением размера файла, однако результат предложенного алгоритма, основанного на ГОСТ Р 34.11-94, несколько лучше, что говорит о его эффективности.

Выводы

Предложен новый алгоритм построения кода аутентификации сообщений на основе алгоритма хэш-функции ГОСТ Р 34.11-94, удовлетворяющий современным требованиям и обладающий большим запасом прочности, который в перспективе может лечь в основу российского стандарта кода аутентификации сообщений.

Список литературы

1. *Зубов А.Ю.* Математика кодов аутентификации. М.: Гелиос АРВ. 2007.
2. FIPS PUB 198 (Federal Information Processing Standards Publication) The Keyed-Hash Message Authentication Code (HMAC). http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
3. *Iwata T., Kurosawa K.* OMAC: One-Key CBC MAC. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/omac/omac-spec.pdf
4. *Prenel B., Oorschot P.C.* MDx-MAC and Building Fast MACs from Hash Functions. http://web.cecs.pdx.edu/~teshrim/spring06/papers/macs/preneel95mdxmac.pdf

Билык Татьяна Александровна *– ведущий инженер Главного управления безопасности и защиты информации Банка России,*

Потехонченко Антон Юрьевич *и* ***Дацун Наталья Николаевна*** *– инженеры 1 категории отдела информационной безопасности Главного управления Банка России по Санкт-Петербургу.*

Контактный телефон (926) 527-53-05. E-mail: bilyk-t@yandex.ru

Видеонаблюдение промышленных предприятий: проблемы и их решения

Д.Н. Стрельцов (Mitsubishi Electric)

Указаны трудности, с которыми сталкиваются руководители предприятий и начальники служб безопасности предприятий при создании современных систем наблюдения. Показаны современные возможности систем видеонаблюдения, позволяющие справиться с проблемами.

Ключевые слова: видеонаблюдение, видеорегистратор, IP-технологии, медиаконвертор, гибридные системы, видеосервер.

К сожалению, человеческая природа такова, что без систем наблюдения не может существовать ни одно предприятие. Еще задолго до появления видеокамер люди пытались обезопасить торговые, производственные и складские помещения. Помните, как в комедии А. Гайдая "Операция Ы" выглядел профессиональный костюм сторожа? Ушанка, тулуп, рукавицы, валенки и ружье. Сейчас охранники одеты чаще всего в хороший костюм, а из технических устройств в их ведении находятся видеокамеры. Развитие технологий серьезно изменило систему контроля, но также принесло с собой и множество проблем, решить которые стремится каждый руководитель торгового или производственного предприятия. В данной статье рассмотрим трудности, стоящие перед руководителями предприятий и начальниками служб безопасности при создании современных систем наблюдения, и возможные способы их решения.

Глобальность – это минус? или одеяло для гиганта

Всеобщая глобализация увеличивает масштабы любого явления, в том числе и производственную область деятельности человека. Отходят на задний план, постепенно вымирая, маленькие предприятия – сейчас царит эпоха производственных и торговых сетей федерального уровня. Новые масштабы приносят новые трудности. Одна из главных – охват системой наблюдения всей территории предприятия или сети, которая может включать до нескольких десятков производственных, складских или торговых точек, расположенных в различных городах.

Чтобы "накрыть" всю территорию, необходима функциональная система, способствующая быстрой коммуникации и мгновенному реагированию на происходящее в цехе или на складе предприятия. Не стоит забывать о том, что оборудовать камерами нужно не только прилегающие территории на случай воровства сторонних посетителей, но и внутренние (складские и производственные) помещения компании, чтобы обезопаситься от собственных работников. Такая система называется технологическим видеонаблюдением.

Аналог прошлого

Легко отказаться от прошлого, приняв современные тенденции, могут не все. Касается это и организации видеонаблюдения на предприятиях. До сих пор многие руководители не торопятся менять старое аналоговое видеооборудование на цифровое, используя его для наблюдения. Это глубоко устаревшее оборудование, качество работы которого несравнимо с современными системами, созданными на базе IP-технологий. Качество изображения, скорость переда-