РЕАЛИЗАЦИЯ ЗАЩИЩЕННОЙ ОФИСНОЙ СИСТЕМЫ НА ОСНОВЕ КРИПТОГРАФИИ

Д.С. Калининский, *магистрант*
И.А. Асначев, *студент*
А.Р. Анисимов, *магистрант*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2022-6-1-141-146

Аннотация. *В данной статье описывается реализация защищенной офисной системы на основе криптографии. Реализация использует гибридную схему обычной криптографии DES и криптографии с открытым ключом RSA. Случайно сгенерированные ключи DES шифруют сообщения и файлы, а сами ключи DES и односторонний хэш сообщений шифруются и подписываются ключами RSA. Система обеспечивает защищенную электронную почту (включая электронную заказную почту и электронного нотариуса), защищенные двусторонние каналы и защищенные файлы пользователей. Временные метки и специальный подписанный файл открытых ключей помогают уменьшить потребность в онлайн-центральном органе, участвующем во всех транзакциях.*

Ключевые слова: *ключ, пользователь, система, PKF, файл, RSA, сумма.*

Как упоминалось в предыдущей статье «Разработка алгоритма защищенной описной системы на основе криптографии» «Первоначально пользователи должны дать команду «Newuser» с паролем, который они могут запомнить. «Newuser» требует физического присутствия пользователей в центральном органе, если требуется проверка подлинности, что имя пользователя соответствует конкретному физическому лицу. Для входа в систему необходимо ввести пароль, соответствующий имени пользователя. Сообщения или файлы любого типа могут быть отправлены другим пользователям с помощью команды «SendSecure» и могут быть получены с помощью команды «ReceiveSecure»». Различные методы шифрования, дешифрования, подписи, временные метки и этапы аутентификации встроены в эти команды на более низком уровне, как описано ниже.

Обзор реализации

В дополнение к PWS в данном проекте используется специальный компонент – CR (англ. Cryptoprocessor «Криптопроцессор), для выполнения различных функций шифрования / дешифрования, хранения и генерации ключей, а также для аутентификации пользователей. CR является частью PWS, также используется специальный файл, называемый PKF (англ. Public Key File «Файл открытого ключа»). Эти открытые ключи подписываются сетевым секретным ключом. (PKF также содержит секретный ключ каждого пользователя в зашифрованном виде, как описано ниже.) Чтобы заменить запомнившиеся имя пользователя и пароль для входа в CR, также можно использовать устройство хранения данных, называемое личной картой данных. Конструкция системы позволяет одновременно использовать CR, реализованные как в ОА, так и в программном обеспечении (ПО). Программный CR был бы дешевле, работал бы хуже и обеспечивал бы меньшую безопасность, чем аппаратный. Для производственной системы аппаратный CR может быть сложно модифицировать, и это должно значительно повысить безопасность. На рисунке 1 представлено изображение этих компонентов.

INPUT – вход; PERSONAL WORK STATION (PWS) – персональная рабочая станция; COMMUNICATION NETWORK – коммуникационная сеть; CENTRAL AUTHORITY (A USER) (CA) – центральный орган (пользователь); PUBLIC KEY FILE (READ ONLY) (PKF) – файл открытого ключа (только для чтения); SECURE AREA (WHEN PKF IS UPDATED) – защитная зона (при обновлении PKF).

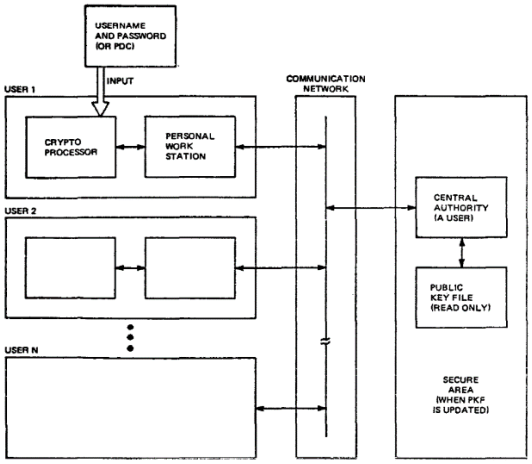

Рис. 1. Системный обзор

Для данной системы было решено использовать DES для основной части шифрования / дешифрования и использовать криптосистему с открытым ключом RSA для обмена ключами и подписями. DES является естественным выбором из-за его скорости при реализации с помощью недорогого специального оборудования. Если DES казался недостаточно безопасным, можно было переключиться на тройное шифрование DES или на какую-либо другую обычную систему. Очевидно, что одного DES было бы достаточно для полной реализации, хотя и с некоторыми значительными сложностями для распределения ключей и подписей. Были включены открытые ключи в гибридную систему, потому что это налагает меньшую нагрузку на центральный орган и обеспечивает большую автономию пользователям, также выбрана схема с открытым ключом RSA из-за симметрии между секретностью и шифрованием подписи в этой системе.

Если RSA когда-нибудь окажется небезопасным, можно переключиться на какую-нибудь другую защищенную систему с открытым ключом. Схема RSA работает медленно даже при использовании специального оборудования, и именно поэтому в данной системе используется гибридный подход. Поскольку цель системы – подписывать целые сообщения или файлы и в то же время применение подписи RSA только к нескольким блокам (для экономии времени шифрования), требуется какая-то односторонняя хэш-функция. Использование DES – для преобразования любого текста в один 64-битный результат, который называется контрольной суммой. Метод проиллюстрирован на рисунке 2. Поскольку используются 64 бита, для оппонента невозможно (при условии, что DES защищен) создать альтернативный текст с той же контрольной суммой, что и данный текст.

PLAIN TEXT PORT (PTP) – порт обычного текста; CHIPHER TEXT PORT (CTP) – порт зашифрованного текста; CHECK-SUM (CS) – контрольная сумма.

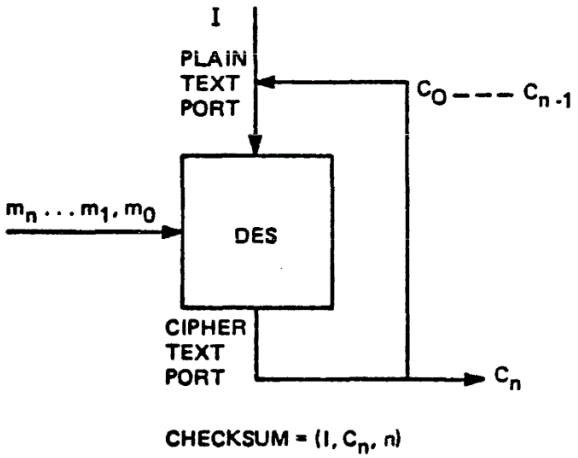

Рис. 2. Вычисление контрольной суммы (I = вектор инициализации, m_o, m_1, … , m_n = 56-битные блоки сообщения, c_o, c_1, ... , C_{n-1} = 64-битные блоки зашифрованного текста)

Открытые ключи RSA всех пользователей хранятся PKF. (Как описано в статье «Криптопроцессор: Аппаратное обеспечение для высокоуровневого набора криптографических команд» К. Мюллера-Шлоера). Этот файл доступен для чтения, за исключением случаев, когда он создан или обновлен CA. CA сначала генерирует одну пару открытого и секретного ключей RSA – PK.N (англ. Network Public Key «Сетевой открытый ключ) и SK.N (англ. Network Secret Key «Сетевой секретный ключ»). Когда пользователь (U) выполняет команду «New user» CA получает «User name», PK.U (англ. User Public Key «Открытый ключ пользователя») и SK.U (англ. User Secret Key «Секретный ключ пользователя), который зашифрован случайным локальным ключом DES (Kloc) и CW (англ. Codeword «Кодовое слово») для восстановления ключа DES. CA формирует CS всего, добавляет TS (англ. Timestamp «Временная метка) и подписывает эти 2 с помощью SK.N. Таким образом, запись PKF выглядит следующим образом:

Username, PK.U, Kloc, CW, {CS, TS}SK.N.

(Здесь < .. , > используется для шифрования DES и { ... } для шифрования RSA) При расшифровке в PK.N точный формат временной метки будет использоваться для аутентификации записи. Пока SK.N остается безопасным, никому не удастся сгенерировать поддельные записи PKF, поскольку расшифрованная CS должна совпадать с CS, сгенерированной из первой части записи. TS - это время, когда была сделана запись, или время, когда была восстановлена запись. Эта TS предотвратит замену старой записи текущей. Время каждой реконструкции PKF должно быть широко распределено; поэтому каждая запись PKF должна быть помечена временем не ранее, чем общая TS. Противник может создать поддельные PK.N и SK.N, а затем создать целую поддельную сеть. Это может быть преодолено путем широкого распространения PK.N. Если доступна карта персональных данных, у каждого пользователя будет своя собственная копия PK.N, предоставленная при регистрации.

Криптопроцессор

Как упоминалось ранее, все криптографические функции данной системы сосредоточены в CP. Первоначально данный компонент был реализован в ПО, но теперь необходимо рассмотреть аппаратную реализацию, совместимой с несколькими шинами, на основе микропроцессора Intel 8086 и чипа Western Digital DES. CP выполняет основные функции шифрования / дешифрования и генерации ключей как для схем DES, так и для схем RSA.

CP предоставляет четко определенный, высокоуровневый, криптоориентированный набор инструкций, который не может быть изменен извне и, следовательно, помогает предотвратить вмешательство злоумышленника. Некоторые конфиденциальные данные, такие как пароли и ключи, хранятся внутри CP, и ими можно управ-

лять только с помощью набора команд CP. (Например, команда «Output Secret Key» не существует) Поскольку генерация ключа RSA на микрокомпьютере происходит относительно медленно, это будет происходить как фоновая активность в CP. CP имеет защищенный раздел памяти STT (англ. Security Status Table «Таблица состояния безопасности». SST в основном заполняется во время входа, используя введенные «User name» и «Password» или, если таковые имеются, аппаратная PDP (англ. Personal Data Card «Карта персональных данных».

Процедурные детали

В данной системе была попытка использовать упрощенные версии стандартных протоколов. В частности, был выбран PKF и TS вместо более сложных протоколов. В большинстве случаев TS в сообщениях, которые отправляются, принимаются и подтверждаются, будут относительно близки по времени, поэтому обе стороны согласуют время сообщения. TS при регистрации или нотариальном заверении, примененные третьей стороной, будут служить для урегулирования любых разногласий. Далее необходимо рассмотреть действия, которые происходят во время входа в систему. Как показано на рисунке 3, запись PKF содержит «User name», PK.U и SK.U, зашифрованный специальным локальным ключом DES (Kloc); и CW, используемое для скрытия Kloc.

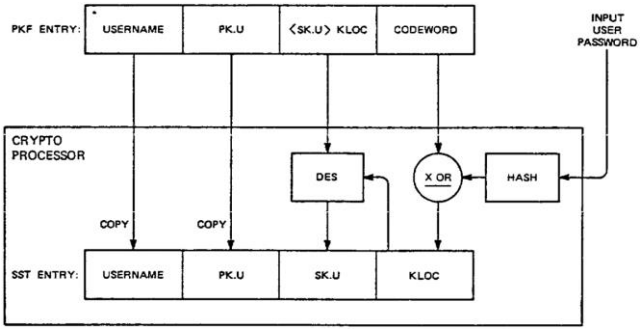

Рис. 3. Использование записи PKF во время входа для инициализации таблицы состояния безопасности CP

Локальный ключ DES представляет собой комбинацию «xor» CW и введенного пароля пользователя (U), поэтому оппонент, имеющий доступ к PKF, не может восстановить Kloc и, следовательно, не может вычислить SK.U. При этом в системе важно, чтобы было разрешение паролей произвольной длины (и поощрялись длинные, легко запоминающиеся), поэтому Kloc формируется сначала с помощью получения CS пароля, а затем ввода CW. Само CW формируется во время команды «New user» путем операции «xor» CS пароля и Kloc. Таким образом:

CW = CS xor Kloc

Где Kloc выбирается случайным образом. Поскольку операция «xor» является самоинверсионной,

Kloc = CS xor CW

В случае использования аппаратной PDC все обрабатывается таким же образом, за исключением того, что информация SST поступает из PDC, а не из PKF. Команда «Sign On» приводит к тому, что PWS временно выделяется пользователю (U), выполняющему операцию. Теперь рассмотрим команду «Send Secure». Пользователь (U) начинается с файла (F) и имени назначения (D). Пользователь (U) генерирует случайный ключ DES (KT) и формирует < F > KT, файл (F), зашифрованный под (KT). Затем пользователь (U) подписывает и шифрует для ключа DES (KT). Наконец, пользователь (U) формирует контрольную сумму (CS1), контрольную сумму всего (CS), что было до этого момента, добавляет временную метку (TS1) и подписывает это. Таким образом:

U - > D, KT, { {KT}SK.U }PK.D, {CS1, TS1}SK.U

Отправляется в (D), где U - > D служит в качестве информации о маршрутизации в открытом виде. В случае, если файл направляется через некого нотариуса (N),

который формирует контрольную сумму (CS2), контрольную сумма всего (CS), добавляет временную метку (TS2) и подписывает результат. Нотариус (N) также может восстановить контрольную сумму (CS1) и проверить, что это CS < F > KT. Таким образом, нотариус (N) добавляет:

{CS2, TS2}SK.N

Наконец, получатель (D) может подтвердить, сформировав контрольную сумму (CS3), контрольную сумму всего полученного (CS), и подписав и зашифровав это для пользователя (U) (вместе с новой временной меткой TS3). Таким образом, пользователь (U) получает обратно то, что добавил нотариус:

{ {CS3, TS3}SK.D }PK.U.

Конечно, нет никакой необходимости в том, чтобы получатель (D) отправлял обратно то, что пользователь (U) первоначально отправил. Нотариус (N) сохранит копию того, что он добавил, но не оригинального зашифрованного файла. Таким образом, весь трафик имеет относительно небольшой размер, за исключением самого зашифрованного файла. Когда открывается защищенный двусторонний канал, результатом является то, что общий ключ DES находится в SST станций связи. Для распределения ключей используется шифрование с открытым ключом. Система защиты файлов использует локальный ключ DES (Kloc) для шифрования / дешифрования файлов.

Заключение

В данной статье была описана реализация система защищенной связи для сети персональных рабочих станций (PWS). Лежащие в основе криптографические механизмы гарантируют высокий уровень безопасности, но при этом полностью прозрачны для пользователя. Функциональность соответствует современным процедурам защиты бумажной почты. Ограничение обработки, связанной с безопасностью, одним аппаратным устройством (криптопроцессором (CR) с четко определенным набором команд высокого уровня обеспечивает более высокую скорость и лучшую защиту чувствительных областей. Использование криптографии с открытым ключом ограничивает потребность в сильно вовлеченном центральном органе. Кроме публикации одного открытого сетевого ключа (PK.N), предварительное распределение ключей не требуется. Пользователи не ограничены своей собственной рабочей станцией, но им гарантирована полная мобильность в сети.

Библиографический список

1. Теренин, А. А. Безопасность офиса коммерческого предприятия // Национальные интересы: приоритеты и безопасность. – 2007. – Т. 3. – № 2 (11). – С. 74-80. – EDN HWIIYZ.

2. Бабенко, Л.К. Новые технологии электронного бизнеса и безопасности / Л.К. Бабенко, В.А. Быков, О.Б. Макаревич, и др. – М.: Радио и связь, 2018. – 376 с.

3. Блэк, У. Интернет: протоколы безопасности. Учебный курс. – М.: СПб: Питер, 2017. – 288 с.

4. Брэгг, Р. Безопасность сетей: полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М.: Эком, 2006. – 912 с.

IMPLEMENTATION OF A SECURE OFFICE SYSTEM BASED ON CRYPTOGRAPHY

D.S. Kalininsky, *Graduate Student*
I.A. Asnachev, *Student*
A.R. Anisimov, *Graduate Student*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *This article describes the implementation of a secure office system based on cryptography. The implementation uses a hybrid scheme of conventional DES cryptography and RSA public key cryptography. Randomly generated DES keys encrypt messages and files, and the DES keys themselves and the one-way hash of messages are encrypted and signed with RSA keys. The system provides secure e-mail (including registered e-mail and electronic notary), secure two-way channels and protected user files. Timestamps and a special signed public key file help reduce the need for an online central authority involved in all transactions.*

Keywords: *key, user, system, PCF, file, RSA, summ.*