РАЗРАБОТКА АЛГОРИТМА ЗАЩИЩЕННОЙ ОФИСНОЙ СИСТЕМЫ НА ОСНОВЕ КРИПТОГРАФИИ

Д.С. Калининский, *магистрант*
В.Н. Сурков, *студент*
Н.В. Горнаева, *студент*
Московский технический университет связи и информатики
(Россия, г. Москва)

DOI:10.24412/2500-1000-2022-6-1-147-149

Аннотация. *В данной статье производится разработка алгоритма защищенной офисной системы на основе криптографии, включая ее полное функциональное описание, состояние из 14 пунктов. Система должна быть практичной, простой и недорогой, но в то же время очень безопасной, а также ее базовый дизайн должен быть доступен любому пользователю (от одного до нескольких тысяч), а аппаратное обеспечение может быть распределено.*

Ключевые слова: *пользователь, имя, ввод, файл, результат, система.*

В данной статье разрабатывается защищенная система обработки данных для офиса или аналогичной организации. Базовый дизайн должен быть доступен любому количеству пользователей (от одного до нескольких тысяч), а аппаратное обеспечение может быть распределено. Разрабатываемая система должна быть практичной, простой и недорогой, базовый метод реализации которой прозрачен для пользователей. Однако главной целью проектирования была безопасность. Также необходимо ограничить потребность в онлайновом (то есть «постоянно присутствующем») центральном органе или центре сертификации. Необходимо визуализировать, что каждый пользователь имеет доступ к PWS (англ. Personal workstation «Персональная рабочая станция»), то есть станции с локальной вычислительной мощностью. Во время использования аппаратного обеспечения каждого PWS будет считаться защищенным, но безопасность не предполагается для соединений между PWS или для отдельного PWS, когда он не используется. Пользователи не ограничены одним PWS, но могут войти в систему в любое удобное время. Описанная система предназначена в качестве дополнения к функциям, обычно предоставляемым операционными системами и сетевыми менеджерами. Система будет обеспечивать следующие основные функции:

1) Защищенная электронная почта, включая электронную заказную почту и электронного нотариуса (одного или несколько пользователей, которые могут подтвердить подлинность подписи, указать временную метку и сохранить копию сообщения);

2) Защищенные каналы двусторонней связи (для обеспечения мгновенного интерактивного диалога);

3) Защищенная файловая система пользователя, такая как безопасная распределенная система требует некоторого использования криптографии. Чтобы достигнуть простоты и низкой стоимости наряду с высокой безопасностью и простотой использования необходимо использовать гибридную систему обычной криптографии и криптографии с открытым ключом.

Функциональное описание

Для начала необходимо перечислить команды, связанные с безопасностью на уровне пользователя, подавляя другие команды, необходимые для системы электронной почты, такие как «SearchMailbox» и т.д. Команды не зависят от конкретной формы реализации (будь то обычная, с открытым ключом или гибридная, как в данной системе), и пользователю не нужно ничего знать о криптографии.

1) Вход в систему (SignOn):

Ввод: Имя пользователя (username), пароль (password).

Результат: Аутентификация пользователя с помощью пароля, инициализация PWS и выделение пользователю.

2) Выход (SignOff):

Ввод: Нет (none).

Результат: Деинициализация PWS путем перезаписи чувствительных областей и ключей и т.д.

3) Регистрация нового пользователя (NewUserRegistration):

Ввод: Имя пользователя (username), пароль (password).

Результат: Регистрация нового пользователя в системе с паролем в качестве средства последующей аутентификации.

4) Обновление публичного ключа (UpdatePublicKey):

Ввод: Имя пользователя (username), пароль (password).

Результат: Замена старой пары открытого и секретного ключей на новую.

5. Обновление пароля (UpdatePassword):

Ввод: Имя пользователя (username), новый пароль (new password), старый пароль (old password);

Результат: Замена старого пароля на новый.

6. Безопасная отправка (SendSecure):

Ввод: Имя получателя (destination-name), файл сообщения (message File).

Необязательный ввод: Имя промежуточного получателя (intermediate-destination name), запрос на регистрацию (request to register) или электронная подпись (notarize).

Результат: Пометка файла сообщения временем, электронная подпись и зашифровка для пользователя, чье имя является именем назначения. В случае необязательного ввода – в первую очередь, перенаправление файла на промежуточное имя получателя для регистрации или электронную подпись.

7) Безопасное получение (ReceiveSecure):

Ввод: Имя отправителя (sender-name);

Результат: Расшифровка и аутентификация файла отправителя.

8) Регистрация (Register):

Ввод: Имя отправителя (sender-name), зашифрованный файл (encrypted file).

Результат: Пометка файла временем, подписание и отправка.

9. Электронная подпись (Notarize):

Ввод: Имя получателя (destination-name), зашифрованный файл (encrypted file).

Результат: Пометка файла временной меткой, подписание, и сохранение копии перед пересылкой.

10) Подтверждение безопасности (AcknowledgeSecure):

Ввод: Имя отправителя (sender-name), зашифрованный файл (Encrypted file).

Результат: Пометка файла временной меткой, подписание и отправка обратно отправителю. Это для использования с заказной почтой.

11) Безопасное открытие (OpenSecure):

Ввод: Имя получателя (destination-name).

Результат: Создание безопасного канала для немедленного интерактивного использования.

12. Безопасное закрытие (CloseSecure):

Ввод: Имя получателя (destination-name).

Результат: Закрытие защищенного канала.

13. Сохранение безопасности (SaveSecure):

Ввод: Имя файла (file name).

Результат: Сохранение файла в массовом хранилище пользователя безопасным способом.

14) Восстановление безопасности (RestoreSecure):

Ввод: Имя файла (file name).

Результат: Расшифровка сохраненного зашифрованного файла.

Первоначально пользователи должны дать команду «New user» с паролем, который они могут запомнить. «New user» 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 «Send Secure» и могут быть получены с помощью команды «Receive Secure».

Заключение

В данной статье разработан алгоритм защищенной офисной системы на основе криптографии, который включает в себя постановку задачи и функциональное описание. Дальнейшее работа заключается в том, чтобы сделать реализацию данной системы, которая будет описана в следующей статье.

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.

5. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. – М.: ИНФРА-М, 2014. – 368 с.

DEVELOPMENT OF AN ALGORITHM FOR A SECURE OFFICE SYSTEM BASED ON CRYPTOGRAPHY

D.S. Kalininsky, *Graduate Student*
V.N. Surkov, *Student*
N.V. Gornaeva, *Student*
Moscow Technical University of Communications and Informatics
(Russia, Moscow)

Abstract. *This article develops an algorithm for a secure office system based on cryptography, including its full functional description, a state of 14 points. The system should be practical, simple and inexpensive, but at the same time very secure, and its basic design should be accessible to any user (from one to several thousand), and the hardware can be distributed.*

Keywords*: user, name, input, file, result, system.*