ЗАЩИТА ПОЧТОВЫХ СООБЩЕНИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Перцев И.Ю.

Прохорчик Р.В. – м-р. техн. наук, ассистент

Рассмотрены современные подходы к защите почтовых сообщений от несанкционированного доступа, их недостатки. В качестве альтернативного метода предложена схема системы защиты, не требующая существенных затрат на установку дорогостоящего программного обеспечения (ПО) и покупки специализированных устройств защиты данных.

Электронный документооборот является неотъемлемой частью современного мира. Бухгалтерские данные, договоры и прочие документы передаются по электронной почте. При этом пользователь не задумается о том, что большинство популярных почтовых сервисов не обеспечивают полную конфиденциальность этих данных. Вся почтовая переписка может быть получена множеством способов, начиная от запроса правоохранительных органов, и заканчивая перехватом почтовых соединений. Можно выделить 2 варианта решения данной проблемы:

использование в компании собственных почтовых серверов;

шифрование текста писем и документов перед отправкой адресату.

Использование собственных почтовых серверов актуально для крупных компаний, т.к. установка и поддержка почтового сервера требует значительных затрат со стороны компании, что трудноосуществимо для небольшой компании. В свою очередь, шифрование текста письма и документов перед отправкой адресату не влечет за собой дополнительных затрат на установку специализированных устройств и настройки ПО. Однако каждый раз перед отправкой сообщения, пользовать должен провести шифрование данных, что требует установки специализированного ПО и на стороне отправителя, и на стороне получателя. Также не следует забывать о человеческом факторе – пользователь может просто забыть зашифровать сообщение или посчитать это ненужным.

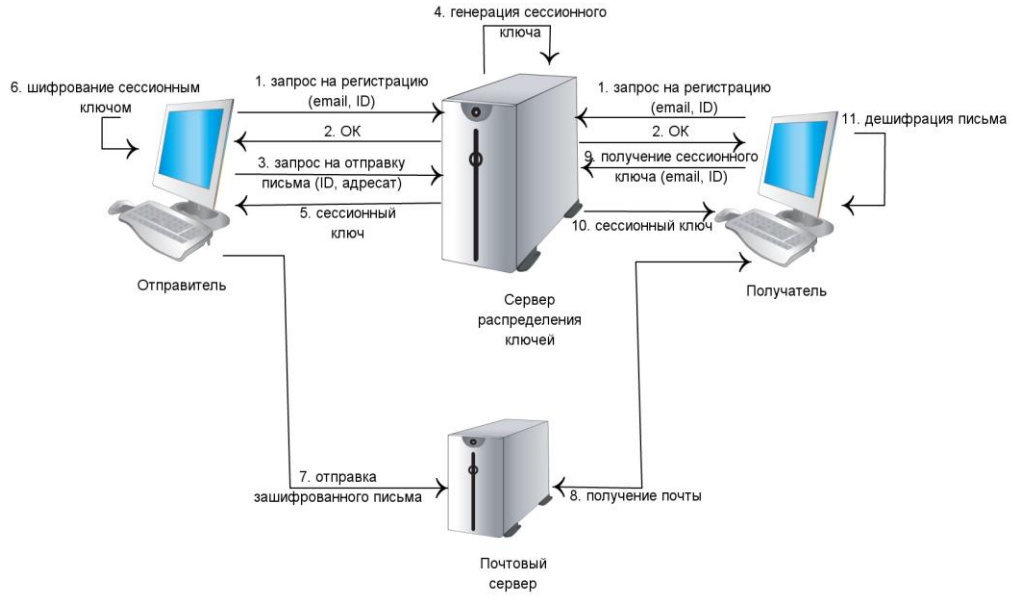

Рис. 1 – Схема взаимодействия элементов системы

В качестве альтернативы рассмотренным методам предлагается использование плагина для почтового клиента, осуществляющего шифрование данных перед отправкой письма адресату. При этом пользователю (или системному администратору) необходимо один раз провести настройку с указанием используемого алгоритма и политики шифрования. Политика шифрования включает в себя набор правил, которые определяют, какие письма должны быть зашифрованы. Дешифрации таких писем осуществляется этим же плагином на стороне адресата при получении новой почты.

Для управления ключами вводится сервер распределения ключей шифрования (рисунок 1). Отправитель и потенциальный получатель (абоненты) должны пройти регистрацию, в процессе которой предоставить на сервер некоторый уникальный идентификатор (например, MAC-адрес) и электронную

почту. Отправка писем с использованием сервера возможна только после подтверждения регистрации администратором. При отправке сообщения, отправитель осуществляет запрос на сервер для получения ключа, сервер проверяет его права. В случае, если пользователь заблокирован или отсутствует шифрование данных не происходит, иначе сервер генерирует ключ, сохраняет его у себя и передает копию отправителю. Отправитель с помощью полученного ключа шифрует сообщение и передает его получателю. Получатель, в свою очередь, осуществляет авторизацию на сервере с помощью уникального идентификатора и передает на сервер почтовый адрес отправителя письма. Сервер ищет в базе совпадение адресов отправителя и получателя и возвращает ранее сгенерированный ключ. После этого получатель может осуществить дешифровку сообщения.

Предложенный метод защиты почтовых сообщений позволяет избежать ряда проблем, выделенных для предыдущих методик: отсутствие дополнительной аппаратуры, отсутствие человеческого фактора. После установки плагина и его первоначальной настройки он работает в автоматическом режиме, шифруя все письма, удовлетворяющие заданным политикам шифрования. Следует отметить, что плагин позволяет запретить изменение настроек для отдельных пользователей, что позволит избежать случайное изменение настроек неопытным пользователем.

В дальнейшем планируется реализовать возможность сокрытия сессионного ключа в теле зашифрованного письма. Это позволит избежать использования сервера распределения ключей и, таким образом, повысить безопасность системы.

Список использованных источников:

1. Шаньгин, В. Защита информации в компьютерных системах и сетях / В. Шаньгин. — Москва, 2012. — 592 с.
2. Stallings, W. Computer Security: Principles and Practice / W. Stallings, L. Brown. — Prentice Hall, 2011. – 816 p.
3. Ciampa, M. Security+ Guide to Network Security Fundamentals / M.Ciampa. — Cengage Learning, 2011. – 656 p.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шелкович А. А.

Бахтизин В. В. – канд. техн. наук, доцент

Качество современного мобильного приложения является одной из его важнейших характеристик. Создание качественного мобильного приложения невозможно без построения системы управления качеством и следования соответствующим международным стандартам. В этой связи большой интерес представляют исследования о области контроля, обеспечения и оценки качества мобильных приложений.

Развитие и распространение мобильных технологий позволило обеспечить доступ к информационным ресурсам повсеместно и в любой момент времени, а техническое совершенствование мобильных устройств сделало возможным их применение для решения широкого круга деловых, практических и ежедневных задач. Развитие глобального рынка мобильных приложений привело к появлению огромного количество продуктов, значительная часть из которых предназначена для решения сходного круга задач и обладает похожей функциональностью. В данных условиях качество мобильного приложения является не только сферой теоретического интереса, но так же определяет возможность практического применения приложения в той или иной ситуации, обеспечивает конкурентоспособность и успех продукта на рынке.

Процессы управления качеством проектов по разработке мобильных приложений должны охватывать все операции, осуществляемые разработчиком с целью определения политики, целей и ответственности в области качества для обеспечения соответствия проекта и программных продуктов предъявляемым к ним требованиям. Основная цель системы управления качеством – создание условий для постоянного улучшения каждого из производственных процессов, взаимное взаимодействие которых приводит к более совершенной системе и, как следствие, и производству более качественных мобильных приложений.

Управление качеством проекта направлено как на управление качественными состояниями самого проекта, так и на качество результата проекта – мобильного приложения. Можно выделить три основных процесса, которые лежат в основе системы управления качеством:

– процесс планирования качества: определение требований и/или стандартов качества, относящиеся к проекту и продукту; документирование, каким образом будет продемонстрировано достигнутое им соответствие;

– процесс обеспечения качества: проверка соблюдения требований к качеству и результатов измерений в процессе контроля качества для обеспечения использования советующих стандартов качества и мер качества;

– процесс контроля качества – мониторинг контрольных точек процессов разработки, направленный на обеспечение качества, оценку исполнения и выработку рекомендаций относительно необходимых изменений.