УДК:004.7

Раунды шифрования протокола HTTPS

Мартынов Е.И., Госуниверситет – УНПК, гр.11-ИК

HTTPS(HyperText Transfer Protocol Secure) - это расширение протокола HTTP, поддерживающее шифрование. Данные, которые передаются по протоколу HTTP, «упаковываются» в криптографический протокол SSL или TSL. HTTPS по умолчанию использует TCP-порт 433. При выполнении запроса браузера к веб-сайту, этот запрос проходит через множество различных сетей, которые могут быть использованы для вмешательства в установленное соединение.

Запросы, как правило, передаются посредством протокола HTTP, в котором и запрос клиента, и ответ сервера передаются в открытом виде.HTTP не использует шифрование по умолчанию, т.к:

•Требуется передавать больше данных

•Невозможно использовать кеширование

•Необходимо использовать больше вычислительной мощности

Когда по каналу передается какая-либо важная информация, которая не должна дойти до злоумышленника, прибегают к использованию HTTPS.

Чтобы подготовить веб-сервер для обработки https-соединений, администратор должен получить и установить в систему сертификат для этого веб-сервера. Сертификат состоит из 2 ключей — public и private. Старые версии браузеров используют ключи длиной 40 бит. Однако ключ с такой длиной является ненадежным, поэтому новые версии браузеров поддерживают шифрование с длиной ключа 128 бит, что значительно уменьшает риск «прослушивания» передаваемой информации. Открытый ключ необходим для шифрования трафика от клиента к серверу в защищённом соединении. Закрытый же служит для расшифровки переданного трафика. После генерации открытого и закрытого ключей, на основе первого происходит аутентификация.

Аутентификация – это проверка подлинности предъявленного

пользователем идентификатора. Положительным результатом аутентификации (кроме установления доверительных отношений и выработки сессионного ключа) является авторизация пользователя, т. е. предоставление ему прав доступа к ресурсам, определенным для выполнения его задач. Механизмы аутентификации с применением цифровых сертификатов, как правило, используют протокол с запросом и ответом. Сервер аутентификации отправляет пользователю последовательность символов, так называемый запрос. В качестве ответа выступает запрос сервера аутентификации, подписанный с помощью закрытого ключа пользователя.

Цифровой сертификат - выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов.

Сертификат открытого ключа содержит имя субъекта, открытый ключ и другие параметры, заверенные подписью удостоверяющего центра. Сертификат атрибутов удостоверяет не открытый ключ субъекта, а какие-либо его атрибуты — принадлежность к какой-либо группе, роль, полномочия и т.п.

Вывод: На данный момент, HTTPS широко используется для защиты информации от перехвата и поддерживается всеми популярными браузерами, что безусловно говорит о его значимости.

Список литературы

1. Простым языком о HTTP [Электронный ресурс] // URL : http://habrahabr.ru/post/215117/ (дата обращения 15.03.14)

2. Как HTTPS обеспечивает безопасность соединения. 29 июля 2013. [Электронный ресурс] // URL: http://habrahabr.ru/post/188042/ (дата обращения 15.03.14)

3. Аутентификация в Интернете [Электронный ресурс] // URL: http://ru.wikipedia.org/wiki/Аутентификация в Интернете

4. HTTPS [Электронный ресурс] // URL: http://ru.wikipedia.org/wiki/HTTPS (дата обращения 15.03.14)