УДК 004.7

ОСОБЕННОСТИ РАБОТЫ ПРОТОКОЛА TLS/SSL

Г. А. Муратов
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Проблемы безопасности персональных данных в интернете остаются одними из самых важных в настоящее время. В статье рассматриваются протоколы шифрования TLS/SSL, структура работы шифрования соединения между клиентом и сервером, показана разница между HTTP и HTTPS, TLS2.0 и TLS3.0. Рассказано, как обезопасить браузер FireFox и ОС Windows 10 от использования старых протоколов шифрования.

Ключевые слова: протокол HTTPS, протоколы шифрования TLS/SSL, Microsoft Windows, FireFox, информационная безопасность, интернет, персональные данные.

TLS/SSL PROTOCOL FEATURES

G. A. Muratov
Don State Technical University (Rostov-on-Don, Russian Federation)

The security of personal data on the Internet remains one of the most important issues at the present time. The article discusses the TLS/SSL encryption protocols, the difference between HTTP and HTTPS, the structure of the encryption of the connection between the client and the server and the difference between TLS2. 0 and TLS3. 0. The paper shows how to protect the FireFox browser and Windows 10 from using old encryption protocols.

Keywords: HTTPS protocol, TLS/SSL encryption protocols, Microsoft Windows, FireFox, information security, Internet, personal data.

Введение. На сегодняшний день для большей части людей пользование интернетом сводится к просмотру веб-страниц, для загрузки которых браузерами применяется протокол HTTP (HyperText Transfer Protocol — протокол передачи гипертекста). Изначально он разрабатывался для передачи гипертекстовых документов, содержащих ссылки, благодаря которым можно было осуществить переход к прочим документам. В настоящее время HTTP является одним из самых распространённых протоколов в интернете.

Данный протокол относится к прикладному уровню модели OSI и, соответственно, использует клиент-серверную архитектуру при передаче данных. Важно при этом, что HTTP отправляет и принимает данные в виде открытого текста. Это значит, что при обращении пользователя к сайту, который использует HTTP, любой человек или устройства, «прослушивающие» сеть, могут видеть абсолютно всё, что передаётся между браузером и сервером, включая логины, пароли, личные сообщения и т. д. На данный момент протокол HTTP в большинстве сайтов не используется без механизма шифрования, что обеспечивает повышенную надежность сайта. Такой механизм передачи данных по защищенному соединению называется HTTPS. Цель данной статьи — показать, каким образом защищаются персональные данные и конфиденциальная информация в процессе серфинга в интернете.

Протокол HTTPS. Протокол HTTPS — это безопасный вариант HTTP, который также применяется в интернете для передачи веб-страниц [1]. В нём для обеспечения безопасной передачи данных на нижележащих уровнях модели OSI применяются криптографические протоколы SSL/TLS (рис. 1) [2].

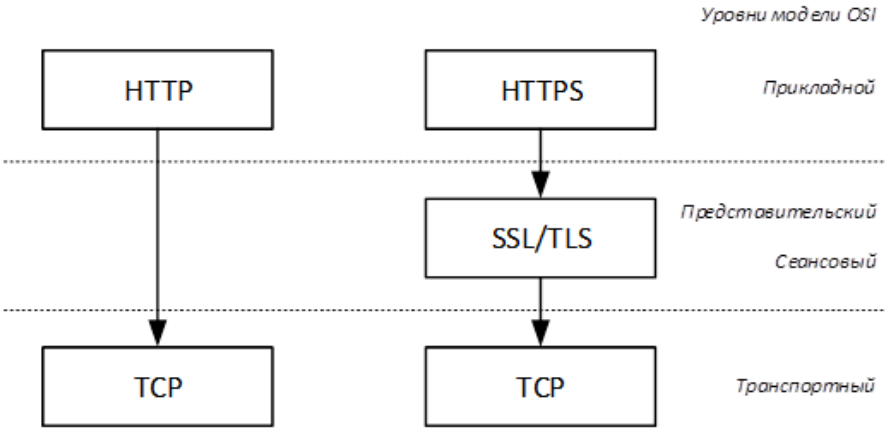

Рис. 1. Сравнение протоколов HTTP и HTTPS

Протокол TLS (Transport Layer Security) считается более современной версией протокола SSL (Secure Socket Layer) [3–4]. Он работает аналогично с SSL, используя шифрование для защиты передачи данных и информации. Эти два термина часто используются взаимозаменяемо в отрасли, однако SSL все ещё широко распространен. Например, когда покупается сертификат SSL, его можно использовать как с протоколом SSL, так и с протоколом TLS.

Для аутентификации в данных протоколах используются асимметричные алгоритмы шифрования (открытый ключ — закрытый ключ), а для сохранения конфиденциальности — симметричные (с одним, секретным, ключом), также используются и сеансовые ключи, которые необходимы для каждого отдельного уникального защищенного сеанса.

Для симметричного алгоритма характерна достаточно высокая скорость обработки данных, в то время как асимметричная криптография связана со сложными математическими проблемами и поэтому требует много вычислительных ресурсов, что замедляет обработку данных, но повышает безопасность.

В соответствии с протоколом TLS, при обращении браузера к защищенному сайту происходит процедура «рукопожатия» SSL/TLS (рис. 2) [5].

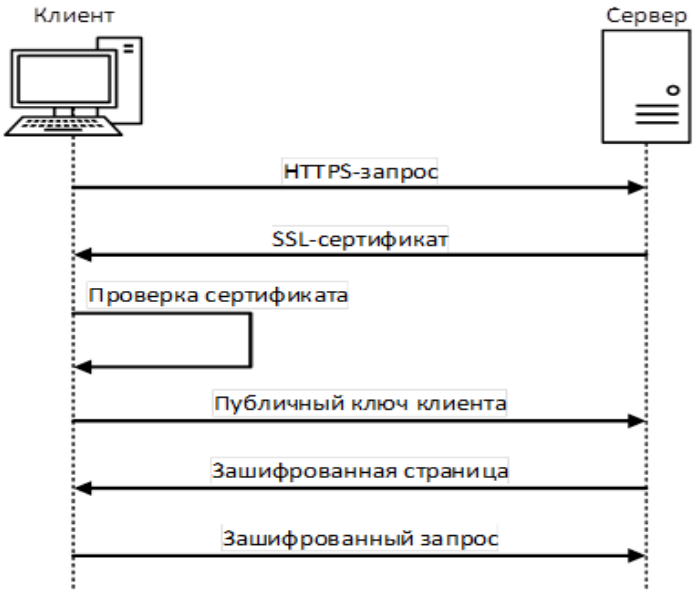

Рис. 2. Схема выполнения процедуры «рукопожатия» в протоколе TLS

«Рукопожатием» называют процесс согласования ключа сеанса, он заложен в основе протокола SSL/TLS. Рассмотрим его последовательность:

1. Клиент отправляет запрос на безопасное соединение с сервером. Он отвечает списком, где перечислен набор поддерживаемых шифров и алгоритмов для создания защищенных соединений, которые будут зашифрованы. Клиент сравнивает полученный список со своим списком поддерживаемых алгоритмов шифрования и выбирает один из них. Затем даёт понять серверу, какой конкретно алгоритм будут использовать при дальнейшей связи.

2. Сервер предоставляет цифровой сертификат, который подтверждает подлинность сервера. Сертификаты содержат открытый криптографический ключ сервера. Как только клиент получает сертификат, он производит его проверку, процедура которой будет рассмотрена далее.

3. Используя открытый ключ сервера, клиент и сервер устанавливают ключ сеанса, который оба будут использовать для последующей части сеанса и для шифрования соединения. После завершения сессии ключ удаляется, процедура повторяется с последующими подключениями к серверу.

Процедура «рукопожатия» будет повторяться с каждым новым соединением с сервером, согласовывая новые сеансовые ключи шифрования.

Как включить TLS 1.3 в Windows 10 [6]. Считается, что версия TLS 1.2 не так хорошо настроена, как версия 1.3, что делает её более уязвимой к атакам. TLS 1.3 удаляет устаревшие и небезопасные функции из предыдущей версии: SHA-1, RC4, DES, 3DES, AES-CBS и MD5 [7]. Новая версия стала чуть защищенней. Рекомендуется использовать её:

1. Сочетаниями клавиш Win + R вызвать командную строку.

2. Ввести inetcpl.cpl и нажать Enter.

3. Появится окно свойств интернета, в нем нужно перейти во вкладку «дополнительно» и в разделе «безопасность» поставить галочку «использовать TLS 1.3» (рис. 3)

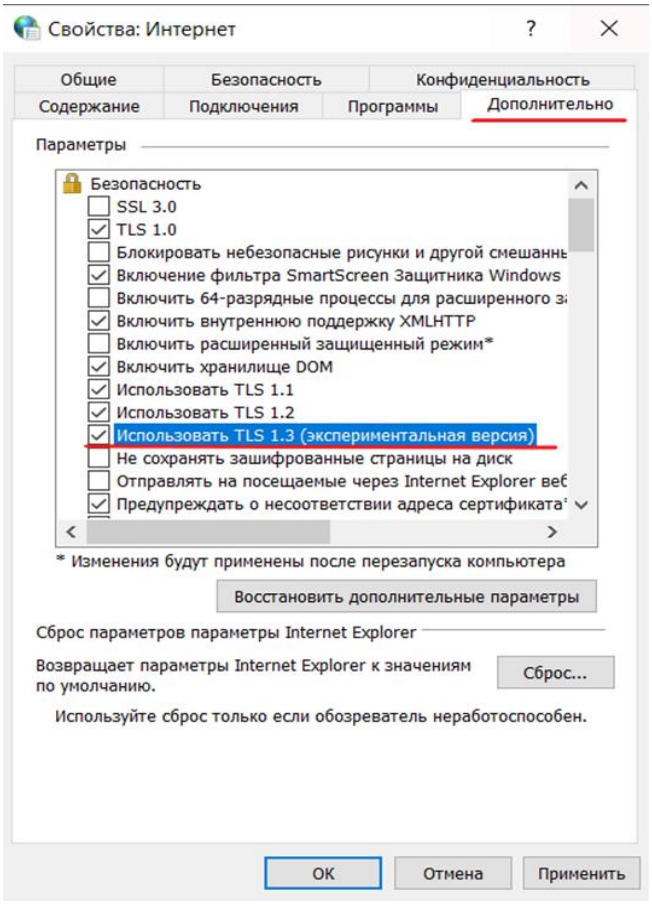

Рис. 3. Окно свойств интернета

В браузере Firefox делается так:

1. Запустив браузер, ввести в адресной строке about:config, нажать Enter.
2. В строку поиска вписать security.tls.version.max flag.
3. Нажать на «+» и проверить значение. Должно быть true (рис. 4).

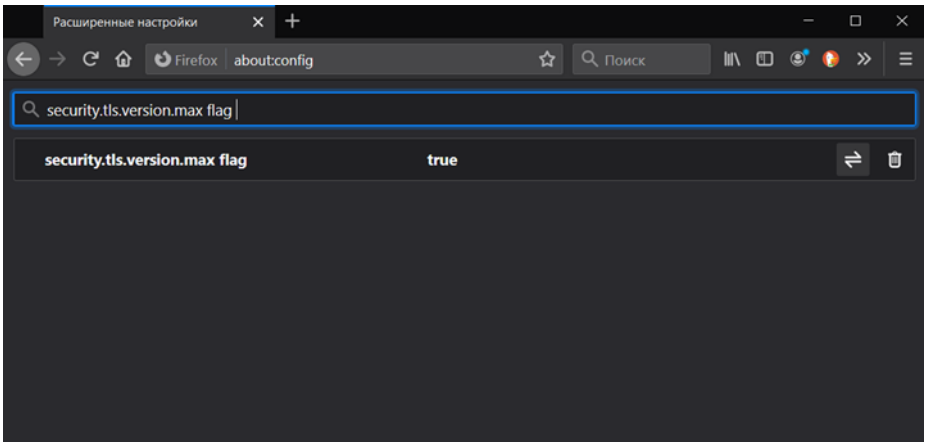

Рис. 4. Браузер Firefox

Заключение. Чтобы персональные данные и любая конфиденциальная информация были более защищены в процессе серфинга в интернете, нужно знать, какие протоколы шифрования использует сайт. HTTPS уже стал стандартным протоколом, но это не означает, что любой сайт его использует. Простую проверку протокола соединения с сервером рекомендуется проводить регулярно во всех источниках.

Библиографический список

1. Простым языком об HTTP // Хабр : [сайт]. — URL: https://habr.com/ru/post/215117/ (дата обращения: 10.12.2020).

2. OSI и ее протоколы. Часть 3 // Компьютерная газета A-Z : [сайт]. — URL: https://nestor.minsk.by/kg/2007/08/kg70811.html (дата обращения: 10.12.2020.)

3. Протокол TLS // Microsoft. Docs : [сайт]. — URL: https://docs.microsoft.com/ru-ru/windows-server/security/tls/transport-layer-security-protocol (дата обращения: 10.12.2020).

4. Browsers end support for TLS 1.0 and 1.1 in March 2020 // GoDaddy. Available from: https://www.godaddy.com/garage/browser-support-tls-10-11 (accessed: 10.12.2020).

5. Что такое TLS-рукопожатие, и как оно устроено // Tproger : [сайт]. — URL: https://tproger.ru/articles/tls-handshake-explained/ (дата обращения: 10.12.2020).

6. Анонимность // SPY-SOFT.NET : [сайт]. — URL: https://spy-soft.net (дата обращения: 10.12.2020).

7. Transport Layer Security Adoption // Wikipedia. Available from: https://en.wikipedia.org/wiki/Transport_Layer_Security Adoption (accessed: 10.12.2020).

Об авторе:

Муратов Григорий Александрович, студент факультета «Энергетика и нефтегазопромышленность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), qwerty2104@list.ru

Author:

Muratov, Grigoriy A., Student, Faculty of Energy and Oil and Gas Industry, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), qwerty2104@list.ru