ЧТО ТАКОЕ БЕЗОПАСНОСТЬ ТРАНСПОРТНОГО УРОВНЯ?

Джон Вагнон (John Wagnon), старший разработчик решений F5 Networks, США

Протокол TLS обеспечивает конфиденциальность и защиту при обмене данными между двумя устройствами.

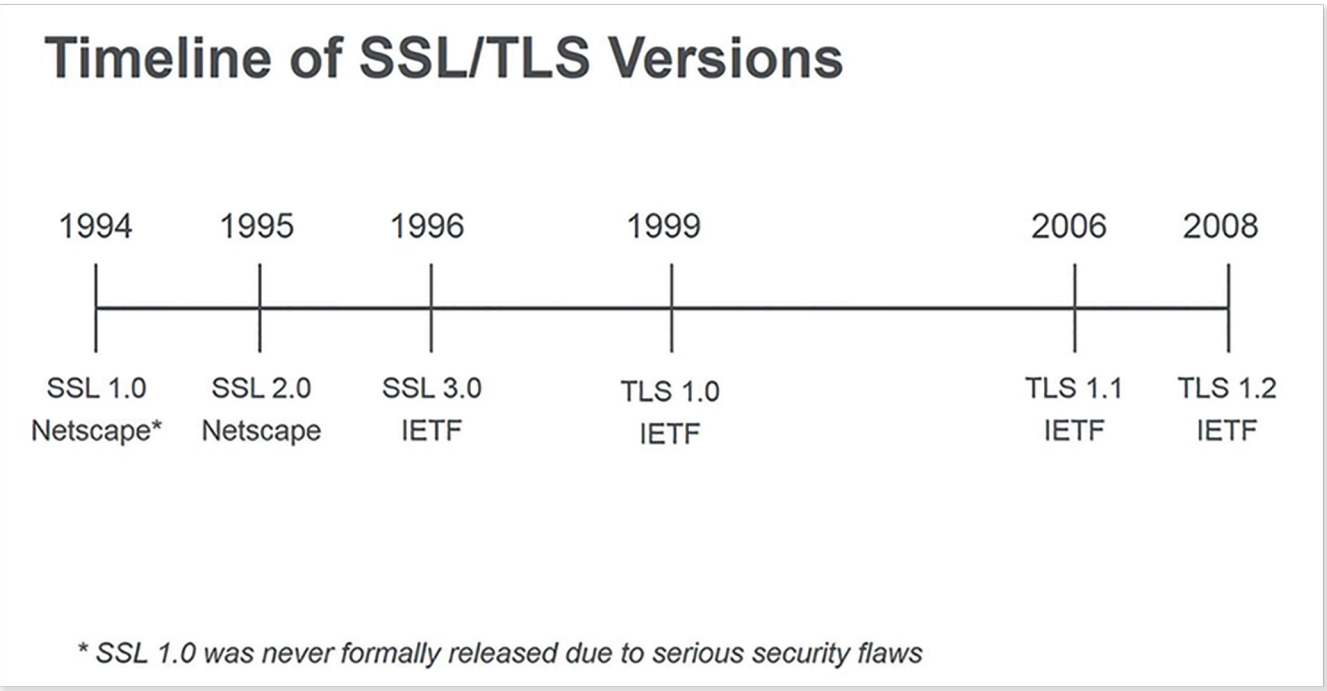
В современном мире пользователи и веб-приложения нуждаются в средствах безопасного взаимодействия. Например, посетив сайт банка чтобы проверить остаток на счету, хочется верить, что это было безопасно. TLS является протоколом, который обеспечивает конфиденциальность и защиту при обмене данными между двумя приложениями. Он определяет точные методы, действия и т. д., которые должны использовать взаимодействующие устройства для обеспечения безопасного обмена данными.

Если 10 людей поодиночке попробуют найти способ безопасного обмена данными между браузером и сервером, то, скорее всего, придумают 10 различных способов. Чтобы избежать этого, собирается группа людей и разрабатывает протокол, в котором точно указано, как именно браузер и сервер выполняют безопасный обмен данными. Неважно, какой браузер и ПО на сервере при этом используется – набор правил для всех есть один.

Данный протокол фактически был создан еще в 1994 году компанией Netscape. Ее инженеры разработали протокол Secure Sockets Layer (SSL) версии 1.0. Но он никогда не использовался, потому что у него было много серьезных проблем с безопасностью. Спустя год (в 1995-м), Netscape выпустила протокол SSLv2, который использовался в течение 12 месяцев. Вот тогда рабочая группа Internet Engineering Task Force (IETF) разработала протокол SSLv3, так как SSLv2 также изобиловал проблемами с безопасностью. Протокол SSLv3 использовался в течение трех лет, а в 1999 году IETF выпустила его следующую версию под названием TLS 1.0. Он являлся гораздо более безопасным, чем его предшественники SSL, а версия 1.0 использовалась на протяжении семи лет, до разработки TLSv1.1 в 2006 году. Новая версия имела ряд улучшений по сравнению с TLSv1.0, но IETF предложила следующую версию TLSv1.2

в 2008 году, которая на сегодняшний день является последней. Сейчас IETF работает над TLSv1.3, который на данный момент не является полностью доступным.

В приведенной ниже таблице показаны новые версии и даты выпуска версий SSL / TLS:



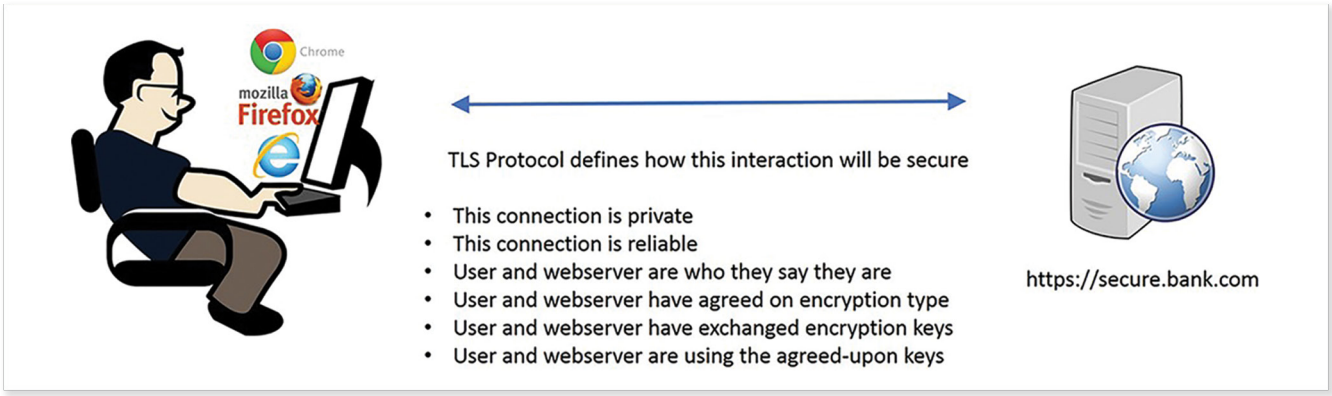
В общем, протокол TLS обеспечивает безопасный обмен данными между браузером и сервером. Он состоит из двух базовых уровней (со многими дополнительными элементами):

1. TLS Record Protocol
2. TLS Handshake Protocol

TLS Record Protocol нужен для того, чтобы гарантировать приватность (посторонний не может видеть или читать данные, которыми обмениваются стороны) и надежность (данные, которыми обмениваются стороны, действительно прибывают по месту назначения) соединения браузера и веб-сервера.

TLS Handshake Protocol используется, чтобы браузер и сервер могли идентифицировать друг друга и согласовать точный тип алгоритма шифрования, который будет использоваться для защиты данных.

ЧТО ТАКОЕ БЕЗОПАСНОСТЬ ТРАНСПОРТНОГО УРОВНЯ?



Таким образом, каждый раз, когда вы посещаете веб-сайт, URL которого начинается с **HTTPS://** – будьте уверены, что браузер и сервер выполнили множество операций, чтобы гарантировать вашу безопасность и конфиденциальность.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com