МЕТОДЫ ЗАЩИТЫ ДАННЫХ В WEB

Бабиков Алексей Константинович
Студент 4 курса, направление: Информационная безопасность Автоматизи-рованных систем, Московский Политехнический университет

Лушина Ольга Владимировна
Ассистент кафедры «SMART-технологий» Московского политехнического университета

Аннотация: *В статье описано применение протоколов SSL и TLS для защиты данных, передаваемых по средствам компьютерных технологий. Протокол SSL призван обеспечить возможность надежной защиты сквозной передачи данных с использованием протокола TCP. SSL представляет собой не один протокол, а два уровня протоколов. Протокол записи SSL (SSL Record Protocol) обеспечивает базовый набор средств защиты, применяемых протоколами более высоких уровней. Эти средства, в частности, может ис-пользовать протокол передачи гипертекстовых файлов (HTTP), призванный обеспечить обмен данными при взаимодействии клиентов и серверов Web*

Ключевые слова: *SSL, TLS, компьютерные технологии, протоколы*

Abstract: *the article describes the use of SSL and TLS protocols to protect data transmitted by means of computer technologies. The SSL Protocol is de-signed to provide reliable protection of end-to-end data transmission using the TCP Protocol. SSL is not a single Protocol, but two layers of protocols. SSL Record Protocol (SSL Record Protocol) provides a basic set of security features used by higher-level protocols. These tools, in particular, can use the hypertext transfer Protocol (HTTP), designed to provide data exchange when interacting with clients and web servers*

Keywords: *SSL, TLS, computer technologies, protocols*

Введение. В связи с развитием информационных технологий необходимо улучшать меры защиты информации от различных атак.

Цель исследования: изучить криптографические протоколы

Задачи исследования:

- Рассмотреть принципы работы протоколов
- Проанализировать историю развития техно-логии

SSL («Secure Socket Layer») – криптографический протокол, который использует ассиметричную криптографию, симметричное шифрование и коды аутентификации для защиты передаваемых данных [2].

TLS («Transport Layer Security») – усовершенствованная версия протокола SSL, основанная на TLS версии 3.0 [1].

Оба эти протокола делают невозможным осуществление несанкционированного доступа и прослушивание пакетов, передаваемых по сети. На рисунке 1 представлено отличие защищённого соединение с сервером от незащищённого.

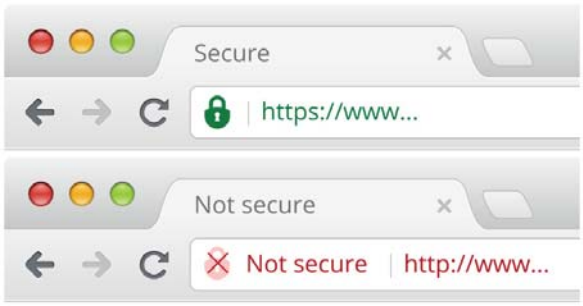

Рисунок 1. Защищённое соединение

Протоколы SSL и TLS применяют в тех случаях, где необходимо обеспечить надлежащий уровень защиты данных, передаваемых пользователем по сети. Например, для сайтов, которые используют платёжные системы или электронные кошельки, эти алгоритмы используются для защиты от перехвата данных злоумышленниками.

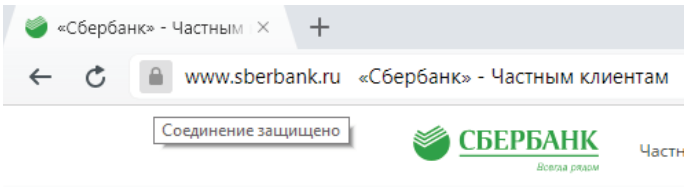

Рисунок 2. Защищённое соединение в платёжных системах

На рисунке 2 можно наблюдать наличие защищённого соединения на официальном сайте одного из наиболее популярных банков России.

История развития протоколов начинается с SSL версии 1.0, разработанным компанией «Netscape Communications» . Далее развитие история развития технологии защиты представлена на рисунке 3.

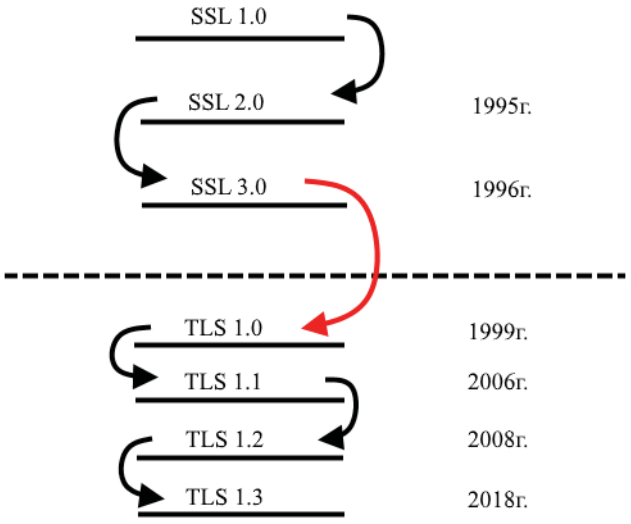

Рисунок 3. История развития технологии

Принцип работы данных протоколов заключается в том, что они выступают в роли фильтров для защиты данных при переходе с прикладного уровня на транспортный уровень в модели «TCP/IP», что изображено на рисунке 4.

Рисунок 4. Защита данных в модели TCP/IP

Для шифрования данных используются ключи разной длины. Надёжность защиты напрямую зависит от этого ключа. Для наиболее важной информации используются ключи, длиной 128 бит. С их помощью возможно обеспечить надлежащий уровень защиты данных [1].

Для передачи на сервере необходимо присутствие SSL-сертификата, содержащего сведения о владельце ключа, о центре сертификации, данные об открытом ключе.

При наличии сертификата на сервере передача данных будет происходить следующим образом:

1. Обмен сообщениями инициализации
2. Обмен сертификатами и ключевым сообщением
3. Обмен секретными данными

Основной особенностью использования SSL и TLS протоколов называется «прозрачность использования». Под этим понятием подразумевается возможность использовать эту защиту данных поверх любых приложений прикладного уровня [2].

Вывод. Изучив протоколы SSL и TLS можно удостовериться в необходимости применения такой технологии для обеспечения надлежащей защиты данных при передаче конфиденциальной или иной секретной информации. Процессы защиты информации, шифрования и дешифрования связаны с кодируемыми объектами и процессами, их свойствами, особенностями перемещения. Такими объектами и процессами могут быть материальные объекты, ресурсы, товары, сообщения, блоки информации, транзакции (минимальные взаимодействия с базой данных по сети). Кодирование кроме целей защиты, повышая скорость доступа к данным, позволяет быстро определять и выходить на любой вид товара и продукции, страну-производителя и т.д. В единую логическую цепочку связываются операции, относящиеся к одной сделке, но географически разбросанные по сети.

Список литературы

1. Титоренко Г.А. Информационные технологии управления. М., Юнити: 2002.
2. Мельников В. Защита информации в компьютерных системах. – М.: Финансы и статистика, Электронинформ, 1997