Астафьев А.В, Шардин Т.О.
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: tima.shardin@mail.ru

Использование технологии безопасного обмена данными на основе протокола рукопожатия в клиент-серверных приложениях

Основной угрозой большинства клиент-серверных приложений на сегодняшний день является перехват данных в ходе информационного обмена, что влечет за собой доступ или получение конфиденциальных данных. Также по различным технологическим причинам, большинство трафика, передаваемого разными способами по Интернету, пересылается открытым образом. То есть злоумышленник, подключившийся к каналу передачи данных, сможет считывать данные, передаваемые пользователем и получаемые им из Интернета.

В связи с этим большинство разработчиков пришли к выводу о необходимости использования технологии безопасного обмена информацией, основанной на идентификации клиента или применению дополнительных мер для проверки подлинности пользователя [1]. Одной из таких технологий зачастую называют протоколом с нулевым разглашением секрета.

Протокол рукопожатия – разновидность криптографического протокола с нулевым разглашением секрета, осуществляющий обмен сообщений между участниками информационного взаимодействия по схеме запрос-ответ [2].

Рассмотрим один из примеров использования данного протокола на практике. Схема работы протокола рукопожатия в клиент-серверном приложении показана на рисунке 1:

Рисунок 1 – Структураная схема протокола рукопожатия

Из рисунка видно, что обмен информацией между клиентом и сервером происходит по защищенному каналу связи, представляющий протокол рукопожатия, использующий ассиметричную систему шифрования. Изначально клиент проходит идентификацию на сервере

по его открытому ключу и при успешной проверке переходит к вводу контрольной фразы для получения данных. Стоит отметить, что участники информационного взаимодействия изначально обговаривают все параметры подключения.

В результате использование данной технологии позволило предотвратить перехват данных в ходе информационного взаимодействия благодаря использованию протокола рукопожатия и использования в нем ассиметричной системы шифрования, обеспечивающая надежность и устойчивость к атакам злоумышленника.

Литература

1. ГОСТ Р 53114–2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

2. Молдовян А.А., Молдовян Д.Н., Левина А.Б. ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ СЕКРЕТА - Санкт-Петербург: СПб: Университет ИТМО, 2016. - 55 с. - экз.

3. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Часть 1. // Монитор. - 1992. - N 6-7. - с. 14 – 19.