Отчёт по лабораторной работе №4 по курсу «Криптография»

Выполнил Попов Николай, группа *M8O-308Б-21*

Задание

1. Выбрать не менее 2-ух web-серверов сети Интернет различной организационной и государственной принадлежности.
2. Запустить Wireshark и используя Firefox установить https соединение с выбранным сервером.

3. Провести анализ соединения.
4. Сохранить данные необходимы для последующего сравнительного анализа:
Имя сервера, его характеристики.
Версия TLS.
Выбранные алгоритмы шифрования.
Полученный сертификат: версия. Валидность сертификата, валидность ключа, удостоверяющий центр.
Время установки соединения (от ClientHello до Finished)
5. Если список исследуемых серверов не исчерпан выбрать другой сервер и повторить соединение.
6. Если браузер поддерживал соединение TLS 1.2 принудительно изменить параметры TLS соединения в Firefox на TLS 1.0 (в браузере перейти по адресу “about:config” и изменить раздел SSL\TLS) и провести попытки соединения с выбранными серверами).
7. Провести сравнительный анализ полученной информации.
8. В качестве отчета представить результаты сравнительного анализа, выводы в отношении безопасности и корректности настройки веб-серверов с учетом их организационной и государственной принадлежности.

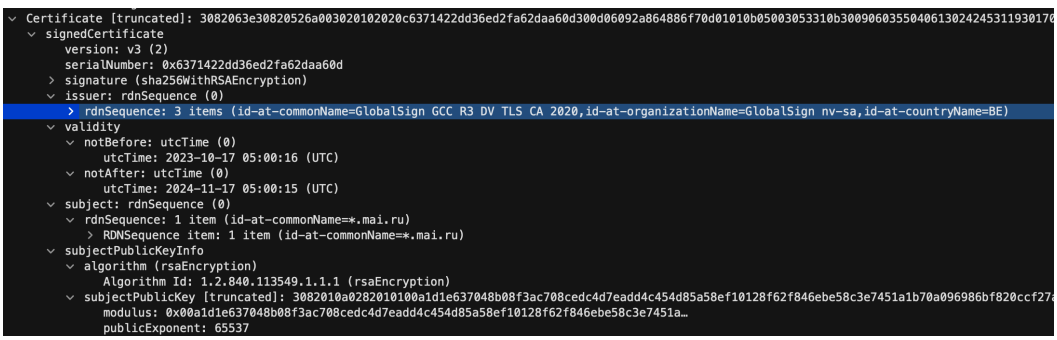
Выбранные сервера:

mai.ru

Версия TLS: 1.2

Алгоритмы шифрования: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Полученный сертификат:



Время установки соединения: 1.59 сек

mipt.ru

Версия TLS: 1.3

Алгоритмы шифрования: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Полученный сертификат:

Время установки соединения: 1.1 сек

При принудительной установке версии TLS = 1.0 оба сервера ошибку с кодом SSL_ERROR_PROTOCOL_VERSION_ALERT или PR_CONNECT_RESET_ERROR

Вывод

В рамках лабораторной работы было проведено исследование безопасности HTTPS-соединений с веб-серверами. Для анализа были выбраны серверы mai.ru и mipt.ru. В результате анализа с использованием инструмента Wireshark и браузера Firefox были изучены параметры безопасности установленных соединений, в том числе версии протокола TLS, алгоритмы шифрования, параметры сертификатов, а также время установки соединения.

Попытка установить соединение с использованием устаревшей версии TLS 1.0 привела к ошибкам соединения на обоих серверах, что подтверждает их настройку на использование более безопасных версий TLS. Важно отметить, что регулярное обновление настроек безопасности и использование современных версий протоколов шифрования являются ключевыми аспектами защиты информации в сети.