МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский Авиационный Институт»
(Национальный Исследовательский Университет)

Институт: №8 «Информационные технологии и прикладная математика»
Кафедра: 806 «Вычислительная математика и программирование»

Лабораторная работа № 4
по курсу «Криптография»

Группа: М8О-308Б-21

Студент(ка): К.А.Белоносов

Преподаватель: А. В. Борисов

Оценка:

Дата: 23.04.2024

Москва, 2024

ОГЛАВЛЕНИЕ

1 Тема

Аутентификация с асимметричными алгоритмами шифрования

2 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 Client Hello 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

3 Теория

Асимметричное шифрование, также известное как криптография с открытым ключом, использует пару ключей для шифрования и дешифрования данных: открытый ключ, который может быть свободно распространён, и закрытый ключ, который остаётся в тайне у владельца.

Основы асимметричной аутентификации

В контексте аутентификации асимметричные алгоритмы используются для подтверждения подлинности отправителя сообщения. Процесс работает следующим образом:

1. Генерация ключей: сначала создаётся пара ключей — открытый и закрытый.
2. Распространение открытого ключа: Открытый ключ распространяется среди пользователей, в то время как закрытый ключ сохраняется в секрете.
3. Подписание данных: Отправитель использует свой закрытый ключ для создания цифровой подписи на сообщении или документе.
4. Проверка подписи: Получатель или любая другая сторона может использовать открытый ключ отправителя для проверки цифровой подписи. Если подпись совпадает, это подтверждает, что сообщение было подписано именно отправителем, и не было изменено после подписания.

Применение в TLS

TLS (Transport Layer Security) — это протокол безопасности, предназначенный для обеспечения безопасности данных, передаваемых по сети интернет. Асимметричные алгоритмы играют ключевую роль в начальной стадии установления TLS-соединения, известной как рукопожатие (handshake), где происходит аутентификация и согласование секретного ключа:

- Аутентификация сервера: Сервер предоставляет свой сертификат, содержащий открытый ключ, клиенту.
- Аутентификация клиента: Клиент может также предоставить свой сертификат серверу, если требуется двусторонняя аутентификация.

- Создание сессионного ключа: с помощью асимметричного шифрования устанавливается сессионный ключ, который затем используется для симметричного шифрования данных.

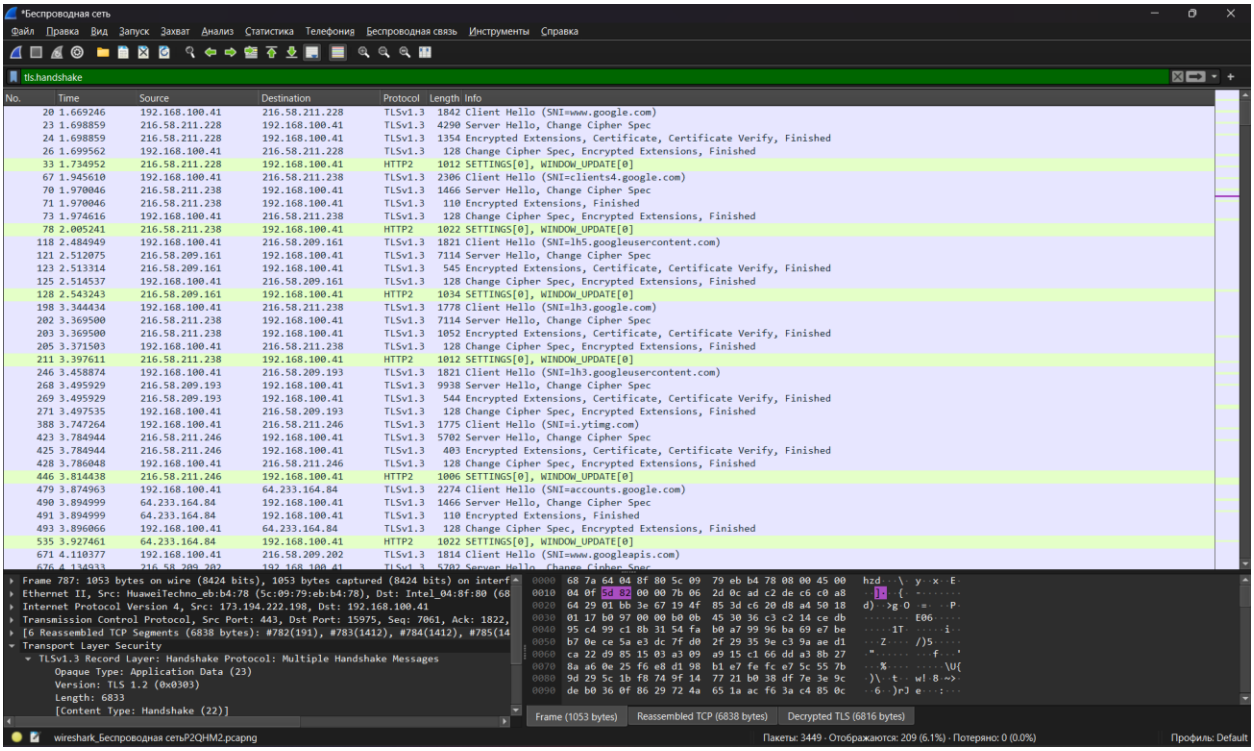
Wireshark — это популярный сетевой анализатор, который позволяет захватывать и анализировать пакеты данных, проходящие через сеть. С помощью Wireshark можно изучить детали TLS-рукопожатия и другие аспекты TLS-сессий. Примеры того, что можно увидеть в Wireshark при анализе TLS:

- Рукопожатие TLS: Захват процесса рукопожатия, включая обмен сертификатами, алгоритмы шифрования и согласование ключей.
- Шифрованные данные: после установления сессионного ключа все передаваемые данные шифруются, и Wireshark будет показывать эти данные как шифрованные.

4 Ход лабораторной работы

Для подключения я выбрал 2 сервера: https://www.ozon.ru/ и https://es.pfrf.ru/

Для подключения к этим серверам я воспользовался утилитой wireshark. Чтобы подробнее изучить соединение с серверами я создал переменную среды: **SSLKEYLOGFILE,** которую используют браузеры для сохранения сессионных ключей. Далее я запустил wireshark с фильтром tls.handshake чтобы отслеживать tls пакеты.



Далее я с помощью браузера подключился к выбранным серверам. В результате появились данные «рукопожатия» из которых я и получил необходимую информацию:

1. Ozon:
    a. Имя сервера: www.ozon.ru
    b. Ip-адрес: 162.159.140.11
    c. TLS: v1.3
    d. Алгоритм шифрования: TLS_AES_128_GCM_SHA256
    e. Версия сертификата: v3
    f. Номер сертификата: 0x4d774bca67a59c79a322e9c6
    g. Удостоверяющий центр: GlobalSign RSA OV SSL CA 2018

h. Валидность: 2023-09-21 15:51:06 (UTC) - 2024-10-22 15:51:05 (UTC)
i. Время установки соединения: 0,019664 с

2. Pfrf
    a. Имя сервера: www.es.pfrf.ru
    b. Ip-адрес: 195.161.52.80
    c. TLS: v1.2
    d. Алгоритм шифрования: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    e. Версия сертификата: v3
    f. Номер сертификата: 7c08755e460a99e0934e3d34
    g. Удостоверяющий центр: GlobalSign GCC R3 DV TLS CA 2020
    h. Валидность: 2023-06-21 18:35:28 (UTC) - 2024-07-22 18:35:27 (UTC)
    i. Время установки соединения: 0,017596 с

При изменении TLS на версию 1.0 оба сайта открылись. Сайт Ozon стал показывать меньше информации, т.к. рекламные сервисы требуют TLS более высокой версии. Сайт пенсионного фонда работает в прежнем режиме

1. Ozon:
    a. Имя сервера: www.ozon.ru
    b. Ip-адрес: 172.66.0.11
    c. TLS: v1
    d. Алгоритм шифрования: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    e. Версия сертификата: v3
    f. Номер сертификата: 0x4d774bca67a59c79a322e9c6
    g. Удостоверяющий центр: GlobalSign RSA OV SSL CA 2018
    h. Валидность: 2023-09-21 15:51:06 (UTC) - 2024-10-22 15:51:05 (UTC)
    i. Время установки соединения: 0,033524 с
2. Pfrf
    a. Имя сервера: www.es.pfrf.ru
    b. Ip-адрес: 195.161.52.80
    c. TLS: v1
    d. Алгоритм шифрования: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

e. Версия сертификата: v3
f. Номер сертификата: 7c08755e460a99e0934e3d34
g. Удостоверяющий центр: GlobalSign GCC R3 DV TLS CA 2020
h. Валидность: 2023-06-21 18:35:28 (UTC) - 2024-07-22 18:35:27 (UTC)
i. Время установки соединения: 0,004193 с

В результате анализа можно заметить, что сертификаты не зависят от версии TLS. Удивительно, что сайт пенсионного фонда работает даже с пониженной версией TLS. Также можно заметить, что изменились алгоритмы шифрования. Возможно, они единственно доступные, при данной версии TLS

5 Выводы

В результате данной лабораторной работы я познакомился с алгоритмами ассимитричного шифрования при аунтефикации. Я посмотрел, как работает алгоритм рукопожатия в TLS. Также я научился работе с новым инструментом Wireshark для отслеживания пакетов. Интересен тот момент, что сайты до сих пор поддерживают старые версии TLS

6 Список используемой литературы

https://habr.com/ru/articles/253521/

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000wkvECAQ&lang=en_US%E2%80%A9

https://habr.com/ru/articles/258285/