

Отчёт по лабораторной работе №4 по курсу «Криптография»

Выполнил Попов Николай, группа М8О-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:

```

Certificate [truncated]: 3082063e30820526a003020102020c6371422dd36ed2fa62daa60d300d06092a864886f70d0101b05003053310b3009060355040613024245311930170
signedCertificate
  version: v3 (2)
  serialNumber: 0x6371422dd36ed2fa62daa60d
  signature (sha256WithRSAEncryption)
  issuer: rdnSequence (0)
  > rdnSequence: 3 items (id-at-commonName=GlobalSign GCC R3 DV TLS CA 2020, id-at-organizationName=GlobalSign nv-sa, id-at-countryName=BE)
  validity
    notBefore: utcTime (0)
    utcTime: 2023-10-17 05:00:16 (UTC)
    notAfter: utcTime (0)
    utcTime: 2024-11-17 05:00:15 (UTC)
  subject: rdnSequence (0)
  > rdnSequence: 1 item (id-at-commonName=*.mai.ru)
  > RDNSequence item: 1 item (id-at-commonName=*.mai.ru)
  subjectPublicKeyInfo
    algorithm (rsaEncryption)
      Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
    subjectPublicKey [truncated]: 3082010a0282010100a1d1e637048b08f3ac708cedc4d7eadd4c454d85a58ef10128f62f846ebe58c3e7451a1b70a096986bf820ccf27
      modulus: 0x00a1d1e637048b08f3ac708cedc4d7eadd4c454d85a58ef10128f62f846ebe58c3e7451a...
      publicExponent: 65537
```

Время установки соединения: 1.59 сек

mipt.ru

Версия TLS: 1.3

Алгоритмы шифрования: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Полученный сертификат:

```
Certificate Length: 1607
Certificate [truncated]: 308206433082052ba003020102020c68e10ddbbf98a2848dbe2113300d06092a864886f70d01010b05003053310b30090603550406130242453119301706
signedCertificate
  version: v3 (2)
  serialNumber: 0x68e10ddbbf98a2848dbe2113
  signature (sha256WithRSAEncryption)
    Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
  issuer: rdnSequence (0)
    > rdnSequence: 3 items (id-at-commonName=GlobalSign GCC R3 DV TLS CA 2020,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)
  validity
    > notBefore: utcTime (0)
      utcTime: 2024-02-06 00:15:18 (UTC)
    > notAfter: utcTime (0)
      utcTime: 2025-03-09 00:15:17 (UTC)
  subject: rdnSequence (0)
    > rdnSequence: 1 item (id-at-commonName=*.mipt.ru)
  subjectPublicKeyInfo
    > algorithm (rsaEncryption)
      Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption)
    > subjectPublicKey [truncated]: 3082010a0282010100bf3f9aae7d1ed1f48bb5f1720eb48a321ec162a64c4cf6002b0ad8b65c5dc797e979dfe798c5c6807b65d7b46e73
      modulus: 0x00bf3f9aae7d1ed1f48bb5f1720eb48a321ec162a64c4cf6002b0ad8b65c5dc797e979df_
      publicExponent: 65537
```

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.

