Отчёт по лабораторной работе №5 по курсу «Криптография»

Выполнил Попов Матвей, группа М8О-308Б-20

Задание

1. Выбрать не менее 5-ти веб-серверов 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 “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.

Ход работы

1. Для начала определимся с веб-серверами, которые мы будем анализировать. У меня это будут сервера сайтов faq8.ru, github.com, youtube.com, mai.ru и gosuslugi.ru
2. Запустим Wireshark и Firefox. Сначала проверим работу серверов с TLS версии 1.2
3. Чтобы определить имя сервера, откроем нужный сайт в Firefox, затем в Wireshark в поле для фильтра введём «`dns`», найдём пакет с именем хоста нужного нам сервера, откроем параметры этого пакета, имя находится в Domain Name System (response) → Quieries

4. Чтобы определить версию TLS и алгоритмы шифрования, в фильтре для пакетов указываем «`tls`», откроем параметры этого пакета, откроем Transport Layer Security, там можно увидеть версию TLS, затем в разделе Cipher Suites будут перечислены используемые алгоритмы шифрования
5. Чтобы получить информацию о сертификате, находим пакет с сообщением ServerHello с помощью фильтра «`ssl.handshake.type == 2`», откроем параметры этого сертификата, перейдём по Transport Layer Security и увидим несколько веток, отвечающих за сертификат.
6. Чтобы определить время установки соединения от ClientHello до Finished, находим пакет с ClientHello, следуем по потоку TCP до пакета с Finished и находим разницу во времени между этими двумя пакетами.
7. Так же хотелось бы отметить,
8. Теперь приступим к сбору информации о серверах. К сожалению, во время лабораторной работы, что удивительно, лёг сервер госуслуг, поэтому их сайт в экстренном порядке был заменён на findanime.net. Ниже приведена информация, которую мне удалось собрать.

faq8.ru

1. Имя сервера: faq8.ru
2. Версия TLS: 1.0
3. Алгоритмы шифрования: нет
4. Сертификат: нет
5. Время установки соединения: 1.31 сек

github.com

1. Имя сервера: github.com
2. Версия TLS: 1.2
3. Алгоритмы шифрования: `ECDSA X9.62`
4. Сертификат: `0C:D0:A8:BE:C6:32:CF:E6:45:EC:A0:A9:B0:84:FB:1C`
5. Время установки соединения: 1.93 сек

youtube.com

1. Имя сервера: www.youtube.com
2. Версия TLS: 1.2
3. Алгоритмы шифрования: `ECDSA`
4. Сертификат: `00:9B:C6:EB:61:E1:1C:C3:08:10:FD:CB:86:7D:9D:21:F5`
5. Время установки соединения: 5.41 сек

mai.ru

1. Имя сервера: mc.yandex.ru
2. Версия TLS: 1.2

3. Алгоритмы шифрования: `ECDSA`
4. Сертификат: `3D:35:EF:EF:0E:B9:DD:A7:D0:B4:51:EA`
5. Время установки соединения: 2.17 сек

findanime.ru

1. Имя сервера: findanime.net
2. Версия TLS: 1.2
3. Алгоритмы шифрования: `ECDSA`
4. Сертификат: `03:FC:D4:17:85:00:A1:98:3F:EA:68:BE:D8:2B:AC:F9:FD:DE`
5. Время установки соединения: 0.718 сек

Из собранных характеристик видно, что все сервера, кроме faq8.ru, работают с TLSv1.2, а faq8.ru работает на незащищённом протоколе http, поэтому поддерживает лишь TLSv1.0. Принудительно отключим версии TLS новее 1.0 и посмотрим, что произойдём, для этого перейдём в Firefox по адресу `about:config` и установим в поле `security.tls.version.max` значение 1. Попробуем снова открыть сайты. Попытки установить соединение с любым из серверов, кроме faq8.ru и youtube.com, приводят к возникновению ошибки `SSL_ERROR_PROTOCOL_VERSION_ALERT`.

Вывод

Проделав лабораторную работу, я изучил некоторые веб-сайты с точки зрения их защищённости и понял, что подавляющее большинство современных сайтов используют современные алгоритмы шифрования и защищённый протокол https. Небезопасным протоколом http пользуются лишь очень маленькие и давно не обновляющиеся сайты, например faq8. Но в целом ему это простительно, так как им пользуется крайне ограниченное число людей, да и те не оставляют там никаких ценных данных.