

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-307Б-21

Студент(ка): Ф. А. Меркулов

Преподаватель: А. В. Борисов

Оценка:

Дата: 19.04.2024

Москва, 2024

ОГЛАВЛЕНИЕ

1.	Тема	3
2.	Задание	3
3.	Теория	4
4.	Ход лабораторной работы.....	7
5.	Выводы	16
6.	Список используемой литературы	17

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 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.

3. Теория

Аутентификация – проверка id на принадлежность пользователю.

Авторизация – проверка прав пользователя.

Hypertext transfer protocol secure (HTTPS) – безопасная версия HTTP, который является основным протоколом, используемым для передачи данных между веб-браузером и веб-сайтом. HTTPS зашифрован для повышения безопасности передачи данных.

HTTPS использует протокол шифрования для шифрования сообщений. Протокол называется Transport Layer Security (TLS), хотя ранее он был известен как Secure Sockets Layer (SSL). Этот протокол обеспечивает безопасность связи с использованием асимметричной инфраструктуры открытых ключей. Этот тип системы безопасности использует два разных ключа для шифрования сообщений между двумя сторонами:

Закрытый ключ - контролируется владельцем веб-сайта и хранится в тайне. Этот ключ хранится на веб-сервере и используется для расшифровки информации, зашифрованной открытым ключом.

Открытый ключ - доступен каждому, кто хочет взаимодействовать с сервером безопасным способом. Информация, зашифрованная с помощью открытого ключа, может быть расшифрована только с помощью закрытого ключа.

TLS-рукопожатие — это процесс, который запускает сеанс связи, использующий TLS. Во время TLS-рукопожатия две взаимодействующие стороны обмениваются сообщениями, чтобы подтвердить друг друга, проверить друг друга, установить алгоритмы шифрования, которые они будут использовать, и согласовать ключи сеанса.

TLS-рукопожатие происходит всякий раз, когда пользователь переходит на веб-сайт по протоколу HTTPS, и браузер сначала начинает запрашивать сервер-источник сайта. TLS-рукопожатие также происходит всякий раз, когда любые другие коммуникации используют HTTPS, включая вызовы API и запросы DNS-over-HTTPS.

TLS-рукопожатие происходит после того, как с помощью TCP-рукопожатия было установлено TCP-соединение.

В ходе TLS-рукопожатия клиент и сервер вместе выполняют следующие действия:

- Указывают, какую версию TLS (TLS 1.0, 1.2, 1.3 и т. д.) они будут использовать
- Решают, какие наборы шифров они будут использовать
- Проверяют подлинность сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации SSL.
- Генерируют сессионные ключи, чтобы использовать симметричное шифрование после завершения рукопожатия

TLS-рукопожатия – это серия датаграмм, или сообщений, которыми обмениваются клиент и сервер. TLS-рукопожатие включает в себя несколько этапов, в ходе которых клиент и сервер обмениваются информацией, необходимой для завершения рукопожатия и обеспечения возможности дальнейшего общения.

Точные шаги в рамках TLS-рукопожатия зависят от используемого алгоритма обмена ключами и наборов шифров, поддерживаемых обеими сторонами. Алгоритм обмена ключами RSA, который в настоящее время считается небезопасным, использовался в версиях TLS до версии 1.3. Это происходит примерно следующим образом:

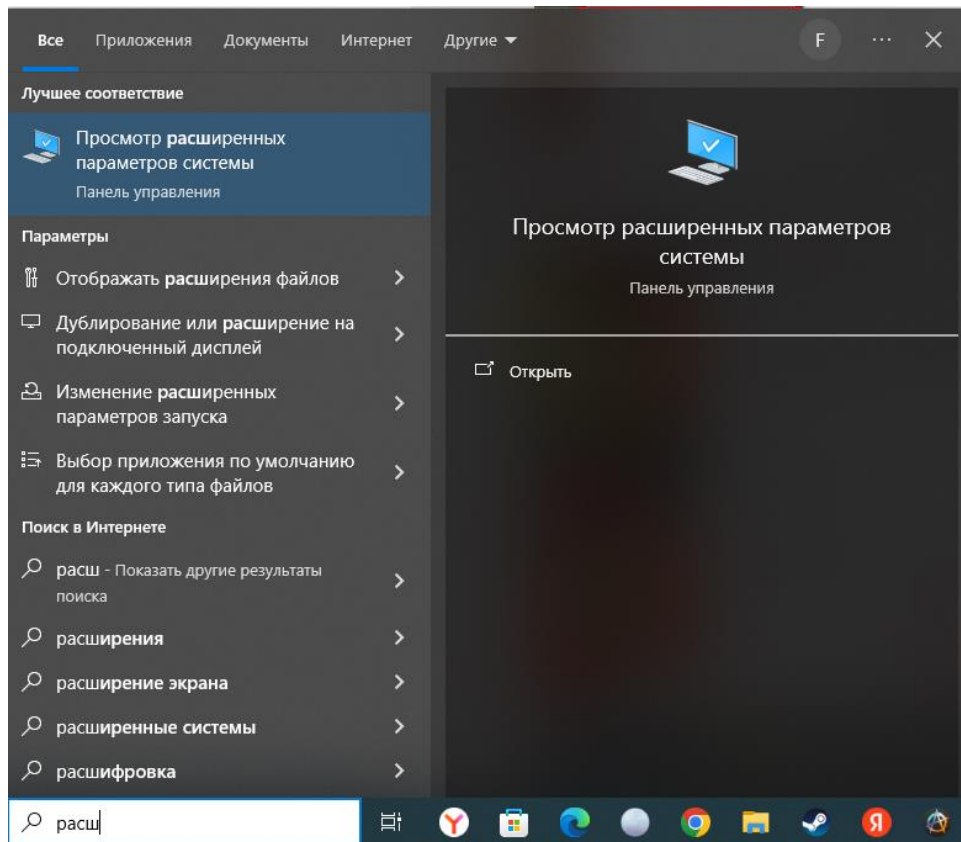
1. Client-hello: Клиент инициирует рукопожатие, посылая серверу сообщение "hello". В сообщении будет указано, какую версию TLS поддерживает клиент, поддерживаемые наборы шифров и строка случайных байтов "client random".
2. Server-hello: В ответ на сообщение "hello" клиента сервер отправляет сообщение, содержащее SSL-сертификат сервера, выбранный сервером набор шифров и "server random" – еще одну строку случайных байтов, генерируемую сервером.
3. Аутентификация: Клиент проверяет SSL-сертификат сервера в центре сертификации, который его выдал. Он подтверждает, что сервер является тем, за кого себя выдает, и что клиент взаимодействует с реальным владельцем домена.
4. Premaster secret: Клиент посылает еще одну строку случайных байтов, которая называется "premaster secret". Premaster secret шифруется открытым ключом и может быть расшифрован

сервером только с помощью закрытого ключа. (Клиент берет открытый ключ из SSL-сертификата сервера).

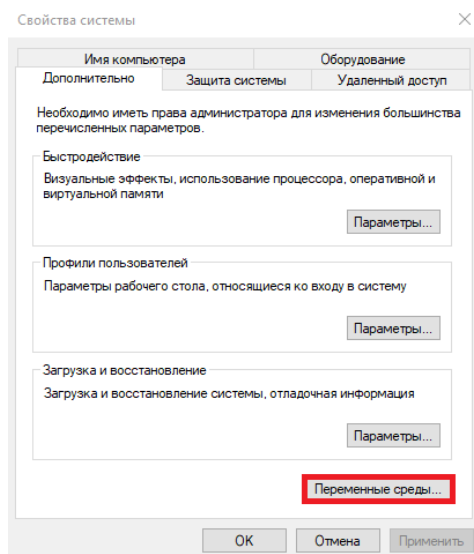
5. Используемый закрытый ключ: Сервер расшифровывает "premaster secret".
6. Создание сессионных ключей: Клиент и сервер генерируют сессионные ключи из random'a клиента, random'a сервера и premaster secret. Они должны прийти к одинаковым результатам.
7. Клиент готов: Клиент отправляет сообщение "ready", зашифрованное сессионным ключом.
8. Сервер готов: Сервер отправляет сообщение "ready", зашифрованное сессионным ключом.
9. Безопасность симметричного шифрования достигнута: Рукопожатие завершено, и связь продолжается с использованием сессионных ключей.

4. Ход лабораторной работы

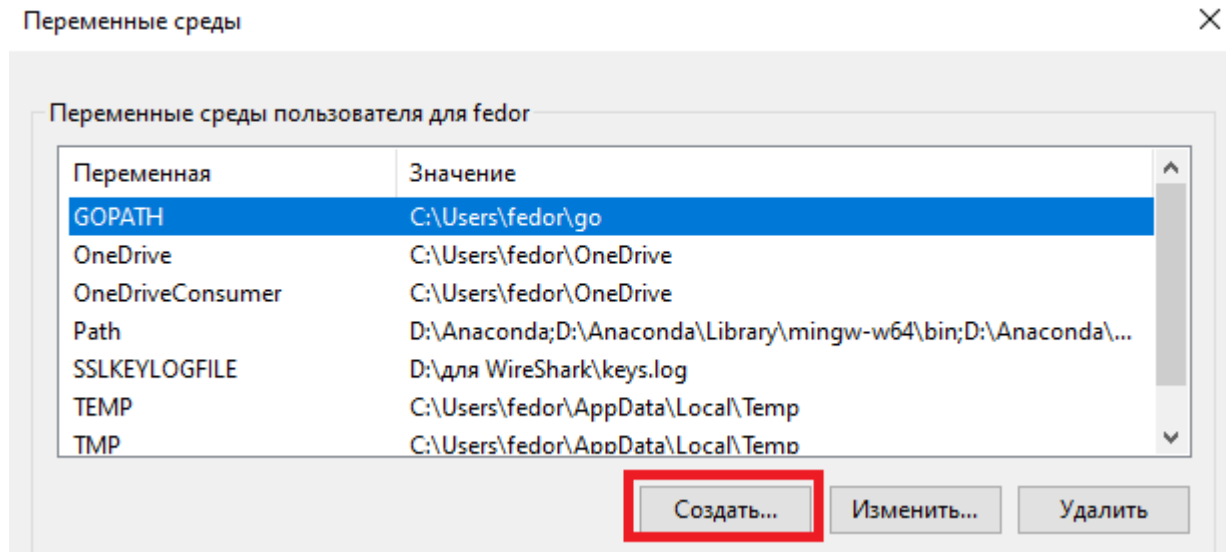
1. С помощью интернета я нашел как сделать расшифровку с помощью **pre-master secret key** сейчас распишу шаги того, что нужно сделать на ОС Windows, так как для меня это было не очевидно



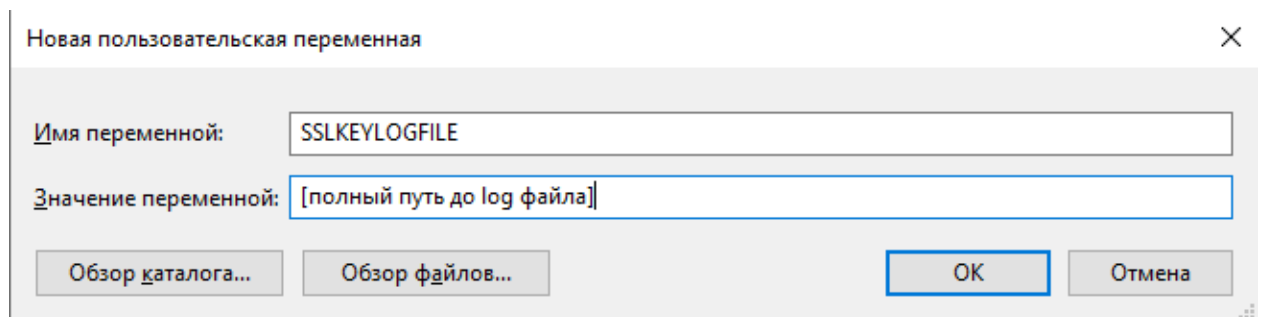
Переходим в “Просмотр расширенных параметров системы”



Нажимаем на кнопку “Переменные среды”

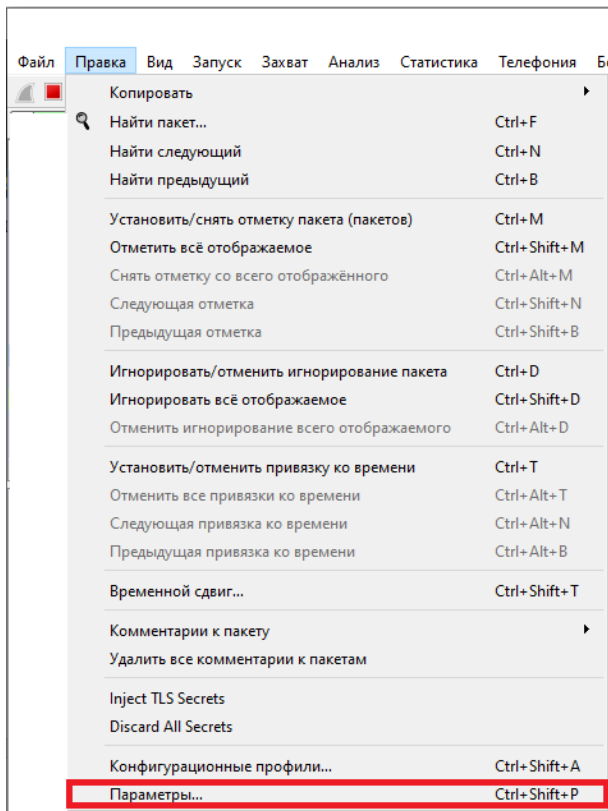


Нажимаем на кнопку “Создать”

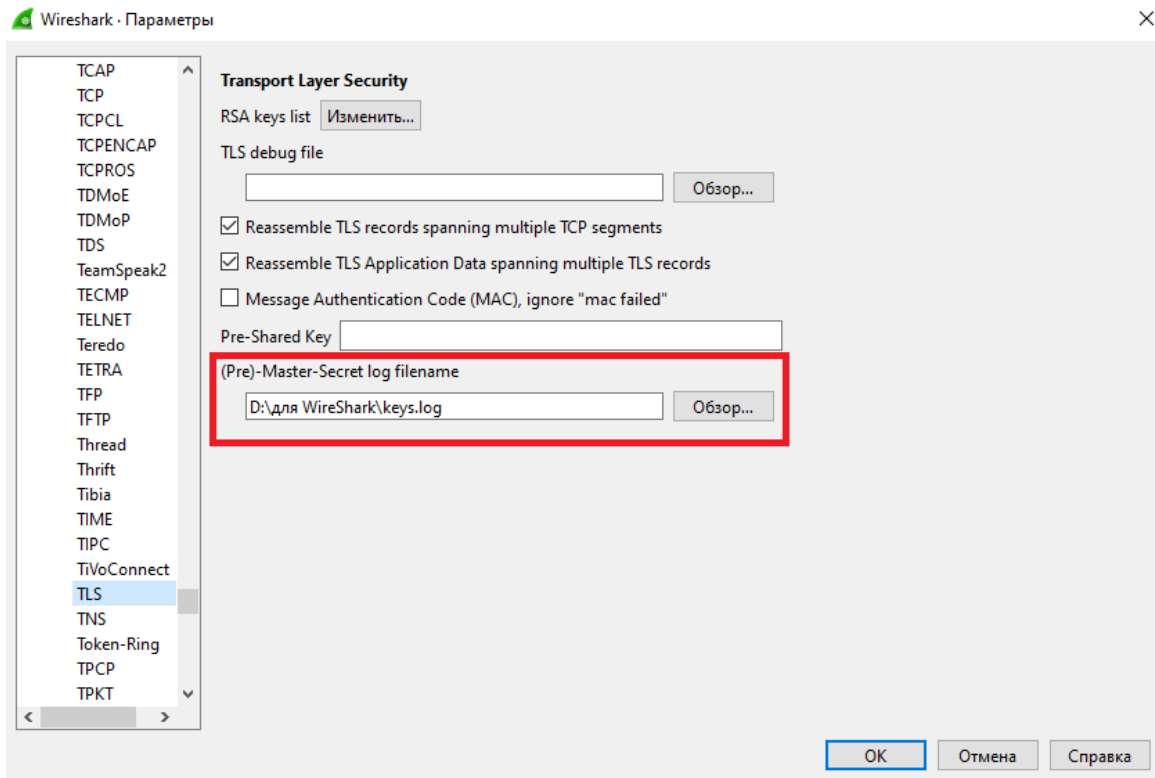


Записываем в “Имя переменной”: SSLKEYLOGFILE, а в “Значение переменной” путь до файла file.log в котором будут храниться логи

2. Укажем в Wireshark этот файл:



Далее в разделе “Protocols” находим “TLS”



3. Запускаем захват пакетов в Wireshark и ставим фильтр `tls && ip.addr == 176.114.124.24`. Это IP-адреса сайта <https://www.avito.ru/> (который я определил с помощью команды `ping www.avito.ru`) он использует TLSv1.2 и его я выбрал первым:

No.	Time	Source	Destination	Protocol	Length	Info
12470	225.818840	192.168.1.65	176.114.124.24	TLSv1.3	714	Client Hello (SNI=www.avito.ru)
12474	225.871587	176.114.124.24	192.168.1.65	TLSv1.3	1514	Server Hello, Change Cipher Spec, Encrypted Extensions
12476	225.871687	176.114.124.24	192.168.1.65	TLSv1.3	490	Certificate, Certificate Verify, Finished
12482	225.875784	192.168.1.65	176.114.124.24	TLSv1.3	714	Client Hello (SNI=www.avito.ru)
12483	225.876511	192.168.1.65	176.114.124.24	TLSv1.3	714	Client Hello (SNI=www.avito.ru)
12498	225.929180	176.114.124.24	192.168.1.65	TLSv1.3	1514	Server Hello, Change Cipher Spec, Encrypted Extensions
12499	225.929677	176.114.124.24	192.168.1.65	TLSv1.3	1514	Server Hello, Change Cipher Spec, Encrypted Extensions
12502	225.929761	176.114.124.24	192.168.1.65	TLSv1.3	490	Certificate, Certificate Verify, Finished
12504	225.929777	176.114.124.24	192.168.1.65	TLSv1.3	490	Certificate, Certificate Verify, Finished
12509	225.936534	192.168.1.65	176.114.124.24	TLSv1.3	118	Change Cipher Spec, Finished
12510	225.938856	192.168.1.65	176.114.124.24	HTTP2	224	Magic, SETTINGS[0], WINDOW_UPDATE[0], PRIORITY[3], PRIORITY[5], PRIOR
12511	225.941956	192.168.1.65	176.114.124.24	TLSv1.3	118	Change Cipher Spec, Finished
12512	225.942437	192.168.1.65	176.114.124.24	TLSv1.3	118	Change Cipher Spec, Finished
12513	225.942730	192.168.1.65	176.114.124.24	HTTP2	241	Magic, SETTINGS[0], WINDOW_UPDATE[0], PRIORITY[3], PRIORITY[5], PRIOR
12514	225.943164	192.168.1.65	176.114.124.24	HTTP2	241	Magic, SETTINGS[0], WINDOW_UPDATE[0], PRIORITY[3], PRIORITY[5], PRIOR
12515	225.943371	192.168.1.65	176.114.124.24	HTTP2	394	HEADERS[15]: GET /, WINDOW_UPDATE[15]
12517	225.989149	176.114.124.24	192.168.1.65	TLSv1.3	325	New Session Ticket

4. Анализ соединения:

Имя сервера: “Client Hello (SNI= www.avito.ru)” (SNI - Server Name Indication), говорит о том, что – имя сервера `www.avito.ru`.

IP-адрес: `176.114.124.24`

Версию TLS определим по Server Hello: Version: TLS 1.2 (0x0303).

Wireshark packet capture analysis of a TLS connection. The packet list shows a Client Hello (12470) and a Server Hello (12474). The packet details pane for packet 12474 shows the TLSv1.3 Record Layer: Handshake Protocol: Server Hello. The Handshake Protocol: Server Hello details show the Version: TLS 1.2 (0x0303). The packet bytes pane shows the raw data of the Server Hello message.

Frame 12474: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: Sercomm_82:ab:ec (b4:a5:ef:82:ab:ec), Dst: GigaByte

Internet Protocol Version 4, Src: 176.114.124.24, Dst: 192.168.1.65

Transmission Control Protocol, Src Port: 443, Dst Port: 46320, Seq: 1

Transport Layer Security

TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 122

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 118

Version: TLS 1.2 (0x0303)

Random: 80aad2475b387edd4218afbb7ff0960f3dc68ac1a7732c2e5b89f

Session ID Length: 32

Session ID: d16d5a1098ed81dd7ac481af998b2d254dff8a85428f45a3t

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 46

Алгоритмы шифрования, выбранный сервером можно также узнать в Server Hello: Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301).

The screenshot shows a Wireshark capture of a TLS handshake. The packet list on the left shows packet 12474 (Server Hello) selected. The packet details pane on the left shows the TLSv1.3 Record Layer and Handshake Protocol. The packet bytes pane on the right shows the raw data of the Server Hello message, with the Cipher Suite field highlighted in red and a red arrow pointing to it.

Frame 12474: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: Sercomm_82:ab:ec (b4:a5:ef:82:ab:ec), Dst: GigaByte

Internet Protocol Version 4, Src: 176.114.124.24, Dst: 192.168.1.65

Transmission Control Protocol, Src Port: 443, Dst Port: 46320, Seq: 1

Transport Layer Security

- TLv1.3 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 122
 - Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 118
 - Version: TLS 1.2 (0x0303)
 - Random: 80aad2475b387edd4218afbb7ff0960f3dc68ac1a7732c2e5b89f
 - Session ID Length: 32
 - Session ID: d16d5a1098ed81dd7ac481af998b2d254dffa885428f45a3t
 - Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
 - Compression Method: null (0)
 - Extensions Length: 46

Версия сертификата: version: v3 (2).

Валидность сертификата и ключа: можно проверить даты начала и окончания действия сертификата.

validity

notBefore: utcTime (0)

utcTime: 2023-04-06 13:03:05 (UTC)

notAfter: utcTime (0)

utcTime: 2024-05-07 13:03:04 (UTC)

Сертификат валиден до 7 мая этого года.

issuer: rdnSequence (0)

rdnSequence: 3 items (id-at-commonName=GlobalSign RSA OV SSL CA 2018,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)

No.	Time	Source	Destination	Protocol	Length	Info
12470	225.818840	192.168.1.65	176.114.124.24	TLSv1.3	714	Client Hello (SNI=www.avito.ru)
12474	225.871587	176.114.124.24	192.168.1.65	TLSv1.3	1514	Server Hello, Change Cipher Spec, Encrypted Extensions
12476	225.871687	176.114.124.24	192.168.1.65	TLSv1.3	490	Certificate, Certificate Verify, Finished

<ul style="list-style-type: none"> Transmission Control Protocol, Src Port: 443, Dst Port: 46320, Seq: 2921, Ack: 661, Len: 436 [3 Reassembled TCP Segments (2838 bytes): #12474(1286), #12475(1460), #12476(92)] Transport Layer Security <ul style="list-style-type: none"> TLSv1.3 Record Layer: Handshake Protocol: Certificate <ul style="list-style-type: none"> Opaque Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 2833 [Content Type: Handshake (22)] Handshake Protocol: Certificate <ul style="list-style-type: none"> Handshake Type: Certificate (11) Length: 2812 Certificate Request Context Length: 0 Certificates Length: 2808 Certificates (2808 bytes) <ul style="list-style-type: none"> Certificate Length: 1692 Certificate [truncated]: 3082069830820580a003020102020c7be56c1a231671f89206bd3b300d06092a1 <ul style="list-style-type: none"> signedCertificate <ul style="list-style-type: none"> version: v3 (2) serialNumber: 0x7be56c1a231671f89206bd3b signature (sha256withRSAEncryption) issuer: rdnSequence (0) rdnSequence: 3 items (id-at-commonName=GlobalSign RSA OV SSL CA 2018,id-at-organizationalUnitName=GlobalSign RSA OV SSL CA 2018) <ul style="list-style-type: none"> RDNSquence item: 1 item (id-at-countryName=BE) RDNSquence item: 1 item (id-at-organizationName=GlobalSign nv-sa) RDNSquence item: 1 item (id-at-commonName=GlobalSign RSA OV SSL CA 2018) validity <ul style="list-style-type: none"> notBefore: utcTime (0) utcTime: 2023-04-06 13:03:05 (UTC) notAfter: utcTime (0) utcTime: 2024-05-07 13:03:04 (UTC) subject: rdnSequence (0) subjectPublicKeyInfo 	<pre> 0090 36 31 33 30 33 30 35 5a 17 0d 32 34 30 35 30 37 61303052 ..240507 00a0 31 33 30 33 30 34 5a 30 76 31 0b 30 09 06 03 55 13030470 v1-0...U 00b0 04 06 13 02 52 55 31 0f 30 0d 06 03 55 04 08 13RU1- 0...U... 00c0 06 4d 6f 73 63 6f 77 31 0f 30 0d 06 03 55 04 07 ..Moscow1 0...U... 00d0 13 06 4d 6f 73 63 6f 77 31 30 30 2e 06 03 55 04 ..'Limit ed Liab 00e0 0a 13 27 4c 69 6d 69 74 65 64 20 4c 69 61 62 69 ..lity Com pany KEH 00f0 6c 69 74 79 20 43 6f 6d 70 61 6e 79 20 4b 45 48 eCommer cel-0... 0100 20 65 43 6f 6d 6d 65 72 63 65 31 13 30 11 06 03 U...a vito.ru0 0110 55 04 03 0c 0a 2a 2e 61 76 69 74 6f 2e 72 75 30 .."0... H... 0120 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 ..0...0 0130 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 000 0140 ee 92 f1 0e 4e 52 1b 3f 4b 64 fb 4a 62 cc 2f 8e ...NR-? Kd-Jb-/.. 0150 83 c0 6e bc 89 02 12 21 07 a8 4d b1 a3 17 9e e3 ..n...! ..N... 0160 f3 2a d6 f8 3f 0a 2e 85 83 76 bb bf 1e 9a c4 d2 ..*?... v... 0170 9a 10 1b ca 35 81 2a 71 95 9a c5 ad 9f c3 38 e8 ..&...?g8- 0180 1c 26 b5 60 17 2f 1f 1f 1e 16 e4 cf f7 ec 56 d8 ..U[X ..RyB2... 0190 a9 92 b2 13 55 5b 06 58 c6 b6 52 79 42 32 2d b4 ...z2o ..D>c..S 01a0 e7 93 84 7a 32 13 6f 9a 81 44 d9 60 eb 96 40 55 ..i#)58' ..1>c..5 01b0 e0 f0 00 69 23 29 45 6f 97 b9 31 3e 63 1c e1 35 @...a:58' ..T..L... 01c0 40 e8 c0 61 3a 35 38 60 82 05 54 f5 4c 2d 8e 63 ..FJ- A-c...c 01d0 ab b5 fc bf 46 ad 4a 16 41 89 63 8e 15 a3 1b 7e ..cu<...b z>...LLV- 01e0 e9 63 75 3c b2 b7 81 62 b4 7a 3e eb 4c 4c 56 a5 6a 9e d3 a7 2b 0f 5b df d7 6c f4 85 c7 e5 38 51 j...+[- l...8Q 01f0 6a 9e d3 a7 2b 0f 5b df d7 6c f4 85 c7 e5 38 51 ..Y- ~>...Y1...S- 0200 ed 59 fe 5f 7e 74 ac 3e c7 d2 59 6c a2 d7 53 a0 ..2...c...YK- 0210 e7 18 5e 00 86 7f 63 ed fe c7 f9 9c c4 59 4b f0 ..U... ..0- 0220 de 32 19 be ca d5 9e e7 55 51 97 eb ee e0 54 e2 ..+... ..0-0 0230 62 d0 3e 09 40 12 bb d0 4a 32 16 5a 65 19 b6 e7 D...+... ..0-8htt 0240 02 03 01 00 01 a3 82 03 4a 30 82 03 46 30 0e 06 p://secu re.globa 0250 03 55 1d 0f 01 01 ff 04 04 03 02 05 a0 30 81 8e lsign.co m/caceta 0260 06 08 2b 06 01 05 05 07 01 01 04 81 81 30 7f 30 /gsrsaov sslca201 0270 44 06 08 2b 06 01 05 05 07 30 02 86 38 68 74 74 8.crt07- +...+0 0280 70 3a 2f 2f 73 65 63 75 72 65 2e 67 6c 6f 62 61 ..0-8htt 0290 6c 73 69 67 6e 2e 63 6f 6d 2f 63 61 63 65 72 74 lsign.co m/caceta 02a0 2f 67 73 72 73 61 6f 76 73 73 6c 63 61 32 30 31 /gsrsaov sslca201 02b0 38 2e 63 72 74 30 37 06 08 2b 06 01 05 05 07 30 8.crt07- +...+0 02c0 01 86 2b 68 74 74 70 3a 2f 2f 6f 63 73 70 2e 67 ..+http: //ocsp.g </pre>
---	---

Время установки соединения легко вычислить как разницу времени между первым Client Hello и последним пакетом, содержащим сообщение Finished от сервера: 225.942437 - 225.818840 = 0.123597 секунды (~124 мс)

То же самое сделаем с сайтом **mos.ru**: `tls && ip.addr == 212.11.151.57`

Имя сервера: `www.mos.ru`

IP-адрес: `212.11.151.57`

Версия TLS: `Version: TLS 1.2 (0x0303)`

Алгоритмы шифрования: `Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)`

Версия сертификата: `version: v3 (2)`

Валидность сертификата и ключа:

`validity`

`notBefore: utcTime (0)`

`utcTime: 2023-10-13 09:57:50 (UTC)`

`notAfter: utcTime (0)`

`utcTime: 2024-11-13 09:57:49 (UTC)`

Удостоверяющий центр: rdnSequence: 3 items (id-at-commonName=AlphaSSL CA - SHA256 - G4,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)

Время установки соединения: 65 мс.

5. Теперь изменим версию TLS на TLS 1.0:

←	→	↻	Firefox	about:config
🔍 security.tls.version				
security.tls.version.enable-deprecated				true
security.tls.version.fallback-limit				4
security.tls.version.max				1
security.tls.version.min				1

Avito:

66164	2740.269682	192.168.1.65	176.114.124.24	TLSv1	202 Client Hello (SNI=www.avito.ru)
66168	2740.322709	176.114.124.24	192.168.1.65	TLSv1	1514 Server Hello
66169	2740.322825	176.114.124.24	192.168.1.65	TLSv1	1514 Certificate
66170	2740.322825	176.114.124.24	192.168.1.65	TLSv1	351 Server Key Exchange, Server Hello Done
66172	2740.324570	192.168.1.65	176.114.124.24	TLSv1	155 Client Key Exchange, Change Cipher Spec, Finished
66173	2740.376294	176.114.124.24	192.168.1.65	TLSv1	336 New Session Ticket, Change Cipher Spec, Finished

Имя сервера: www.mos.ru

IP-адрес: 176.114.124.24

Версия TLS: Version: TLS 1.0 (0x0301)

Алгоритмы шифрования:

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Версия сертификата: version: v3 (2)

Валидность сертификата и ключа:

validity

notBefore: utcTime (0)

utcTime: 2023-04-06 13:03:05 (UTC)

notAfter: utcTime (0)

utcTime: 2024-05-07 13:03:04 (UTC)

Удостоверяющий центр: rdnSequence: 3 items (id-at-commonName=GlobalSign RSA OV SSL CA 2018,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)

Время установки соединения: 107 мс.

mos.ru:

Имя сервера: www.mos.ru

IP-адрес: 212.11.151.57

Версия TLS: Version: TLS 1.0 (0x0301)

Алгоритмы шифрования:

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Версия сертификата: version: v3 (2)

Валидность сертификата и ключа:

validity

notBefore: utcTime (0)

utcTime: 2023-10-13 09:57:50 (UTC)

notAfter: utcTime (0)

utcTime: 2024-11-13 09:57:49 (UTC)

Удостоверяющий центр: rdnSequence: 3 items (id-at-commonName=AlphaSSL CA - SHA256 - G4,id-at-organizationName=GlobalSign nv-sa,id-at-countryName=BE)

Время установки соединения: 36 мс.

Анализ

И **avito.ru**, и **mos.ru** используют TLS 1.2, что является хорошей практикой. Однако после принудительного изменения параметров TLS соединения в Firefox на TLS 1.0 и попытки соединения с выбранными

серверами они оба меня пустили, хотя соединение через TLS 1.0 может представлять собой риск безопасности.

Я считаю, что обоим серверам рекомендуется отключить поддержку TLS 1.0, чтобы исключить потенциальные уязвимости и соответствовать лучшим практикам безопасности.

Также сравнив tls-handshake для сервисов **Avito** и **mos.ru**, я выяснил, что:

- Оба сайта используют и ту же версию tls;
- Они используют различные алгоритмы шифрования
- Время установки соединения с **mos.ru** быстрее, чем с **Avito**. Это значит, что физический сервер находится ближе;
- Центр сертификации **mos.ru** и **Avito** находятся в Бельгии;

5. Выводы

В процессе выполнения данной ЛР я познакомился с принципами TLS-рукопожатий, прочитал зашифрованные пакеты с помощью Wireshark и сравнил защищенность сервисов avito.ru и mos.ru.

6. Список используемой литературы

1. <https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/>
2. <https://www.cloudflare.com/ru-ru/learning/ssl/what-happens-in-a-tls-handshake/>
3. <https://www.youtube.com/watch?v=efzQEAm7-Jc>
4. <https://www.cloudflare.com/learning/ssl/what-is-https/>