

Отчет по лабораторной работе №7 :
Сервис тестирования корректности настройки
SSL на сервере Qualys SSL Labs – SSL Server
Test

Дедков Сергей

2015

Содержание

| | | |
|----------|--|-----------|
| 1 | Цель работы | 2 |
| 2 | Ход работы | 2 |
| 2.1 | Изучить лучшие практики по развертыванию SSL/TLS . . | 2 |
| 2.2 | Изучить основные уязвимости и атаки на SSL последнего времени – POODLE, HeartBleed | 2 |
| 2.3 | Обзор домена из списка Recent Best | 4 |
| 2.4 | Обзор домена из списка Recent Worst | 5 |
| 2.5 | Обзор известного сайта по выбору | 7 |
| 2.5.1 | Интерпретировать результаты в разделе Summary . | 7 |
| 2.5.2 | Расшифровать все аббревиатуры шифров в разделе Configuration | 10 |
| 2.5.3 | Прокомментировать большинство позиций в разделе Protocol Details | 12 |
| 2.5.4 | Сделать итоговый вывод о реализации SSL на заданном домене | 13 |
| 3 | Вывод | 13 |

1 Цель работы

2 Ход работы

2.1 Изучить лучшие практики по развертыванию SSL/TLS

- Приватный ключ и сертификат
- Используйте 2048-битные закрытые ключи
- Защитите закрытый ключ
- Обеспечьте охват всех используемых доменных имен
- Приобретайте сертификаты у надежного удостоверяющего центра
- Используйте надежные алгоритмы подписи сертификата
- Используйте безопасные протоколы
- Используйте безопасные алгоритмы шифрования
- Контроль за выбором алгоритма шифрования
- Поддержка Forward Secrecy.
- Отключите Renegotiation по инициативе клиента
- Отключите TLS compression
- Отключите RC4
- Будьте в курсе атаки BEAST
- Отключить SSL v3

2.2 Изучить основные уязвимости и атаки на SSL последнего времени – POODLE, HeartBleed

- POODLE

Специалист по безопасности Бодо Мёллер (Bodo Möller) с коллегами из компании Google опубликовал подробности об уязвимости в дизайне протокола SSL 3.0. Уязвимость под кодовым названием POODLE («пудель», Padding Oracle On Downgraded Legacy Encryption, CVE-2014-3566) позволяет расшифровать содержимое защищённого канала коммуникации. В общем, на всех системах нужно срочно блокировать использование SSL 3.0, потому что работающего способа обойти эксплоит не существует.

SSL 3.0 (RFC6101), использующий шифр RC4, устарел примерно на 15 лет. На замену ему создали TLS 1.0, TLS 1.1 и TLS 1.2, но он до сих пор широко используется в браузерах, веб-серверах и т.д. И многие реализации TLS обратно совместимы с SSL 3.0.

Злоумышленник может умышленно принудить клиента подключиться именно по SSL 3.0, эмулируя разрывы связи, и после этого эксплуатировать уязвимость.

Google пишет, что для защиты достаточно отключить поддержку SSL 3.0 или шифрования в режиме сцепления блоков (CBC mode). Однако, в этом случае возникнут серьезные проблемы с совместимостью. Поэтому рекомендуемый способ обхода — поддержка механизма TLS_FALLBACK_SCSV, который не позволяет злоумышленнику снизить защиту канала до SSL 3.0. Механизм также предотвращает снижение защиты с TLS 1.2 до 1.1 или 1.0, что может помочь в предотвращении будущих атак.

Браузер Chrome и серверы Google поддерживают TLS_FALLBACK_SCSV с февраля, так что есть достаточно доказательств, что метод действительно эффективен.

Дополнительно, для Google Chrome также представили патч, который не позволяет соединяться по SSL 3.0. Аналогичная опция появится в Firefox 34, который ожидается к выходу 25 ноября: там поддержку SSL 3.0 отключат по умолчанию.

В SSLv3 обнаружена возможность Padding Oracle атаки, которая позволяет злоумышленнику, имеющему какую-либо возможность отправлять свои данные на сервер по SSLv3 от имени жертвы, расшифровывать по 1 байту за 256 запросов. Происходит это из-за того, что в SSLv3 padding не учитывается в MAC.

Теоретически, реализовать атаку можно на любой сервис, где есть возможность влиять на отправляемые данные со стороны атакующего. Проще всего это реализовать, например, если злоумышленнику необходимо получить Cookie на HTTPS-странице, добавляя свой код на HTTP-страницы, который делает подконтрольные запросы на HTTPS-страницы, и подменяя шифрованные блоки.

Главной проблемой RC4 является наличие смещений: чем больше соединений и потоков шифрования используется для отправки одних и тех же данных (например, пароля или HTTP-куки), тем больше можно извлечь из трафика информации, которая помогает осуществить дешифрование. Ниже будет показано, как можно совместить эффективную атаку на CBC-шифрование при использовании SSL 3.0 (при условии, что злоумышленник может модифицировать сетевой обмен между клиентом и сервером). При этом, в

отличие от уязвимостей BEAST и Lucky 13, здесь нет каких-то обходных решений. У нас есть только небезопасный протокол SSL 3.0, и чтобы обеспечить надёжное шифрование, нужно избегать его использования.

Самая серьёзная проблема CBC-шифрования в SSL 3.0 заключается в том, что дополнение блоков (паддинг) может быть произвольным (за исключением последнего байта), на него не распространяется MAC (Message Authentication Code). Целостность дополнения не может быть полностью подтверждена в ходе дешифрования, поскольку в SSL 3.0 сообщение сначала подписывается с помощью MAC, затем дополняется паддингом, и уже после — шифруется блочным шифром. Паддинг от 1 до L байт (где L — размер блока в байтах) используется для получения целого числа блоков перед шифрованием. Легче всего пробить защиту, если есть целый блок паддинга, который (до шифрования) состоит из L-1 произвольных байт, за которыми следует одиночный байт со значением L-1.

- HeartBleed

Ошибка (переполнение буфера) в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера. Информация об уязвимости была опубликована в апреле 2014 года, ошибка существовала с конца 2011 года.

Heartbeat-пакет состоит из данных, которые сервер должен вернуть в неизменном виде (это гарантирует, что сервер расшифровывал пакет), и случайных заполняющих байтов. OpenSSL не проверял корректность этого пакета: возможен, например, пакет длиной 16 байт, в котором написано, что длина данных 64 килобайта (поле размера двухбайтовое). Подверженные ошибке версии OpenSSL выходили за пределы буфера и передавали клиенту столько памяти, сколько он запросил, позволяя атакующему получать не предназначенные для этого данные. RFC предписывает не отвечать на такие «отравленные» пакеты.

2.3 Обзор домена из списка Recent Best

Выбранный домен: `encoredentalplan.com` (198.39.202.30)

Общий рейтинг обозначается буквами A-F. В данном случае оценка домену выставлена B. В разделе `summary` можно увидеть выставленные оценки по 4 параметрам: Сертификат, Поддержка протокола, Обмен ключами, Стойкость шифра. (см. рисунок 1)

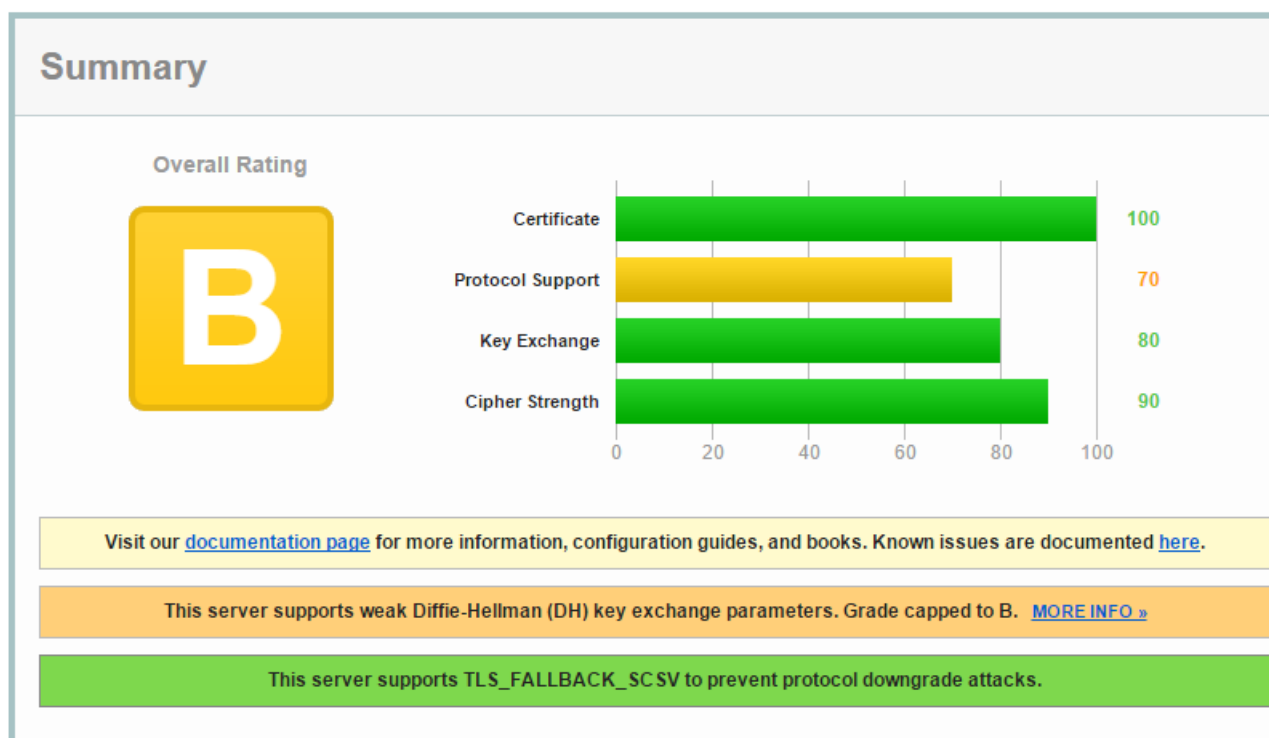


Рис. 1: Summary домена из списка Recent Best

В пояснительной информации ниже указано почему оценка была снижена до B - слабые параметры протокола Диффи — Хеллмана. Значит может быть проведена атака Logjam Attack.

Так же указано, что сервер поддерживает TLS_FALLBACK_SCSV, который не позволяет злоумышленнику снизить защиту канала до SSL 3.0. Механизм также предотвращает снижение защиты с TLS 1.2 до 1.1 или 1.0, что может помочь в предотвращении будущих атак.

Из прочей информации можно отметить следующее(см. рисунок 2):

- Присутствуют слабые наборы шифров.
- На некоторых платформах обнаружены несоответствия

2.4 Обзор домена из списка Recent Worst

Выбранный домен: receiver.tvc.org (67.51.200.102)

Аналогично предыдущему примеру можно увидеть оценки по 4м параметрам. (см. рисунок 3)

Из пояснительной информации:



| | | | | |
|---|--|--------------------------------------|-----------------------------------|-------------------|
|  | Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites always at the end) | | | |
| | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) | DH 1024 bits (p: 128, g: 1, Ys: 128) | FS WEAK | 256 |
| | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) | DH 1024 bits (p: 128, g: 1, Ys: 128) | FS WEAK | 128 |
| | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) | DH 1024 bits (p: 128, g: 1, Ys: 128) | FS WEAK | 256 |
| | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) | DH 1024 bits (p: 128, g: 1, Ys: 128) | FS WEAK | 128 |
|  | Handshake Simulation | | | |
| | Android 2.3.7 | No SNI ² | Protocol or cipher suite mismatch | Fail ³ |
| | Android 4.0.4 | | Protocol or cipher suite mismatch | Fail ³ |
| | Android 4.1.1 | | Protocol or cipher suite mismatch | Fail ³ |
| | Android 4.2.2 | | Protocol or cipher suite mismatch | Fail ³ |
| | Android 4.3 | | Protocol or cipher suite mismatch | Fail ³ |

Рис. 2: Прочая информация домена из списка Recent Best

- The server does not support Forward Secrecy with the reference browsers.

Домен не поддерживает прямую секретность, следовательно не гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования, не будут скомпрометированы при компрометации одного из долговременных ключей. С алгоритмами шифрования, которые не поддерживают Forward Secrecy, возможно расшифровать ранее зашифрованные разговоры с помощью закрытого ключа сервера. Нужно поддерживать и предпочитать ECDHE (аббревиатура ECDHE расшифровывается как «эффемерный алгоритм Диффи-Хеллмана с использованием эллиптических кривых») алгоритмы шифрования. Для поддержки более широкого круга клиентов, необходимо также использовать DHE, как запасной вариант после ECDHE.

- This server uses RC4 with modern browsers. Grade capped to C.

Алгоритм RC4 является небезопасным и должен быть отключен. В настоящее время известно, что для взлома RC4 требуются миллионы запросов, много пропускной способности и времени. Таким образом, риск все еще относительно невелик, но вполне возможно, что атаки будут масштабнее в будущем. Если снимать RC4 нужно заранее проверить, будут ли существующие пользователи затронуты; другими словами, проверить, есть ли клиенты, которые поддерживают только RC4.

- This server is vulnerable to MITM attacks because it supports insecure

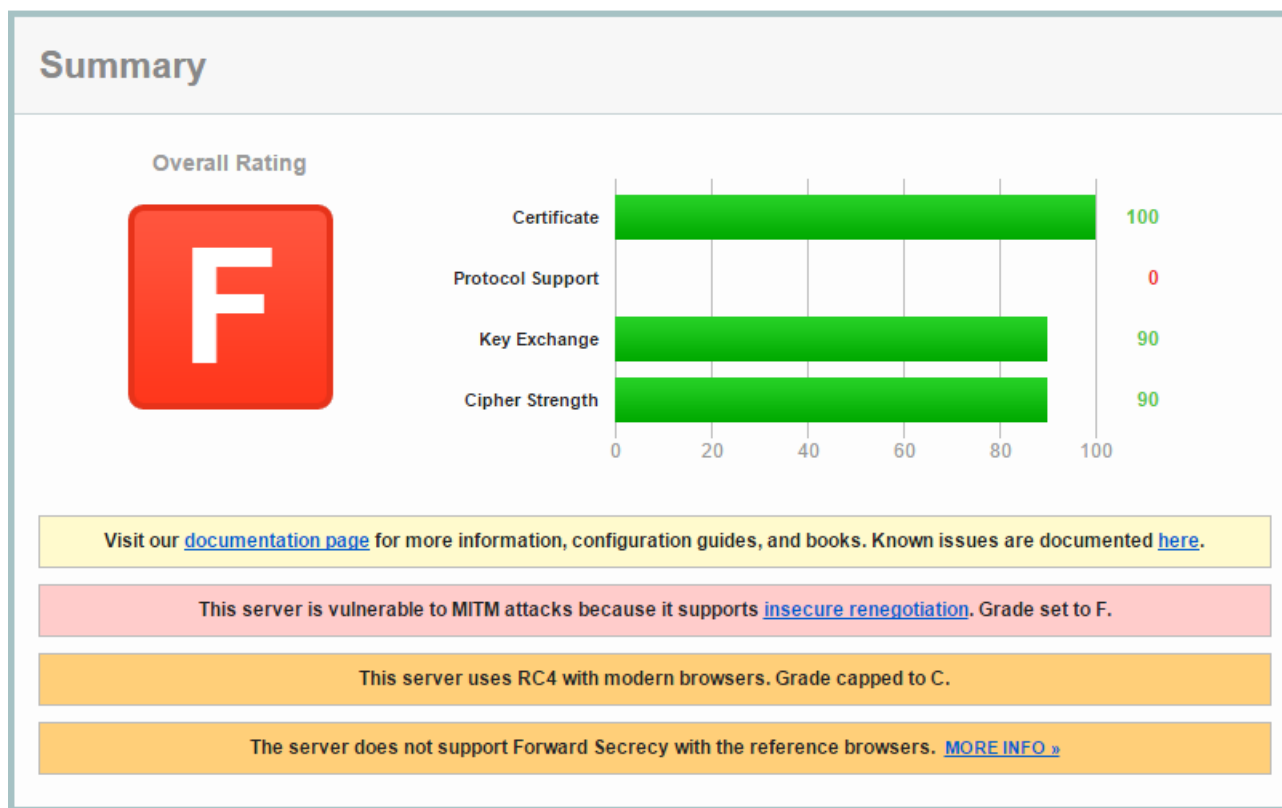


Рис. 3: Summary домена из списка Recent Worst

renegotiation. Grade set to F.

Сервер поддерживает небезопасное пересогласование ключей, отчего возможны такие типы атак, как Cross-Site Request Forgery и Cross-Site Scripting.

Прочую информацию можно увидеть на рисунке 4.

2.5 Обзор известного сайта по выбору


Выбранный домен: rzd.ru (217.175.140.90)

2.5.1 Интерпретировать результаты в разделе Summary

На рисунке 5 можно увидеть результаты и оценки проверки.

Из пояснительной информации (описание раньше не встречавшихся замечаний):

- The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C.



| Protocol Details | |
|---|---|
| Secure Renegotiation | Supported |
| Secure Client-Initiated Renegotiation | Supported DoS DANGER (more info) |
| Insecure Client-Initiated Renegotiation | Supported INSECURE (more info) |
| BEAST attack | Mitigated server-side (more info) TLS 1.0: 0x4 |
| POODLE (SSLv3) | No, SSL 3 not supported (more info) |
| POODLE (TLS) | No (more info) |
| Downgrade attack prevention | No, TLS_FALLBACK_SCSV not supported (more info) |
| TLS compression | No |
| RC4 | Yes WEAK (more info) |
| Heartbeat (extension) | No |
| Heartbleed (vulnerability) | No (more info) |
| OpenSSL CCS vuln. (CVE-2014-0224) | No (more info) |
| Forward Secrecy | No WEAK (more info) |

Рис. 4: Прочая информация домена из списка Recent Worst

На рисунке 6 можно увидеть, что на сервере не поддерживается TLS 1.2 и TLS 1.1, зато поддерживается TLS 1.0, SSL 3, SSL 2. При этом SSL 3 и SSL 2 считаются незащищенными.

- Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2.

Используемый алгоритм подписи на сервере: SHA1. Это можно увидеть в разделе Authentication. (см. рисунок 7)

Т.к. SHA1 считается небезопасным алгоритмом шифрования, предлагается обновить его на более современный и криптостойкий SHA2.

- This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F.

В виду того, что используется SSL шифрование на сервер можно осуществить атаку POODLE(см. выше). Так же возможно осуществлять атаку на сервер, где используется TLS(для некоторых реализаций), как в данном случае.

- This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F.

Возможность FREAK атаки. азвание уязвимости «атака FREAK»

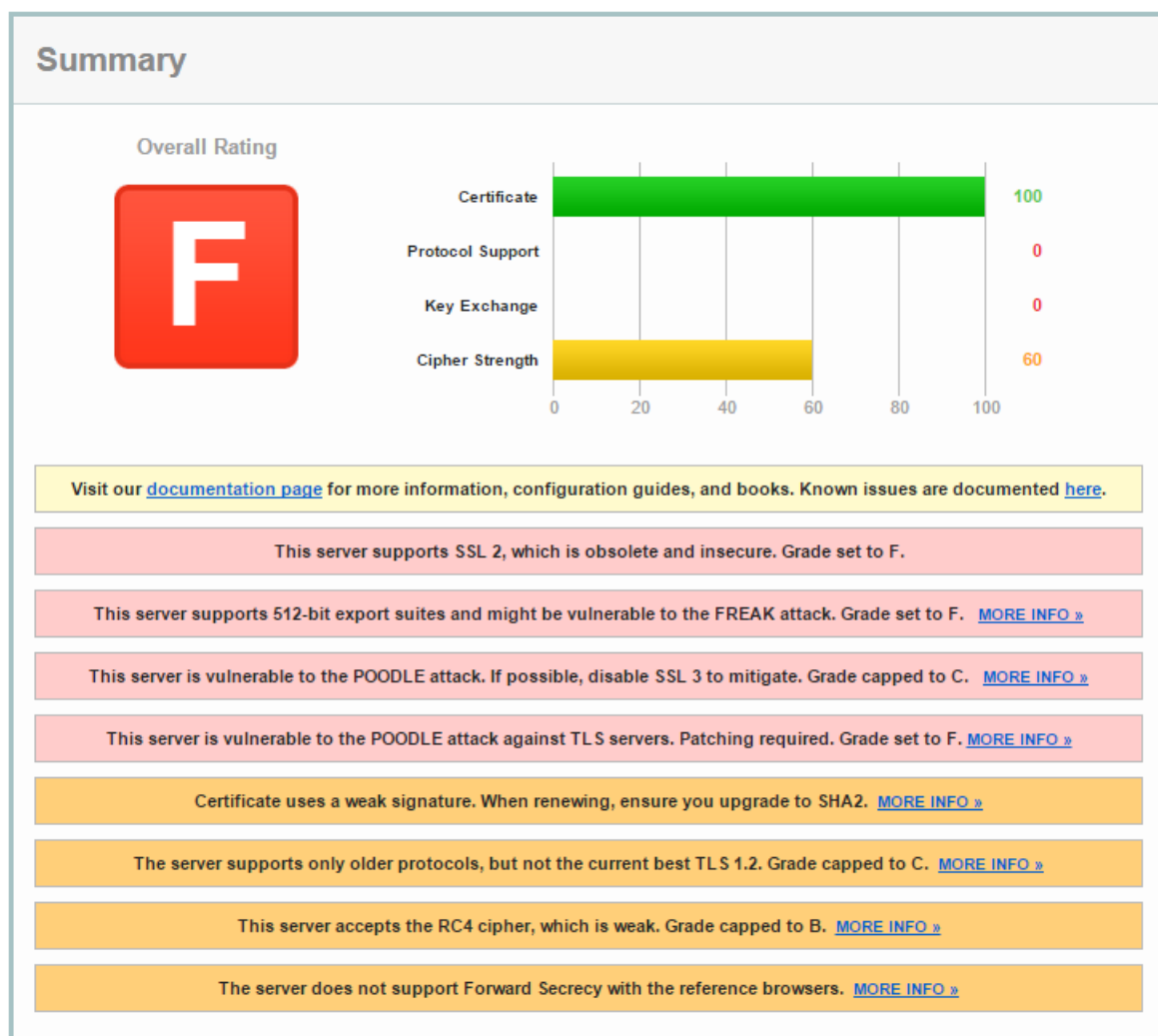


Рис. 5: Summary rzd.ru

| | | |
|-----------|----------|-----|
| Protocols | | |
| TLS 1.2 | | No |
| TLS 1.1 | | No |
| TLS 1.0 | | Yes |
| SSL 3 | INSECURE | Yes |
| SSL 2 | INSECURE | Yes |

Рис. 6: Protocols rzd.ru

происходит от фразы «Factoring attack on RSA-EXPORT Keys», означающей способ подбора открытых ключей к «экспортному»

Рис. 7: Алгоритм подписи rzd.ru

шифрованию RSA. Суть уязвимости заключается в том, что злоумышленники могут заставить браузеры использовать более слабое шифрование, чем принято обычно. Тогда они смогут взломать его за считанные часы, получив не только доступ к чужим личным данным, но и возможность управлять содержимым страниц в браузере вплоть до кнопки лайка Фейсбука.

Причина появления FREAK лежит в старом требовании властей США, принятом ещё в 1990-е годы. После внедрения шифрования в браузер от Netscape государство требовало от технологических компаний оставлять в своих алгоритмах шифрования «лазейку» для спецслужб при экспортировании своих продуктов за рубеж.

Агентства вроде АНБ и ФБР опасались, что не смогут расшифровать слишком стойкий шифр, если понадобится вести слежку за пользователями в других странах. Несмотря на то, что требование не применять сильную криптозащиту в «экспортных» продуктах было снято в конце 1990-х, более слабое шифрование было интегрировано в множество программ и оставалось незамеченным публикой до недавнего времени.

«Экспортное» шифрование использовало ключи безопасности длиной в 512 бит, а не 1024, как было принято обычно. По данным исследователей, такой ключ можно было подобрать в течение семи часов при помощи мощности 75 обычных компьютеров или аренды аналогичной мощности за 100 долларов в «облачном» сервисе вроде Amazon Web Services. Демонстрацию подбора 512-битного ключа впервые публично провели в 1999 году.

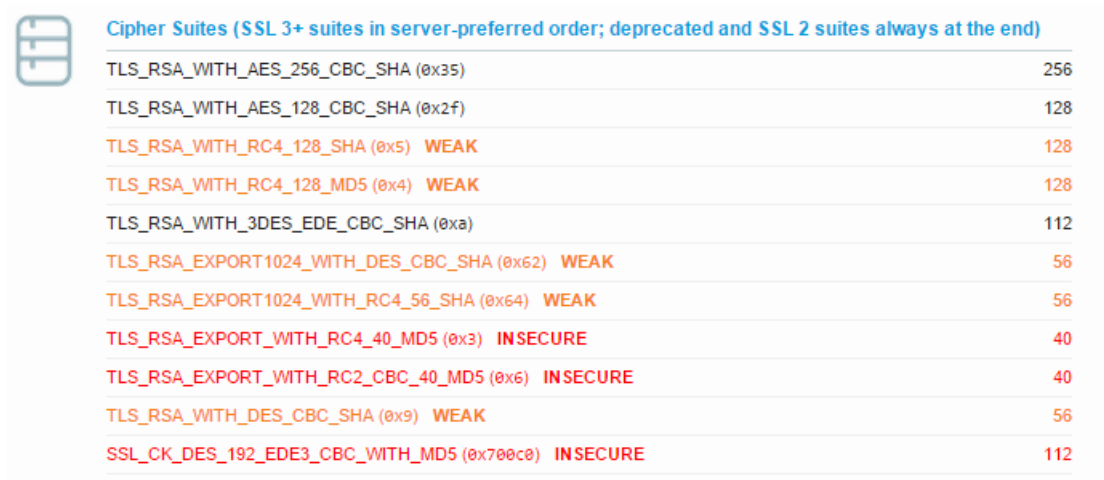
- This server supports SSL 2, which is obsolete and insecure. Grade set to F.

Поддержка SSL2, который считается устаревшим и не безопасным.

2.5.2 Расшифровать все аббревиатуры шифров в разделе Configuration

На рисунке 8 приведены используемые шифры. Ниже расшифровка аббревиатур:

- TLS (англ. Transport Layer Security — безопасность транспортного уровня), как и его предшественник SSL (англ. Secure Sockets Layer — уровень защищённых сокетов) — криптографические протоколы, обеспечивающие защищённую передачу данных между узлами



| | | |
|--|----------|-----|
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) | | 256 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) | | 128 |
| TLS_RSA_WITH_RC4_128_SHA (0x5) | WEAK | 128 |
| TLS_RSA_WITH_RC4_128_MD5 (0x4) | WEAK | 128 |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) | | 112 |
| TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x62) | WEAK | 56 |
| TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x64) | WEAK | 56 |
| TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) | INSECURE | 40 |
| TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) | INSECURE | 40 |
| TLS_RSA_WITH_DES_CBC_SHA (0x9) | WEAK | 56 |
| SSL CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) | INSECURE | 112 |

Рис. 8: Ипользуемые шифры rzd.ru

в сети Интернет[1]. TLS и SSL используют асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

- SSL (англ. secure sockets layer — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
- RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.
- Advanced Encryption Standard (AES), также известный как Rijndael — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.
- Режим сцепления блоков шифротекста (англ. Cipher Block Chaining, CBC) — один из режимов шифрования для симметричного блочного шифра с использованием механизма обратной связи. Каждый


блок открытого текста (кроме первого) побитово складывается по модулю 2 (операция XOR) с предыдущим результатом шифрования.

- Secure Hash Algorithm 1 — алгоритм криптографического хеширования. Описан в RFC 3174. Для входного сообщения произвольной длины (максимум $2^{64} - 1$ бит, что примерно равно 2 эксабайта) алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом сообщения. Используется во многих криптографических приложениях и протоколах.
- RC4 (англ. Rivest cipher 4 или англ. Ron's code, также известен как ARCFOUR или ARC4 (англ. alleged RC4)) — потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA).
- MD5 (англ. Message Digest 5) — 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности.
- Triple DES (3DES) — симметричный блочный шифр, созданный Уитфилдом Диффи, Мартином Хеллманом и Уолтом Тачманном в 1978 году на основе алгоритма DES, с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом полного перебора ключа.

2.5.3 Прокомментировать большинство позиций в разделе Protocol Details

Прокомментируем позиции в разделе Protocol Details. (см. рисунок 9)

- Secure Renegotiation - Supported.
Сервер поддерживает безопасное пересогласование ключей.
- POODLE (SSLv3) Vulnerable INSECURE (more info), POODLE (TLS) Vulnerable INSECURE (more info), Downgrade attack prevention No, TLS_FALLBACK_SCSV not supported (more info)
Существует поддержка SSL3, и при этом не установлен механизм TLS_FALLBACK_SCSV. Таким образом клиент может соединиться с сервером используя SSL3, в этом случае может быть использована атака POODLE.



| Protocol Details | |
|---|--|
| Secure Renegotiation | Supported |
| Secure Client-Initiated Renegotiation | No |
| Insecure Client-Initiated Renegotiation | No |
| BEAST attack | Not mitigated server-side (more info) SSL 3: 0x35, TLS 1.0: 0x35 |
| POODLE (SSLv3) | Vulnerable INSECURE (more info) |
| POODLE (TLS) | Vulnerable INSECURE (more info) |
| Downgrade attack prevention | No, TLS_FALLBACK_SCSV not supported (more info) |
| TLS compression | No |
| RC4 | Yes WEAK (more info) |
| Heartbeat (extension) | No |
| Heartbleed (vulnerability) | No (more info) |
| Open SSL CCS vuln. (CVE-2014-0224) | No (more info) |
| Forward Secrecy | No WEAK (more info) |
| Next Protocol Negotiation (NPN) | No |
| Session resumption (caching) | No (IDs assigned but not accepted) |

Рис. 9: Описани протокола rzd.ru

Прочие моменты комментировались выше.

2.5.4 Сделать итоговый вывод о реализации SSL на заданном домене

Как видно из оценки и прочих данных реализация SSL на сайте rzd.ru не очень хороша. Существует ряд уязвимостей и атак, которыми могут воспользоваться злоумышленники.

3 Вывод

В результате выполнения работы были изучены лучшие практики по развертыванию SSL, возможные уязвимости. Получен опыт использования инструмента тестирования SSL на сервере (SSL Server Test). Помимо этого в ходе обнаружения недостатков серверов были изучены какие типы атак могут быть совершены на них, причины этого и каким образом можно предотвращать эти атаки.