Лабораторная работа №6.
SSL/TLS

Климов Сергей

14 мая 2016 г.

Оглавление

1 Цель работы

- Изучить лучшие практики по развертыванию SSL/TLS.
- Изучить основные уязвимости и атаки на SSL последнего времени - POODLE, HeartBleed.

2 Изучение практик по развертыванию SSL/TLS

- Использование 2048-битных закрытых ключей, например:
  - 2048-битный RSA
  - 256-битные ECDSA закрытые ключи.
- Необходимо защищать закрытые ключи, предоставляя доступ к ним как можно меньшему числу сотрудников. Рекомендуемые меры:
  - Генерируйте закрытые ключи и запросы на сертификат (CSRs) на доверенном компьютере. Некоторые CA предлагают генерацию ключей и CSRs для вас, но это нецелесообразно.
  - Используйте парольную защиту закрытых ключей, чтобы предотвратить их компрометацию в тех случаях, когда они хранятся в резервных системах. Парольная защита закрытых ключей не помогает на промышленном сервере, потому что злоумышленник может получить ключи из процесса памяти. Есть аппаратные устройства, которые могут защитить секретные ключи даже в случае компрометации сервера, но они стоят дорого и, таким образом, оправданы только в организациях с высокими требованиями безопасности.
  - После компрометации отзывайте старые сертификаты и генерируйте новые ключи.
  - Обновляйте сертификаты каждый год и всегда с новыми закрытыми ключами.
- Необходимо обеспечить охват всех используемых доменных имен, которые будут использоваться.
- Приобретение сертификатов у надежного удостоверяющего центра.
- Использование надежных алгоритмов подписи сертификата.
- Использование безопасных протоколов, например TLS v1.0 - TLS v1.2.
- Использование безопасных алгоритмов шифрования, т.е. только те алгоритмы шифрования, которые обеспечивают аутентификацию и шифрование в 128 бит или более.
- Контроль выбора алгоритма шифрования. В SSL версии 3 и более поздних версиях протокола, клиенты отправляют список алгоритмов шифрования, которые они поддерживают, и сервер выбирает один из них для организации безопасного канала связи. Не все сервера могут делать это хорошо, так как некоторые выбирают первый поддерживаемый алгоритм из списка. Таким образом, выбор правильного алгоритма шифрования является критически важным для безопасности.
- Поддержка Forward Secrecy. Forward Secrecy — это особенность протокола, который обеспечивает безопасный обмен данными, он не зависит от закрытого ключа сервера. С алгоритмами шифрования, которые не поддерживают Forward Secrecy, возможно расшифровать ранее зашифрованные разговоры с помощью закрытого ключа сервера. Нужно поддерживать и предпочитать ECDHE алгоритмы шифрования. Для поддержки более широкого круга клиентов, вы должны также использовать DHE, как запасной вариант после ECDHE.

3 Уязвимости POODLE и HeartBleed

- POODLE (CVE-2014-3566) - Для получения доступа к данным злоумышленники вначале должны эмулировать несовместимость реализаций защищенного соединения между клиентом и сервером для того, чтобы клиентское ПО инициировало переход от более безопасных протоколов TLS на уровень SSL 3.0 – т.н. “downgrade dance”. После этого у злоумышленников появляется возможность получить доступ к критичной информации – например, к заголовкам, которые хранят в cookie авторизационную информацию. Атака возможна по схеме Man in the middle – хакер должен перехватывать информацию между клиентом и сервером и иметь возможность модифицировать ее.
- Heartbleed (CVE-2014-0160) - 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. Heartbleed осуществляется отправкой некорректно сформированного Heartbeat-запроса, в котором реальный размер строки очень мал, а число, символизирующее длину передаваемой строки, очень велико. Так можно получить в ответ от сервера больше всего скрытой информации. Таким образом, у жертвы возможно за один запрос узнать до 64 килобайт памяти, которая была ранее использована OpenSSL.

4 Изучение отчетов ресурса SSL Server Test

4.1 Домен из раздела Recent Best

В качестве домена из раздела Recent Best был выбран домен black-khat.com (203.7.2.247). Отчет представлен на рисунке 1.

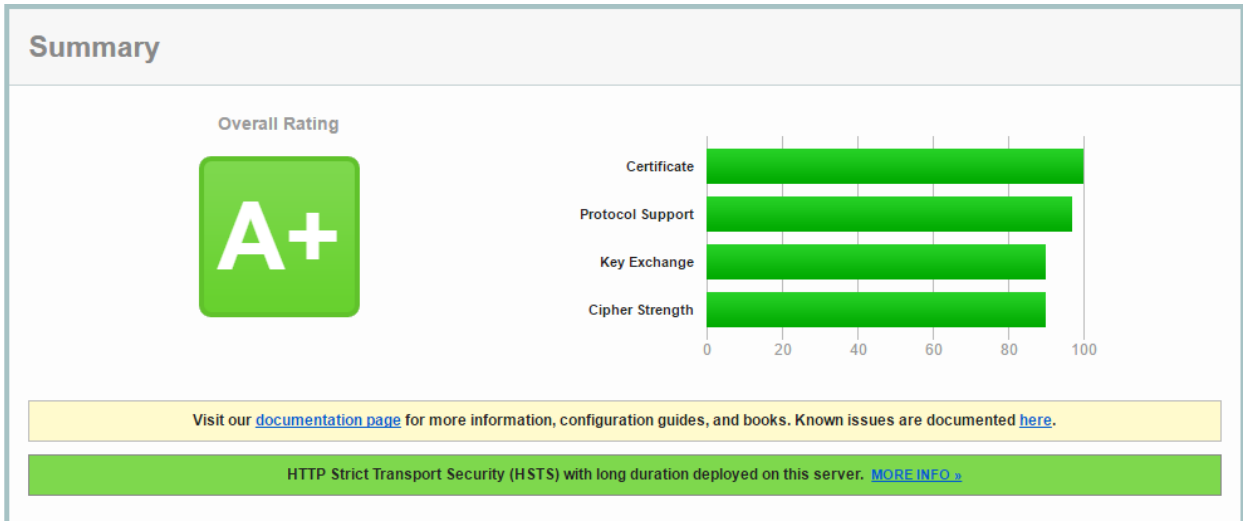

Рис. 1: Отчет для сайта black-khat.com

Данный сервер поддерживает длительное форсированное защищенное соединение через HTTPS, что позволяет сразу же устанавливать безопасное соединение, вместо использования HTTP-протокола. Механизм использует особый заголовок Strict-Transport-Security для принудительного использования браузером протокола HTTPS даже в случае перехода по ссылкам с явным указанием протокола HTTP.

В качестве домена из раздела Recent Worst был выбран домен secure.ecommerce.aliant.net (142.166.145.159). Отчет представлен на рисунке 2.

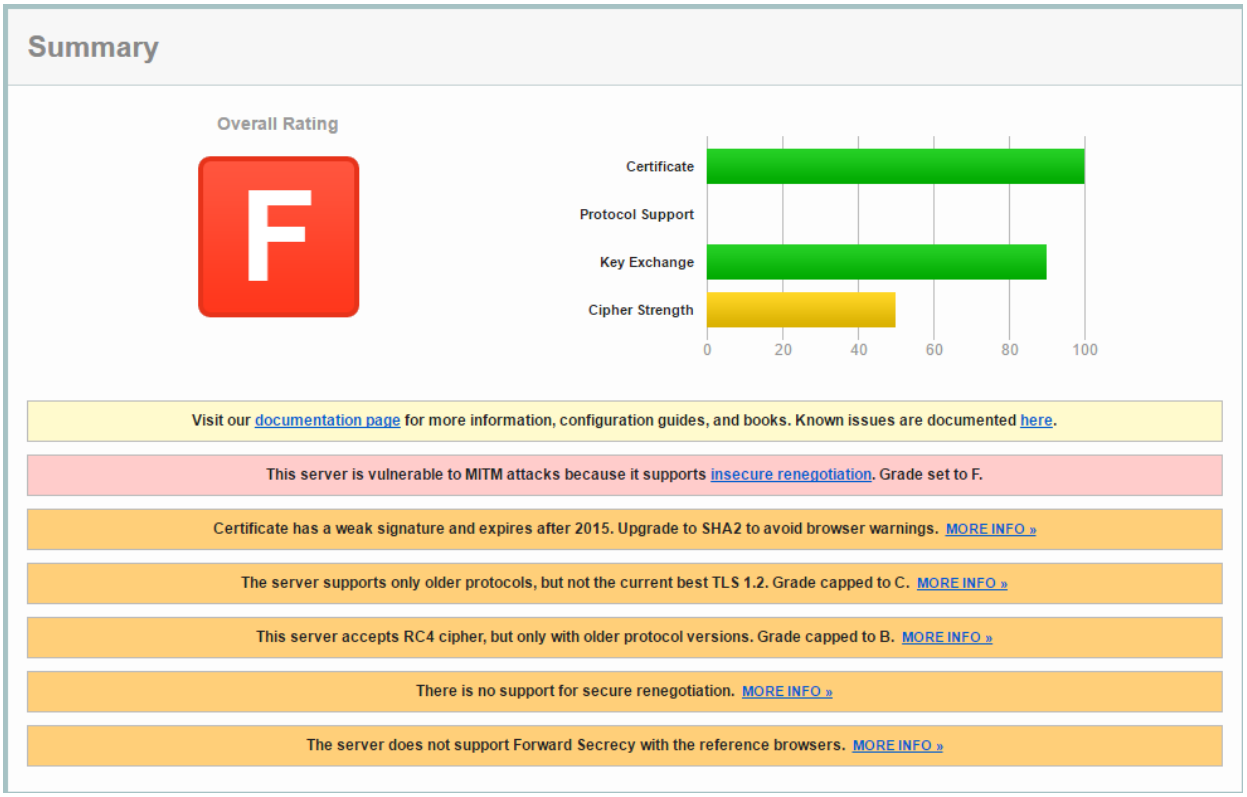

Рис. 2: Отчет для сайта secure.ecommerce.aliant.net

- Этот сервер подвержен MITM атакам;
- Сертификат имеет слабое шифрование подписи и истекает после 2015г.

- Сервер поддерживает только старые протоколы TLS, а не современную его версию - 1.2.
- Этот сервер принимает шифр RC4, но только с более старыми версиями протокола.
- Сервер не поддерживает Forward Security для браузеров.

Для самостоятельного анализа был выбран сервер bankofamerica.com (171.161.148.150). Результаты анализа приведены на рисунке 3

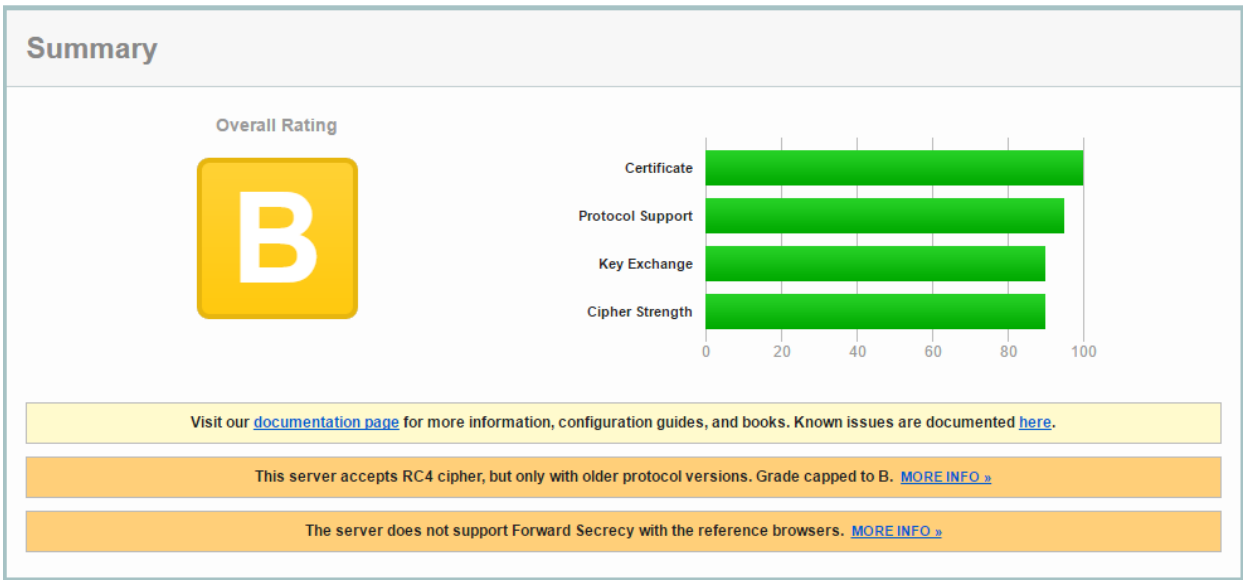

Рис. 3: Отчет для сайта bankofamerica.com

Как видно из рисунка 3, сервис bankofamerica.com поддерживает все типы протоколов TLS, однако он принимает шифр RC4 только с более старыми версиями протокола и не поддерживает Forward Security для браузеров.

4.2 Расшифровка аббревиатур

Аббревиатуры представлены ниже:

```
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)   256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)      256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)   128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)      128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)      112
TLS_RSA_WITH_RC4_128_SHA (0x5)    INSECURE        128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)   ECDH secp256r1 (eq. 3072 bits RSA)   FS   256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)   ECDH secp256r1 (eq. 3072 bits RSA)   FS   128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)   ECDH secp256r1 (eq. 3072 bits RSA)   FS
```

Расшифровка аббревиатур:

- TLS_ECDHE - алгоритм Диффи-Хэлмана на эллиптических кривых;
- RSA - алгоритм шифрования с открытым ключем;
- AES_128 - алгоритм шифрования с длиной ключа в 128 бит;
- GCM и CBC - режимы блочного шифрования;
- SHA256 - хэш-функция с длиной ключа 256 бит.

4.3 Описание позиций в разделе Protocol Details

Содержимое раздела Protocol Details представлено ниже:

- Проверка сертификата:

```
Secure Renegotiation     Supported
Secure Client-Initiated Renegotiation    No
Insecure Client-Initiated Renegotiation No
```

- Уязвимость к атакам Poodle, Bcast, Downgrade

```
BEAST attack     Not mitigated server-side (more info)    TLS 1.0: 0xc035
POODLE (SSLv3)   No, SSL 3 not supported (more info)
POODLE (TLS)     No (more info)
Downgrade attack prevention      Yes, TLS_FALLBACK_SCSV supported (more info)
```

- Используется слабый алгоритм RC4

```
RC4      Yes    INSECURE (more info)
```

- Сервер защищен от атак HeartBleed

```
Heartbeat (extension)    No
Heartbleed (vulnerability)       No (more info)
```

- Совместимость Forward Security с браузерами

```
Forward Secrecy With some browsers (more info)
```

- Не поддерживает ALPN и NPN

```
ALPN     No
NPN      No
```

- Параметры сессии.

```
Session resumption (caching)     No (IDs assigned but not accepted)
Session resumption (tickets)     No
```

- Реализация HSTS.

```
Strict Transport Security (HSTS)         No
HSTS Preloading Not in: Chrome  Edge  Firefox  IE  Tor
```

- Реализация HPKP (отсутствует).

```
Public Key Pinning (HPKP)        No
```

- Совместимость с SSL2 (совместим).

```
SSL 2 handshake compatibility    Yes
```

4.4 Вывод о реализации SSL на выбранном домене

Исходя из отчета, сервис bankofamerica.com имеет среднюю защищенность: использует доверенный сертификат и защищен от основных типов атак, однако сервер использует устаревший алгоритм RC4, который является уязвимым. Так же сервис имеет поддержку Forward Security для большинства браузеров.

5 Выводы

В данной лабораторной работе было произведено озакомление с сервисом проверки защищенности серверов Qualys SSLLABS и рассмотрены последние самые опасные уязвимости: POODLE и HeartBeat. Были рассмотрены отчеты по безопасности различных серверов с разными рейтингами. Были рассмотрены основные параметры, которые сервис прверяет на предмет защищенности сервера, их существует достаточно большое количество, поэтому настоить сервер на использование безопасного соединения с должной степенью защищенности является нетривиальной задачей.