Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий

Сервис тестирования корректности настройки SSL на сервере Qualys SSL Labs – SSL Server Test

Выполнил: Сухинин А.А. гр. 53501/3 _____
Принял: Выглежанина К.Д. _____

2015 г.

1 Цель работы

Изучить лучшие практики по развертыванию SSL/TLS, ознакомиться с основными уязвимостями, оценить возможности сервиса SSL Server Test.

2 Ход работы

2.1 Изучение

Изучить лучшие практики по развертыванию SSL/TLS

1. Используйте 2048 битные приватные ключи.
2. Хорошо защищайте приватные ключи.
3. Обеспечивайте эффективное покрытие доменных имен, возможно даже с избытком.
4. Получайте сертификаты от надежных и соответствующих CA.
5. Используйте сильные алгоритмы для подписи. Например, хэширующая функция SHA1 считается уже недостаточно надежной. Вместо нее следует использовать SHA2.
6. Настраивайте систему для работы с несколькими сертификатами одновременно.
7. Не используйте протокол SSL v2. Протоколам SSL v3 и TLS v1.0 также лучше предпочитать TLS v1.1 и TLS v1.2
8. Используйте защищенные алгоритмы симметричного шифрования. Ключи должны быть не менее 128 бит. Не следует использовать RC4.
9. Используйте Forward Secrecy. Данная возможность позволяет защищенную передачу информации не зависящую от приватного ключа. Поэтому, в случае его утечки все накопленная ранее информация не будет открыта.
10. Запрещайте проверку защищенности со стороны клиента
11. Не используйте слишком много защиты, так как это может привести к низкой производительности.
12. Используйте защищенные cookies.

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

Принцип использования уязвимости HeartBleed представлен на рис. 1. Данной атаке подвержены следующие версии OpenSSL:

1. OpenSSL 1.0.2-beta
2. OpenSSL 1.0.1 - OpenSSL 1.0.1f

Рис. 1. Принцип использования уязвимости.

Уязвимость POODLE позволяет злоумышленнику 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 атакуемого. 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.

2.2 Практическое задание

Выбрать со стартовой страницы SSL Server Test один домен из списка Recent Best и один домен из списка Recent Worst – изучить отчеты, интерпретировать результаты в разделе Summary

SSL Report: syndle.nl (141.138.202.120)

Сервер защищен от down-grade атаки. Не использует слабозащищенных протоколов и алгоритмов. Небольшие "недостатки"касаются того, что сервер не поддерживает слишком старые версии аутентификации. Например для IE 6.

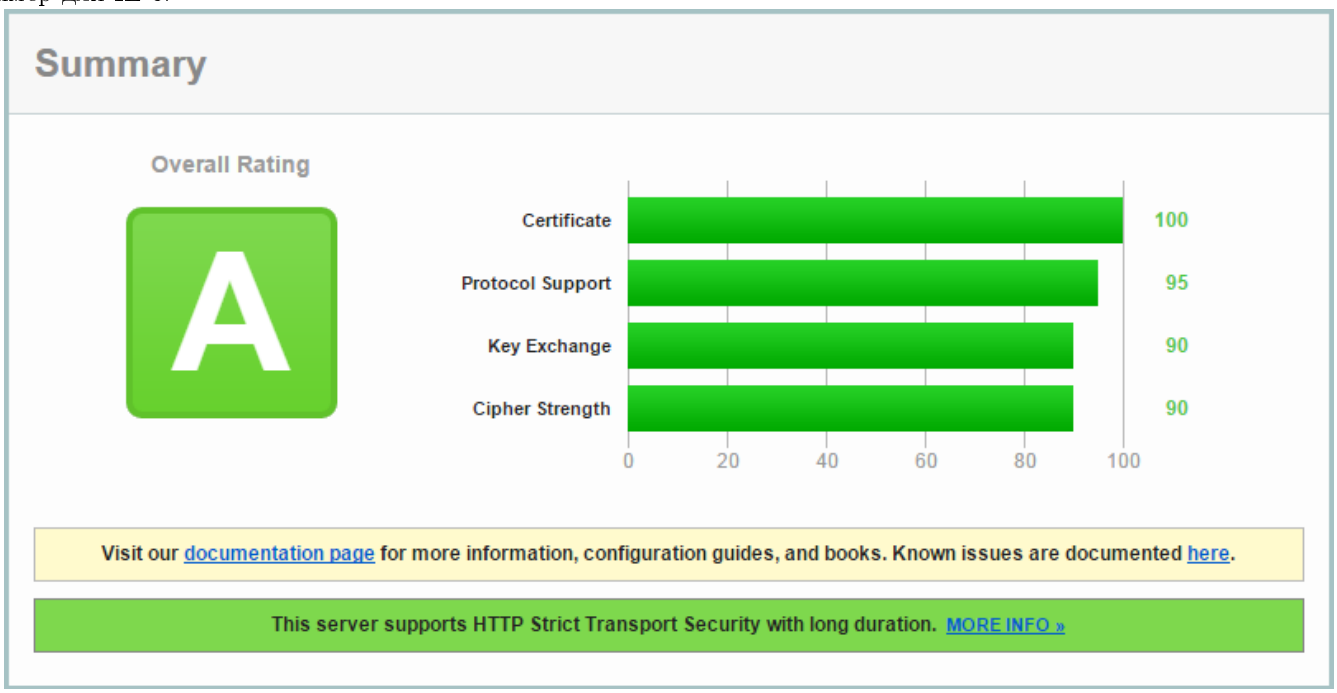

Рис. 2. Summary recent best.

SSL Report: sminc-owncloud.ddns.net (86.135.169.104)

Данный сервер настроен похожим образом. Единственная его проблема то, что сертификат не подтвержден. Вероятно используется самподписанный сертификат. Однако это не является большой проблемой, если проект находится в процессе разработки.

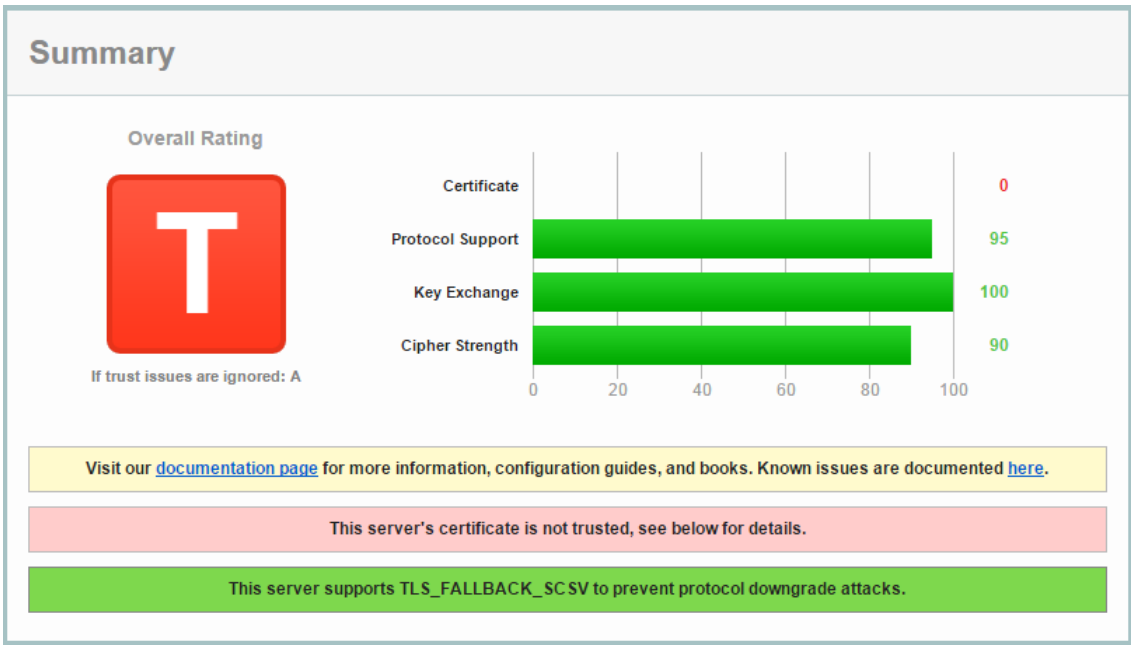

Рис. 2. Summary recent worst.

SSL Report: fwallet.tk (151.80.164.83)

Для исследования был выбран сервер, используемый в текущем учебном проекте. Данный сервер имеет ряд существенных недостатков:

1. Использование слабых параметров для алгоритма Диффи-Хелмана во время обмена ключами.
2. Сервер подвержен атаке POODLE, следует отключить SSL v3.
3. Сервер поддерживает алгоритм потокового шифрования RC4, который является недостаточно надежным.
4. Сервер не поддерживает Forward Secrecy, таким образом в случае утечки секретного ключа, данные пользователей могут быть расшифрованы.

В то же время сервер не подвержен down-grade атакам.

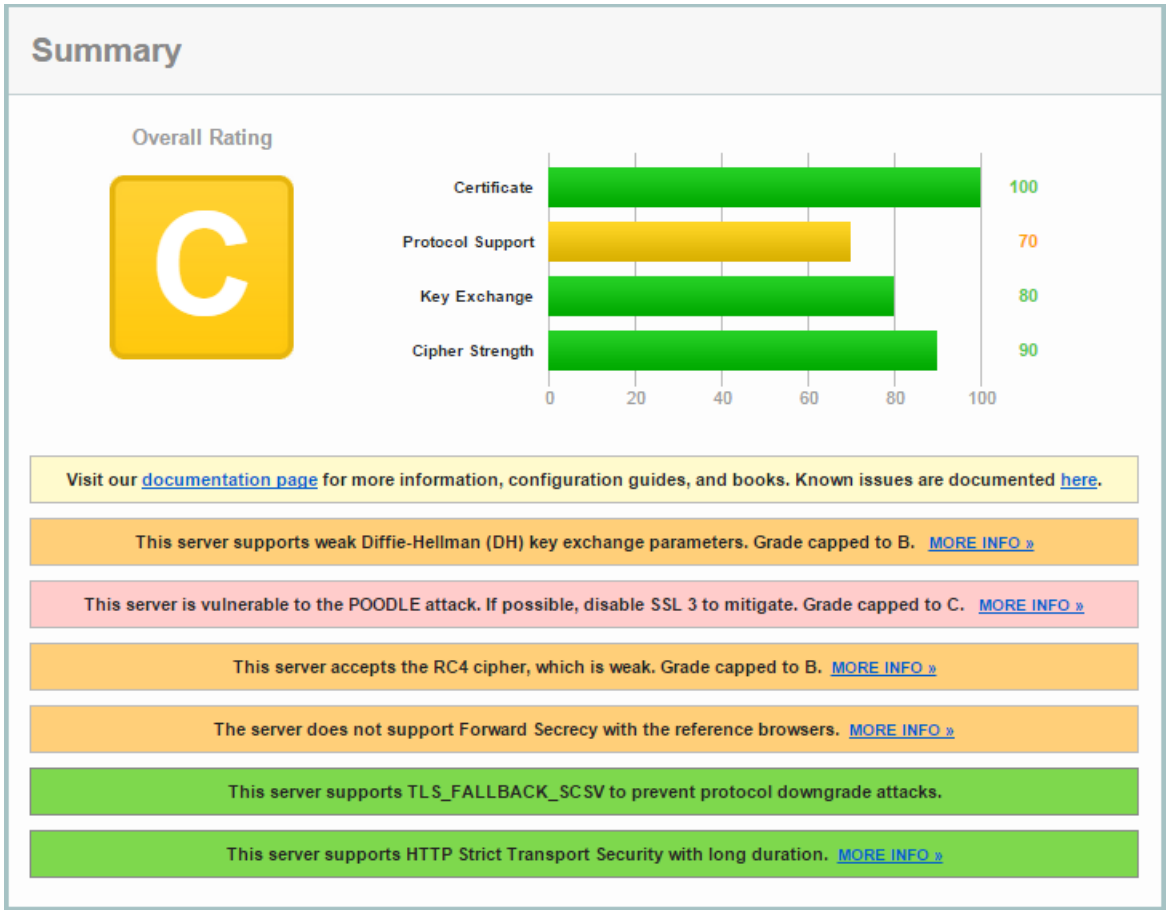

Рис. 3. Сервер, поддерживающий SSL/TLS.

Расшифровать все аббревиатуры шифров в разделе Configuration

Каждая строка содержит информацию об используемых алгоритмах:

1. для обмена ключами
2. для шифрования сообщений
3. информацию о режиме шифрования
4. используемой хэширующей функции

Для обмена ключами используются два алгоритма RSA и DHE(Diffie-Hellman Ephemeral).

Для симметричного шифрования данных используются алгоритмы RC4(потоковый алгоритм, слабозащищен), AES (все хорошо), camellia, SEED (на основе сетей фейстеля).

В качестве хэширующей функции используется SHA и SHA256 битный.

Также используются два режима шифрования CBC (chaining block chiper) и GCM (Galois/Counter mode)

```
TLS_RSA_WITH_RC4_128_SHA (0x5)   WEAK 128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 128
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41) 128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 128
TLS_RSA_WITH_SEED_CBC_SHA (0x96) 128
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x9a)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 112
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 256
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84) 256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)   DH 1024 bits (p: 128, g: 1, Ys: 128)   FS   WEAK 256
```

Прокомментировать большинство позиций в разделе Protocol Details

Первые три пункта касаются пересмотра сертификата и защищенности этого процесса.

Далее идет отчет об уязвимостях POODLE, BEAST и down-grade attack.

Сообщение о том, что используется слабый алгоритм RC4.

Статус уязвимости heartbleed.

Предупреждение что Forward Secrecy не всегда работает.

Предупреждение о слабых параметрах алгоритма DH.

Совместимость с SSL v2 handhake.

```
Secure Renegotiation Supported
Secure Client-Initiated Renegotiation No
Insecure Client-Initiated Renegotiation No
BEAST attack Not mitigated server-side (more info)   SSL 3: 0x2f, TLS 1.0: 0x2f
POODLE (SSLv3) Vulnerable   INSECURE (more info)
POODLE (TLS) No (more info)
Downgrade attack prevention Yes, TLS_FALLBACK_SCSV supported (more info)
TLS compression No
RC4 Yes   WEAK (more info)
Heartbeat (extension) Yes
Heartbleed (vulnerability) No (more info)
OpenSSL CCS vuln. (CVE-2014-0224) No (more info)
Forward Secrecy With some browsers (more info)
Next Protocol Negotiation (NPN) No
Session resumption (caching) Yes
Session resumption (tickets) Yes
OCSP stapling No
Strict Transport Security (HSTS) Yes   max-age=31536000; includeSubDomains
Public Key Pinning (HPKP) No
Long handshake intolerance No
TLS extension intolerance No
TLS version intolerance No
Incorrect SNI alerts -
Uses common DH prime Yes   Replace with custom DH parameters if possible (more info)
SSL 2 handshake compatibility Yes
```

Сделать итоговый вывод о реализации SSL на заданном домене

Конфигруация сервера, обслуживающего данный домент сделана плохо, либо не сделана вообще. Сервер использует доверенный сертификат и защищен от некоторых атак (heart-bleed, down-grade, beast), однако все же содержит уязвимости (poodle, использование алгоритма RC4 и т.п.). Кроме того, сервер не поддерживает forward secrecy для всех браузеров, что является дополнительной угрозой. В качестве итога, можно сказать, что в случае необходимости специалист способен нанести значительный урон данному сервису. Таким образом, первичными задачами для исправления являются:

1. Настройка алгоритма DH
2. Отключение SSL v3
3. Отключение протокола RC4

3 Выводы

В ходе данной работы были изучены "best practice"использования SSL/TLS. Были рассмотрены основные возможности сервиса Qualys SSL Labs – SSL Server Test. Данный сервис позволяет провести анализ качества защищенности домена. В качестве резюме можно получить статус самых известных уязвимостей для данной сервера, а также информацию о поддерживаемых протоколах и режимах работы. Кроме того, сервис тут же предлагает дополнительную информацию по вопросам решения указанных проблем.

В качестве вывода, можно отметить важность анализа конфигурации SSL/TLS, особенно, при коммерческом использовании. Данный анализ можно удобно выполнить при помощи данного инструмента, однако если требуется особенно тщательная проверка, то она должна быть проведена дополнительно.