

Санкт-Петербургский Политехнический Университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Методы и средства защиты информации

Отчет по лабораторной работе №5

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

Работу выполнил:

Косолапов С.А.

Группа: 53501/3

Преподаватель:

Вылегжанина К.Д.

Санкт-Петербург
2016

Содержание

1	Цель работы	2
2	Программа работы	2
2.1	Изучение	2
2.2	Практическое задание	2
3	Изучение	2
3.1	Изучить лучшие практики по развертыванию SSL/TLS	2
3.2	Изучить основные уязвимости и атаки на SSL последнего времени – POODLE, HeartBleed	3
3.2.1	POODLE	3
3.2.2	HeartBleed	4
4	Практическое задание	6
4.1	Recent Best	6
4.1.1	Интерпретировать результаты в разделе Summary	6
4.1.2	Расшифровать все аббревиатуры шифров в разделе Configuration	7
4.1.3	Прокомментировать большинство позиций в разделе Protocol Details	8
4.1.4	Сделать итоговый вывод о реализации SSL на заданном домене	9
4.2	Recent Worst	9
4.2.1	Интерпретировать результаты в разделе Summary	9
4.2.2	Расшифровать все аббревиатуры шифров в разделе Configuration	9
4.2.3	Прокомментировать большинство позиций в разделе Protocol Details	11
4.2.4	Сделать итоговый вывод о реализации SSL на заданном домене	12
5	Выводы	12

1 Цель работы

Ознакомиться с особенностями протокола SSL и сервисом, предоставляющим возможность тестирования корректности настройки серверов с SSL.

2 Программа работы

2.1 Изучение

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

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. Выбрать для анализа интернет-домен защищенный SSL-шифрованием (старайтесь выбрать что-то достаточно известное, но не слишком очевидное), проделать следующие шаги:

1. Интерпретировать результаты в разделе Summary
2. Расшифровать все аббревиатуры шифров в разделе Configuration
3. Прокомментировать большинство позиций в разделе Protocol Details
4. Сделать итоговый вывод о реализации SSL на заданном домене

3 Изучение

3.1 Изучить лучшие практики по развертыванию SSL/TLS

Актуальная версия от SSL Labs от 8 июня 2016 года: ¹.

1. Закрытый ключ и сертификат
 - (a) Использование надёжных закрытых ключей, для большинства веб-сайтов достаточно 2048 бит
 - (b) Защитить закрытые ключи: генерировать на доверенном компьютере, не доверять генерацию центрам сертификации (CA); изначально защищать ключи паролем, чтобы исключить компрометацию во время бэкапов; если произошла компрометация, немедленно отзываться сертификаты и выдавать новые; обновлять сертификаты как можно чаще; генерировать новые закрытые ключи с новым сертификатом
 - (c) Убедиться в достаточном покрытии имён хоста
 - (d) Приобретать сертификаты у надёжных CA
 - (e) Использовать стойкие алгоритмы подписи сертификатов: безопасность сертификата зависит от 1) надёжности закрытого ключа и 2) того, насколько сильная будет функция цифровой подписи. До последнего времени использовалась SHA1, которая сейчас считается небезопасной, и осуществляется переход на SHA256
2. Конфигурация
 - (a) Использование полных цепочек сертификатов: исключение ситуаций, когда отсутствуют промежуточные сертификаты
 - (b) Использование защищённых протоколов:
 - SSLv2 небезопасен
 - SSLv3 небезопасен при использовании с HTTP (POODLE атака)
 - TLS v1.0 не рекомендуется использовать, однако на практике необходим; главное слабое место - BEAST - устранено для большинства браузеров, но по-прежнему остаются другие проблемы

¹<https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>

- TLS v1.1 и TLS v1.2 - оба на данный момент без вопросов к безопасности, однако новые алгоритмы использует только v1.2, поэтому ориентироваться надо на него
- (c) Использование защищённых шифров: нужно исключить использование ADH, RC4, 3DES и других устаревших методов шифрования
- (d) Выбрать лучшие шифры
- (e) Использование Perfect Forward Secrecy (свойство некоторых протоколов, которое гарантирует при скомпрометированном одном закрытом ключе не будут скомпрометированы сессионные ключи)
- (f) Использовать сильный обмен ключами. ECDHE лучше, чем DHE. На данный момент наилучшим выбором будет кривая secp256r1
- (g) Улучшения в отношении известных проблем

3. Производительность

- (a) Не нужно слишком много безопасности: это будет медленно
- (b) Использовать возобновление сессии
- (c) Использовать WAN-оптимизацию и HTTP/2
- (d) Кэшировать публичный контент
- (e) Использовать OCSP Stapling - проверку на предмет отозванности как часть TLS handshake
- (f) Использование быстрых криптографических примитивов

4. HTTP и безопасность приложений

- (a) Защищать всё!
- (b) Исключить смешанный контент
- (c) Осознавать и признавать "Third-Party Trust"(доверие третьей стороне) - контент может быть загружен также со сторонних сервисов, которые используются доверенным
- (d) Защищённые cookies
- (e) Безопасное сжатие HTTP
- (f) Развёртывание HSTS (HTTP Strict Transport Security) - сеть безопасности для TLS. Цель проста: после активации запрещены любые незащищённые коммуникации
- (g) Развёртывание CSP (Content Security Policy) - механизм безопасности, позволяющий ограничивать операции браузеров
- (h) Не кэшировать "чувствительный" контент
- (i) Рассматривать другие угрозы (кроме SSL/TLS)

5. Валидация. Для публичных сайтов рекомендуется SSL Labs Server Test

6. Продвинутое решения

- (a) Public Key Pinning
- (b) DNSSEC и DANE

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

3.2.1 POODLE

Padding Oracle On Downgraded Legacy Encryption (CVE-2014-3566) - именно так расшифровывается название. Уязвимость позволяет расшифровать содержимое зашифрованного канала коммуникации SSL v3.0.

SSL v3.0 использует шифр RC4. По статистике Microsoft 2013 года², почти 39% коммуникаций осуществляется с использованием RC4. К сожалению, более свежую статистику найти не удалось, но сейчас RC4, судя по всему, практически не используется.

²<https://blogs.technet.microsoft.com/srd/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4/>

По классификации это атака типа Man In The Middle (Человек посередине). Злоумышленник отправляет на сервер свои данные по протоколу SSLv3 от имени цели, и постепенно он может расшифровывать данные ответов на запросы, что возможно, так как у SSLv3 нет привязки к MAC-адресу.

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.³

Для защиты от атаки лучше всего не использовать SSLv3 как на клиентах, так и на серверах. Несмотря на то, что "заплатки" на POODLE есть для всех используемых браузеров, лучше уйти от SSLv3 к более новым и не скомпрометированным алгоритмам (каким и почему описано выше).

Схематично атаку можно изобразить следующим образом:

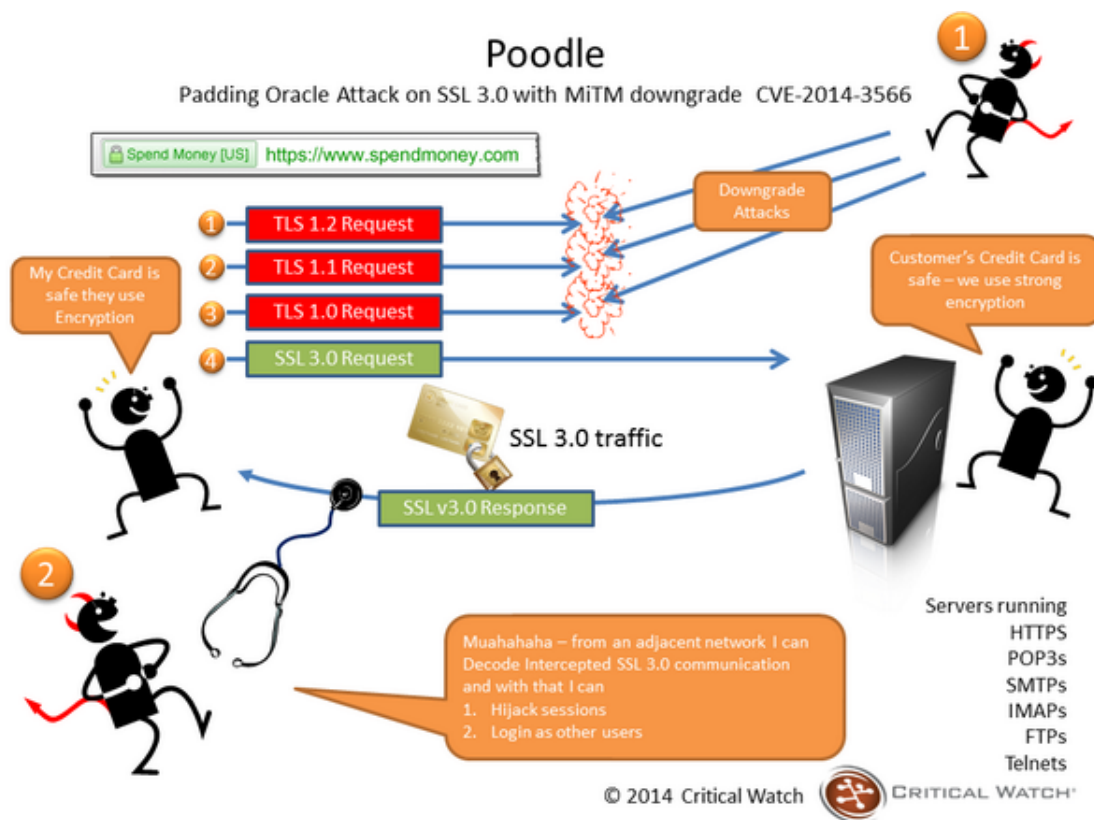


Рис. 1: Принцип работы атаки POODLE

3.2.2 HeartBleed

HeartBleed (CVE-2014-0160) - ошибка, заключающаяся в переполнении буфера в OpenSSL. Позволяет несанкционированно читать память на сервере или клиенте, в том числе и для извлечения закрытого ключа сервера. Информация об уязвимости была опубликована в апреле 2014 года, ошибка существовала с конца 2011 года. SSLv3 на тот момент использовали многие сайты, в том числе банки, платёжные системы, VPN-провайдеры, сервисы почты Yandex и Yahoo.

Подробная информация об уязвимости размещена на специальном сайте, посвящённом ей.⁴ Между тем, забавно, но при подключении по HTTPS к этой странице, выясняется, что соединение не защищено и появляется ошибка ERR_CERT_COMMON_NAME_INVALID.

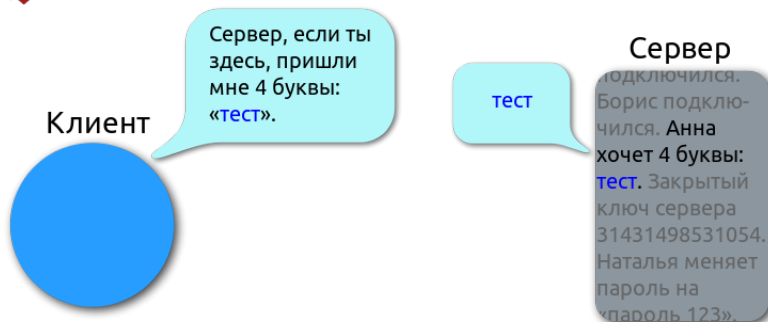
Название HeartBleed происходит от названия реализации TLS/DTLS расширения Heartbeat, в котором была найдена уязвимость. В результате эксплойта можно добиться утечки памяти как с сервера на клиент, так и с клиента на сервер. При этом никаких следов атака не оставляет, и, учитывая долгое время поддержания подключения, невозможно установить, как много и какая информация стала доступна злоумышленнику.

Схематично атаку можно изобразить следующим образом следующим образом:

³<https://habrahabr.ru/company/dsec/blog/240499/>

⁴<http://heartbleed.com/>

Heartbeat — нормальная работа



Heartbleed — эксплуатация ошибки

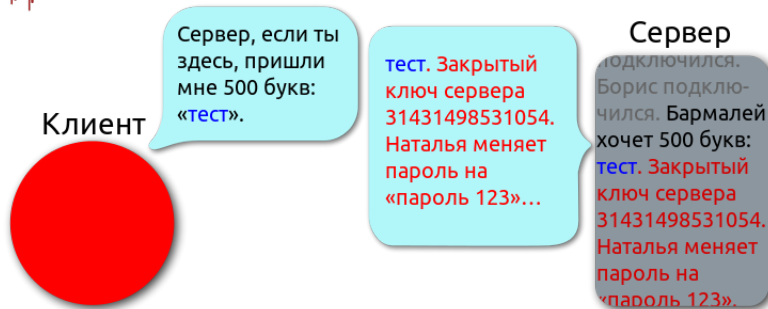


Рис. 2: Принцип работы атаки Heartbleed

4 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. Выбрать для анализа интернет-домен защищенный SSL-шифрованием (старайтесь выбрать что-то достаточно известное, но не слишком очевидное), проделать следующие шаги:

4.1 Recent Best

4.1.1 Интерпретировать результаты в разделе Summary

SSL Report: [google.ru](https://www.ssllabs.com/ssltest/analyze.html?d=google.ru) (2607:f8b0:4005:801:0:0:0:2003)

Assessed on: Mon, 27 Jun 2016 21:16:22 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

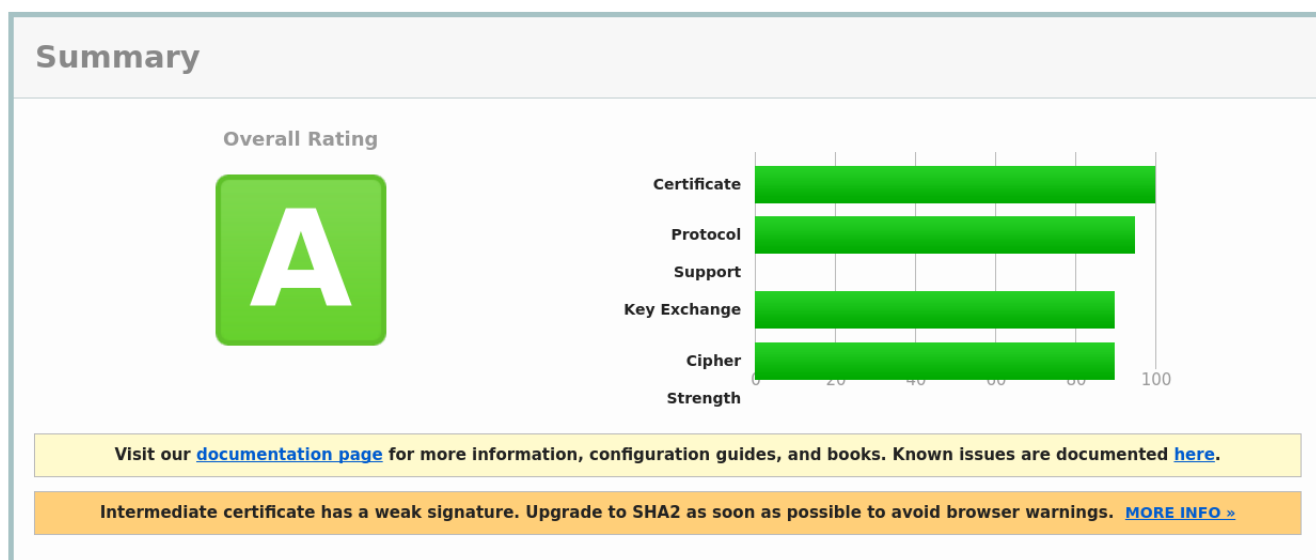


Рис. 3: Recent best: google.ru (google.com/google.at/...)

Google.com выбран, как наиболее известный домен, одна из вариаций которого (google.at) была обнаружена в recent best. Однако это не наилучший результат (A). Вот пример лучшего результата (A+):

SSL Report: [citrix.com](https://www.ssllabs.com/ssltest/analyze.html?d=citrix.com) (2001:4868:10c:3:0:0:0:15)

Assessed on: Mon, 27 Jun 2016 21:32:10 UTC | [Clear cache](#)

[Scan Another »](#)

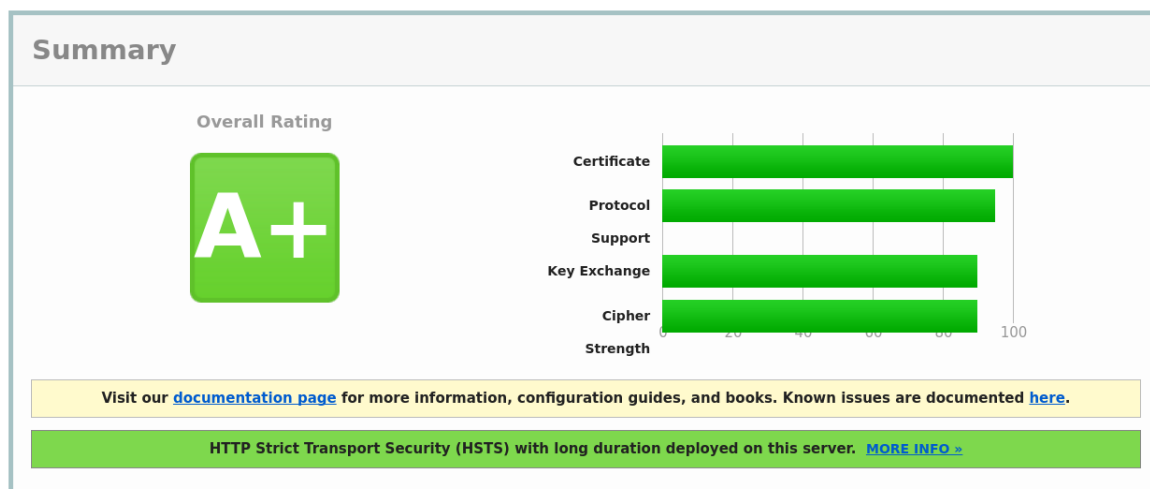


Рис. 4: Recent best A+: citrix.com

Интересно, что сигнатура одинаковая - RSA. Однако строчка описывается по-разному для сайтов. Для citrix.com:

Signature algorithm SHA1withRSA Weak, but no impact on root certificate

Для сайта google.ru.:

Signature algorithm SHA1withRSA WEAK

Однако для citrix.com есть пометка "DigiCert Global Root CA In trust store ". Т.е. доверие Root CA перевешивает недостаточно стойкий, по мнению SSL Labs, алгоритм подписи.

4.1.2 Расшифровать все аббревиатуры шифров в разделе Configuration

```
Protocols
TLS 1.2 Yes
TLS 1.1 Yes
TLS 1.0 Yes
SSL 3 No
SSL 2 No
```


Таким образом, поддерживает все современные надёжные протоколы и не поддерживает скомпрометированные SSLv3 и SSLv2.

```
Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end
→ )
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS 128
OLD_TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcc13) ECDH secp256r1 (eq. 3072 bits RSA)
→ FS 256P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH secp256r1 (eq. 3072 bits RSA) FS
→ 256P
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS 128
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) 128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) 128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) 128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) 112
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS 256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS 256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS 256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) 256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) 256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) 256
(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android
→ devices)
```

Аббревиатуры:

TLS - transport layer security
ECDHE - elliptic curve Diffie-Hellman ephemeral
RSA - Rivest, Shamir, Adelman
AES - American encryption standard
GCM SHA-256 - secure hash algorithm (256-bits) with Galois/counter mode
ChaCha - stream cipher
Poly1305 - cryptographic message authentication code
CBC - cipher block chaining

4.1.3 Прокомментировать большинство позиций в разделе Protocol Details



Protocol Details	
DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc013
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	With modern browsers (more info)
ALPN	Yes
NPN	Yes h2 spdy/3.1 http/1.1
Session resumption (caching)	Yes
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Chrome Not in: Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
SSL 2 handshake compatibility	Yes

Рис. 5: Protocol details

Сервис не поддерживает опасные протоколы, скомпрометированный потоковый шифр RC4, опасную версию OpenSSL, тем самым исключая распространённые атаки: DROWN, BEAST, POODLE, Heartbleed. Поддерживает безопасное повторное установление соединения, поддерживает ALPN, закрепление открытого ключа, HSTS предзагрузку, OSCP stapling.

4.1.4 Сделать итоговый вывод о реализации SSL на заданном домене

Данный домен в большой степени удовлетворяет приведённым в начале работы современным критериям безопасности использования SSL/TLS. Он использует большинство современных и продвинутых технологий, при этом исключает взаимодействие посредством скомпрометированных протоколов.

4.2 Recent Worst

4.2.1 Интерпретировать результаты в разделе Summary

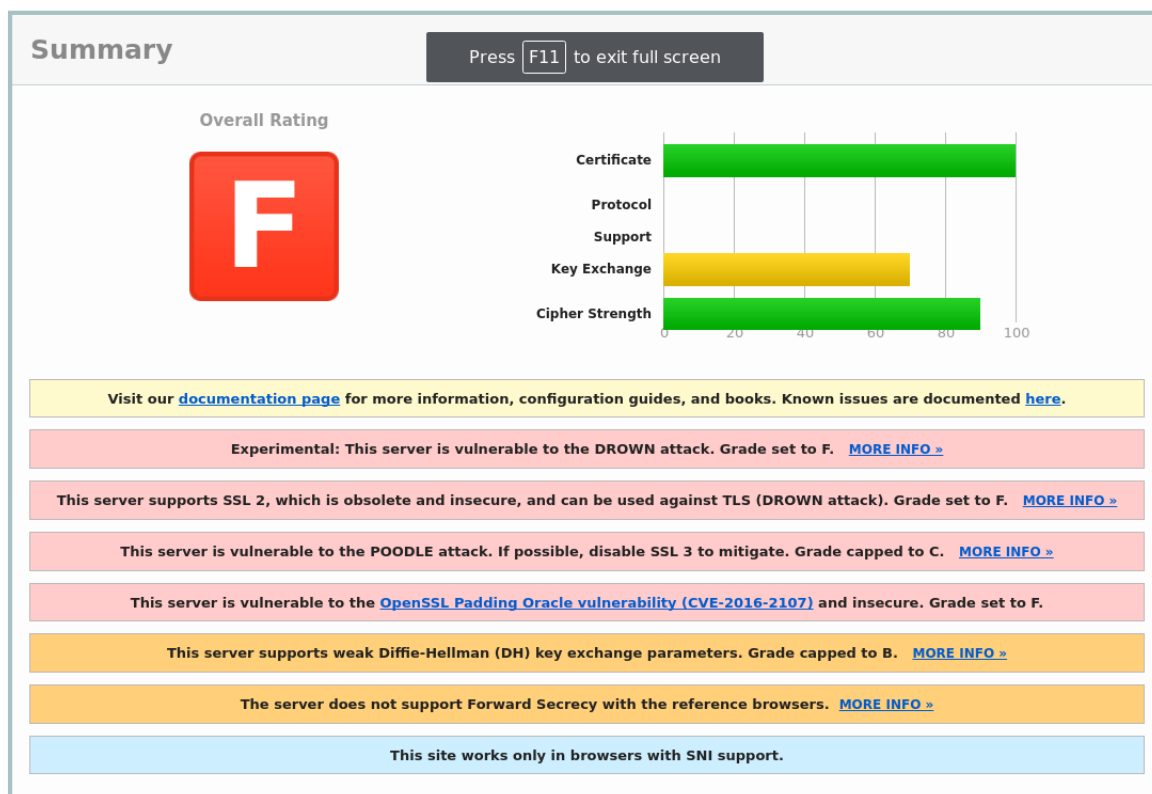


Рис. 6: Recent worst: myplan.moreactive.com

4.2.2 Расшифровать все аббревиатуры шифров в разделе Configuration

Protocols

TLS 1.2 Yes

TLS 1.1 Yes

TLS 1.0 Yes

SSL 3 2 INSECURE Yes

SSL 2 2 INSECURE Yes

(2) This site requires support for virtual secure hosting (SNI), but SSL 2 and SSL 3 do not
→ support this feature.

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end
→)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 1024 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 1024 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 1024 bits	FS	WEAK	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	DH 1024 bits	FS	WEAK	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256			
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256			
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256			
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	256			
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 1024 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 1024 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 1024 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	DH 1024 bits	FS	WEAK	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 1024 bits	FS	WEAK	112
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128			
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128			
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128			
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x41)	128			
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112			

Этот сервис поддерживает использование скомпрометированных протоколов SSLv3 и SSLv2. Также видим, что для большинства протоколов используется пометка WEAK. Аббревиатуры:

TLS - transport layer security
DHE - Diffie-Hellman ephemeral
RSA - Rivest, Shamir, Adelman
AES - American encryption standard
Camelia - symmetric key block cipher
GCM SHA-384 - secure hash algorithm (384-bits) with Galois/counter mode
CBC - cipher block chaining
3DES - triple data encryption standard
EDE - mode of 3DES (encrypt - decrypt - encrypt)

4.2.3 Прокомментировать большинство позиций в разделе Protocol Details

Protocol Details	
	IP Address Port Export Special Status
	54.187.98.185 443 Yes Yes Not checked (same host)
	54.244.3.166 443 Yes Yes Vulnerable (same key with SSL v2)
DROWN (experimental)	<p>(1) For a better understanding of this test, please read this longer explanation</p> <p>(2) Key usage data kindly provided by the Censys network search engine; original DROWN test here</p> <p>(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and incomplete</p> <p>(4) We perform real-time key reuse checks, but stop checking after first confirmed vulnerability</p> <p>(5) The "Special" column indicates vulnerable OpenSSL version; "Export" refers to export cipher suites</p>
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) SSL 3: 0x39, TLS 1.0: 0x39
POODLE (SSLv3)	Vulnerable INSECURE (more info) SSL 3: 0x39
POODLE (TLS)	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	Yes
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	Yes INSECURE (more info)
Forward Secrecy	Weak key exchange WEAK
ALPN	No
NPN	No
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	Yes
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE Tor
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	Yes Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	No
SSL 2 handshake compatibility	Yes

Рис. 7: Protocol details for myplan.moreactive.com

Данный сервер подвержен DROWN-атаке, потому что он поддерживает SSLv2 и закрытый ключ используется другим сервером, поддерживающим SSLv2. Схематично она изображена ниже.

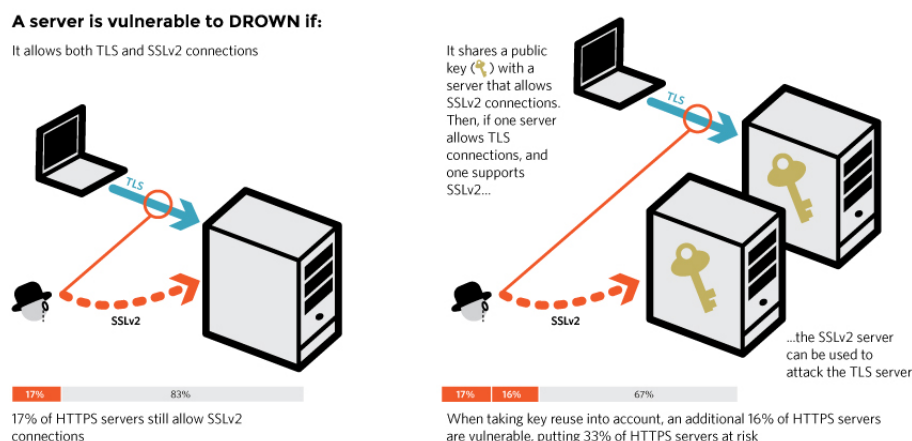


Рис. 8: Схема DROWN-атаки

Так как сервер поддерживает SSLv3, он подвержен атаке POODLE, а также ещё одной подобной атаке - OpenSSL Padding Oracle vuln.

Сервер поддерживает слабый Forward Security, не поддерживает возобновление сеанса, использует распространённые простые числа для алгоритма Диффи-Хеллмана.

Остальные настройки в порядке. Сервис не подвержен атаке POODLE по TLS, BEAST-атаке, а также Heartbleed. Поддерживает безопасное повторное установление соединения. Поддерживает Downgrade attack prevention. Продвинутой возможности, таких как HSTS preloading, OCSP stapling не поддерживает.

4.2.4 Сделать итоговый вывод о реализации SSL на заданном домене

Таким образом, домен имеет довольно слабую защиту от взлома SSL/TLS. Он подвержен атакам на протоколы SSLv2 и SSLv3 в силу их использования. Алгоритмы, используемые в настройках домена, в настоящее время считаются слабыми и устаревшими. В результате, имеем плохо защищённый домен, SSL/TLS на котором можно взломать.

5 Выводы

В настоящее время безопасность передачи данных по защищённым протоколам, используемым асимметричными алгоритмами, является крайне важной в силу их постоянного использования и совершенствования средств и методик проведения атак и нахождения уязвимостей. Решающую роль в данном случае имеет человеческий фактор - своевременное реагирование на инциденты, регулярное обновление ПО, отвечающего за безопасность и, немаловажно, правильная и грамотная его настройка. Существуют рекомендации по использованию SSL/TLS, которые регулярно обновляются и совершенствуются в соответствии с тенденциями мира информационной безопасности. Если следовать этим рекомендациям, шанс на взлом соединения и утечку конфиденциальных данных практически отсутствует.

Несмотря на открытую информацию о необходимой конфигурации систем с SSL/TLS, немалое количество доменов всё же имеют настройки, позволяющие проводить атаки на используемые протоколы. Используются устаревшие и скомпрометированные протоколы и шифры, несмотря на очевидность недопустимости их использования для обеспечения безопасности. Главной причиной, как уже было указано выше, является человеческий фактор.