Stunnel-msspi

Подводные камни туннеля по ГОСТу

Казанцев Виталий 2024г.

Кратко, что это такое?

- **stunnel-msspi** — *это форк проекта stunnel с поддержкой криптографических алгоритмов ГОСТ при установке защищённых TLS-соединений через интерфейс mspi.*

- **Msspi** — *(Microsoft Secure Socket Provider Interface) интерфейс, который обеспечивает безопасное взаимодействие между приложениями и криптографическими провайдерами. Он позволяет приложениям использовать криптографические возможности, предоставляемые провайдерами, для обеспечения безопасности данных.*

Принцип работы

Оригинальная реализация stunnel при установке защищённых TLS-соединений использует библиотеку OpenSSL, которая ограниченно поддерживает криптографические алгоритмы ГОСТ. Для обеспечения работы ГОСТ-алгоритмов в полном объёме в stunnel-msspi используется интерфейс msspi , который поддерживает ГОСТ-алгоритмы, используя установленный в систему крипто провайдер.

Основные отличия форка

- *Нет необходимости указывать параметр key , так как закрытый ключ находится по сертификату автоматически.*
- *В параметре cert кроме пути до файла сертификата может быть указано имя сертификата, идентификатор ключа или отпечаток сертификата. Например, cert = /path/to/my.example.com.cer , или cert = my.example.com , или cert = bf3c4aa0255b7c65914a45866d86abbe1c18d512.*
- *При наличии ПИН-кода на закрытый ключ, может быть использован параметр pin (НЕ РЕКОМЕНДУЕТСЯ). Например, pin = 12345678.*

Основные отличия форка

- *При использовании verify со значением 3 , параметр CApath будет использован в качестве имени хранилища сертификатов, в котором будет осуществлена проверка сертификата удалённой стороны на валидность. Например, verify = 3 и CApath = TrustedPeople.*

- *При использовании mspi = 0 , включается режим обратной совместимости с оригинальной реализацией OpenSSL .*

Где можно применить?

- *Подключение пользователя к доменам требующим TLS аутентификацию.*
- *Создание шлюза для сервисов, подключаемых к адресам требующих TLS аутентификацию.*
- *Создание шифрованного туннеля для работы различных протоколов.*

Что потребуется для сервис-шлюза

- *Установить stunnel-msspi*
- *Сконфигурировать stunnel-msspi*
- *Настроить его автоматический запуск*
- *Установить предпочитаемый web сервер (Apache, Nginx, IIS ..)*
- *Сконфигурировать web сервер*

Стандартная минимальная конфигурация stunnel-mspi

- **[Test-Domain]** - в скобках указываем название туннеля, название носит информационный характер, и участвует только в логах
- **connect = test.domain.ru:443** - указываем адрес внешнего ресурса к которому поднимаем туннель и порт подключения, по умолчанию https это 443
- **client = yes** - указывается что наше подключение клиентское, то есть мы инициируем подключение.
- **accept = 44301** - указываем порт который слушает stunnel для подключения наших сервисов.
- **cert = b3c1c8d4b2786c5a7e70733eada81c42ce887ab5**

  - отпечаток сертификата установленного в хранилище my КриптоПро
- **verify = 2** - уровень проверки сертификата сервера подключения. От уровня 3 полная проверка, до уровня 0 проверка не осуществляется.

Стандартная минимальная конфигурация stunnel-mspi

```
output=C:\services\stunnel\stunnel.log
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1
log = overwrite
debug = 7

[Test-Domain]
connect = test.domain.ru:443
client = yes
accept = 44301
cert = b3c1c8d4b2786c5a7e70733eada81c42ce887ab5
verify = 2
```

Стандартная минимальная конфигурация Apache

```
<Location /local-test-domain/>
        Proxy Pass http://127.0.0.1:44301/
        ProxyPassReverse http://127.0.0.1:44301/
    #Разбор ответа по типу содержимого
        AddOutputFilterByType SUBSTITUTE text/html
        AddOutputFilterByType SUBSTITUTE application/xml
    #Подставляем к ссылкам и источникам /local-test-domain/
        Substitute s|href="/|href="/local-test-domain/|n
        Substitute s|href="https://test.domain.ru:443/|href="http://stunnel.local.ru/local-test-domain/|n
        Substitute s|src="/|src="/local-test-domain/|n
        RequestHeader set Host "test.domain.ru"
</Location>
```

Что может пойти не так?

- **Проблема :** *Туннель поднимается, но на отправленный запрос получаем ошибку недоступности запрошенного ресурса.*
- **Возможная причина :** *В http header host, stunnel отправляет имя машины на которой он поднят, и принимающая сторона разбирая запрос, не знает куда далее его перенаправить.*
- **Решение :** *Проксировать обращение к stunnel с подстановкой необходимого значения header.*

Что может пойти не так?

- **Проблема :** *При поднятии туннеля, получаем ошибку проверки цепочек. Работает только с параметром verify = 0. Стандартное подключение в браузере без туннеля проходит TLS аутентификацию.*
- **Возможная причина :** *В свойствах сертификата «Точка распределения списка отзыва (CRL)» указан недоступный ресурс, скорей всего локальный путь до файла.*
- **Решение :** *Перевыпустить сертификат где будет указан публичный адрес списка отзыва. Принять риск и использовать verify = 0.*

Что может пойти не так?

- **Проблема :** *Под Windows Server туннель обрывается при поднятии. Каких либо ошибок в логе нет. При разборе соединения в Wireshark видим отсутствие шага получения клиентского сертификата при согласовании.*
- **Возможная проблема :** *Использование RSA сертификата созданного openssl.*
- **Решение :** *Используем версию stunnel-msspi_5_56_020. с КриптоПро RSA Microsoft Enhanced Cryptographic Provider v1.0*

https://github.com/CryptoPro/stunnel-msspi/releases

Что может пойти не так?

- **Проблема :** *Сертификат установлен под localmachine, связь с закрытым ключом есть, но в логах stunnel соединение TLS завершает с 0 трафиком. Если запустить stunnel не как сервис а под пользователем, то все работает.*
- **Возможная причина :** *При обращении к сертификату нарушается связь с закрытым ключом. Служба не имеет доступ к ветке реестра куда был помещен контейнер закрытого ключа. Понять это можно по выводу команды* **certmgr.exe -list -store mMy** *которая покажет все установленные сертификаты под localemachine в личном хранилище. Если поле Контейнер начинается с REGISTRY\\ то подключение будет завершаться с нулевым трафиком.*

Решение :

- *Перейти в папку где установлен КриптоПро. Обычно это C:\Program Files (x86)\Crypto Pro\CSP*

- *Удалить установленный сертификат командой*

certmgr.exe -delete -store mMy -thumbprint 44c1c9b432bc86375d2c0a3a0c6bef10ca031476

- *установить сертификат из pfx файла командой*

certmgr.exe -install -file mycert.pfx -store mMy -pfx -autodist -pin 0000

Наиболее используемые команды

- Просмотреть установленные сертификаты в хранилище доверенные корневые : **certmgr -list -store uRoot**
- Установка сертификатов из pfx файла : **certmgr -install -all -file certificate.pfx -pfx -autodist -pin 12345678**
- Удаление сертификата : **certmgr –delete**
- Проверка зарегистрированного контейнера : **csptest -keys -check -cont /var/opt/cprocsp/keys/tunnel/t9C34003.000/**

Итоги

- Для более стабильной работы используем Linux.
- Для работы одного сотрудника используем stunnel-msspi и отредактированный c:\windows\system32\drivers\etc\hosts
- Для работы многих сервисов разворачиваем отдельный шлюз с stunnel-msspi + web server в режиме прокси.

Спасибо за внимание!

Буду рад услышать ваши вопросы, замечания, предложения.

kazantsev.v@dobrozaim.ru