# ОС UNIX, лекция 10: OpenSSL и конфигурирование серверных служб

Пожидаев М. С.

7 октября 2020 г.

# X.509

Стандарт, разрабатываемый ITU-T, направленный на формализацию механизмов проверки подлинности и защиты информации на основе алгоритмов открытого ключа.
Стандарт X.509 находится в центре современной системы удостоверяющих центров и управляемым ими множеством выпущенных сертификатов для проверки подлинности информации в Интернете.

# SSL и TLS

SSL (Secure Sockets Layer) — криптографический протокол для сетевых соединений, позволяющий:

- проверить подлинность сервера;
- зашифровать сетевой траффик;
- подтвердить целостность данных.

TLS (Transport Layer Security) — наследник протокола SSL, основанный на SSL 3.0. Изначальным автором протоколов была Netscape Communications.

# Применение SSL и TLS

1. Подтверждение, что данные были переданы сервером, адрес которого указан в адресной строке или даже принадлежащим определённому юридическому лицу (https).
2. Подтверждение, что почтовый клиент передаёт письма для пересылке доверенному почтовому серверу.
3. Шифрование сообщений в мессенджере.

# Сертификаты и удостоверяющие центры

Сертификат — множество атрибутов (доменное имя, название организации и пр.), ассоциированных с открытым ключом и подписанных владельцем другого сертификата. Не может быть неподписанным. Выдаётся всегда на некоторый период и может быть отозван.

Удостоверяющий центр (certification authority) — организация, являющаяся владельцем общеизвестного и доверенного открытого ключа. Сертификаты удостоверяющих центров включаются в операционные системы и всегда самоподписанные.

# LetsEncrypt

LetsEncrypt — бесплатный удостоверяющий центр, предоставляющий сертификаты для подтверждения доменов.

1. Сертификаты предоставляются на три месяца.
2. Не подтверждает юридическое лицо.
3. Предоставляет свободную утилиту `certbot`, которая автоматизирует получение и перевыпуск сертификата.

# Порядок получения сертификата

1. Создание закрытого ключа.
2. Создание запроса сертификата, содержащего открытый ключ и заполненные информационные поля, из которых чаще всего ключевую роль играет `commonName`.
3. передача запроса сертификата удостоверяющему центру, который выдаёт подписанный сертификат.

# Порядок работы на примере HTTPS

1. Браузер производит подключение к серверу по определённому имени.
2. Сервер передаёт свой сертификат, который содержит открытый ключ .
3. Браузер проверяет, что адрес в сертификате совпадает с адресом, который ввёл пользователь.
4. Браузер проверяет, что сертификат подписан одним из известных ему удостоверяющих центров.
5. Далее сервер может предоставить подпись переданных данных, которые подтверждают, что это действительно данные с адреса, который ввёл пользователь.

# OpenSSL

OpenSSL — свободная реализация алгоритмов стандарта X.509 и протоколов SSL/TLS.

```
openssl genrsa -out
openssl req -new -key proba.key -out proba.csr
openssl x509 -signkey proba.key -in proba.csr -req -days 365 -out proba.crt
```

# Порядок конфигурирования веб-сервера

1. Установка веб-сервера.
2. Активация автоматического запуска.
3. Подключение нужных модулей.
4. Создание сертификата (можно с использованием `certbot`).
5. Указание основных параметров сайта, включающих перенаправления, пути к сертификату, закрытому ключу и пр.

# Установка и запуске сервера

```
sudo apt-get install -y apache2 apache2-bin\
libapache2-mod-php libphp-adodb php-mysql\
mysql-server mysql-client
sudo systemctl enable apache2
sudo systemctl enable mysql
sudo a2enmod rewrite
```

# Конфигурация обработки HTTP

```
ServerName foobar.com
ServerAdmin webadmin@foobar.com
 ...
<Directory "/var/www/html">
  AllowOverride  All
  Options −Indexes +FollowSymLinks
  RewriteEngine On
  RewriteRule ^/?(.*) https://foobar.com/$1 [R]
</Directory>
```

# Конфигурация обработки HTTPS

```
ServerName foobar.com
ServerAdmin webadmin@foobar.com
 ...
 SSLCertificateFile   /etc/letsencrypt/live/foobar.com/fullchain.pem
 SSLCertificateKeyFile   /etc/letsencrypt/live/foobar.com/privkey.pem
Include  /etc/letsencrypt/options-ssl-apache.conf
```

# Спасибо за внимание!

Веб-сайт: http://marigostra.ru/
E-mail: msp@luwrain.org