УДК 004.021

АВТОМАТИЧЕСКОЕ ПОЛУЧЕНИЕ СЕРТИФИКАТОВ ДЛЯ ОРГАНИЗАЦИИ ПРОТОКОЛОВ HTTPS

К.Х. ГРИГОРЯН
(Представлено: Д.В. ПЯТКИН)

Рассматривается автоматическое получение сертификатов для организации протоколов https. Показан способ автоматизации процесса получения сертификатов для доменного имени. Важным аспектом процесса перевода сервера с http на https является фактор серверного окружения. В частности, подразумевается, что если на сервере устновлено по apache2, то необходима перезагрузка. Текущие технологии позволяют обеспечить надежную защиту данных, в частности при использовании https.

Конфиденциальность передаваемых данных в сети является важным аспектом деятельности банковских систем или веб-приложений, хранящих персональные данные пользователя.

Утечка таких данных может нанести значительный вред как отдельным лицам, так и крупным организациям.

Для сохранения персональных данных выделено и разработано ряд мер и технологий, одной из которых является *https протокол.*

Lets Encrypt

Есть целый набор способов получить ssl-сертификат, но стоит выделить сервис Lets Encrypt, который отличает надежность и скорость получения сертификатов (за счет упразднения лишних шагов и возможности автоматизировать этот процесс), а также ряд программных средств, которые облегчают владельцу домена взаимодействие с этим сервисом.

Для автоматической выдачи сертификата конечному доменному имени используется ***протокол аутентификации класса «challenge-response»*** (вызов-ответ, вызов-отклик) под названием Automated Certificate Management Environment (ACME). В этом протоколе к веб-серверу, запросившему подписание сертификата, производится серия запросов для подтверждения факта владения доменом (domain validation).

Для получения запросов клиент ACME настраивает специальный TLS сервер, который опрашивается сервером ACME с применением Server Name Indication (Domain Validation using Server Name Indication, DVSNI).

С целью настройки системы обновления сертификатов на сервере, имеется ряд модулей для получения ssl сертификатов. Также важным аспектом используемого ПО является автоматическое привязывание сертификатов и перевод клиентов на 443 порт, для поддержания https.

Важным аспектом процесса перевода сервера с http на https является фактор серверного окружения. В частности, подразумевается, что если на сервере устновлено по apache2, то необходима перезагрузка.

В случае работы с nginx достаточно будет использовать мягкую перезагрузку. Это приводит к мысли о том, что необходимо найти ПО для управления apache2/nginx.

Следовательно, после получения сертификата и добавления его в конфигурацию сайта необходимо автоматически перезагрузить сервер.

После этого сервер будет использовать обновленные конфигурации.

За короткое время клиент получает полностью работоспособный сайт с протоколом https.

Процесс верификации можно разделить на несколько стадий:

Создание открытого ключа по адресу domain/.well-known/acme-challenge/{challenge-token} – этот процесс необходим для подтверждения прав на домен.

Затем необходимо сделать ***запрос с предоставлением данного файла сервису***.

После удачной проверки начинается ***процесс получения серификата***.

После обмена запросами имеем сертификаты в файлах fullchain.pem, cert.pem, chain.pem.

Сертификаты, как правило, выдаются на 2–3 месяца. Это необходимо учесть и добавить настройку для cron.

В основной файл конфигурации cron(/etc/crontab) необходимо добавить строку, представленную в листинге 1.

Листинг 1 – Листинг cron для Lets Encrypt

```
1:      0 0 0 */4 * /usr/local/bin/php /pathtoscript/LetsEncrypt.php
```

Таким образом, мы задали, что раз в три месяца будет обновляться сертификат.

В заключение можно сделать следующие **выводы:**

- текущие технологии позволяют обеспечить надежную защиту данных, в частности при использовании https;

- если раньше получение сертификата было сложной задачей, то при помощи сервиса Lets Encrypt эта задача перестала вызывать какие-либо проблемы у владельцев web-ресурсов.

ЛИТЕРАТУРА

1. METANIT.COM Сайт о программировании [Электронный ресурс]. – Режим доступа: https://metanit. com/nosql/mongodb/1.1.php. – Дата доступа: 18.09.2017.
2. Руководство по MongoDB. Моделирование данных [Электронный ресурс]. – Режим доступа: http://proselyte. net/tutorials/mongodb/data_modeling/. – Дата доступа: 17.09.2017.
3. Википедия : свободная энцикл. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/ wiki/JSON/. – Дата доступа: 21.09.2017.
4. W3II Latest web development tutorials [Электронный ресурс]. – Режим доступа: http://www.w3ii. com/ ru/mongodb/mongodb_advantages.html. – Дата доступа: 23.09.2017.