SSL - ACME Challenges

Overview

SSL certificates are critical to ensuring web connections are to the correct server. In order for a Certificate Authority (CA) to confirm the owner of a domain name, they perform a challenge to the ACME standard. There are many different types of challenges, but since SSL certificates should be renewed automatically, only a few challenges work effectively.

LetsEncrypt is a free popular CA, which allows for 2 different types of automated challenges to prove domain ownership.

HTTP-01

The HTTP-01 challenge is most common type of challenge, with the CA giving a token to the ACME client, such as certbot, which it then added to a web server based at your domain. Once the web server is ready, the CA requests the resource multiple times to check whether it exisits and is valid. The system of creating a temporary webserver is quick and easy to automate.

There are a few caveats to the HTTP-01 challenge:

* Only 10 redirects deep, any more redirects will fail the challenge
* Can only be performed if port 80 are open and available to the ACME client
* Cannot issue wildcard certificates
* If there are mutliple webservers balancing load, all must have a copy of the token for verification

DNS-01

The DNS-01 challenge requires the domain owner to add a specific TXT record under the domain name to prove ownership. While being more complicated to setup and automate, it works in scenarios where HTTP-01 will not, such as if incomming port 80 connections were blocked by an ISP.

LetsEncrypt will give the ACME client, such as acme.sh, a token which the client will add to the DNS records. Once complete LetsEncrypt will check the records and if it finds a match, the certificate will be created.

For DNS-01 challenges to be automated, the DNS provider must have an API so that the ACME client can login and make requests without user interaction. The main issue with API credentials being on a server, is if it is comprised by an attacker the impact can be significant. Therefore, it is common to use a specific server for creating the DNS TXT record and receiving the SSL certificate, then automatically copying it over to the webserver for use.

HTTP-01 - Certbot

Install using:

sudo apt-get install certbot

DNS-01 acme.sh

Install using:

curl https://get.acme.sh | sh

This will:

* Create the ~/.acme.sh/ folder for certs
* Create an alias acme.sh
* Create a daily cron job to check and renew certs if required

Add DNS provider API keys to environment variables (possible risk if server is comprimised), https://github.com/acmesh-official/acme.sh/wiki/dnsapi :

export Key="<key>"

export Secret="<secret>"

Run following command to create certificate:

acme.sh --issue --dns dns\_ -d example.com

This will create a certificate and put it in the ~/.acme.sh directory.