Persistent DNS Validation in the ACME protocol

IETF 123 Madrid

Henry Birge-Lee
Princeton University

Motivation for persistent validation

- Traditionally, ACME dns-01 requires the client to perform a DNS record “change” by uploading a random token to “_acme-challenge”
- Increasingly, cloud providers are offering an issuance delegation service where “_acme-challenge” is CNAMEd to a cloud-provider controlled zone
- When a CNAME is used at “_acme-challenge” the DNS change in question is not occurring in the actual zone of the domain being validated but instead in the zone pointed to by the “_acme-challenge” CNAME
- When dns-01 validation follows a CNAME, it is no longer enforcing a true DNS record change but instead confirming that a particular static value is in place in the zone in question which indicates the domains desire to complete DCV

Activity at CA/Browser Forum

- The widespread prevalence of CNAME DNS challenge completion led to a discussion at the CA/Browser Forum about whether a CA could run such a service on behalf of its subscribers
- This resulted in the failed ballot SC-082 which would have explicitly permitted CAs to instruct subscribers to install CNAMEs instead of actual challenge verification TXT records
- Root programs didn’t like that the original intent of the method was to perform a DNS change but the CNAME technique is actually a static DNS value

Solution: permit validation using a “persistent” static value

- Defined in newly proposed ballot SC-088 https://github.com/slghtr-says/servercert/pull/3
- CAs and Root programs have spoken favorably for the new ballot which invents a new method for persistent DNS change
- This method is designed to strongly support automation
- Syntax and security controls are much better than the original CNAME method

Advantages over existing CNAME method

1. the infrastructure serving the zone used for ACME challenges could be compromised (potentially affecting many domains that all pointed to that same shared infrastructure)
2. CAs need to perform another potentially plaintext DNS lookup to complete the dns-01 challenge
3. only one CNAME record can exist at a label preventing this technique from delegating control to multiple cloud providers
4. availability issues with the ACME challenge zone could impact certificate availability
5. the ACME client needs an additional communication channel to communicate with the ACME challenge zone
6. a unique CNAME value must be provided to each of a cloud provider's customers otherwise this technique creates a major security breach between customers
7. a separate DNS zone and automated DNS infrastructure must be provisioned making this technique less practical for smaller operators.

Syntax of persistent validation in SC-088

- _validaton-persist.example.com IN TXT “authority.example; accounturi=https://authority.example/acct/123”
- authority.example: a valid CAA domain name for the CA signing the certificate
- accounturi: the ACME account that is allowed to request certs using this method

Proposed ACME dns-persist-01 method

- Uses the same syntax for checking records

- Method string name “dns-persist-01”
- Contains no token parameter (validation record can be fully derived by client before contacting ACME server)
- `GET /acme/authz/1234/1 HTTP/1.1 Host: example.com`
- `HTTP/1.1 200 OK { "type": "dns-persist-01", "url": "https://example.com/acme/authz/1234/1", "status": "pending" }`

Security considerations

- A stable persistent zone change has always been capable of satisfying the dns-01 challenge given that an adversary can upload a CNAME record that points to an adversary controlled zone
- If we assume the access level required to upload a CNAME record and a TXT record are similar, permitting validation using a stable TXT record provides comparable security to the existing dns-01 challenge
- This method does imply an ACME account compromise can easily lead to misisusance. However, ACME account compromises can already lead to misissuance due to validation reuse
- Eliminating the need for live DNS credentials on ACME clients or extra services that exist solely to serve ACME challenges overal improves security

Questions

Feel free to contact me at: birgelee@princeton.edu

Draft is at: https://birgelee.github.io/birgelee-acme-dns-persist-01/draft-birgelee-acme-dns-persist.html (updated intro and abstract since first send to list)

Additional security analysis: https://groups.google.com/a/groups.cabforum.org/g/servercert-wg/c/4tATbCpQRpM/m/8mH-SX87BAAJ

Will be on datatracker soon