Domain Verification Techniques

https://datatracker.ietf.org/doc/html/draft-sahib-domain-verification-techniques-02

Shivan Kaul Sahib (Brave Software)
Shumon Huque (Salesforce)

DNS Operations Working Group
IETF 112

What is domain verification?

Many providers on the internet need users to prove that they control a particular domain before granting them some sort of privilege associated with that domain.

For e.g. Let’s Encrypt has a DNS-based challenge for a user to prove that they control a particular domain (and hence should be issued a cert for it)

Refresher

1. Overview of existing techniques
    a. TXT + examples
    b. CNAME + examples
2. Recommendations
    a. Targeted domain verification
    b. Time bound checking for verification records
    c. DNSSEC

IETF 111 presentation:
https://datatracker.ietf.org/meeting/111/materials/slides-111-dnsop-sessa-domain-verification-techniques-01

Feedback from WG

1. High degree of interest on mailing list [1][2][3] and on the mic @ 111
2. Challenge replay attack by a provider (issue #21)
3. Arbitrary RRDATA => parser bugs (issue #22)
4. Predictable QNAME for CNAMEs (issue #23)
5. Domain re-validation requirements should be clearly mentioned (issue #19)
6. Multi-vantage-point checking for domain verification records (issue #18)
7. Detailed security analysis is needed!

Call for adoption?