IETF Hackathon

IETF 120

20-21 July 2024

Vancouver, Canada

Hackathon Plan

Purpose:

- Familiarize participants with "Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC".
- Identify implementation approaches for the draft

Problem: SLH-DSA-MTL mode signatures introduce new requirements for signing zones, serving signed zones, and verifying RRSIGs.

Drafts:

- Merkle Tree Ladder (MTL) Mode Signatures
- Stateless Hash-Based Signatures in Merkle Tree Ladder Mode (SLH-DSA-MTL) for DNSSEC

Specific problems to solve

- Provide understanding of MTL Mode of Operation
- Explain how a zone is SLH-DSA-MTL signed
- Explore implementation for signing, serving and verfication of RRSIGs by validating resolvers

Solving the Problem

- Walkthroughs of SLH_DSA-MTL RRSIG creation
- "dig" the example signed zone hosted @mtl.dnsjedi.org (thanks to Dr. Roland van Rijswijk-Deij of the University of Twente)
- Discussons with DNS software providers

What Got Done

What got done

- Participants were able to do digs against the example SLH-DSA-MTL signed zone
- Participants gained an understanding of MTL Mode of Operation and our draft describing how it is applied to DNSSEC
- Implementations approaches relative to authoritative name servers were discussed
- Requirements relative to validating resolvers were discussed

What We Learned

What we learned: Addressing implementation of MTL Mode for DNSSEC needs to be a collaborative process that incorporates the input of DNS software implementors, name server operators, validating resolver operators, protocol design experts, security experts and more.

"dig" it @mtl.dnsjedi.org during IETF 120

dig @mtl.dnsjedi.org example.com A +dnssec +norecurse

```
example.com. 3600 IN A 192.0.2.1
example.com. 3600 IN RRSIG A 50 2 3600 20250701183541 20240701183541 53939
example.com. APnCCOkVSqjw6zKSPz40U6AAAEkgbrJ3DnyxAAAAAAAAAAAAAAAHAAOG
VodklRgciVyAG660gDJAS/blgaqTfYU04u9LWETNe9PjWTkxvxviqKtd IWEZhhI=
```

dig @mtl.dnsjedi.org example.com SOA +dnssec +norecurse

```
example.com. 3600 IN SOA ns.example.com. admin.example.com. 1719858941
7200 3600 1209600 3600
example.com. 3600 IN RRSIG SOA 50 2 3600 20250701183541 20240701183541
53939 example.com. AWOXFesN5grvg1Vk/TE3ZNEAAEkg ... (base64 length is
10871 bytes)
```

Wrap Up

Team members:

- Burt Kaliski
- Andrew Fregly