Updates to draft-ietf-lamps-caa-security

IETF 123 Madrid

Henry Birge-Lee
Princeton University

Grace Cimaszewski Princeton University
Cyrill E. Krähenbühl Princeton University
Liang Wang Princeton University
Aaron Gable ISRG
Prateek Mittal Princeton University

Ecosystem Updates

- SC-085 passed at the CA/Browser Forum requiring that all CAs validate DNSSEC for DCV and CAA DNS lookups.
- This allows the security properties outlined by the security tag to be upheld for DNSSEC domains
- Even CAs that don’t understand or support the security CAA tag will:
  - Validate DNSSEC signatures on CAA records
  - Fail closed if a CAA record does not contain a valid signature or corresponding NSEC
  - Fail closed if they don’t support the security tag due to the critical flag

Document updates

- Incorporation of working group suggestions
  - Security considerations that are inherited from CAA tags in general were removed
  - Security considerations about the use of recursive to authoritative DoH/DoT were added with explicit differences to DNSSEC
- Additional examples of DNS records
  - Some methods for satisfying the security tag like known-account-specifier and private-key-control involve data placed in DNS records
  - Draft-sheth-identifiers-dns-00 presents a syntax for these records and recommend that they end in “-persist”
  - This syntax is also adopted by the draft of the CA/Browser Forum ballot SC-088
  - Examples of these records were added using this syntax

Next steps

- More community feedback
  - Please review the draft and let us know your thoughts
- Implementation in Open MPIC
  - For web PKI CAs, tag will need to be corroborated using MPIC. This is on the Open MPIC road map
- Implementation in Let’s Encrypt codebase