ISSUE: SVCB AT PARENT

DPRIVE, IETF 111
July 2021

Paul Wouters
Drafts involved:

• draft-rescorla-dprive-adox-latest-00

• DNS client performs query for NS, receives NS, glue and and SVCB specifying (encrypted) DNS transports to client nameservers.

• draft-schwartz-dprive-name-signal-00

• Suggests “temporary” workaround until serving SVCB at parent works
Deployment is a 10+ year problem

- To serve SVCB records at the parent (that is at the ‘wrong’ end of the zone cut), we need:
  - Update all major DNS software
  - Deploy DNS updates at authoritative servers worldwide
  - Deploy DNS updates at recursive servers worldwide
  - Applications must bypass System DNS to avoid leaks when system might be pointing to old DNS recursor.
Deployment is a 10+ year problem

- To serve SVCB records at the parent (that is at the ‘wrong’ end of the zone cut), we need:
  - Update EPP protocol (I see no draft for this)
  - Deploy updated EPP protocols at Registries and Registrars
  - Update Web Portals at (sub)Registrars
  - Write up a CDS/CDNSKEY/CSYNC solution for SVCB because Registrants are not DNS Hosters
Results of SVCB ‘at parent’

• SVCB at the parent is not going to reliable or available for many years

• “Interim” workarounds will become permanent protocol

OR

• Two tier DNS is created where browsers will only use one “trusted” tier

• Further centralization of DNS resolvers.

• Splitting the DNS world into “browser DNS” and “other DNS”
Issues with draft-schwartz-dprise-name-signal

• Encodes SVCB in QNAME of NS record (“dnscurve hack”)
• NS keys can never change, as you can’t get 10k customers to all update their NS record for your nameserver’s key.
• NS at parent is glue, so is unauthenticated and unsigned
  • Facilities easy encrypted DNS intercept
    • Inject SVCB-style NS records to your encrypted server
      • Could be done by Nation States or ISPs
• See earlier discussion on encoding something like this inside DS record:
  • Requires no DNS software modification
  • Secured with DNSSEC against abuse
  • CDS/CDNSKEY sees some deployment, CSYNC does not?
Advise to WG: Reality Check

• Let’s not pretend SVCB at parent is a feasible solution
• Let’s not write “temporary workarounds” until it would.