Use cases for DANE and bidirectional TLS authentication in the DNS

Bill Woodcock / PCH

Turtles-all-the-way-down, dogfood, etc.

CA certs are a huge vulnerability, to the DNS no less than HTTP or other protocols, and we've understood this for more than twenty years.

DNSSEC is fine if you actually validate in the client (but nobody seems to do that) AND the zone data was protected up until the point where it was signed (but nobody seems to do that) AND it's ok if everybody sees the same records (but many people depend on that not happening).

So while DNSSEC is great for authenticating content, it doesn't address party authorization.

We already depend on authorization throughout the DNS publishing chain:

Split-horizon is common in enterprise, but typically depends on IP-address-based access-gating to recursive resolvers which have special access to “internal” namespaces. Access to the special recursors in turn depends upon VPN authentication. Lots of external dependencies. Work-from-home and zero-trust have made this critical. TLS client auth PKI outside of DANE/TLSA is a disaster.

There’s also huge demand for closed-community recursive resolvers with special features (ad-blocking, etc.) but that also depends on VPN auth right now, which is one too many moving parts.

Top-talking recursors are prioritized by authoritatives, but that depends on static IP address lists, which is a disaster to keep up-to-date. DANE/TLSA solves this problem as well.

XFR zone transfer from hidden primaries is typically only available to authorized authoritative anycast distribution networks, but manual out-of-band TSIG key management doesn't scale and has resulted in rampant shared-key reuse and static configuration. Again, bidirectional TLS auth solves this problem.

Unsigned zone data prior to the application of the ZSK is particularly at risk. Way too many zones are managed by parties who don't have the cybersecurity expertise needed to protect this link, so bidirectional TLS auth by default between the zone origin and the signer would make DNSSEC a lot more trustworthy as well.

Tl;dr:

We need to be able to authenticate both parties to any DNS transaction; TLS bidirectional auth is the only sane way of doing that; DANE TLSA records are the only sane mechanism for TLS key distribution at scale.

Therefore, we need DANE distribution of TLS client and server keys and TLS bidirectional authentication available generically throughout the DNS.

It doesn’t make sense to do this piecemeal, one-link-at-a-time, since it’s the same problem at each link in the chain.

Thanks, -end-, etc.