DNSSEC serialization: a DANE view

Paul Hoffman

VPN Consortium

Overview

- Why we might care
- What serialization looks like
- How to get this data into security protocols
- How this work might proceed in the IETF

Important note: I am not Adam Langley, nor Dan Kaminsky

Why DNSSEC serialization is interesting for secure clients

- Getting all the DNSSEC data needed to validate a particular DNS record with no DNS lookups, as one blob, is much faster than getting it using recursive DNS requests
- Some clients can’t reliably get DNSSEC data (filtering firewalls, broken proxies, ...)
- Doing DNSSEC validation in the client means that the client doesn’t need to trust a DNS resolver to validate DNS

What serialized DNSSEC looks like

- A binary blob containing all the data that would be needed by a validating DNSSEC resolver in one step
- Some optimizations are possible if you want to save ~20% of the size (less than 1K)
- There have been a few proposals for what the structure of the blob should be

Getting this data into secure protocols

- New extension to the protocol
- New PKIX extension in an end-entity certificate
- New PKIX extension in a superfluous certificate
- New OCSP extension carried in a OCSP message in the protocol
- Do another request (DNS, HTTP, ...)

How this might proceed in the IETF

- Need to standardize on a serialization without bikeshedding, premature optimization, and so on
- Need to decide which mechanism will be used to carry this in each security protocol
- These two should be able to proceed in parallel