What Does A DANE Response Mean?

Paul Hoffman, VPN Consortium

IETF London, March 2014

v2

Let's define the undefinable

- "The DNS is for delivery of information about a domain, such as its address"
- "The DNS is for discovery of information about a domain, such as whether it has an IPv6 address"
- If you don't see the difference between these two, you're not going to understand why we're having this presentation

Delivery

- Some feel that the DNS is a system for delivering information about a domain
- Historical context: simple lookup
- Mostly: the IP address of the host and how to find the SMTP server
- Also: “stuff about the domain” (TXT)

Discovery

- Historical context: that's what applications are for
- Does this host have a server for this application protocol? (SRV, 1996)
- Keys (IPSECKEY & SSHFP 2005)

Distinction with/without a difference

- For many people, these ideas are very different
  - Discovery is a misuse of the DNS
  - DNSSEC is only an integrity check, not a proof of intent by the zone owner
- For many people, these ideas are the same
  - Every query results in “discovery”
  - Every “discovery” is followed by a “delivery”

How this affects DANE

- If you see this keying material in TLS, you can trust it
- If you see different keying material in TLS, you should not trust it
- If you don’t see TLS, you should assume an MITM attack
- Statements like these might not just be “discovery”, they could also be considered “security policy”

So?