Stateless DNS encryption

draft-krecicki-dprive-dnsenc-01

Witold Kręcicki

Internet Systems Consortium

Priorities

- Independence of the underlying transport protocol (UDP, TCP, SCTP)
- Single protocol for authoritative and recursive servers - no protocol fragmentation
- As much compatibility with DNS as possible
- No need for external mechanisms (such as CA/PKI)
- Small to none overhead on round-trips
- Small overhead on message size
- Statelessness on the server side

Open problems

Key retrieval for auth servers

- Best solution - signed key at the delegation point in parent zone (like DS records)
- ... but that requires adoption by domain operators, problematic
- Key at the apex leaks information about the domain client wants to query
- DLV-like mechanism?
- **Proposed solution: Key at the apex as a discouraged option, pushing registrars to allow publishing NSK records at the delegation point (and providing DNSENC!)**

Key retrieval for recursive servers

- Best solution - key in signed in-addr.arpa record
- ... but that requires access to in-addr.arpa, problematic
- Key in /etc/resolv.conf - no easy way to roll over keys
- Name in /etc/resolv.conf - verified by DNSSEC (not in -01):

```
nameserver 192.0.2.1 recursive.example.com

recursive.example.com. IN A 192.0.2.1
recursive.example.com. IN RRSIG A ...
recursive.example.com. IN NSK ...
recursive.example.com. IN RRSIG NSK ...
```

- **Proposed solution: both in-addr.arpa and name in /etc/resolv.conf**

Encapsulation method

- New OpCode - cleanest, less overhead
- ... but will cause problems with proxies/forwarders/firewalls
- EDNS option - larger overhead, better chances of working
- Also - possibility to use DNS Cookies to prevent DoS
- **Proposed solution: further research to see how forwarders treat unknown EDNS option and unknown OpCode, (or keep both)**

Defining encryption schemes

- Symmetric - ECIES, DLIES, RSAOAEP
- Asymmetric - AES, ?
- Will need a crypto review

Naming

- Name for the standard - is "Stateless DNS Encryption" appropriate?
- DNSENC sounds a lot like DNSSEC (and DNSCRYPT is taken) - other options?
- NSK $\rightarrow$ NSENCKEY ? (there are a lot of keys in DNS, we don't want any confusion)

Other details

- Asymmetric crypto is CPU-intensive, lower it by returning single-use AES key for next query in server response?
  - Small state (key+ID - 64 bytes)
  - List of keys in server limited in size - in case one times out client falls back to symmetric key
  - Possibility of DoS attack (user can force server to flush all keys by issuing a lot of requests), rate-limiting/cookies as a solution?
- Problems with forward secrecy - additional RT is usually not a problem for recursive servers, but what about authoritative?

```
100 END
```

Thanks for watching.