Overview

DNS
Plaintext over UDP / TCP

www.example.com
123.123.123.123
server_name: www.example.com
CommonName: www.example.com

TLS 1.2
Or lower

Unencrypted
Encrypted

DNS QUERY
DNS RESULT

TLS Client Hello w/SNI
TLS Server Hello w/ certificate
HTTP Request
HTTP Response

www.example.com

DNS Provider
User
www.example.com
Updates since IETF 102

Draft adopted

-00, -01, -02 published

Deployment by Cloudflare and Firefox Nightly

Lots of discussion on the list
Summary of changes from initial draft

Independent client key shares for ESNI, TLS

- Prevents DNS from dictating key exchange mechanism

Added nonce, AEAD covering of KeyShareClientHello

- Replay protection

Added version

- Future compatibility
Pending changes for -03

Use ESNI RRTyde instead of TXT (Issue #109)

- Simplifies CNAME setup by removing prefix
- Easier to deploy new types if managed without users
- “more correct”/“don’t overload TXT”
Operational Issues

Hard failure if DNS and server get out of sync

Multi-CDN case
Hard failure if DNS and server get out of sync

Risks

● DNS over-caching issues
● Bigger risk if keys rotated quickly for forward secrecy

Impact

● Site unavailable
Hard failure if DNS and server get out of sync

Possible solution

- Fallback hostname in ESNI structure
- Default certificate covers fallback hostname
- Fresh ESNI sent as part of EncryptedExtensions

Assumptions

- TLS-terminating server is in sync with proxy server
- Additional 1-RTT handshake is ok
Multi-CDN case

Overview

● example.com has DNS load balancing of A/AAAA
  ○ Returns set of A records corresponding to multiple providers

● www.example.com has DNS load balancing via CNAME
  ○ Returns CNAME that terminates at www.example.com.cdn1.com or www.example.com.cdn2.com randomly
Multi-CDN case

Failure case

- A/AAAA record request independent of TXT/ESNI record request
- A/AAAA for CDN1, TXT/ESNI for CDN2

CDN1/2 have different ESNI keys, or only CDN1 supports ESNI

Result: Failed connection with no fallback or unnecessary privacy leak
Multi-CDN case

Requirements for a solution

- Prefer soft failures to hard failures
- No serialization of DNS queries
- Works in majority of deployment scenarios
- Prefer few changes to authoritative servers
Encrypted SNI

E. Rescorla, K. Oku, N. Sullivan, C. Wood
draft-ietf-tls-esni-02