SNI Encryption

draft-huiitema-tls-sni-encryption-02

Christian Huiitema

IETF 99, Prague, July 2017
Why SNI Encryption now?

- Deployment of HTTPS, SMTP/TLS, ...
- Standardization of RFC 7858, DNS over TLS.
- Over 60% of traffic going to CND, multi-tenant data centers, etc.
- SNI sticks out as tool for Censorship and Surveillance
Writing down attacks and options

• List of options, collected from many discussions
  • But first, eliminate the known-broken options.

• List of attacks, collected from the TLS mailing list.
  • If there are more, please send them.
Solution 1: HTTP Fronting (Co-tenancy)

- Simple solution
  - TLS to “fronting.example.com”
  - HTTP to “hidden.example.com”

- Possible addition of Tunneling
  - CONNECT to hidden.example.com

- Trust issue
  - Fronting delivers Hidden content
  - Fronting knows who connects to Hidden
  - What if?...

- Discovery issue
  - Who Fronts for Hidden?...
Delegation Token Proposal

• Some new kind of Certificate:
  • “Fronting” is an authorized fronting service for “Hidden”
• Type of Access
  • HTTPS Fronting
  • HTTPS CONNECT
  • Maybe TLS 1.3 solution
• Expiration date
• ...
• Signed by Hidden

• Attack: Spoofing Hidden
  • Need strong proof of Hidden’s identity
  • Maybe CT log reference + DNS TLSA as redundant proof
• Attack: Spoofing Fronting
  • Add IP addresses to CERT?
• Attack: DOS on Fronting
  • Add proof of agreement?
• Attack: Turncoat
  • Revocation, or short validity?
Solution 2: TLS in TLS Quasi Tunnel

- Depends on TLS 1.3 features
  - 0-RTT
  - Encrypted certificates
- Requires changes in implementations
  - Expect C-Hello #2 in 0-RTT data...
Solution 3: Combined Tickets

- Elegant solution
  - Requires Fronting to “understand” the ticket
    - E.g., Shared K_sni STEK?
- Requires ticket extension
  - Fronting SNI extension
- Only works for resumption
  - Use other process for initial connection, e.g. HTTP Connect, or TLS Quasi Tunnel
Combined Ticket?

```c
struct {
    uint32 ticket_lifetime;
    uint32 ticket_age_add;
    opaque ticket_nonce<1..255>;
    opaque ticket<1..2^16-1>;
    Extension extensions<0..2^16-2>;
} NewSessionTicket;
```

- Define required extensions
- Fronting SNI
- Define Client Behavior
- Other specifications
- Align with “Delegation Token”
Is this IETF Work? (I think Yes)

• Standardize the “Delegation Token”
• Standardize the “Combined Ticket”
• Work on a common architecture
  • Maybe align combined ticket and delegation token