Private DNS

Phillip Hallam-Baker

Objectives

- Privacy
  - Confidentiality
  - Traffic Analysis
- Authenticity
  - Eliminate response spoofing
  - Guarantee user’s choice of resolver
- Service
  - Protect resolver (resource exhaustion)
  - Protect third parties (amplification)

Constraints (from OCSP Experience)

- Must work in 100% of network circumstances
  - In hotels, coffee shops, etc. etc.
- Cannot increase latency
  - Almost as good is not sufficient

- A modest performance penalty is acceptable for dealing with edge cases (no more than 5%)

Architecture I

- Service connection establishment
  - User specifies resolution service ‘dns.example.com’
  - Use HTTPS/JSON Web service to establish connection to service
    - Hosts to use
      - IP Address / Kerberos Ticket / Shared Secret / Algorithms
      - Protocol version / formats / options
  - TLS & WebPKI used to establish connection
    - Performance is not an issue as this is not inside the transaction loop

Architecture II

- Resolution Protocol
  - UDP
    - Simple session layer
    - 1 request packet, 0-16 response packets
    - Every message is authenticated and encrypted
    - Messages can contain padding to guard against traffic analysis attack
  - TLS
    - Wrap above packets in HTTPS or TLS in addition
    - Provides a fallback protocol with near 100% connectivity

Applications

- Anonymous use
  - The service connection establishment request is not authenticated

- Enterprise customer
  - Likely early adopter market
  - Private-DNS is likely connecting to split horizon DNS
    - Service connection establishment request is authenticated

Complexity Strategy

- Resolution protocol is very simple
  - Framing is described in 2 pages using TLS schema syntax
- JCX Service connection mechanism can be simple or complex as needed
  - Reusable component
    - Private-DNS
      - What is the A record of example.net
    - Omnibroker
      - “How does alice@example.com connect to geolocate at example.net”
    - Omnipublish
      - “geolocate service starting at example.net”

Open Questions

- Is an additional layer of crypto desirable?
  - Can easily add an intermediate layer of crypto
    - Use a public key as the long term host key
    - Negotiate session key for use each time IP address changes.
  - A: Probably, now just waiting for CFRG ECC outcome