DNS Cookies

Are People Hungry Enough Yet?

(With material on BIND Beta feature)

Donald Eastlake 3rd

Huawei Technologies

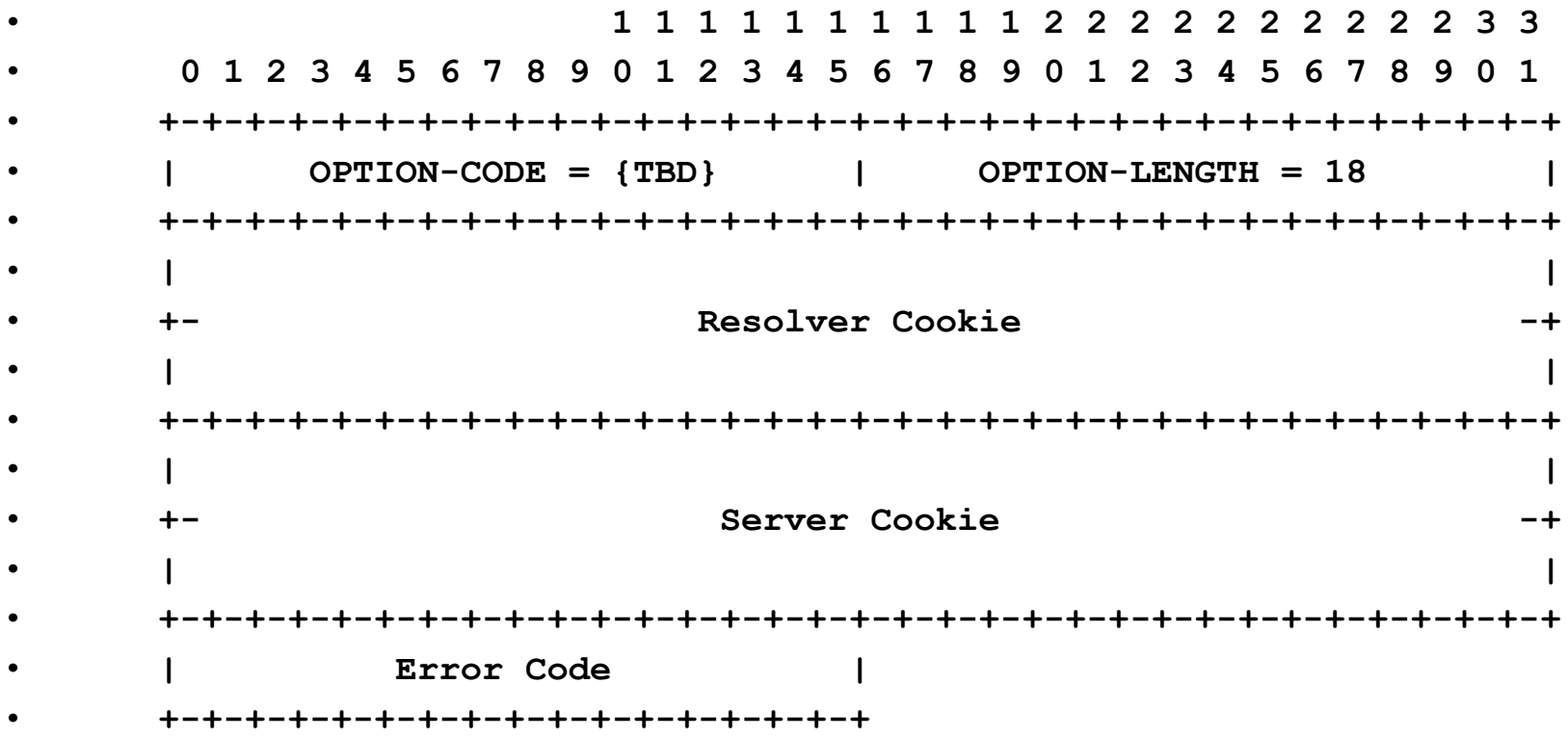
+1-508-333-2270 <d3e3e3@gmail.com>

DNS Cookies (Yummy!)

- **draft-eastlake-dnsext-cookies-04.txt** specifies an OPT option that protects against off path DNS denial of service, traffic amplification, and poisoning attacks.
  - Resolvers can include a 64-bit cookie in queries and check it in responses. For example, a pseudo-random function of the server IP and a resolver secret.
  - Servers can include a 64-bit cookie in responses and check it in future queries. For example, a pseudo-random function of the resolver IP, a server secret, and (to be sure to distinguish resolvers behind a NAT) the resolver cookie.

DNS Cookies (Yummy!)

- **Proposed OPT option:**



DNS Cookies (Yummy!)

- Three policies:
  - Disabled: Don't send cookies, ignore cookies on receipt.
  - Enforced: Always send cookies, require cookies on receipt:
    - Good cookie message, learn other party's cookie even if that message is an error message.
    - No cookie response discarded.
    - Bad cookie response discarded.
    - No cookie query discarded.
    - Bad cookie query, response rate limited short error response.

DNS Cookies (Yummy!)

- Three policies (cont.):
  - Enabled: Always send cookies.
    - Good cookie message, learn other party's cookie even if the message is an error message and switch to enforced as soft state for that other party.
    - No cookie response OK.
    - Bad cookie response discarded but server cookie is learned if resolver cookie in response correct.
    - No cookie query, response rate limited.
    - Bad cookie query, response rate limited short error message.

DNS Cookies (Yummy!)

- Eastlake Draft misc:
  - Resolver and server secrets periodically rolled over, old secret remembered for a little while for verification only.
  - Compatible with forgery resistance mechanisms in RFC 5452.
  - “Enabled” policy is backwards compatible.
  - Last presentation to an IETF WG was to DNSEXT WG in March 2008.

Source Identity Token

- **In BIND 9.10.0b1**
- Based on DNS Cookies
  - No error code field
  - Variable length sever cookie
  - Uses Experimental EDNS OPT 65,001
  - http://www.isc.org/downloads/

  - Source Identity Token slide material from Mark Andrews marka@isc.org

Source Identity Token

- Token Format:
  - Client Cookie (64 bit hash)
  - Server Cookie: 128-bits as follows:
    - Nonce (32 bits), Time (32 bits), Hash (64 bits)

- Tokens are valid for 1 hour with 300 seconds of clock skew supported for server clusters.
- DNS Server Cookies have infinite life times with the only control being to change the secret.

Source Identity Token

- Hash Computation Methods:
  - AES
  - HMAC-SHA1
  - HMAC-SHA256

- hash = trunc(hmacX(secret,
  client|nonce|when|address), 8);

Questions

- Draft has bunch of error code stuff. Too complex? BIND Beta feature has no error code stuff. Too simple?
- Draft has fixed size opaque server hash. BIND Beta feature has structured server hash. Which way to go?
- Other questions and comments welcome…