DNS Cookies

Are People Hungry Enough Yet?

(With material on BIND Beta feature)

draft-eastlake-dnsext-cookies-05.txt

Donald Eastlake 3rd d3e3e3@gmail.com

Mark Andrews marka@isc.org

DNS Cookies (Yummy!)

- An OPT option that provides weak protection against off path DNS denial of service, traffic amplification, and poisoning attacks.
  - Clients include a 64-bit cookie in queries and check it in responses. Typically a pseudo-random function of the server IP and a client secret.
  - Servers include a variable size (minimum 64-bit) cookie in responses and check it in future queries. Typically a pseudo-random function of the client IP, a server secret, and (to be sure to distinguish clients behind a NAT) the client cookie. Other material such as a time-stamp or nonce can be included.

DNS Cookies (Yummy!)

- **Proposed OPT option:**

```
•                            1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
•        0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
•       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
•       |      OPTION-CODE = {TBD}      |     OPTION-LENGTH = 18        |
•       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
•       |      Error Code (2 bytes)     |
•       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
•       |                                                               |
•       +-                    Client Cookie (8 bytes)                  -+
•       |                                                               |
•       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
•       |                                                               |
•       /                   Server Cookie (8 to 32 bytes)               /
•       /                   Omitted by client if unknown                /
•       +-+-+-+-+-+-…
```

DNS Cookies (Yummy!)

- Clients and servers only need to recognize their own cookies.

- If not implemented or not enabled, no cookie in requests, servers respond as they do now.

- When implemented and enabled:
  - Client includes a COOKIE OPT in requests with a client cookie and a server cookie if they know a cookie for the server.

DNS Cookies (Yummy!)

- When implemented and enabled (cont.):
  - Server looks for COOKIE OPT in requests:
    - If none or malformed, server can
      1. Discard request. 2. Return a minimal length error.
      3. Process request normally.
    - Cookie OK except for bad/absent server cookie:
      1. Discard request. 2. Return a minimal length error.
      3. Process request normally and return with a COOKIE OPT with a distinctive error code in it.
         - » Must take choice 2 or 3 occasionally for bootstrap.
    - Good COOKIE OPT including good server cookie OK: Process normally.

DNS Cookies (Yummy!)

- When implemented and enabled (cont.):
  - Client looks for COOKIE OPT in responses:
    - If good COOKIE OPT with good client cookie in response, client caches server cookie and processes response normally.
    - If no/malformed cookie or one with bad client cookie, client discards the response.
    - If response has a good client cookie but a COOKIE OPT error code indicating that the server received the request with a bad server cookie, then the client should retry immediately with the new server cookie it just received.

DNS Cookies (Yummy!)

- Miscellaneous:
  - See draft for full details including factoring in whether request is over TCP which provides similar weak protection.
  - 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.

BIND 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/

BIND 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.

BIND Source Identity Token

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

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