Interoperable DNS Server Cookies

Ondřej Surý – Willem Toorop – Donald E. Eastlake 3rd – Mark Andrews

draft-ietf-dnsop-server-cookies-02
Why DNS Cookies?
DNS Cookies Operation

- Valid Server Cookie? Large answers
- Valid Server Cookie? RRL Disabled!
DNS Cookies in Anycast

client

server cookie

client

server cookie

client

server cookie

client

server cookie

client

server cookie

client
Hackathon @IETF104 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop
- Focus on the Server Cookie
- Interoperable Server Cookies for:

  - BIND
  - 9
  - PowerDNS
  - NSD
  - KnotDNS
  - Unbound
Hackathon @IETF104 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop
- Focus on the Server Cookie
- Interoperable Server Cookies for: Bind, NsDns, KnoppDns, Unbound

Mission Accomplished picture by cathyjonelson
draft-sury-toorop-dnsop-server-cookies

• Merge with draft-eastlake-dnsop-server-cookies-00
• Changes based on review comments
• Add section on Server cookie updating
• Resulting in:
  draft-sury-toorop-dnsop-server-cookies-00

• Next step, Implementation experience
Hackathon @IETF105 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop
- Also implement client side

Client-Cookie = MAC_Algorithm(
    Client IP Address | Server IP Address, Client Secret )

- Server IP Address for minimal authentication
- Client IP Address for privacy
Hackathon @IETF105 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop
- Also implement client

\[
\text{Client-Cookie} = \text{MAC\_Algorithm}\left( \text{Client\_IP\_Address} | \text{Server\_IP\_Address}, \text{Client\_Secret} \right)
\]

- Client IP not (cheaply) available before send
- Client IP can change
- Cookie construction for every query
3. Constructing a Client Cookie

When implementing the DNS Cookies, several DNS vendors found impractical to include the Client IP as the Client Cookie is typically computed before the Client IP address is known. Therefore, the requirement to put Client IP address as input to was removed, and it simply RECOMMENDED to disable the DNS Cookies when privacy is required.
3. Constructing a Client Cookie

When implementing the DNS Cookies, several DNS vendors found impractical to include the Client IP address as the Client Cookie is typically computed before the Client IP address is known. Therefore, the requirement to input the Client IP address as input was removed. It is RECOMMENDED to disable the DNS Cookies when privacy is required.
• Comments from Philip Homburg on dnsop mailing-list
  • Server cookie is based on Client IP too
  • Client Cookie can only be used from same IP

• Not quite right yet...
Hackathon @IETF106 Results

Client-Cookie = MAC Algorithm(
   Client IP Address | Server IP Address, Client Secret )

Client-Cookie = 64 bits of entropy

- Server IP Address for minimal authentication
  - Create new random Client Cookie for each new Server
  - If Server returns Server Cookie:
    - Register Client IP alongside Client Cookie & Server Cookie
- Client IP Address for privacy
  - Bind UDP socket to Client IP .... Reset Cookies on failure
Hackathon @IETF106 Results
draft-ietf-dnsop-server-cookies-02

- Rewritten *Constructing a Client Cookie* Section
- New *Security and Privacy Considerations* Section

- **Next step**, Implementation experience
Hackathon @IETF107 Results
draft-ietf-dnsop-server-cookies-02

- Implementation of privacy friendly Client Cookies in
  - getdns
  - https://github.com/getdnsapi/getdns/pull/471 ... Will be in 1.6.1 release

- Verbal reassurance from Witold Krecicki
  - Client IP can be tracked with Bind
Goal was to harmonize Server Cookies

2.9.0+ has updated DNS Cookies

9.16+ has updated DNS Cookies

NSD & unbound have PoC impl.

Text in draft is good enough for considered Resolver implementations.

Next step?
• Goal was to harmonize Server Cookies
• 2.9.0+ has updated DNS Cookies
• 9.16+ has updated DNS Cookies
• PoC impl.
• Text in draft is good enough for considered resolver implementations.

• Next step?

Mission Accomplished picture by cathyjonelson