

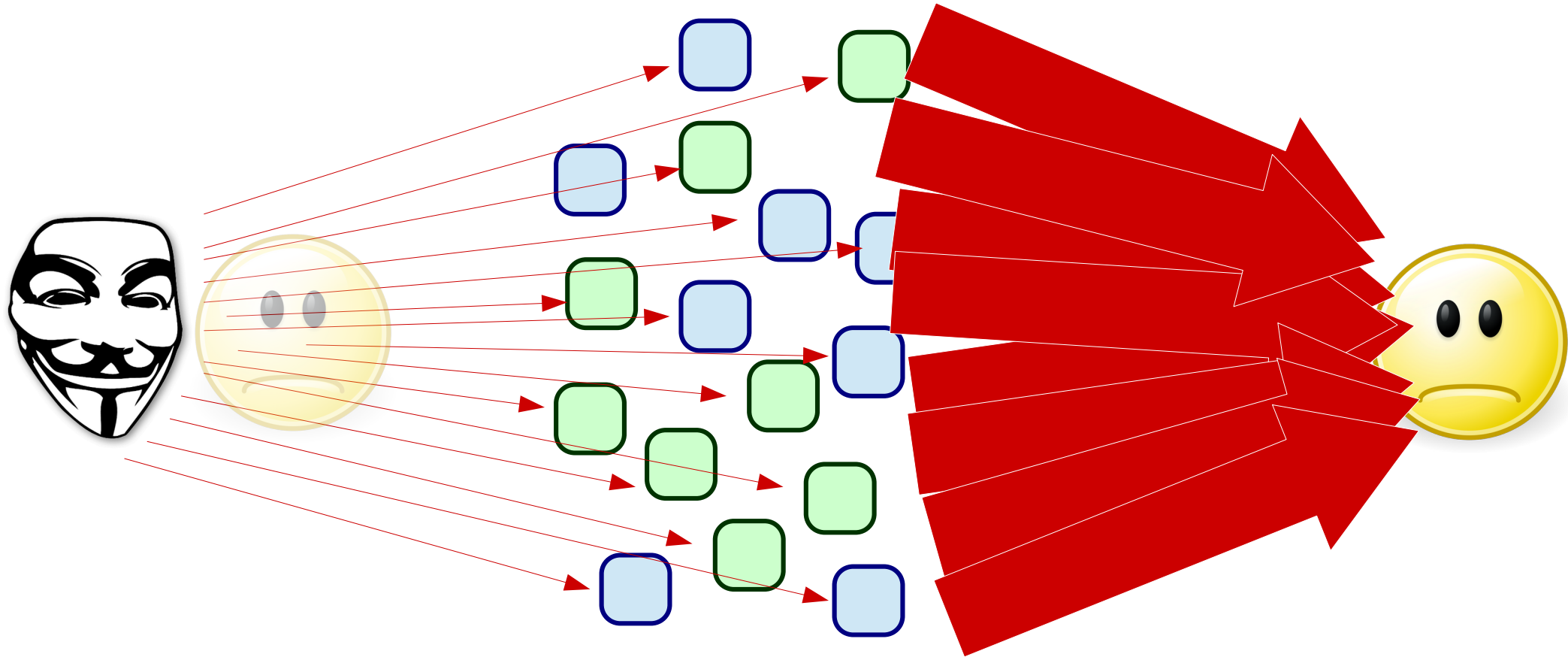
# Interoperable DNS Server Cookies



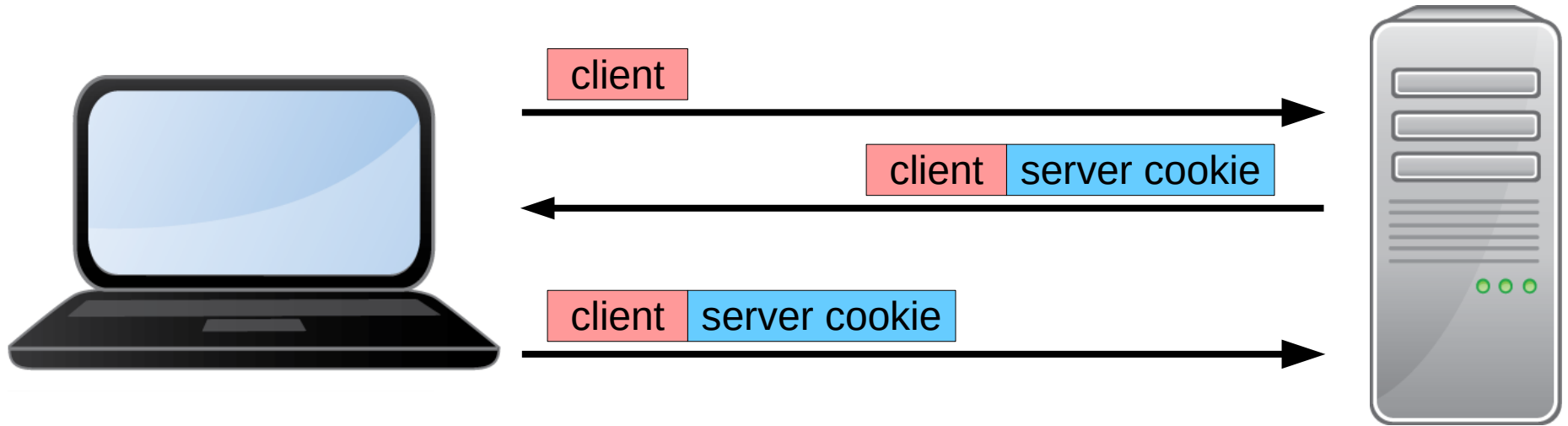
picture  
PUBLIC  
DOMAIN

Ondřej Surý – Willem Toorop – Donald E. Eastlake 3<sup>rd</sup> – Mark Andrews  
[draft-ietf-dnsop-server-cookies-02](#)

# Why DNS Cookies?

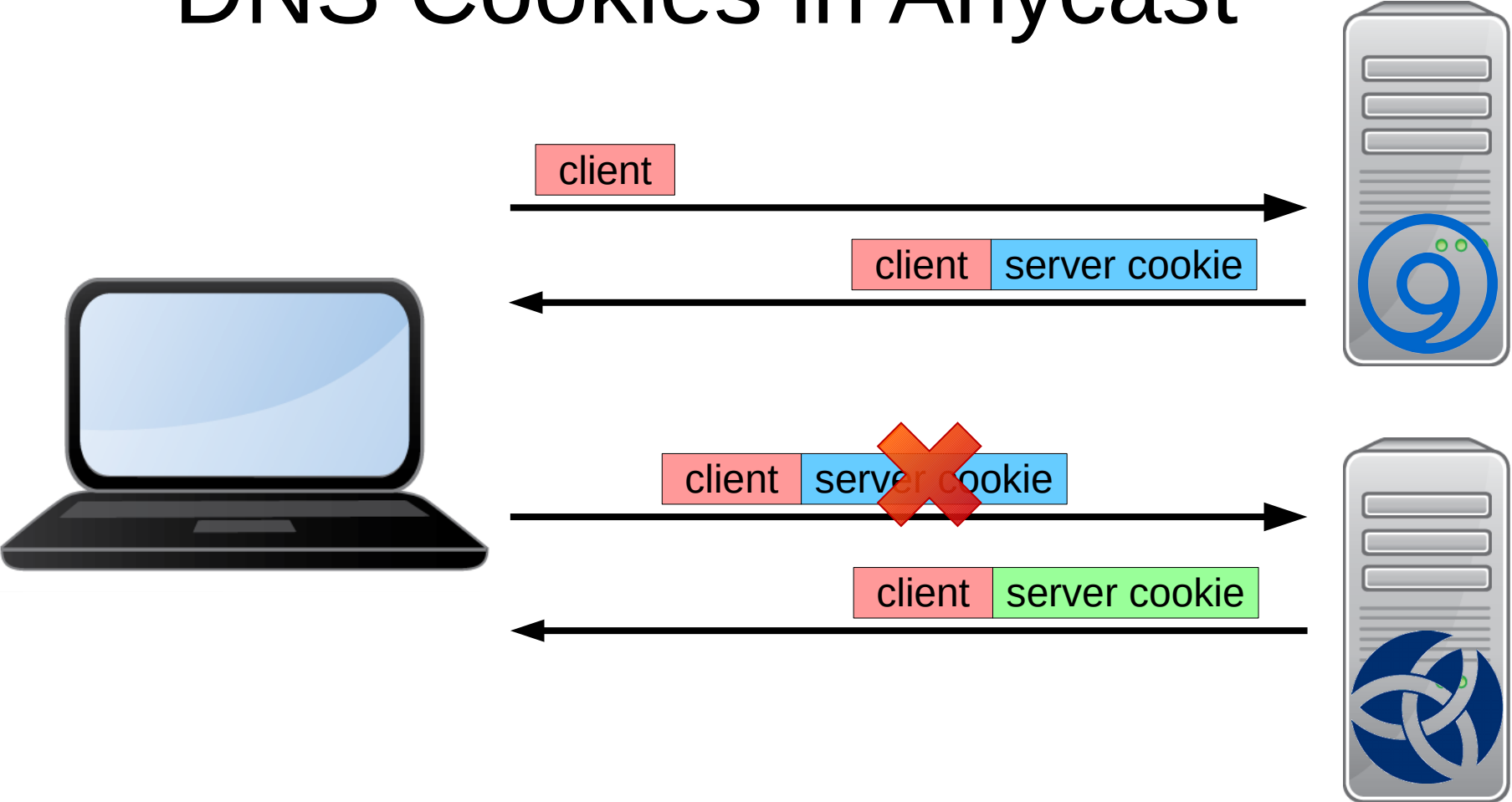


# DNS Cookies Operation



- Valid Server Cookie? Large answers
- Valid Server Cookie? RRL Disabled!

# DNS Cookies in Anycast



# Hackathon @IETF104 Results

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



# Hackathon @ IETF Results

**MISSION**

- Witold Kreciński, Ondřej Surý, Pieter Lexis, Willem Toorop
- Focus on the Security
- Interoperability



**KNS  
DNS**

**ACCOMPLISHED**

**ambound**

Mission Accomplished picture



# `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 )
```

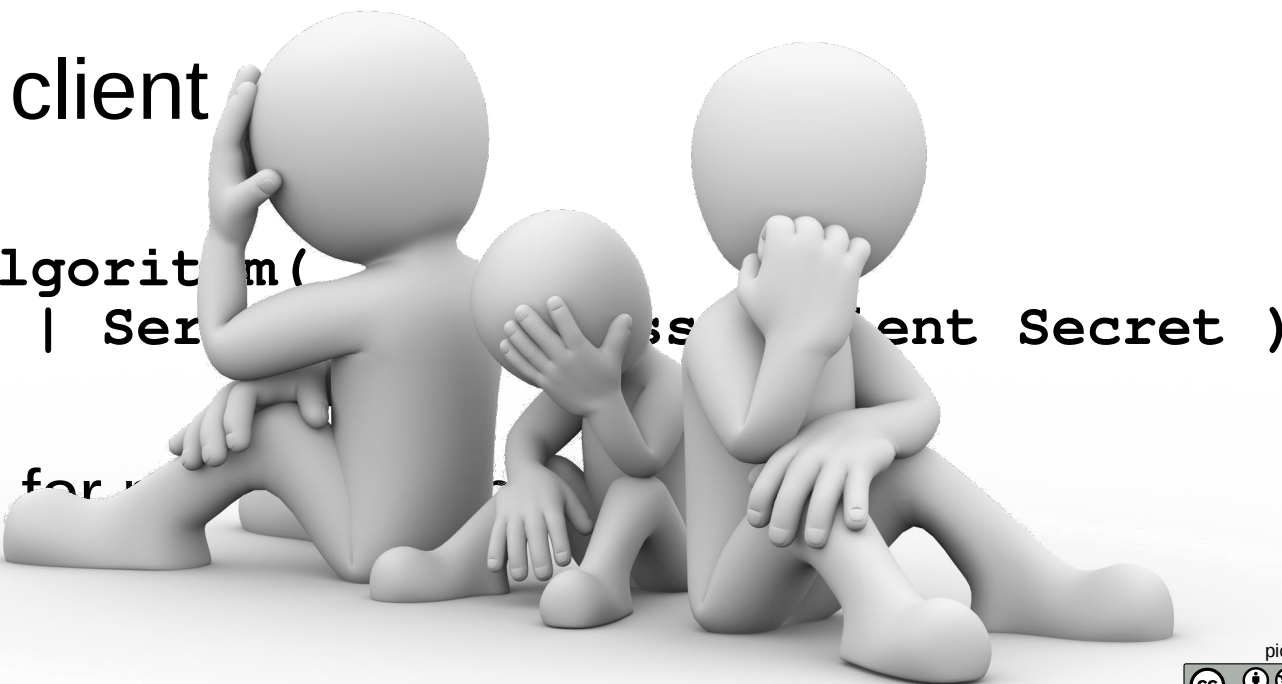
- `Server IP Address` for minimal authentication
- `Client IP Address` for privacy



# Hackathon @IETF105 Results

- Witold Krecicki, Ondřej Surý, Pieter Lexis, Willem Toorop

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



# draft-sury-toorop-dnsop-server-cookies-00

- Draft adopted by dnsop WG:

[draft-ietf-dnsop-server-cookies-00](#)

## 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.

draft-sury-toorop-dnsop-server-cookies-00

- Draft adopted

**MISSION**

draft-ietf-dnsop-server-cookies-00

### 3. Constructing Client IP

When implementing the Client IP for several DNS vendors for the Client IP, the Client IP is computed before the Client IP address is known. Therefore, the requirement to use the Client IP address as input to the Client IP was removed. It is required to disable the DNS Cookies.

**ACCOMPLISHED**

Mission Accomplished picture



by cathyjonelson

## `draft-ietf-dnsop-server-cookies-00`

- 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

## `draft-ietf-dnsop-server-cookies-01`

- 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







<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



# draft-ietf-dnsop-server-cookies-02

- 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?

# draft-ietf-dnsop-server-cookies-02

**MISSION**

- Goal was to make sure all DNS servers supported cookies
-  KNOT DNS 2.9.0+ updated DNS Cookies
-  BIND 9.10.0+ supported DNS Cookies
-  NSD 4.0.0+ supported DNS Cookies
- Text in draft is generated for considered resolver implementations

**ACCOMPLISHED**

• Next step?



Mission Accomplished picture



