Interoperable DNS Server Cookies

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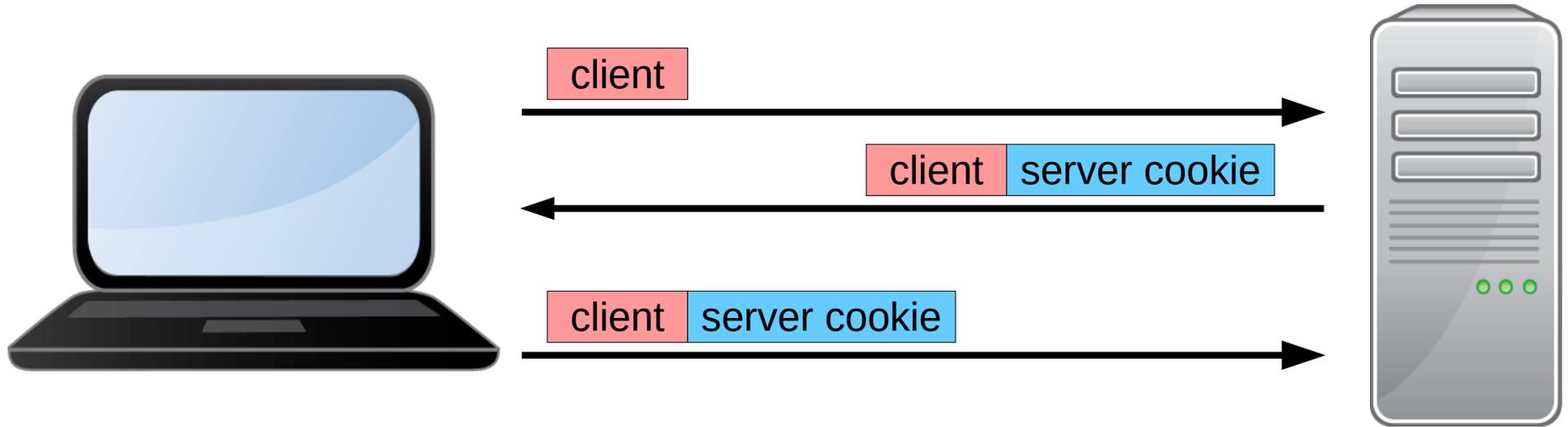Donald E. Eastlake 3rd
Mark Andrews

CC0 Public Domain *from* publicdomainpictures.net

`draft-sury-toorop-dnsop-server-cookies-00`
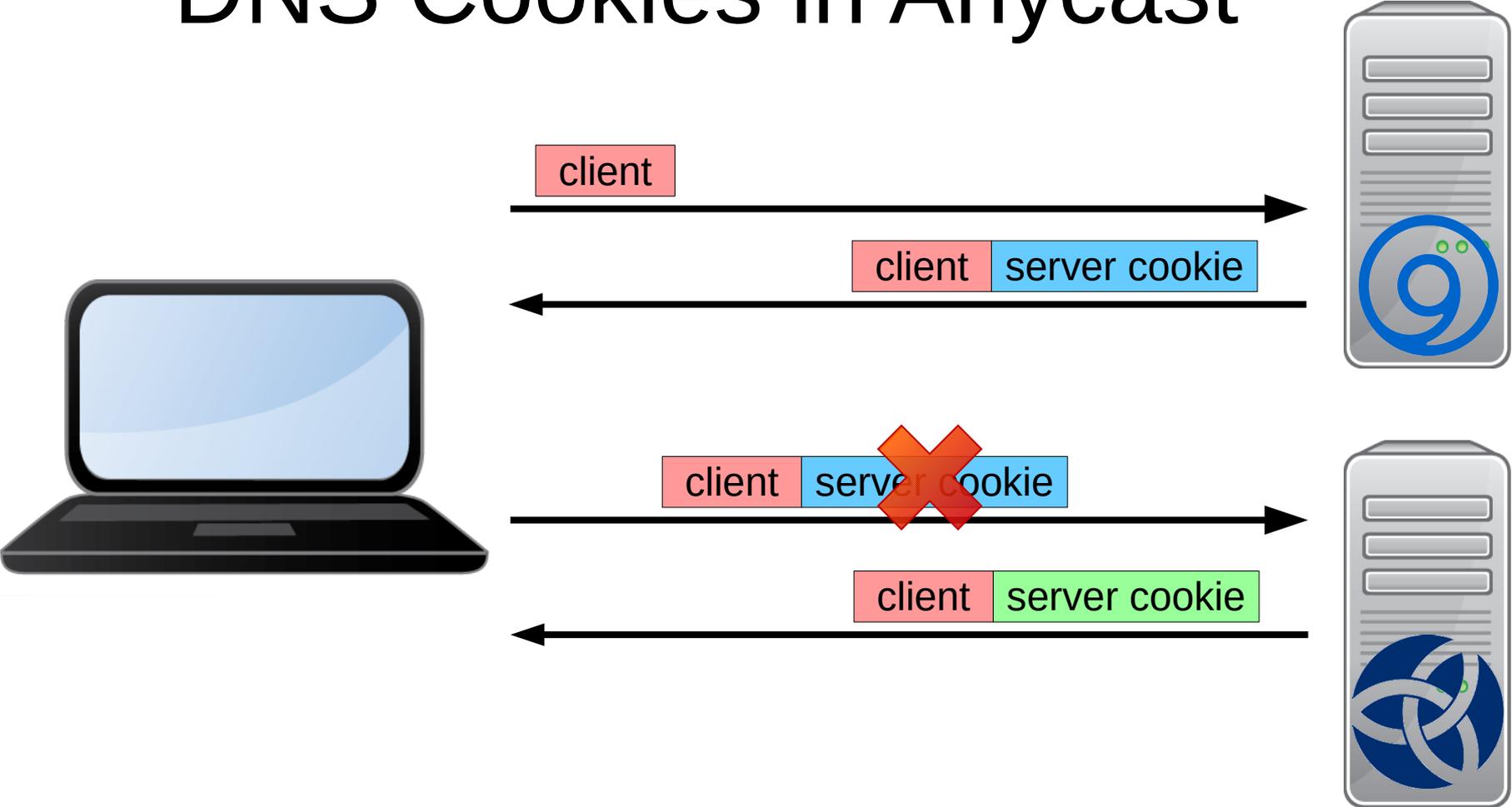
Why DNS Cookies

- DNS Native Protection Mechanism against Amplification Attacks

- To be helpful it needs to be enabled everywhere

- Multi-vendor cooperation desirable

DNS Cookies Operation

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

DNS Cookies in Anycast

Hackthon @IETF104 Results

- `draft-sury-toorop-dns-cookies-algorithms-00`

- Witold Krecicki, Pieter Lexis, Willem Toorop

- Interoperable Server Cookies for:

Donald & Mark joined

- Merge of:
  - `draft-sury-toorop-cookie-algorithms-00`
  - `draft-eastlake-dnsop-server-cookies-00`
- Into
  - `draft-sury-toorop-dnsop-server-cookies-00`

draft-sury-toorop-dnsop-server-cookies

- Include client IP in Server Cookie hash calculation

- Use only SipHash2.4 with this Version

- IANA sub-registry "DNS Server Cookie versions":

```
+---------+------------+----------------------+
| Version | Algorithm  | Server Cookie Length |
+---------+------------+----------------------+
| 0       | Reserved   | -                    |
| 1       | SIPHASH24  | 16                   |
| 2-240   | Unassigned | -                    |
| 240-254 | Private use| -                    |
| 255     | Reserved   | -                    |
+---------+------------+----------------------+
```

- Operator advise on Server Secret roll-over

- Implementation advise for smooth roll-over

- Appendix with Test vectors

Hackthon @IETF105 Results

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

- Interoperable Server Cookies for:

Hackthon @IETF105 Results

```
3.   Constructing a Client Cookie

    The Client Cookie is a nonce and should be treated as such.
    It is RECOMMENDED but not required that the following pseudorandom
    function be used to construct the Client Cookie:

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

    where "|" indicates concatenation.
```

- Source IP for Client cookie is impractical

- Text to RECOMMEND it for Stub resolvers

Next steps

- Upload WG version with new Client Cookie generation advise

- Test interoperability on production quality implementations

https://github.com/NLnetLabs/draft-sury-toorop-dns-cookies-algorithms