Interoperable DNS Server Cookies

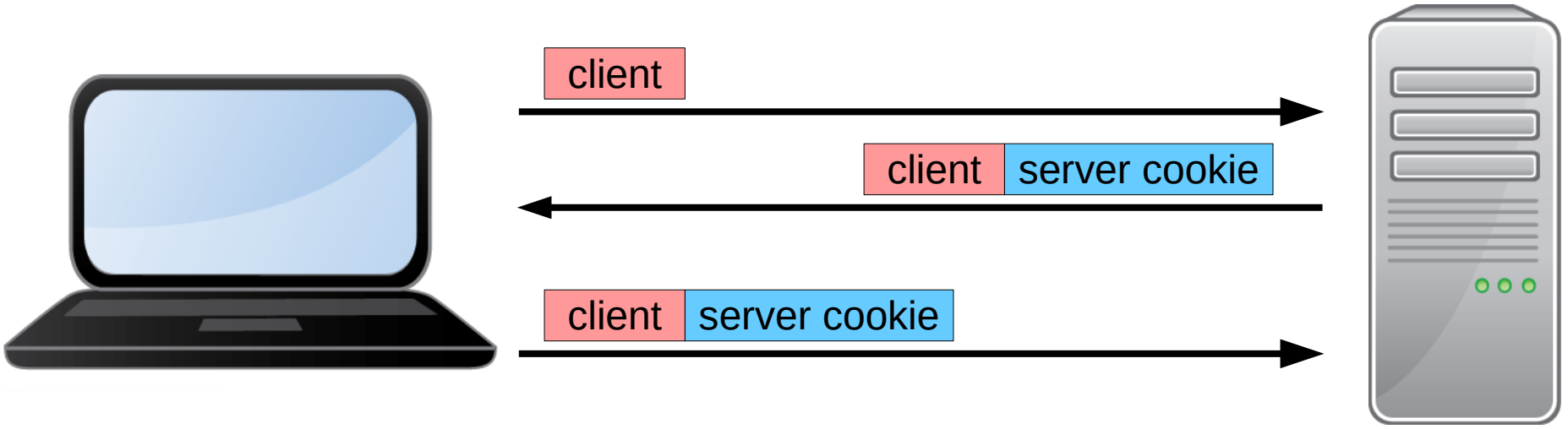
Willem Toorop
Ondřej Surý
Donald E. Eastlake 3rd
Mark Andrews

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

Why DNS Cookies

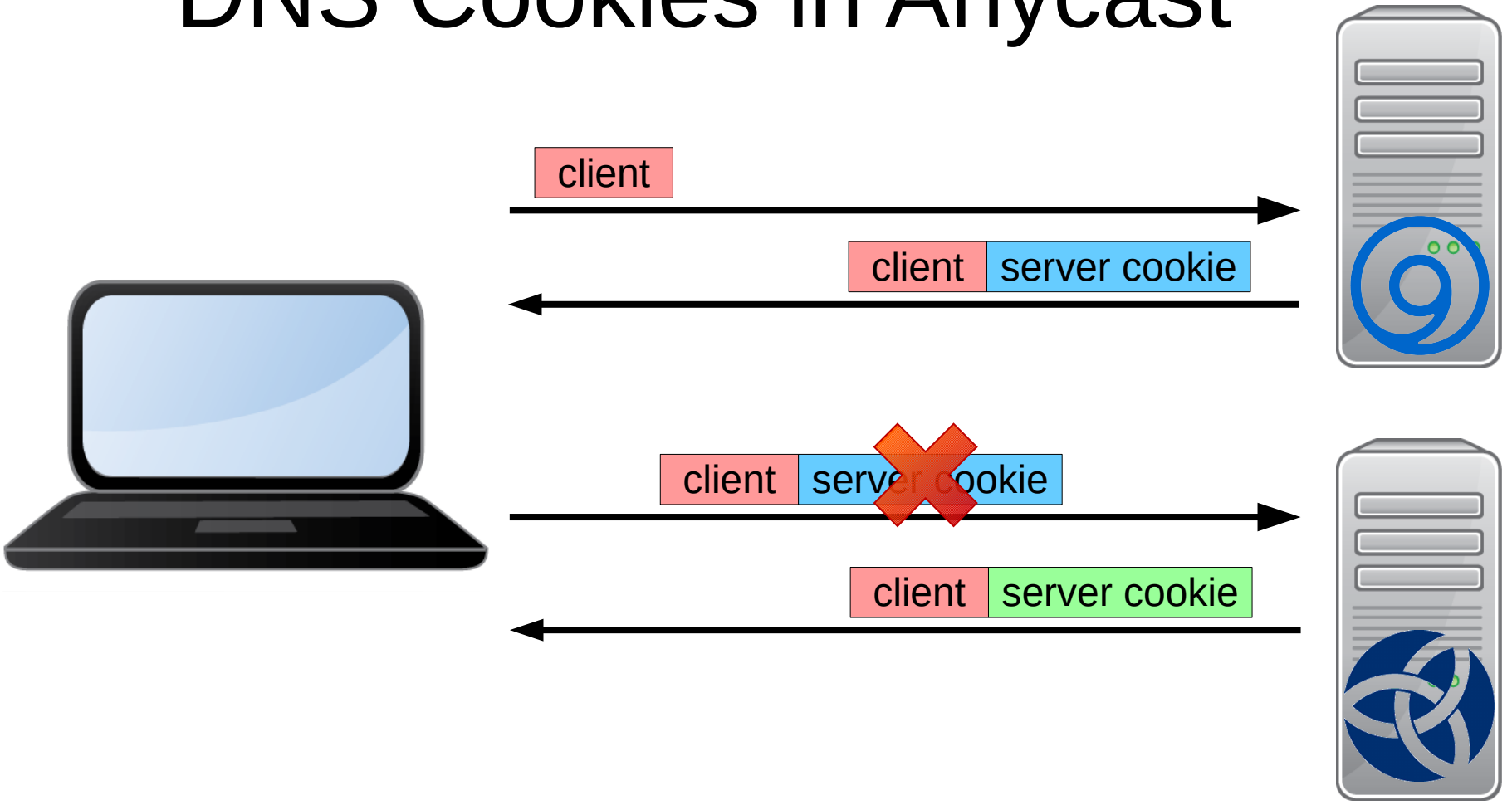
- DNS Native Protection Mechanism against Amplification Attacks
- To be helpful it needs to be enabled everywhere
- Multi-vendor cooperation desirable

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 with:
  - draft-eastlake-dnsop-server-cookies-00
- 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	-

Still TODO’s

- Operator advise on Server Secret roll-over
- Implementation advise for smooth roll-over
- Appendix with Test vectors

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

Questions?