Modern DNS & Security

@PowerDNS_Bert
bert.hubert@powerdns.com

NLIX DAYS 2019

https://powerdns.org/nlix2019

POWERDNS
AN OX COMPANY

The domain name system

[8] J. Postel, "Internet Name Server", IEN 116, USC/Information Sciences Institute, August 1979.

IEN 116

J. Postel
ISI
August 1979

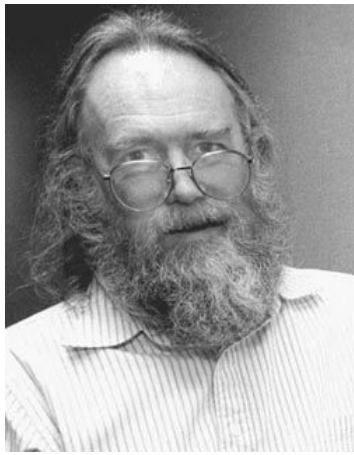
Obsoletes: 89, 61

INTERNET NAME SERVER

INTRODUCTION

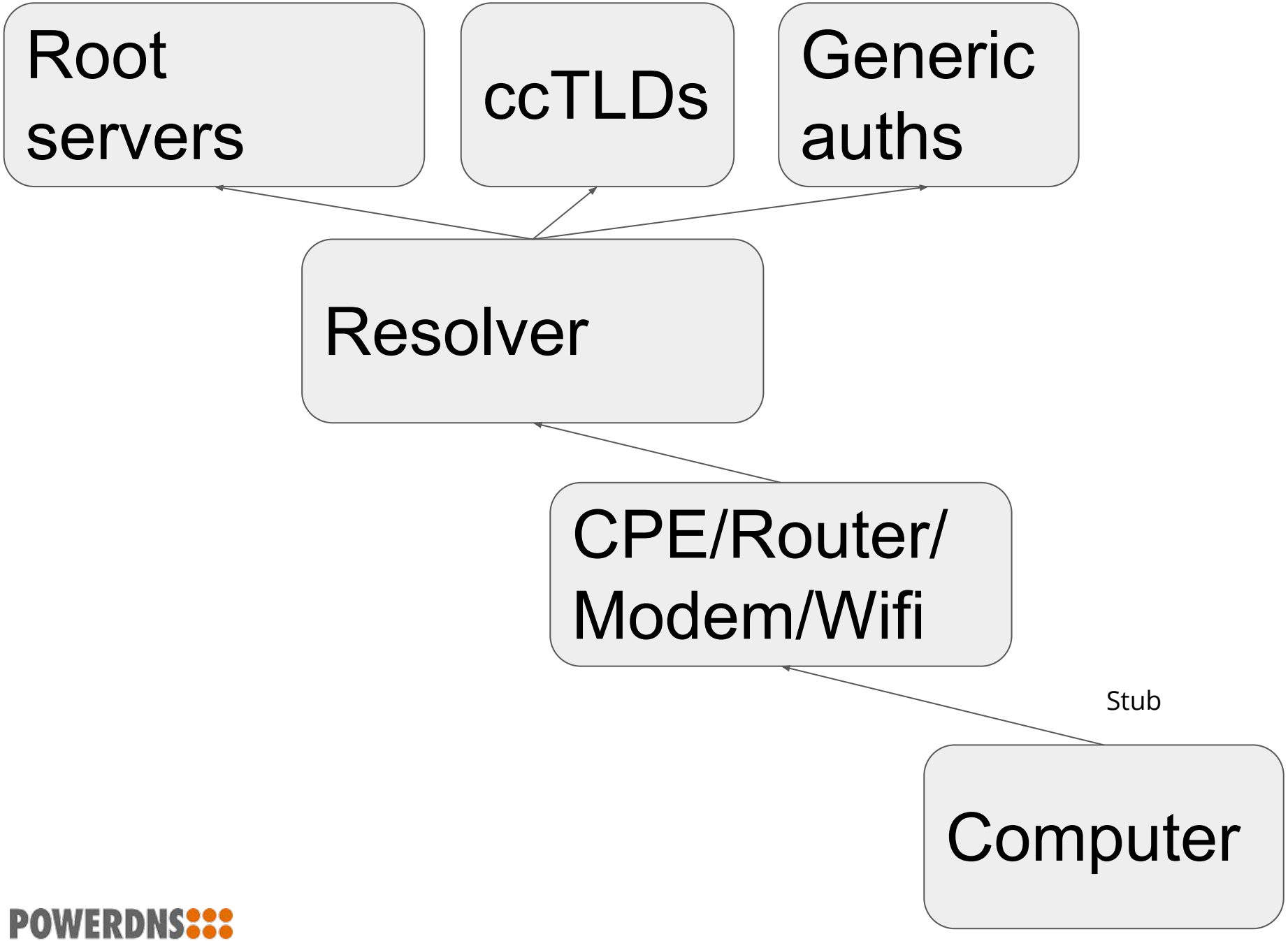
This memo defines the procedure to access an Internet Name Server. Such a server provides the actual addresses of hosts in the internet when supplied with a host name. An Internet Name Server is a dynamic name-to-number translation service.

This server utilizes the User Datagram Protocol (UDP) [2], which in turn calls on the Internet Protocol (IP) [3].



DNS is the last plaintext protocol on the internet.

(or is it?)


Root servers
ccTLDs
Generic auths
Resolver
CPE/Router/ Modem/Wifi
Stub
Computer

2015:

DNS over TLS. “Simple” encrypted DNS **transport** over port 853

2018:

DNS over HTTPS. “Simple” encrypted DNS **transport** over real HTTPS on port 443

- *With headers, cookies and tracking*

And then.. Network operators & operating system vendors did nothing... DNS is boring! So for now, we are stuck with plaintext..

Except suddenly: American browser vendors & CDNs decided to fight for our privacy!

“DNS over Cloud”

New trust model: Browser talks straight to the CDN, bypassing your OS, network & your security settings

May break:

- Security filtering
- Security monitoring
- **CDN performance**
- Split horizon / VPN
- Your privacy (?!)

- Enterprise impact: who controls your network?
  - Endpoints/IoT harder and harder to manage
  - DoC means “management from network” is going away
  - BYOD?
- Trust the cloud?

- DNS over UDP provides almost no tracking possibilities
  - NAT serves as a privacy layer
- DNS over TLS already comes with session resumption tickets (which are vital for performance, but can last days)
- DNS over HTTPS sends agent headers, language settings and even supports cookies
- **Potentially enables persistent per-device tracking across locations.**

Rationale:

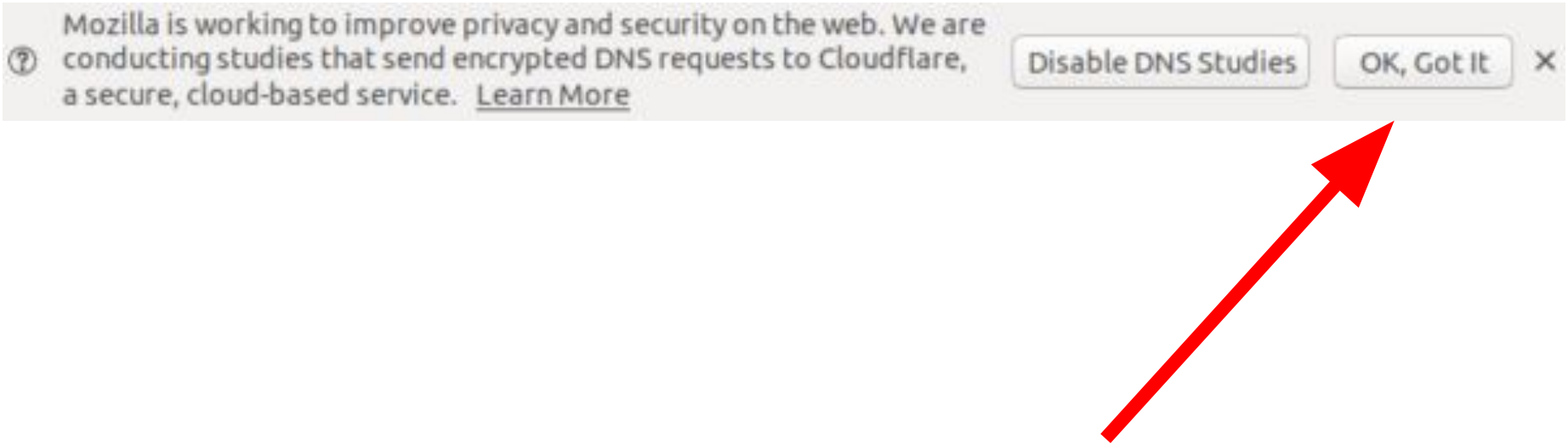
- NXDOMAIN redirection
- Turkish/Chinese/Russian freedom fighters
- Countries with no privacy regimes (like the US)
- Must get “everyone” on DoH to provide cover & impact
- “Piratebay”

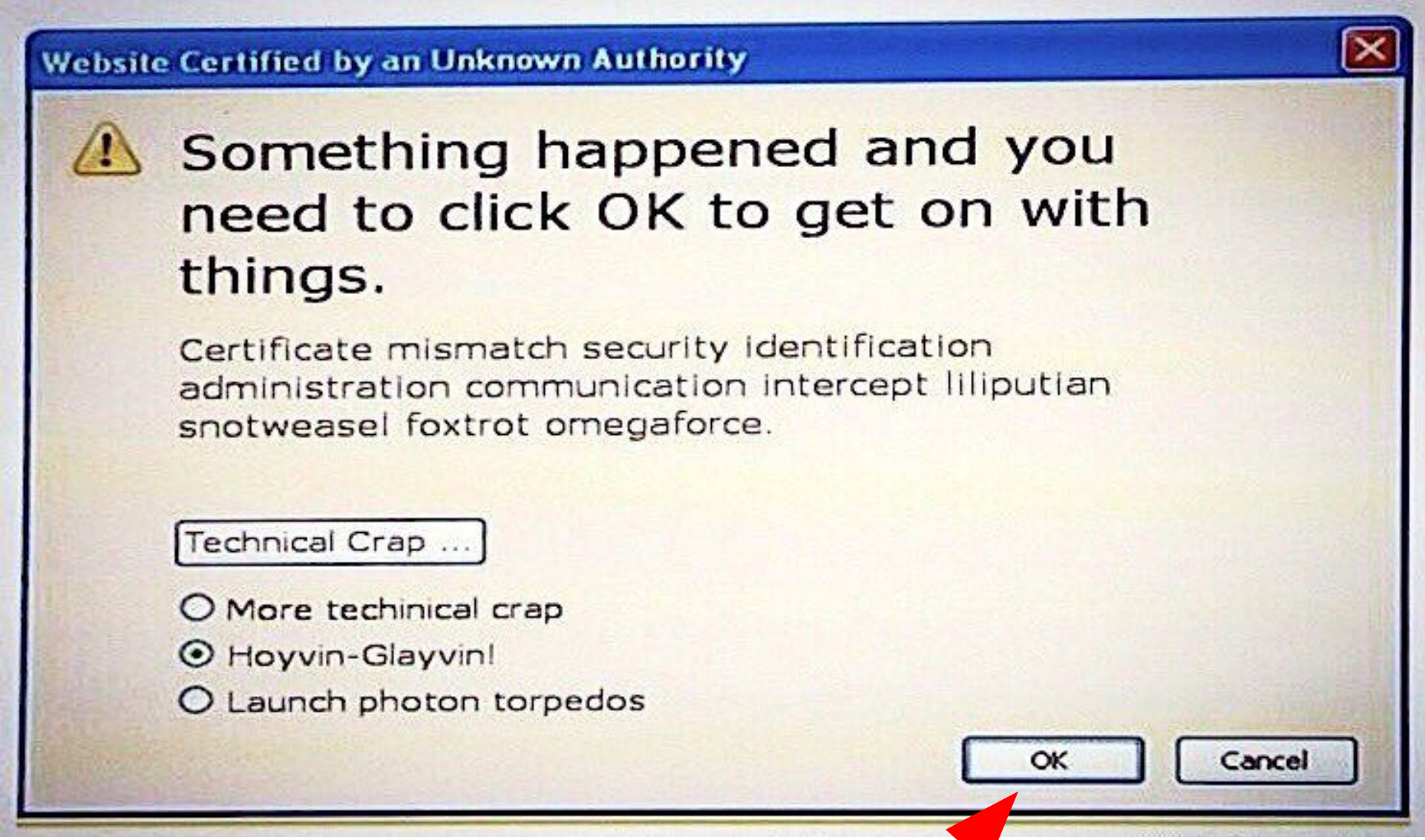
Mozilla:

“We have implemented DNS over HTTPS and will deploy it by default for our US users.

The user will be informed that we have enabled use of a *TRR* and have the opportunity to turn it off at that time, **but will not be required to opt-in to get DoH**“

https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw
https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/


Mozilla is working to improve privacy and security on the web. We are conducting studies that send encrypted DNS requests to Cloudflare, a secure, cloud-based service. Learn More
Disable DNS Studies
OK, Got It



POWERDNS
AN OX COMPANY

Mozilla/Firefox:

- Can receive enterprise configuration settings to not enable DNS over HTTPS

- Will stop doing DNS over HTTPS if you ‘NXDOMAIN’ the special domain name use-application-dns.net

Google:

- Android P attempts DoT already, will attempt to do DoH if provider offers it and publishes somehow
- Will not surprise users with sudden changes. Chrome will use DoH if current DNS does it
- However, capability is there to have users opt-in. *Users might be nagged about this if provider offers no encryption, no DNSSEC, slow DNS or messes with DNS.*

https://mailarchive.ietf.org/arch/msg/dns-privacy/kpt6ZYMN5H3DsXPVi_QIdmbAdJw

Impact of DNS over Cloud:

- No more visibility / security filtering
- Applications pick their own DNS provider: bandwidth to that provider must be SUPER 24/7
  - **Congestion to Cloudflare -> all of your internet is slow**
- Intranet may break, VPNs may break
- Your intranet & server names will leak to Cloudflare

What to do?

- Turn on DNS over TLS on your resolvers, see Android phones use it!
  - And likely Chrome later
- Run DoH, will not see any use, but practice is good
  - Firefox, several apps do use it
  - **Discovery is a problem**
- Ponder enterprise/use-application-dns.net setting to prevent use of DoH

Further reading

- On Firefox moving DNS to a third party provider
- The big DNS Privacy Debate at FOSDEM
- DNS Privacy at IETF 104 (Geoff Huston)
- More DOH (Geoff Huston)

Modern DNS & Security

@PowerDNS_Bert
bert.hubert@powerdns.com

NLIX DAYS 2019

https://powerdns.org/nlix2019

POWERDNS
AN OX COMPANY