ICANN 70
VIRTUAL COMMUNITY FORUM

DNS over HTTPS
Myth Busting and Realities of Current Deployments

Agenda

ICANN 70 VIRTUAL COMMUNITY FORUM

- Introducing the Panel and Experts
- Defining DNS over HTTPS
- The Resolver Perspective
- The Browser Perspective
- Regional Internet Registry Perspective
- Question & Answer

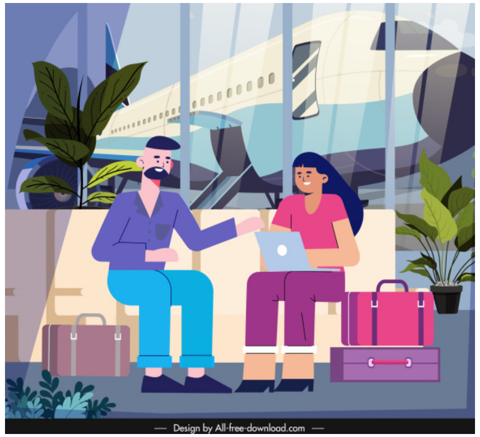
Introducing…

- Katie Noyes (GAC Public Safety Working Group) – Federal Bureau of Investigation
- Janos Drienyovszki (GAC Public Safety Working Group) – European Commission
- Richard Leaning (Director, Trust and Safety) – Cloudflare
- Eric Rescorla (Chief Technology Officer) - Mozilla Firefox
- Marco Hogewoning (Manager, Public Policy and Internet Governance) – RIPE NCC

With contributions from: Google, EUROPOL, U.S. National Security Agency (NSA), U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (DHS-CISA)

Defining DNS over HTTPS

- **What:** A protocol enabling domain name system resolution over a Hypertext Transfer Protocol Secure (HTTPS) connection
- **Why:** To protect and prevent unauthorized access and manipulation of DNS Traffic
- **How:** DoH was published as request for comment (RFC) 8484 by the Internet Engineering Task Force (IETF) in October 2018; discussions surrounding implementation are ongoing
- **Example** (At its simplest):



User runs a “Google” query over the Airport Wifi on the way to ICANN70 in Cancun, MX

To Be Discussed…

Encrypted Query (URL to IP Address)

Response

Translates query “best restaurants in Cancun” to Internet Protocol addresses…123.12.123.12 and returns response

The Resolver Perspective

Richard Leaning

Director, Trust and Safety

CLOUDFLARE®

The Browser Perspective

Eric Rescorla

Chief Technology Officer

Mozilla Principle #4: Individuals’ security and privacy on the internet are fundamental and must not be treated as optional.

This setting has two security problems

- How do I select a resolver to talk to?
  - ... and how do I know it’s not an attacker?
- How do I securely connect to the selected resolver?
  - Prevent attackers from observing requests and responses
  - Prevent attackers from delivering false response

Secure resolution requires addressing both of these issues

Where do you get your recursive resolver

- Where do you get your recursive resolver
  - Typically provided by your local network
  - Usually this means your ISP
  - Or your enterprise network
  - ... or the coffee shop/airport network you joined
  - Opaque to the user
  - No real way to know its policies
- Some users choose their own resolvers
  - Google Public DNS, Cloudflare, Quad9, Umbrella
  - These resolvers have varying security and privacy policies

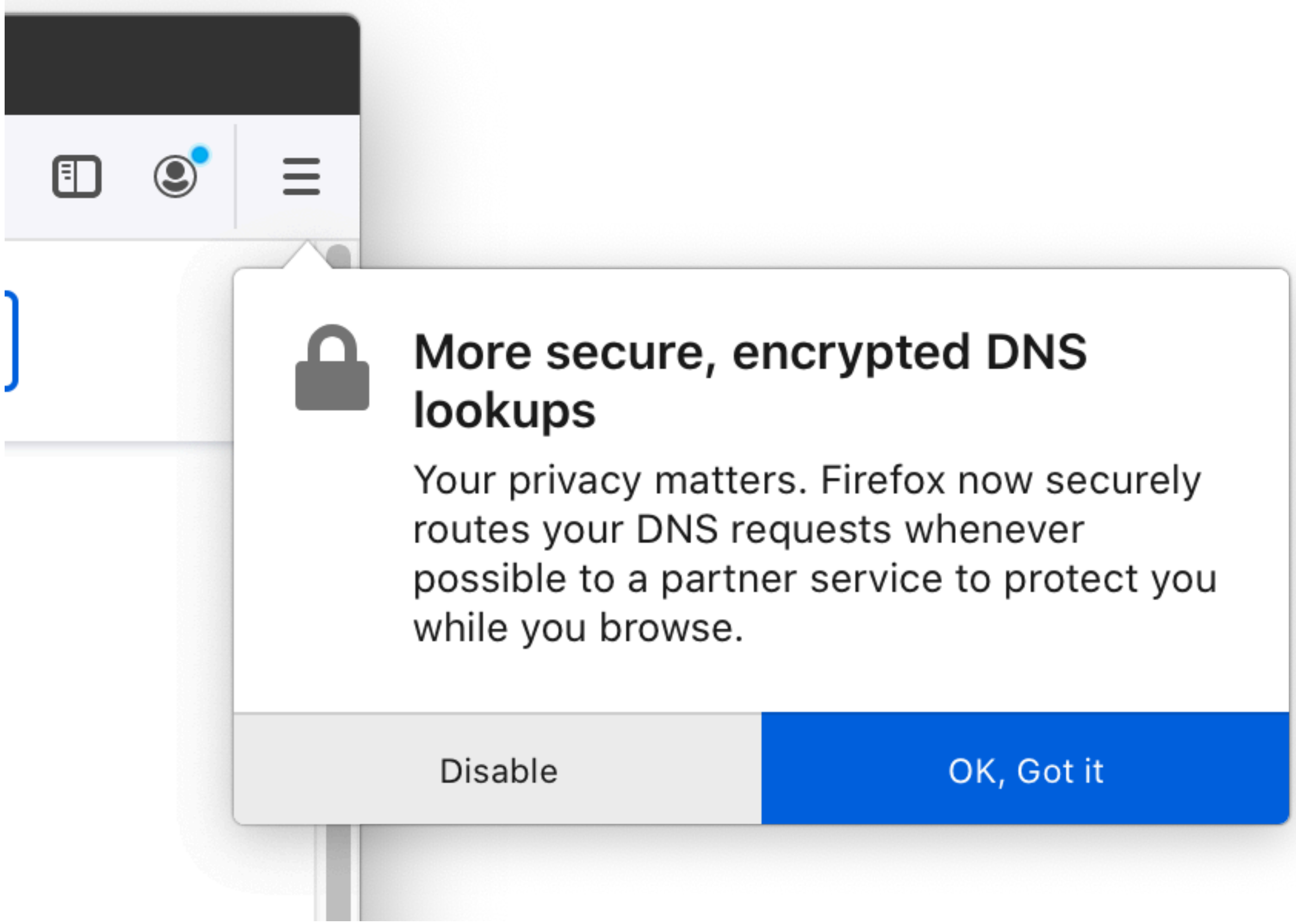
Our Approach

- Trusted Recursive Resolvers (TRR)
  - Selects a resolver that Mozilla has vetted
  - Security and privacy policies guaranteed by contract
- DNS over HTTPS (DoH)
  - IETF Proposed Standard (RFC 8484)
  - Secures data between you and the recursive resolver
  - Protects you against attackers on your network
  - Ensures that you are talking to a TRR

Our strategic approach to rolling out DoH

- Roll out DoH enabled by default
- Allow users to disable DoH or select their own resolver
- Honor enterprise configurations
- Honor opt-in DNS filtering and work with ISPs to support better detection of opt-in filtering
- Create and publish policies that improve privacy and security of the Internet

User prompt



More secure, encrypted DNS lookups

Your privacy matters. Firefox now securely routes your DNS requests whenever possible to a partner service to protect you while you browse.

TRR Policy Requirements

- Privacy Requirements
  - The resolver may retain user data but should do so only for the purpose of operating the service and must not retain that data for longer than 24 hours.
- Transparency Requirements
  - Published privacy notice
  - Yearly transparency report
- Blocking and Modification Provisions
  - No by default blocking or filtering unless required by law
  - Blocklists must be published [currently under reconsideration]

For the full policy see https://wiki.mozilla.org/Security/DOH-resolver-policy

Current Status

- On by default in the United States
  - Cloudflare is the default provider
  - Other TRRs: NextDNS and Comcast
  - Firefox will automatically detect a Comcast resolver (where possible) and switch to Comcast
- Rollout in Canada planned for 2021.
- Early exploration of other jurisdictions but no concrete plans

The Regional Internet Registry Perspective

Marco Hogewoning

Manager, Public Policy and Internet Governance

RIPE NCC

Question & Answer

ICANN 70
VIRTUAL COMMUNITY FORUM

- Please feel free to ask questions:
  - By typing <question> in the chat to flag you would like a response
  - By “raising your hand” and waiting to be recognized by the facilitator

Many thanks to our panelists and contributors and we look forward to continuing the conversation