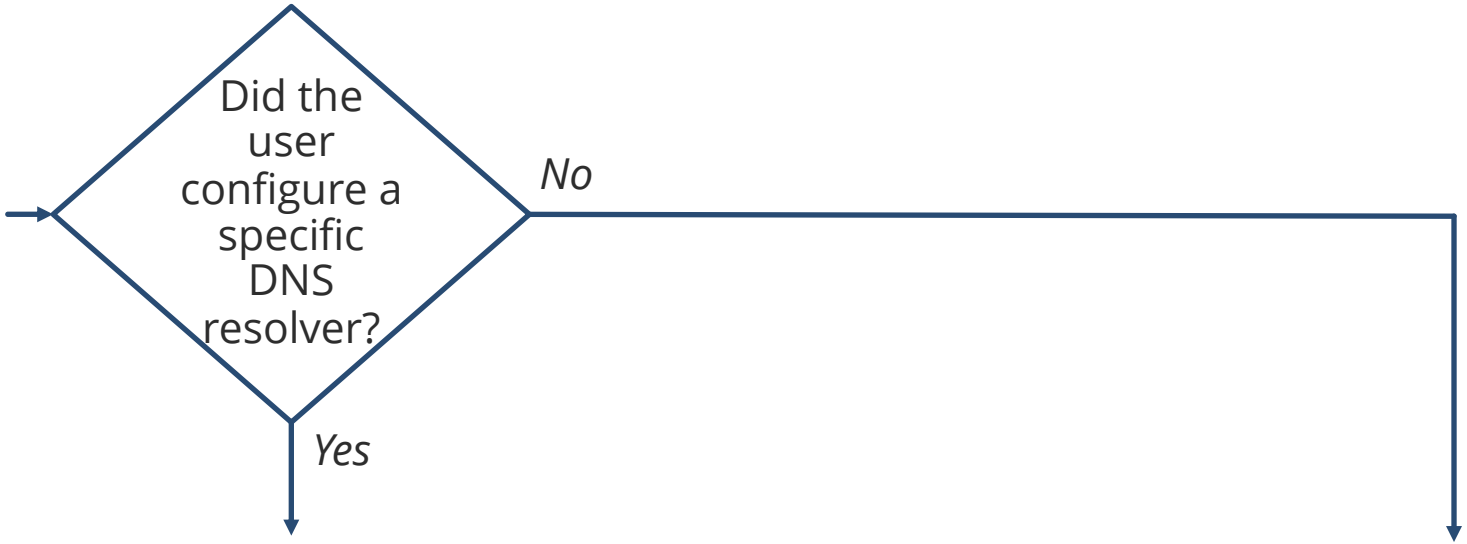
The DoH resolver discovery problem

ICANN 67 DNSSEC Workshop

Vittorio Bertola, Head of Policy & Innovation
11 March 2020

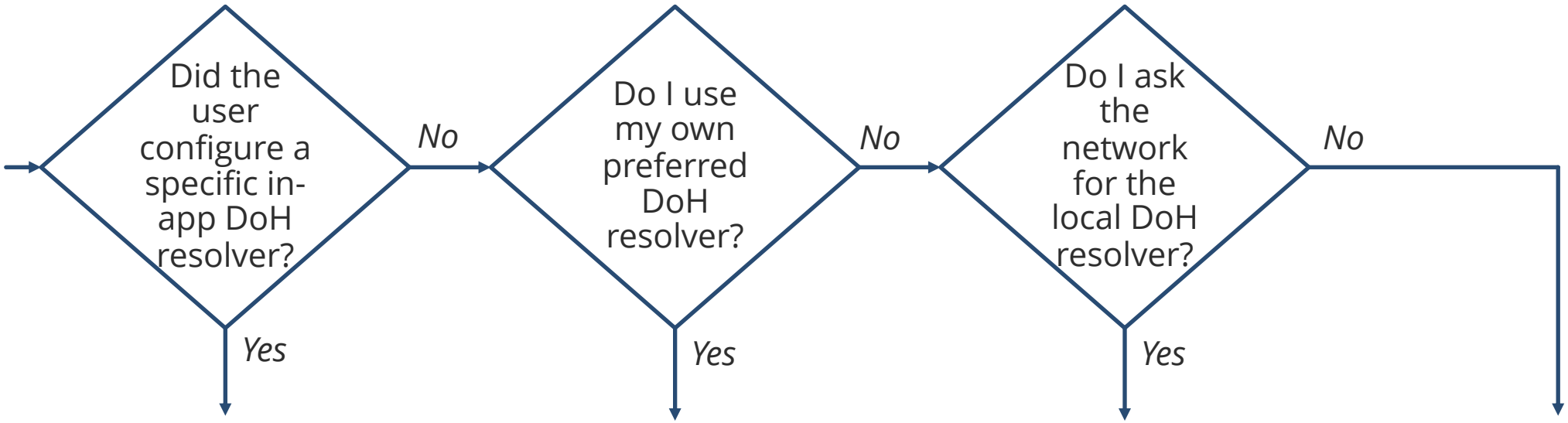
Stay Open.

The traditional DNS resolver choice algorithm



...but this does not work if you want to use DoH, since
you cannot contact a DoH resolver just by its IP address;
you need a DoH URI template

The new in-app DoH resolver choice algorithm(s)



Straightforward and supported by everyone, but very few users do this

Mozilla Firefox
Lots of policy, security, privacy, legal issues

Impossible
Currently there is technically no way to do this

Google Chrome
Microsoft Win 10
Needs some kind of database of which DoH resolver serves each network

Stay Open.

How do you discover the local DoH resolver…

…if you are unable to ask the local network?

The problems

- There is currently no way to ask the local network whether a local DoH resolver exists, and retrieve its URI template
- There also is no easy and reliable way to ask the local network *«who is your ISP?»*
- Even if there were a way (e.g. through a DHCP extension), there would still be two other problems:
    1. The local network's reply might be too insecure and impossible to authenticate
    2. Though the user has not configured a DoH resolver, somewhere else in the operating system he/she might have configured a DNS resolver different from the local one

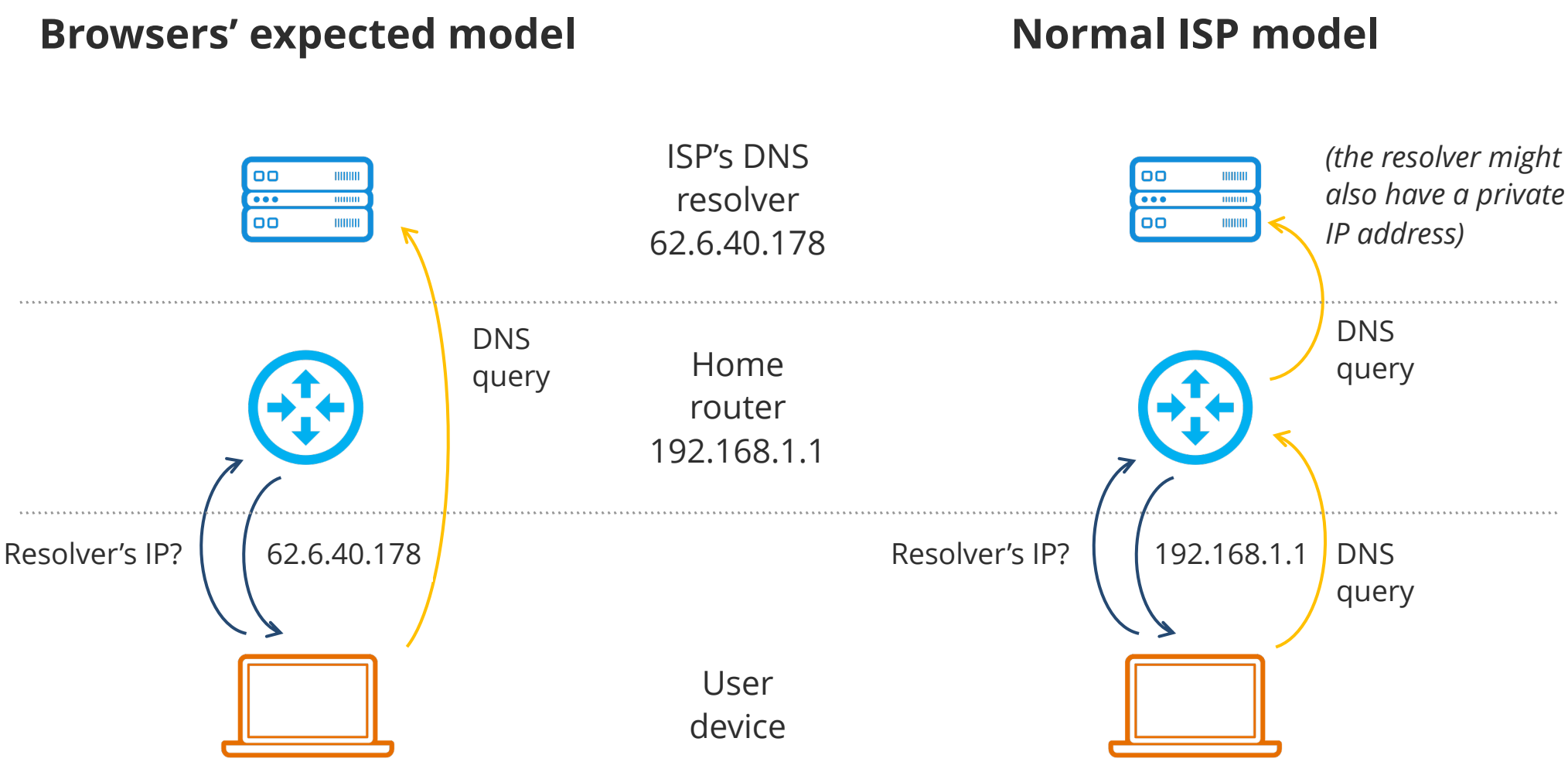
The temporary solution

- The application can **retrieve the IP address of the unencrypted DNS resolver** that has been configured in the operating system
- The application can **use that IP address as a proxy** to determine the operator that the user wants to get DNS resolution from
- The application then has a **conversion table** with the IP address of the DNS resolver and the URI template of the DoH resolver for each ISP/DNS operator
- The application looks up the IP address in the table and finds the corresponding DoH resolver
- This works also if the user selected a non-local DNS resolver

The problems with the initial solution

- It requires the application maker to **build and maintain a list of each and every ISP and DNS operator** that also has a DoH resolver
  - Google published a draft process for inclusion (not as restrictive as Mozilla's)
  - Microsoft expects to curate by hand a list of «tens» of operators (there are ~100.000 autonomous systems on the Internet)
  - This looks impossible to do in a comprehensive way, so smaller ISPs, personal servers etc will be out of luck
- It **does not work if the resolver supplied to the user has a private IP address**
  - Which is the common case in Internet access networks by telcos (at least in Europe)
  - Changing this behaviour would require updating millions of home routers
  - Not all of them can be updated or are managed by the ISP
- Also **it does not work if the ISP's/network's main resolver has a private IP address**

The difference between the two models



Stay Open.

Draft proposal for resolver discovery

Draft-ietf-dnsop-resolver-information

The draft

- A way to ask the network for information about the local resolver (which may include its DoH URI)
- Two methods for doing it:
    1. Via DNS, through a query for a specialized RRTYPE (RESINFO) for the reverse IP address (*d.c.b.a*.in-addr.arpa)
    2. Via HTTPS, retrieving a document from a well-known URL from a web server on the resolver, contacted by its IP address
- Assumes that you can trust a reply received from the local network (point of contention)

The problems with the draft

- Two methods are too many - everyone would need to implement them both or risk being incompatible
- The HTTPS method has two big problems
    - It works with private IP addresses, but it does not work with forwarders (connects to the wrong server)
    - It also requires modifying heavily all resolvers and CPEs to add support, adding a web server to them
- The DNS method only has one
    - It just requires adding support for a specific query on the main resolver platform (good)
    - But the current one does not work with private IP addresses

Stay Open. OX

A possible solution: «2FA» of the network

- Devise a workable DNS-based metod for resolver discovery
  - Like the one in the draft, but with a special-use domain name instead of the reverse IP address
- Verify out-of-band whether the reply makes sense
  - Through a list of known operators («step 2» temporary solution, as a growth path from the current temporary solution)
  - Through checks on the PKI certificate provided by the DoH server on connection
  - Other ideas?

- Not a useful solution for the applications that distrust the local resolver by principle
- But a reasonably secure solution for the applications that want to trust the local resolver when their users do so

Stay Open.

Thank you!

vittorio.bertola@open-xchange.com

Stay Open.