DNS in Applications

One Application’s Perspective
Why
Mission Statement

Individuals’ security and privacy on the internet are fundamental and must not be treated as optional.

-- Mozilla Manifesto
HTTPS

Securing HTTP has been a huge challenge
Mission Accomplished (Mostly)
Attention moves to new problems

Bad site behaviour (tracking, breaches, etc...)

Hardening (SPECTRE and friends, ...)

Gaps in encryption (traffic analysis, unencrypted content, ...)
ESNI and Encrypted DNS

Encrypting DNS is good

But we also care about who gets the information
Trusted Recursive Resolver Principle

Individual control, with strong privacy properties for defaults
Why not
DNS is not a single coherent namespace

An important value of a single communications network resides within the concept of a single referential framework, where my reference to some network resource can be passed to you and still refer to the same resource.

-- Geoff Huston
Lots of reasons for applications not to do DNS

- Content filtering
- Malware detection and blocking
- Captive portals
- Enterprise service access
- Network specific service access
- Routing policies
- Regulatory mandates

Applications will screw it up
DoH providers will screw it up
It’s a race to the bottom
One main reason

DNS is an effective control point
Not a good reason

DNS is was an effective control point
Alternative name resolution happens

Application-layer resolution happens; e.g., RFC 7838

Effective control requires covering these also

No effective control without engaging with endpoints
DNS for captive portals

IETF capport working group formed for the same problem:

People started encrypting web traffic,
... and it became harder to intercept and redirect to a portal

Using DNS here is worse than using cleartext HTTP
Content filtering by DNS name

Works only in the broadest sense

Using DNS results in under- or over-blocking
e.g., blocking all of a host that has one censored page

Endpoint cooperation is necessary to be fully effective
DNS is NOT an effective control surface
DNS is plumbing

This is not a problem you can fix with UX

Most people don’t care about plumbing until it stops working

They should not need to care
Where from here
In the long term

Applications will encrypt what they can

Applications will choose who they trust with data

Entities looking to exert control will have to engage with owners of endsystems
In the short term

People still rely (heavily) on DNS for many of these use cases

Disable application DNS where controls are in place

... use an unauthenticated signal for this

Agree that this is a stop-gap