DNS Filtering Details for Applications

DNSOP IETF 122

Mark Nottingham, Cloudflare

Motivation

- Increasing legal requirements to block/filter/censor DNS
  - Often targeting "public" resolvers
    - E.g., Tribunal Judiciare de Paris, RG 24/11187
- Reason for failure is not apparent to end user, resulting in:
  - Confusion with technical errors (increased support load)
  - Lack of transparency regarding blocking authority

Solution:

Expose Details to Clients

Not so fast...

- DNS resolvers:
  - can be configured by attacker-controlled networks
  - can be spoofed by on-network attackers
  - have many, many instances around the world
  - might use the facility to control access for reasons other than legally required ones
  - might use the facility to attack users

Not All DNS Resolvers are Bad.

Browser Security User Experience

- Extensive experience (e.g., browser TLS errors) has shown:
  - Users click through warnings / dialogues to get what they want
  - Users often don't understand the threat model
- Adding another "voice" (of the network) to a dialogue (client/server) adds complexity and opportunity for misunderstanding / attacks.
- Browsers' stance is to avoid opening new attack vectors

Mitigation

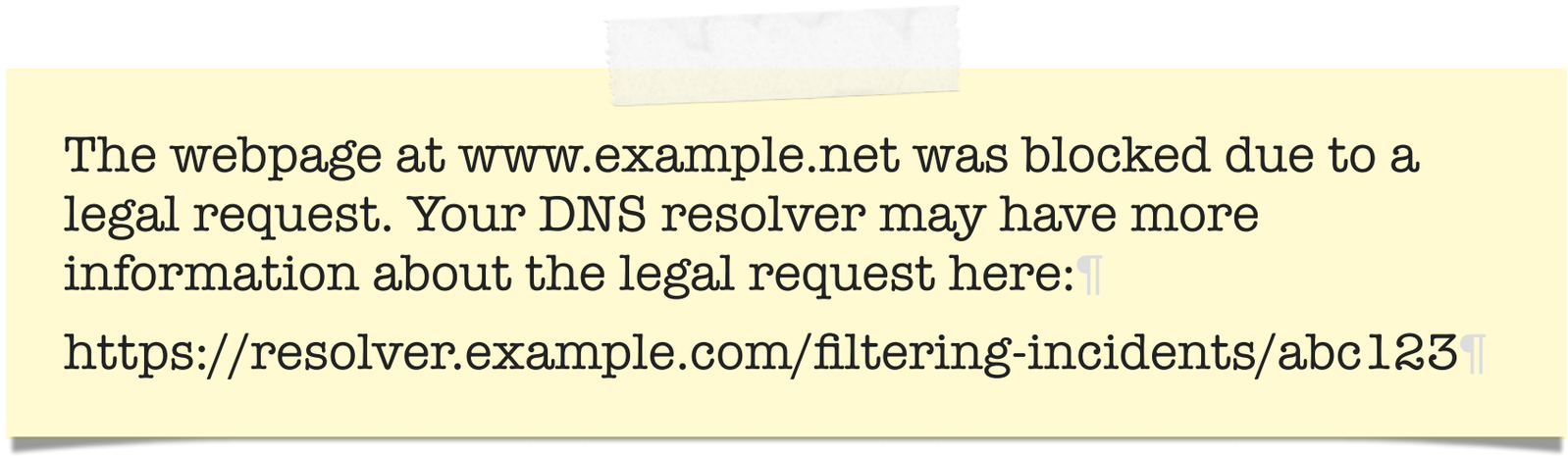
Limit to ~trusted resolvers

- E.g.,
  - Configured explicitly by client
  - Configured explicitly by OS
  - Known resolvers
- Problem: resolver configuration often unavailable to applications
- Problem: this gives discretion to browsers as to who they trust

Mitigation

Present as a diagnostic message

- Bare amount of information with technical framing



Mitigation

Limit the details exposed

- -00 exposed resolver / blocking authority / description
  - Used registry + URI Template for lookup
- -01 exposes details URI
  - Aligns with presentation as a diagnostic message

The Registry

- Original purpose:
    1. Allow lookup of longer details
    2. Provide transparency about what is being shown to end users
- (1) no longer necessary, (2) still is?
    - Constraint makes both DNS resolver and browser behaviour more publicly available

Discuss