DNS Access Denied Error page

draft-reddy-dnsop-error-page-02

IETF 108

July 2020

T. Reddy (McAfee)

N. Cook (Open-Xchange)

D.Wing (Citrix)

M.Boucadair (Orange)

Agenda

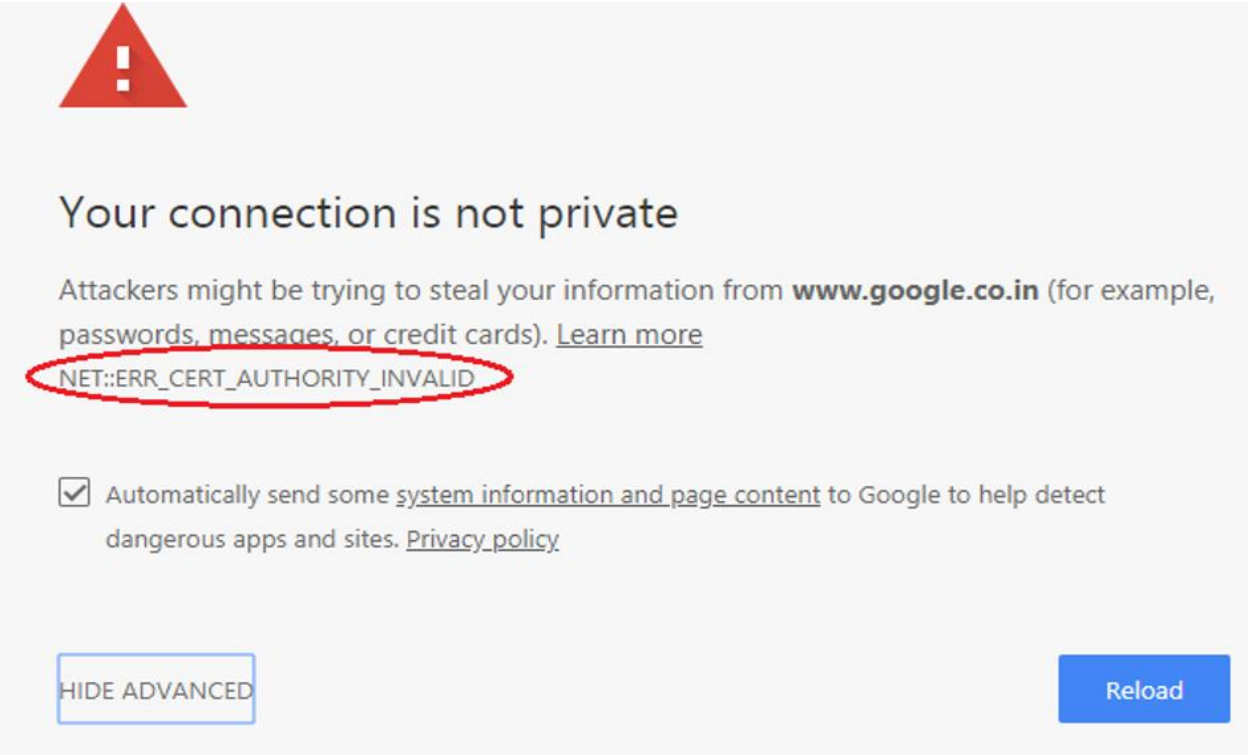
- Problem statement
- Solution overview
- Security Considerations
- Error Page

Problem statement (1/3)

- DNS filtering is deployed for security, parental control, internal security policy and filtering required by law enforcement agency.
  - Enterprise DNS firewall block access to malware domains.
  - Home network security based on DNS filtering.
  - MUD RFC8520 domain ACL for IoT devices
  - ISPs offer malware filtering service, court order etc.

Problem statement (2/3)

- Forging the response to provide the IP address of the error page for HTTPS enabled domains
  - Certificate error message
  - Repeated attempts to unsuccessfully reach the domain
  - User may try to reach the domain using insecure interfaces
  - Manually install local root certificate.



Problem statement (3/3)

- "Censored" and "Blocked" error codes in dnsop-extended-error provides additional information about the cause of the DNS error but
  - User does not know the exact reason the domain is blocked
  - User does not know the entity blocking access to the domain
  - End user needs to know the contact details of IT/InfoSec to raise a complaint.
  - Domain blocked based on the content category and is security vendor specific.
- "Forged answer" does not work for HTTPS unless local root cert is installed.

Security Risk	Bot Nets
	Confirmed Spam Sources
	Keyloggers and Monitoring
	Malware Sites
	Phishing and Other Frauds
	Proxy Avoidance and Anonymizers
	SPAM URLs
	Spyware and Adware

Questionable/Legal	Cheating
	Cult and Occult
	Gambling
	Hacking
	Hate and Racism
	Illegal
	Marijuana
	Pay to Surf
	Questionable
	Violence
	Weapons

Solution Overview

- This document describes a mechanism to provide an error page URL to the user.
- HTTPS DNS record ietf-dnsop-svcb-https in the “Service Form” provides the error page URL in the new service parameter “eut”
- Returned along with the “Forged Answer” extended error code in the additional data section.
- Any other RR in the response is ignored.

```
foo.example.com.  7200  IN HTTPS 1 . (
 eut=https://block.example.net/block-page=ZXhhbXBsZS5jb20K )
```

Security Considerations

- **DoH/DoT mandatory** to process the DNS response to avoid forgery
- DoH/DoT server is authorized by the user or pre-configured in the OS/Browser.
- Client knows it is accessing an error page URL, it knows
  - Not to send cookies
  - Not to send credentials
  - Disable JavaScript
  - Auto-Enable private browsing mode for the error page
  - Load the error page in a container isolated from other web activity.

Error Page

- The recommended non-normative contents of an error page:
  - The exact reason for blocking access to the domain.
  - The domain name blocked.
  - Pointer to the regulatory text/URL.
  - Organization blocking the access to the domain
  - Contact details of IT/InfoSec to raise a complaint.
- Error page honors Accept-Language header.

draft-reddy-dnsop-error-page-02

- Comments and suggestions are welcome