DNS Access Denied Error page

draft-reddy-dnsop-error-page-05

IETF 109

Nov 2020

T. Reddy (McAfee)

N. Cook (Open-Xchange)

D. Wing (Citrix)

M. Boucadair (Orange)

Agenda

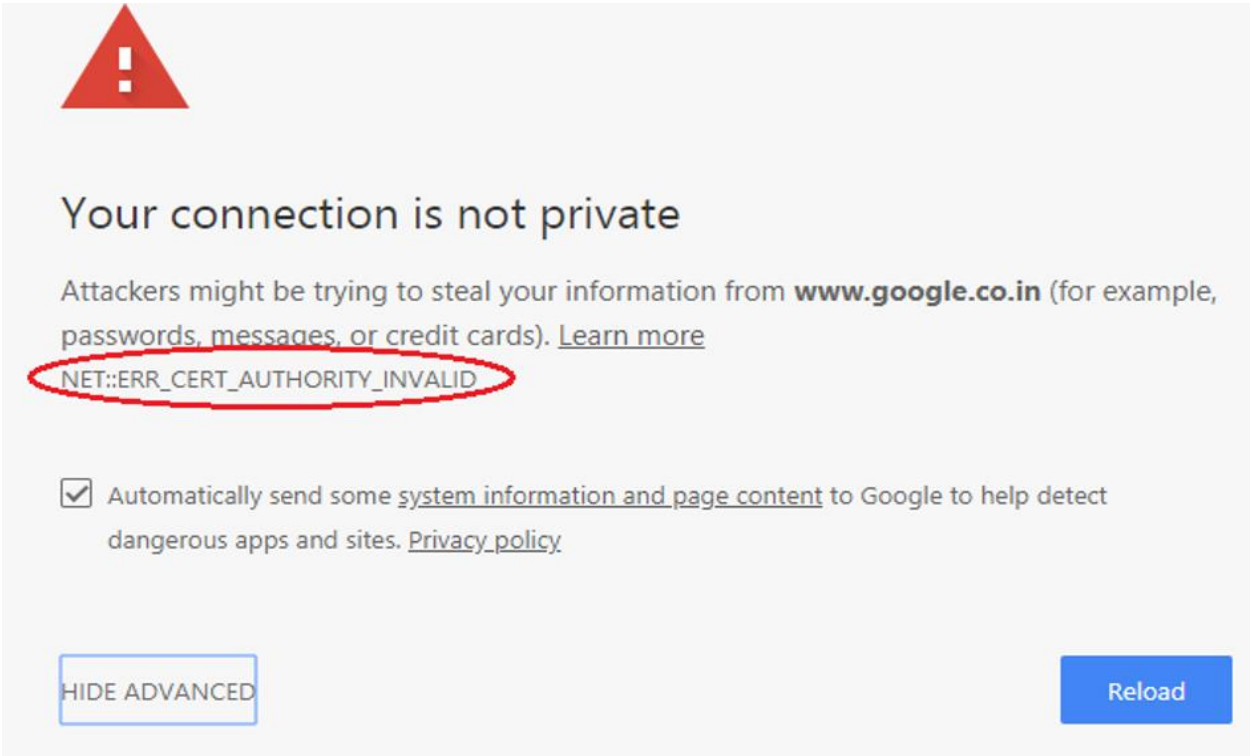
- A reminder of the problem
- Comments raised by the WG and changes to address these comments
  - Comment #1: RR Type
  - Comment #2: Processing of the error URI
  - Comment #3: Data origin issues
  - Comment #4: Malicious DoT/DoH Servers
- An update of the Security Considerations

The Problem: Reminder (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.

The Problem: Reminder (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.



The Problem: Reminder (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

RR Type

- This document describes a mechanism to provide an error page URI
- Comment #1: Concerns with the use HTTPS RR Type
  - New Error page URI EDNS0 option to include the URI template

```
 0   1   2   3   4   5   6   7   8   9   0   1   2   3   4   5
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                          OPTION-CODE                          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                         OPTION-LENGTH                         |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                ERROR-PAGE-URI-LENGTH  (fixed size)            |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                   ERROR-PAGE-URI (variable size)              /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                   ERROR-PAGE-SIG-ALG (fixed size)             |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
/                    ERROR-PAGE-SIG  (variable size)            /
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

URI template

Signature of URI template

An Example

Example URI template is
https://block.example.net/block-page{?target-domain}

example.com blocked by the DNS server
https://block.example.net/block-page?targetdomain=ZXhhbXBsZS5jb20

Base64url encoding of example.com

Processing Rules of the Error URI EDNS0

- Comment #2: How to handle the error page URI injected by an on-path attacker?
- Updated the text to better clarify the following:
  - Encrypted DNS is mandatory
  - Strict privacy profile is mandatory for DoT
  - If opportunistic privacy profile is used, ignore the error page URI
  - More than one Error page URI EDNS0 option, discard all URI EDNS0 options.
  - Returned along with the “Censored”, “Blocked”, “Filtered” or “Forged” extended error code in the additional data section.
  - If the scheme is not “https”, reject the error page URI
  - If the pre-configured DNS server does not perform filtering, discard the error page URI.

Signature and Verification

- Comment #3: Issues with data origin authentication
- The signature algorithm must be compatible with the key in the DNS server's certificate

- Signature Computation: Error page URI template, private key of the Encrypted DNS sever, signature algorithm supported by the client

- Signature Validation: The signature in the ERROR-PAGE-SIG field, error page URI Template and DNS server's certificate's public key as inputs to the signature algorithm.

- Same set of algorithms in the TLS client for validating the signature in the CertificateVerify message from the server and in the DNS client to validate the signature for the Error page URI Template.

Security Considerations

- Encrypted DNS mandatory to process the DNS response to avoid forgery
- Data origin authentication of Error Page URI is mandatory.
- Comment #4: How to handle malicious DoH/DoT servers (phishing attack)
  - ❑ Isolated environment to process the error page URI (like captive portals)
    - Label the page as not trusted
    - Not to send cookies
    - Disable JavaScript
    - Prevent user-interaction
    - Block auto-fill of credentials/personal Information
    - Auto-Enable private browsing mode for the error page
    - Load the error page in a container isolated from other web activity.

Next Steps

- All received comments were handled
- Consider WG adoption
- Comments and suggestions are welcome

Thank you