HTTPbis M. Bishop
Internet-Draft E. Nygren
Updates: 8336 (if approved)
Akamai
Intended status: Standards Track January 8, 2019
Expires: July 12, 2019

DNS Security with HTTP/2 ORIGIN
draft-bishop-httpbis-origin-fed-up-00

Abstract

The definition of the HTTP/2 ORIGIN frame "relaxes" the requirement to check DNS for various reasons. However, experience has shown that such relaxation leads to security risks and is inadvisable. This document restores the original requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 12, 2019.

Table of Contents

1. Introduction

[ORIGIN] describes a method whereby an HTTP/2 server can enumerate the HTTP origins for which it purports to be authoritative. This set can be greater or lesser than the set of origins over which the client might originally have considered the server to be authoritative. Of course, the client will generally not send requests to a server unless it considers the server to be authoritative for that origin.

Section 2.4 of [ORIGIN] states that:

> ...clients "MAY avoid consulting DNS to establish the connection's authority for new requests to origins in the Origin Set; however, those that do so face new risks, as explained in Section 4.

In Section 4 of [ORIGIN], the attacks this enables are described, along with the note that "Clients that blindly trust the ORIGIN frame's contents will be vulnerable to a large number of attacks.

See Section 2.4 for mitigations."

The mitigation recommended in Section 2.4 is to require the use of TLS and that the certificate presented be authoritative for the origin in question; the latter is a requirement already present in [HTTP2] for HTTP/2 connections using TLS. In Section 4, it is further recommended that:

> ...clients opting not to consult DNS ought to employ some alternative means to establish a high degree of confidence that the certificate is legitimate.

Several methods of increasing certificate trust are referenced. However, during the discussion of [SecondaryCerts], the ability to perform attacks using a misissued or compromised certificate has been a concern. These attacks are fundamentally enabled by the relaxation of the requirement to verify DNS ownership, and ongoing community concern about these attacks demonstrates that there is no longer consensus that these checks do not serve a purpose.

2. Some Alternative Means

[ORIGIN] leaves open-ended the decision of when to consider the certificate alone sufficient to trust a server's claim of authority over an origin. However, it enumerates some possibilities:

> For example, clients might skip consulting DNS only if they receive proof of inclusion in a Certificate Transparency log [RFC6962] or if they have a recent Online Certificate Status Protocol (OCSP) response [RFC6960] (possibly using the "status_request" TLS extension [RFC6066]) showing that the certificate was not revoked.

These mitigations are assuredly helpful in assuring general certificate validity, but they fail to fully prevent attacks from misissued or compromised certificates. In particular, a certificate which is fraudulently obtained or compromised can remain usable by an attacker for nearly two weeks.

2.1. Certificate Transparency

Certificate Transparency [RFC6962] defines an experimental protocol for publicly logging the existence of Transport Layer Security (TLS) certificates as they are issued or observed, in a manner that allows anyone to audit certificate authority (CA) activity and notice the issuance of suspect certificates as well as to audit the certificate logs themselves.

The expectation is that domain owners (or agents acting on their behalf) would actively monitor such logs for domains they control, verify that any newly-issued certificates are in fact legitimate, and have the certificate revoked if not.

This does significantly reduce the odds of a misissued certificate having a long usable lifetime. However, it does not reduce that lifetime to zero. A Signed Certificate Timestamp is not proof of inclusion in a Certificate Transparency log - it is a promise to include a certificate in a future log. Verification of certificate inclusion requires having a Signed Tree Head from that CT log which is newer than the SCT by at least that log's "maximum merge delay."

[CertificateTransparency] A misissued certificate remains invisible to inspecting parties for up to this period of time, plus whatever time is required to detect the certificate after inclusion. The "maximum merge delay" of most CT logs is twenty-four hours. (See [GoogleTrustedCT], [AppleTrustedCT].)

2.2. OCSP

Revocation checking has been a known challenge for TLS clients, with OCSP Stapling emerging as the solution of choice. While an OCSP endpoint can often be blocked by an attacker or otherwise be unavailable, the "status_request" TLS extension [RFC6066] can enable a client to request and the server to provide a recent OCSP response as part of the TLS handshake. This assists in verifying the non-revoked state of the certificate without creating a single point of failure.

However, the timeline for a revoked certificate still permits a surprising period of exercise, as described in [CABForum]:

- CAs have up to 24 hours to revoke a compromised certificate after notification; longer for other reasons
- Certificate Revocation Lists and OCSP responses have a maximum validity period of ten days

This means that an attacker-held certificate remains potentially valid for use by an attacker for as long as eleven days following the discovery of a compromise or misissuance, plus any amount of time required to discover the situation.

Additionally, the fact that a certificate has not been revoked is not proof that the issuer was permitted to issue it in the first place. An attacker-controlled CA could be used to hijack any site and could return a fully normal OCSP response. This indicates that OCSP without a publicly-auditable CT entry does not provide sufficient proof, especially when private CAs are trusted by the user agent.

3. Balancing Concerns

The primary reasons for avoiding the DNS resolution were two-fold. First and more simply, there is a latency cost to performing DNS resolutions, and this permits clients to minimize latency before issuing requests.

Second and more serious is the fact that DNS is typically performed over clear-text. In addition to the origin itself, other parties learn that the client is interested in contacting the origin:

- The DNS server operator
- The client's Internet Service Provider
- Other clients which can observe local network traffic

By avoiding a DNS resolution for an origin, clients can avoid these parties gaining additional information. However, as described in this draft, doing so exposes clients to different security concerns.

3.1. Improving Privacy

Given recent developments such as DNS over TLS [DoT] and DNS over HTTPS [DoH], there are now alternative means to avoid disclosure of a client's DNS activities to anyone other than the DNS server operator.

[DoT] or [DoH] can be used for DNS resolution when available in order to limit unnecessary disclosure of a client's DNS activity to third parties.

3.2. Limiting Scope of Certificate Compromise

In order to successfully use a fraudulent certificate, an attacker needs one of the following situations to occur:

- The attacker controls the client's DNS resolution and can provide its own IP address as that of the victim domain.
- The attacker controls the path between the client and the victim domain's real address, and can hijack a TCP connection intended for the victim domain's server
- The client supports [ORIGIN], the fraudulent certificate contains both the victim domain and an attacker-controlled domain, and the attacker can induce the client to access an attacker-owned domain
- The client supports both [ORIGIN] and [SecondaryCerts], and the attacker can induce the client to access an attacker-owned domain

Following the DNS verifications in [HTTP2], only the first two situations will result in the client considering the attacker authoritative for the victim domain. However, if the client relaxes DNS checks as specified in [ORIGIN], the latter two attack configurations become possible as well.

As a result, DNS resolution MUST continue to be performed prior to accepting a server as valid for an HTTP origin.

3.3. Updates to RFC 8336

[ORIGIN] is modified as follows:

- The fifth paragraph of Section 2.4 is deleted
- The first three paragraphs of Section 4 are replaced with the contents of Section 4 from this document
- The informative reference to [AltSvc] (Section 5.2) is made a normative reference (in Section 5.1)

4. Security Considerations

Clients that blindly trust the ORIGIN frame's contents will be vulnerable to a large number of attacks.

Omitting the requirement to consult DNS when determining authority for an origin would mean that an attacker who possesses a valid certificate no longer needs to be on path to redirect traffic to them; instead of modifying DNS, they need only convince the user to visit another website in order to coalesce connections to the target onto their existing connection.

Before considering a server to be authoritative for any given origin,
clients MUST validate that the destination IP address is valid for the origin either by direct DNS resolution or resolution of a validated Alternative Service [AltSvc].

5. IANA Considerations

This document has no actions for IANA.

6. References

6.1. Normative References

[AltSvc] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", RFC 7838, DOI 10.17487/RFC7838, April 2016, <https://www.rfc-editor.org/info/rfc7838>.

[DoH] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[DoT] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[HTTP2] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[ORIGIN] Nottingham, M. and E. Nygren, "The ORIGIN HTTP/2 Frame", RFC 8336, DOI 10.17487/RFC8336, March 2018, <https://www.rfc-editor.org/info/rfc8336>.

6.2. Informative References

[AppleTrustedCT] "Certificate Transparency Policy", n.d., <https://support.apple.com/en-us/HT205280>.

[CABForum] CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", n.d., <https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.6.1.pdf>.

[CertificateTransparency] "Certificate Transparency: Getting Started", n.d., <http://www.certificate-transparency.org/getting-started>.

[GoogleTrustedCT] "List of Trusted CT Logs", n.d., <https://www.gstatic.com/ct/log_list/log_list.json>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <https://www.rfc-editor.org/info/rfc6066>.

[RFC6960] Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 6960, DOI 10.17487/RFC6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/info/rfc6962>.

[SecondaryCerts]
Bishop, M., Sullivan, N., and M. Thomson, "Secondary Certificate Authentication in HTTP/2", draft-ietf-httpbis-http2-secondary-certs-03 (work in progress), October 2018.

Authors' Addresses

Mike Bishop
Akamai

Email: mbishop@evequefou.be

Erik Nygren
Akamai

Email: erik+ietf@nygren.org