The "SNI" Alt-Svc Parameter
draft-bishop-httpbis-sni-altsvc-01

Abstract

   HTTP Alternative Services provides a mechanism for an origin to
   declare that its content is accessible via some other combination of
   host, port, and protocol. In the process of using such an
   alternative, an observer can identify that the client is requesting
   resources from a particular hostname.

   This document extends HTTP Alternative Services, in combination with
   Secondary Certificate Authentication, to enable clients not to
   disclose the origin to which they intend to connect.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Confidentiality and authentication during communication are primary
goals of using TLS to secure traffic on the Internet. However, due
to the nature of TLS, certain information is inherently not
confidential - notably, the hostname and the corresponding
certificate of the origin to which the client is connecting are
transferred unencrypted in the Server Name Indication extension [SNI]
and the server's Certificate message [TLS12].

While the client identity can be obscured by using TLS renegotiation
immediately after the handshake (in TLS 1.2) or by using TLS 1.3
[TLS13], the server is not afforded such privacy considerations.

Servers may also have wildcard certificates which do not enumerate
specific subdomains, but clients will disclose the first subdomain
used on a connection via the SNI extension when establishing the
connection.

[SNIEncryption] discusses a potential solution to these issues in
Section 3, HTTP Co-Tenancy Fronting, but notes both discoverability
and server authentication issues with that approach. This document
provides a mechanism to address both limitations.

1.1. Usage

In [AltSvc], once a client has received a validated Alternative
Service record for an origin, it "SHOULD use that alternative service
for all requests to the associated origin as soon as it is available,
provided the alternative service information is fresh (Section 2.2)
and the security properties of the alternative service protocol are
desirable, as compared to the existing connection." However, the
client "MUST have reasonable assurances that the alternative service
is under control of and valid for the whole origin ... established
through use of a TLS-based protocol with the certificate checks
defined in [RFC2818]." This causes the origin to be disclosed in the
SNI extension while connecting to the alternative, and the origin's
certificate to be returned by the alternative, creating the same
privacy issues as connecting directly to the origin.

The extension described in Section 2 enables an origin to declare
that reasonable assurances should be obtained, not by requesting the
desired hostname in the TLS handshake, but by requesting it via
[SecondaryCerts]. The validation checks from [RFC2818] are applied
to this certificate.

Because the entire exchange happens inside TLS, a passive observer
cannot identify the hostname(s) the client might be requesting.

1.2. Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in BCP
14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

The key words "MUST (BUT WE KNOW YOU WON'T)", "SHOULD CONSIDER",
"REALLY SHOULD NOT", "OUGHT TO", "WOULD PROBABLY", "MAY WISH TO",
"COULD", "POSSIBLE", and "MIGHT" in this document are to be
interpreted as described in [RFC6919].

Field definitions are given in Augmented Backus-Naur Form (ABNF), as
defined in [RFC5234].

2. The "sni" Alt-Svc Extension

When an origin wishes to nominate a "fronting server", it includes
the "sni" parameter in its alternative service entry.

Syntax:

sni = host

"host" is defined in Section 3.2.2 of [RFC3986].

When processing such an alternative, clients SHOULD present the
hostname given in the "sni" parameter in the SNI extension during the
TLS handshake. If the resulting certificate is also for the origin
which published the alternative service, the client MUST validate the
certificate in the handshake for authenticity according to [RFC2818].

Otherwise, the client MAY choose not to validate the certificate, but
MUST NOT make requests to any origin corresponding to this
certificate unless the certificate has been successfully validated.
In this case, the client SHOULD send a "CERTIFICATE_REQUEST" frame
including an SNI extension indicating the origin which published the
alternative service immediately upon connecting. If no corresponding
"CERTIFICATE" frame is presented by the server after a reasonable
timeout, or if the server's SETTINGS frame does not include the
"SETTINGS_HTTP_CERT_AUTH" setting, the client MUST consider the
alternative connection to have failed.

3. Security Considerations

[AltSvc] permits clients to ignore unrecognized parameters. As a
result, servers publishing records with the "sni" parameter cannot be
assured that clients will not include their origin in the SNI header
when connecting to the nominated alternative. If, for security
reasons, an origin wishes its identity never to be disclosed when the
alternative is being used, an alternative mechanism would be required
to ascertain client support before generating the Alt-Svc record.

Clients will need to connect directly to the origin at least once in
order to receive the Alt-Svc entry via an HTTP header or "ALTSVC"
frame, thus disclosing their use of the origin to the network on the
first connection. This could be mitigated by future work defining a
way to publish alternative services in a mechanism which can be
retrieved confidentially, such as via DNS in combination with
[RFC7858] or [DoH].

However, servers which publish Alt-Svc records over unencrypted
channels (HTTP connections without TLS) or channels without client
authorization (DNS, or publicly accessible HTTP resources) enable
active observers to build a map of fronting servers by collecting
Alt-Svc advertisements. Servers SHOULD CONSIDER this trade-off in
deciding when and how to make Alt-Svc records available to
unauthenticated parties.

4. IANA Considerations

The "Hypertext Transfer Protocol (HTTP) Alt-Svc Parameter Registry"
defines the name space for parameters, as described in [AltSvc]. It
is maintained at http://www.iana.org/assignments/http-alt-svc-
parameters [1].

This document registers the following parameter:

Name: "sni"

Specification: This document

5. References

5.1. 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>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <https://www.rfc-editor.org/info/rfc2119>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818,
           DOI 10.17487/RFC2818, May 2000,
           <https://www.rfc-editor.org/info/rfc2818>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform
           Resource Identifier (URI): Generic Syntax", STD 66,
           RFC 3986, DOI 10.17487/RFC3986, January 2005,
           <https://www.rfc-editor.org/info/rfc3986>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax
           Specifications: ABNF", STD 68, RFC 5234,
           DOI 10.17487/RFC5234, January 2008,
           <https://www.rfc-editor.org/info/rfc5234>.

[RFC6919] Barnes, R., Kent, S., and E. Rescorla, "Further Key Words
           for Use in RFCs to Indicate Requirement Levels", RFC 6919,
           DOI 10.17487/RFC6919, April 2013,
           <https://www.rfc-editor.org/info/rfc6919>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SecondaryCerts]
           Bishop, M., Sullivan, N., and M. Thomson, "Secondary
           Certificate Authentication in HTTP/2", draft-bishop-
           httpbis-http2-additional-certs-05 (work in progress),
           October 2017.

[SNI]   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>.

[TLS12]   Dierks, T. and E. Rescorla, "The Transport Layer Security
           (TLS) Protocol Version 1.2", RFC 5246,
           DOI 10.17487/RFC5246, August 2008,
           <https://www.rfc-editor.org/info/rfc5246>.

[TLS13]   Rescorla, E., "The Transport Layer Security (TLS) Protocol
           Version 1.3", draft-ietf-tls-tls13-23 (work in progress),
           January 2018.

5.2. Informative References

[DoH]   Hoffman, P. and P. McManus, "DNS Queries over HTTPS",
           draft-ietf-doh-dns-over-https-02 (work in progress),
           November 2017.

[RFC7858] 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>.

[SNIEncryption]
           Huitema, C. and E. Rescorla, "SNI Encryption in TLS
           Through Tunneling", draft-ietf-tls-sni-encryption-00 (work
           in progress), August 2017.

5.3. URIs

   [1] http://www.iana.org/assignments/http-alt-svc-parameters

Appendix A. Acknowledgements

   Conversations with Benjamin Schwartz helped to flesh out this idea.

Author's Address

    Mike Bishop
    Akamai

    Email: mbishop@evequefou.be