Workgroup:
Oblivious HTTP Application Intermediation
Internet-Draft:
draft-pauly-ohai-svcb-config-00
Published: 5 March 2022
Intended Status: Informational
Expires: 6 September 2022
Authors: T. Pauly   T. Reddy
         Apple Inc.   Akamai

Distribution of Oblivious Configurations via Service Binding Records

Abstract

This document defines a parameter that can be included in SVCB and
HTTPS DNS resource records to denote that a service is accessible as
an Oblivious HTTP target, along with one or more oblivious key
configurations.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://
datatracker.ietf.org/doc/draft-pauly-ohai-svcb-config/.

Discussion of this document takes place on the Oblivious HTTP
Application Intermediation Working Group mailing list
(mailto:ohai@ietf.org), which is archived at https://
mailarchive.ietf.org/arch/browse/ohai/.

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 6 September 2022.

Table of Contents

1. **Introduction**

   Oblivious HTTP [OHTTP] allows clients to encrypt messages exchanged
   with an HTTP server accessed via a proxy, in such a way that the
   proxy cannot inspect the contents of the message and the target HTTP
   server does not discover the client's identity. In order to use
   Oblivious HTTP, clients need to possess a key configuration to use
   to encrypt messages to the oblivious target.

   Since Oblivious HTTP deployments will often involve very specific
   coordination between clients, proxies, and targets, the key
   configuration can often be shared in a bespoke fashion. However,
   some deployments involve clients discovering oblivious targets more
   dynamically. For example, a network may want to advertise a DNS
   resolver that is accessible over Oblivious HTTP and applies local
   network resolution policies via mechanisms like Discovery of

Designated Resolvers ([DDR]. Clients can work with trusted proxies to access these target servers.

This document defines a mechanism to distribute Oblivious HTTP key configurations in DNS records, as a parameter that can be included in SVCB and HTTPS DNS resource records [SVCB]. The presence of this parameter indicates that a service is an oblivious target; see Section 3 of [OHTTP] for a description of oblivious targets.

This mechanism does not aid in the discovery of proxies to use to access oblivious targets; the configurations of proxies is out of scope for this document.

2. Conventions and Definitions

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.

3. The ohttp-configs and ohttp-path SvcParamKeys

The "ohttp-configs" SvcParamKey Section 6 is used to convey one or more key configurations that can be used by clients to issue oblivious requests to a target server described by the SVCB record.

In wire format, the value of the parameter is one or more KeyConfig structures [OHTTP] concatenated together. In presentation format, the value is the same concatenated KeyConfig structures encoded in Base64 [BASE64].

The meaning of the "ohttp-configs" parameter depends on the scheme of the SVCB record. This document defines the interpretation for the "https" [SVCB] and "dns" [DNS-SVCB] schemes. Other schemes that want to use this parameter **MUST** define the interpretation and meaning of the configuration.

The "ohttp-path" SvcParamKey Section 6 is used to convey the URI path of the oblivious target to which oblivious HTTP requests can sent. In both wire format and presentation format, this is a UTF-8 encoded string that contains the path segment of a URI. If this path parameter is not present, oblivious requests can be made to the root "/" path.

3.1. Use in HTTPS service records

For the "https" scheme, which uses the HTTPS RR type instead of SVCB, the presence of the "ohttp-configs" parameter means that the

service being described is an Oblivious HTTP service that uses the default "message/bhttp" media type [OHTTP] [BINARY-HTTP].

When present in an HTTPS record, the "ohttp-configs" **MUST** be included in the mandatory parameter list, to ensure that implementations that do not understand the key do not interpret this service as a generic HTTP service.

Clients **MUST** validate that they can parse the value of "ohttp-configs" as a valid key configuration before attempting to use the service.

3.2. Use in DNS server SVCB records

For the "dns" scheme, as defined in [DNS-SVCB], the presence of the "ohttp-configs" parameter means that the DNS server being described is an Oblivious DNS over HTTP (DoH) service. The default media type expected for use in Oblivious HTTP to DNS resolvers is "application/dns-message" [DOH].

The "ohttp-configs" parameter is only defined for use with DoH, so the "alpn" SvcParamKey **MUST** indicate support for a version of HTTP and the "dohpath" SvcParamKey **MUST** be present. The "ohttp-configs" **MUST** also be included in the mandatory parameter list, to ensure that implementations that do not understand the key do not interpret this service as a generic DoH service.

Clients **MUST** validate that they can parse the value of "ohttp-configs" as a valid key configuration before attempting to use the service.

3.2.1. Use with DDR

Clients can discover an oblivious DNS server configuration using DDR, by either querying _dns.resolver.arpa to a locally configured resolver or querying using the name of a resolver [DDR].

In the case of oblivious DNS servers, the client might not be able to directly use the verification mechanisms described in [DDR], which rely on checking for known resolver IP addresses or hostnames in TLS certificates, since clients do not generally perform TLS with oblivious targets. A client **MAY** perform a direct connection to the oblivious target server to do this TLS check, however this may be impossible or undesirable if the client does not want to ever expose its IP address to the oblivious target. If the client does not use the standard DDR verification check, it **MUST** use some alternate mechanism to verify that it should use an oblivious target. For example, the client could have a local policy of known oblivious target names that it is allowed to use, or the client could coordinate with the oblivious proxy to either have the oblivious

proxy check the properties of the target's TLS certificate or filter
to only allow targets known and trusted by the proxy.

Clients also need to ensure that they are not being targeted with
unique key configurations that would reveal their identity. See
Section 5 for more discussion.

3.2.2. Use with DNR

The SvcParamKeys defined in this document also can be used with
Discovery of Network-designated Resolvers (DNR) [DNR]. In this case,
the oblivious configuration and path parameters can be included in
DHCP and Router Advertisement messages.

While DNR does not require the same kind of verification as DDR,
clients still need to ensure that they are not being targeted with
unique key configurations that would reveal their identity. See
Section 5 for more discussion.

3.2.3. Handling Oblivious DoH Configurations

Oblivious DoH was originally defined in [ODOH]. This version of
Oblivious DoH uses a different key configuration format than generic
Oblivious HTTP. SVCB records using the "dns" scheme can include one
or more ObliviousDoHConfig structures using the "odoh-configs"
parameter.

In wire format, the value of the "odoh-configs" parameter is one or
more ObliviousDoHConfigs structures [ODOH] concatenated together. In
presentation format, the value is the same structures encoded in
Base64 [BASE64].

All other requirements for "ohttp-configs" in this document apply to
"odoh-configs".

4. Deployment Considerations

Deployments that add the "ohttp-configs" SvcParamKey need to be
careful to add this only to services meant to be accessed using
Oblivious HTTP. Information in a single SVCB record that contains
"ohttp-configs" only applies to the oblivious service, not other
HTTP services.

If a service offers both traditional HTTP and oblivious HTTP, these
can be represented by separate SVCB or HTTPS records, both with and
without the "ohttp-configs" SvcParamKey.

5. Security and Privacy Considerations

When discovering designated oblivious DNS servers using this mechanism, clients need to ensure that the designation is trusted in lieu of being able to directly check the contents of the target server's TLS certificate. See Section 3.2.1 for more discussion.

As discussed in [OHTTP], client requests using Oblivious HTTP can only be linked by recognizing the key configuration. In order to prevent unwanted linkability and tracking, clients using any key configuration discovery mechanism need to be concerned with attacks that target a specific user or population with a unique key configuration.

There are several approaches clients can use to mitigate key targetting attacks. [CONSISTENCY] provides an analysis of the options for ensuring the key configurations are consistent between different clients. Clients **SHOULD** employ some technique to mitigate key targetting attack. One mitigation specific to this mechanism is validating that SVCB or HTTPS records including the "oblivious-configs" are protected by DNSSEC [DNSSEC]. This prevents attacks where a unique response is generated for each client of a resolver.

6. IANA Considerations

IANA is requested to add the following entry to the SVCB Service Parameters registry ([SVCB]).

Number	Name	Meaning	Reference
TBD	ohttp-configs	Oblivious HTTP key configurations	(This document)
TBD	ohttp-path	Oblivious HTTP request path	(This document)
TBD	odoh-configs	Oblivious DoH key configurations	(This document)

Table 1

7. References

7.1. Normative References

[BASE64]   Josefsson, S., "The Base16, Base32, and Base64 Data
            Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006,
            <https://www.rfc-editor.org/rfc/rfc4648>.

[BINARY-HTTP] Thomson, M. and C. A. Wood, "Binary Representation of
            HTTP Messages", Work in Progress, Internet-Draft, draft-
            ietf-httpbis-binary-message-01, 3 February 2022,

<https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-binary-message-01>.

[DDR]   Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T.
             Jensen, "Discovery of Designated Resolvers", Work in
             Progress, Internet-Draft, draft-ietf-add-ddr-05, 31
             January 2022, <https://datatracker.ietf.org/doc/html/
             draft-ietf-add-ddr-05>.

[DNR]   Boucadair, M., Reddy, T., Wing, D., Cook, N., and T.
             Jensen, "DHCP and Router Advertisement Options for the
             Discovery of Network-designated Resolvers (DNR)", Work in
             Progress, Internet-Draft, draft-ietf-add-dnr-05, 13
             December 2021, <https://datatracker.ietf.org/doc/html/
             draft-ietf-add-dnr-05>.

[DNS-SVCB]   Schwartz, B., "Service Binding Mapping for DNS Servers",
             Work in Progress, Internet-Draft, draft-ietf-add-svcb-
             dns-02, 1 February 2022, <https://datatracker.ietf.org/
             doc/html/draft-ietf-add-svcb-dns-02>.

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

[OHTTP]   Thomson, M. and C. A. Wood, "Oblivious HTTP", Work in
             Progress, Internet-Draft, draft-ietf-ohai-ohttp-01, 15
             February 2022, <https://datatracker.ietf.org/doc/html/
             draft-ietf-ohai-ohttp-01>.

[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/rfc/
             rfc2119>.

[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/rfc/rfc8174>.

[SVCB]   Schwartz, B., Bishop, M., and E. Nygren, "Service binding
             and parameter specification via the DNS (DNS SVCB and
             HTTPS RRs)", Work in Progress, Internet-Draft, draft-
             ietf-dnsop-svcb-https-08, 12 October 2021, <https://
             datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-
             https-08>.

7.2. Informative References

[CONSISTENCY] Davidson, A., Finkel, M., Thomson, M., and C. A. Wood,
             "Key Consistency and Discovery", Work in Progress,

          Internet-Draft, draft-wood-key-consistency-02, 4 March
          2022, <https://datatracker.ietf.org/doc/html/draft-wood-
          key-consistency-02>.

   [DNSSEC]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "DNS Security Introduction and Requirements", RFC
              4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-
              editor.org/rfc/rfc4033>.

   [ODOH]   Kinnear, E., McManus, P., Pauly, T., Verma, T., and C. A.
              Wood, "Oblivious DNS Over HTTPS", Work in Progress,
              Internet-Draft, draft-pauly-dprive-oblivious-doh-11, 17
              February 2022, <https://datatracker.ietf.org/doc/html/
              draft-pauly-dprive-oblivious-doh-11>.

Authors' Addresses

   Tommy Pauly
   Apple Inc.

   Email: tpauly@apple.com

   Tirumaleswar Reddy
   Akamai

   Email: kondtir@gmail.com